Asia/Pacific Group on Money Laundering

ASIA/PACIFIC GROUP ON MONEY LAUNDERING

Typologies Report

MONEY LAUNDERING ASSOCIATED WITH LARGE-SCALE TRANSNATIONAL FRAUDS

Adopted by APG Members at the 14th Annual Meeting

India, 22 July 2011

.

CONTENTS

EXECUTIVE SUMMARY

In recent years large-scale transnational fraud (LSTF) has transformed from a localised crime problem into a global crime threat, the true scale of which is difficult to ascertain with any degree of certainty. However, it is widely accepted that losses run into tens of billions dollars annually. The purpose of this study is to consider the methods and techniques criminals use to launder the proceeds of LSTF. Authorities identify that these billions of dollars are laundered using a variety of techniques, and it is widely accepted that at some stage in the laundering cycle, the majority of these funds pass through the banking system.

The case studies highlighted in the report illustrate the risks for laundering the proceeds of LSTF associated with the various industries, channels, designated services and products and payments methods. These risks lie in the placement, layering and integration stages of money laundering. The special feature of money laundering associated with LSTF is that it is difficult to differentiate the money laundering activities from the predicate offence itself; unlike money laundering related to drug trafficking for example, the money laundering commences simultaneously with the commission of the predicate offence. They work hand in hand.

From the responses received, it is apparent that the LSTF presents a serious risk and jurisdictions throughout the region have identified their residents as victims of these frauds. For some victims, the impacts extend beyond personal financial loss to other family members; loss of entire family or retirement savings, loss of a home, psychological trauma, depression and suicide have been recorded in various studies.

Money laundering associated with proceeds of LSTF occurs through multiple jurisdictions. Criminals make use of shell companies, money services business and stooge accounts etc to provide a veil of legitimacy to the transactions and to complicate the audit trail. The rapid movement of funds and the cross-jurisdictional nature pose challenges to law enforcement agencies (LEAs), financial intelligence units (FIUs), financial institutions and regulators. The challenge lies in the timely identification of the fraud and the location and movement of the proceeds. Detection of the proceeds relies on the proactive sharing of relevant information both domestically and internationally.

Much is known about the various guises and forms of the predicate fraud offence and the initial placement and layering of the proceeds. However, due to limited intelligence and feedback, the project team found limited opportunities to examine how and where these funds are integrated and accessed. The levels of suspicious transaction reporting in relation to LSTF are relatively high, but the quality is questionable. While most jurisdictions reported having the structure and apparatus that are required to meet international AML/CFT standards, the 'effectiveness' of many regimes in tackling money laundering associated with LSTF is not evident.

The impact from money laundering associated with LSTF has a truly global reach and it is therefore necessary for jurisdictions to work together, both in terms of public and private enterprise, to provide a global response.

The followings areas are considered as having potential to enhance the global response to tackling money laundering associated with the LSTF:

- To undertake jurisdiction and sector risk assessments in order to critically review and assess the nature, scope and impact of the problem;
- To formulate comprehensive strategies, policies and action plans to ensure the better allocation of resources and operational priorities;
- To engage public and private stakeholders and coordinate prevention and enforcement measures so that intelligence, information, typologies and trends can be shared in a proactive and timely manner; and
- To enhance international cooperation through cross-jurisdictional exchange platforms such as the establishment of Regional Task Forces and Central Databases.

1 INTRODUCTION

1.1 INTRODUCTION

1. APG mutual evaluations, APG typologies collections and typologies workshops continue to highlight threats from money laundering associated with LSTF, in particular telemarketing / boiler room / lottery frauds. Jurisdictions which have conducted investigations of these frauds and associated money laundering highlight the involvement of transnational organised crime groups and highly profitable criminal activity.

2. Laundering of proceeds from boiler room / heritage / lottery frauds is a lucrative, relatively low risk, global criminal activity. Their trans-national nature presents numerous multi-jurisdictional issues for preventative measures, enforcement, prosecution and asset recovery. The failure to rapidly exchange information and the lack of coordinated multi-jurisdictional action to combat and identify the syndicates involved enhanced money laundering vulnerabilities. Increased national and international collaboration is required to combat these offences.

3. Telemarketing and related frauds present a good example of how transnational organised crime activity has adapted and grown with globalisation. Telemarketing frauds and associated ML have proliferated, utilising an increasingly wide spectrum of modus operandi to present a fraudulent solicitation to a prospective victim. Global in nature, the perpetrators, victims and the bank accounts used to launder the proceeds of such fraud are normally located in different jurisdictions.

4. A number of jurisdictions, including Hong Kong and Malaysia, have successfully prosecuted money-laundering offences associated with cross border telemarketing fraud. It is apparent that criminals may take account of AML/CFT controls in various jurisdictions when designing money laundering schemes associated with these frauds. Experience suggests that some financial institutions are successful in identifying accounts used for this type of crime; however, criminals are quick to react and adapt money flows in response to preventative measures. Jurisdictions' experience in this regard is worthy of further examination.

1.2 NEED FOR THE TYPOLOGY

5. Despite the scale of the problem, there remains a lack of recent regional or global money laundering typologies associated with these LSTF. While a significant amount of research has already been undertaken on the fraud itself, this has largely been conducted by jurisdictions where victims are resident or where operators of certain frauds, such as boiler rooms, are located. Many jurisdictions may not be fully aware of this research, the recommendations made and best

practices identified. Given the continuing vulnerabilities for money laundering associated with LSTF, there is a need for up-to-date typologies.

1.3 SCOPE

6. The objectives of this typology report are to:

- Sort / group the types of LSTF, by sharing knowledge held by law enforcement and other specialist agencies concerned with these type of fraud, thereby increasing understanding and raising global awareness;
- Identify the techniques and methods of money laundering associated with LSTF;
- Share case studies of ML and TF associated with LSTF;
- Identify any trends or patterns within jurisdictions and across the region for money laundering related to LSTF;
- Identify problems and possible solutions with regard to law enforcement investigations on money laundering associated with LSTF;
- Examine best practices in FIU, investigation, regulatory and supervisory approaches to this activity;
- Consider mechanisms for international cooperation and identify opportunities to enhance this area and harmonise efforts to facilitate the recovery of stolen assets;
- Identify emerging policy issues, including whether any issues arise which are not adequately covered by the international AML/CFT standards; and
- Share key findings of the analysis with law enforcement and regulatory authorities to promote best practice and with the financial services sector to promote effective risk mitigation and preventative measures.

7. A number of key questions were raised in the project plan. Not all of these are answered in the report; which has clearly undermined the original concept to a certain extent. For example, from the materials received it proved impossible to draw any conclusion with regard to 'which fraud types generate the most proceeds of crime?' However, insight is provided into some other key areas such as the techniques and methods of ML that have been identified in relation to the proceeds of telemarketing fraud and their level of sophistication.

8. The basis of the report tends towards more practical areas such as addressing what case studies exist; demonstrating techniques, methods and the primary risk factors in the case studies, what factors might assist the private sector and regulators to detect money laundering associated with LSTF and what factors might assist law enforcement to successfully investigate money laundering associated with LSTF.

9. This report also considers ongoing developments in international cooperation when discussing possibilities for increased co-operation between FIUs, LEAs and the private sector. The report also has identified a number of areas requiring technical assistance and training.

1.4 METHODOLOGY

10. This report is based on a number of different sources. The first is a review of existing literature and reports that have been generated by international bodies, national governmental agencies and the academic sector. It is important to acknowledge that none of the money laundering methods or techniques identified in this report are new; all have been examined, in their own right and in some detail, in various other reports.

11. The second and perhaps most important source is the compilation and analysis of the responses to a questionnaire distributed to APG members in September 2010. APG has the largest membership of any FSRB and has a diverse membership. The responding jurisdictions reflect this mix and differed considerably in the scope of information provided. This has determined the information from which the project team could undertake meaningful analysis. This is a theme that is further discussed in the main body of the report.

12. Following initial analysis of the questionnaires, a workshop on money laundering associated with LSTF was conducted during the APG typologies meeting held in Dhaka, Bangladesh in October 2010. The workshop was well attended by members of APG and representatives of several international organisations. The following jurisdictions participated in a day long break out session facilitated by the project co-leaders.

Bangladesh	Bhutan	Cambodia	Canada	China
France	Hong Kong, China	India	Indonesia	Japan
Macao, China	Malaysia	Philippines	Thailand	Chinese Taipei

13. Following the workshop, the requirement for some further limited data collection specific to issues that had been raised during the break out session was identified. A further questionnaire was sent out in November and a small number of returns were received in December.

14. The project team would like to acknowledge the input and support of all participating jurisdictions and also the support and guidance of the secretariat in the completion of this typology project.

2 LITERATURE AND ACTIVITIES REVIEW

15. Information and guidance on money laundering associated with LSTF can be found in a wide range of sources. FATF and a number of FSRB's have conducted a number of typologies in the past, which while not directly focused on fraud-related money laundering, have discussed the methods and techniques identified in this report. Money laundering methods and techniques are diverse. In addition, FIUs and other LEAs regularly publish typologies, suspicious indicators, trends and sanitised cases that often include transnational fraud.

16. There are also a number of significant pieces of work currently underway that examine and seek to refine key areas in terms of operations or cooperation that the findings of this report suggest could have a significant impact of the ability of all stakeholders to counteract this type of fraud.

2.1 PREVIOUS TYPOLOGIES EXERCISES

FATF Typologies - Money Laundering using Trust and Company Service Providers (2010)

17. This report compares the potential risks described in the 2006 report to the actual risks based on the new case studies and typologies. Trust and Company Service Providers (TCSPs) provide an important link between financial institutions and many of their customers, especially in respect of legal persons. The report highlights the vital role that beneficial ownership information can play in the detection and prevention of the misuse of corporate vehicles and this was underscored by the fact that TCSP's feature significantly in the returns provided in this typology.

18. The report acknowledges that although TCSPs are less conducive in the initial placement phase of ML than banks, they are prone to be used particularly in the layering stage of money laundering. In particular, the report highlights the case with which the sources and uses of funds as well as legal beneficial ownership information can be concealed through the establishment of multiple accounts and the conduct of complex transactions on behalf of clients constitutes an area of potential threat. The report and its findings, including related case studies and money laundering indicators, is considered particularly relevant in the context of this research.

'The responses received from the jurisdictions that participated in this typologies exercise, reveal that TCSPs are increasingly involved in ML schemes. TCSPs and/or their principals have in many jurisdictions been under investigation on, and at times convicted of money laundering and proceeds of crime related offences. While some jurisdictions have reported more cases of misuse of TCSPs by criminals for ML purposes than others, it is undoubted that the potential risk for misuse is evident across jurisdictions'.

FATF Typologies - Money Laundering Through Money Services Businesses (2010)

19. Money services businesses (MSB) have throughout the years increased their role as financial intermediaries, providing a number of different services. In the context of this typology, it is the role of MSB in the transfer of funds (remittance) and the provision of new payment methods that are of particular interest. Both of these services were highlighted in a number of case studies provided. The report highlights the fact that MSB offer significant opportunities for criminals wishing to launder funds derived from illegal activities, including fraud, unless appropriate safeguards are in place. There is a perception that those safeguards are not fully in place in this sector and that aspect is discussed in further detail in the report.

20. The typology offers very detailed analysis of methodologies involving money remittance and also provides some useful case examples including money laundering from Internet fraud, telemarketing fraud (Nigerian fraud) and a list of indicators.

FATF Typologies – Money Laundering and Terrorist Financing through New Payment Methods (2010)

21. This typology followed the 2006 report, which examined the growing use of New Payment Methods (NPM) and an increased awareness of their ML and TF risks, updating existing research with case studies and trends over the last four years. Based on the analysis of 30 case studies, three main typologies were identified, of which two, third party funding (including strawmen and nominees) and exploitation of the non face-to-face nature of NPM accounts featured in the case studies are provided in this typologies.

'Anonymity, high negotiability and utility of funds as well as global access to cash through ATMs are some of the major factors that can add to the attractiveness of NPM for money launders. Anonymity can be reached either 'directly' by making use of truly anonymous products (i.e. without any customer identification) or 'indirectly' by abusing personalized products (i.e. circumvention of verification measures by using fake or stolen identities, or using strawmen or

nominees etc.'

22. Two cases studies are provided showing use of mobile phone payments to move funds associated with fraud and such cases also featured in this typology, as provided by the Philippines. A further six cases studies are that related to fraud.

23. In a similar area, the FATF report **'Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems' (2008)** was also considered useful for this research. This study does not replace or duplicate the 2006 report on New Payment Methods but can be used to supplement that report. In the report's executive summary it is specifically highlighted that the risk of fraud is amongst the concerns of commercial websites and Internet payment systems.

2.2 INTERNATIONAL ACTIVITIES AND MATERIAL

24. There are a number of guidance or discussion documents published by international organizations, or domestic authorities, which provide useful background information on issues relating to efforts to interdict money laundering associated with LSTF.

Mass Marketing Fraud: A Threat Assessment (International Mass-Marketing Fraud Working Group)

25. This 2010 threat assessment report was prepared to provide governments and the public with a current assessment of the nature and scope of the threat that mass marketing fraud poses around the world. The report concludes that the threat is extreme and that money laundering continues to be a critical component of mass marketing fraud schemes.

'Like all successful criminal enterprises, mass marketing fraudsters take great care to conceal the origins, beneficiaries, destinations, and uses of their proceeds and to impede authorities' efforts to track and seize the funds. Recent mass-marketing fraud investigations reveal that fraudsters continue to request victim payments via cash-based methods, including cheques, money orders, paper currency hidden within magazines and cards and commercial wire transfer services, as well as bank debits, bank transfers and credit card charges'.

Enterprise-wide STR Sharing: Issues and Approaches (Egmont Group of Financial Intelligence Units)

26. It is widely accepted that these frauds operate in multiple jurisdictions to exploit vulnerabilities that exist from different legal systems and in particular the ability to share information and affect cooperation across borders in real time. The Egmont Group has recently been studying the issues and approaches of enterprise wide STR sharing and it is readily apparent that there are clear benefits of such practice in terms of combating money laundering associated with LSTF. A White Paper was issued in February 2011 in assisting jurisdictions to identify and address the challenges. The FATF has also discussed the findings of this research in Expert Group B, which is charged with, amongst other things, recommending changes to R.40 'International Cooperation' in preparation for the fourth round of mutual evaluations. This has resulted in a proposed amendment to R.15 to include the fact that financial institutions should be required to implement group-wide programmes against ML/TF; including policies and procedures for sharing information within the group for such purposes.

27. Although there are undoubtedly a number of complex issues with this practice the report is clear in its conclusion that 'the major benefits from enterprise-wide STR sharing are expected to result from more effective AML/CFT compliance by financial groups operating in multiple jurisdictions'.

> ***Convergence of fraud and money laundering***
>
> *'Reports from the financial sector indicate the increasing convergence of money laundering and large-scale fraud. As the use of banks to perpetrate massive fraud is becoming more prevalent, many banks are looking into combining their AML and fraud units. To effectively counter complex, multi-jurisdictional fraud, FIUs and law enforcement agencies are needed to increasingly cultivate partnerships with banks for proactive initiatives and to enhance their understanding of sophisticated transactions. Banks ability to share STRs within their financial groups may contribute greatly to their analytical efforts to detect fraud'* [and therefore by definition the money laundering associated with it].

Published Law Enforcement Typologies

28. A number of jurisdictions publish annual typologies reports that contain sanitized case examples, often include cases of fraud. Often, these are included as part of an FIU annual report although some jurisdictions do have the resources and experience to publish stand alone typologies reports. The information contained in these reports combines case study information collected by law enforcement, financial intelligence units and other partner agencies. These reports provide examples of how criminals have attempted to exploit financial systems and also include 'red flag' indicators. The project team considered these sources essential training material and guidance for law enforcement, regulators and financial institutions.

29. Australia's FIU, AUSTRAC, publishes such reports. The project team considered the annual typologies report published by AUSTRAC as outstanding training and reference material.

> *'The close cooperation between reporting entities, law enforcement agencies and AUSTRAC has enabled the production of material such as the AUSTRAC Typologies and Case Studies Reports to assist all parties in understanding how criminals and the financiers of terrorism conduct their activities. As in the previous two reports, the case studies in this report identify various mechanisms and methodologies used to conceal, launder or move illicit funds'.*

2.3 GAPS IN EXISTING MATERIAL

30. There is abundant information on the multiple sectors and vehicles used to launder the proceeds of LSTF. These sources are widespread and given the responses received during the typologies workshop there exists the perception that some jurisdictions in the region are unaware of much of this material. Some of these sources include detailed examination of the entities involved and the flow of funds. Published cases by law enforcement or similar bodies routinely include information on the suspicious indicators and the factors which led, or should have led, to a disclosure being made to the relevant FIU. These provide excellent training material which may not be effectively leveraged by some jurisdictions.

31. However, there is absence of any over arching research that examines, or attempts to examine, the true extent of funds being laundered that are the result of a predicate offence of fraud or where these funds end up, i.e. the ultimate beneficiaries. The scale of the problem has not gone unnoticed, with the FATF working group on typologies reportedly considering research into money laundering and carbon credit fraud, which has the potential to dwarf many other types of large-scale fraud in terms of the volume of funds.

> *'The European Commission estimates that VAT fraud costs the Member States around Euro 60 billion annually, although it is difficult to measure the precise scale of carousel fraud. Due to the levels of trade needed to generate substantial VAT repayments that represent the proceeds of crime, the associated money flows are far larger than the losses.'*
>
> *FATF (2007) ' Report on Laundering the Proceeds of VAT Carousel Fraud'*

32. There is also an absence of work into many areas this report set out to examine but failed to do so as a result of the scale of the problem and the limitations of the information received. These include, as an example, what emerging risks and vulnerabilities might occur in the future, including regulatory developments and displacement, as a result of implementation of measures designed to combat this form of money laundering?

3 ANALYSIS OF THE QUESTIONNAIRES

3.1 GENERAL

Introduction

33. Making definitive findings of the overall scale of fraud and associated ML or the amounts involved is not possible from the research. The wide range of fraudulent activities reported, combined with the difficulty jurisdictions experienced in quantifying the scale of the problem underscores the challenge. In reality, a sizeable portion of frauds are often undiscovered and therefore unreported. The information and data provided by the responding jurisdictions provide, at best, a snapshot of the actual situation. Nevertheless, from other informed sources it is possible to estimate with some degree of accuracy that the losses in each jurisdiction ranging from hundreds to thousands of million each year.

34. This section of the report provided a detailed analysis of the responses to the questionnaires. In its design the research recognised that measuring the nature and scale of ML associated with frauds are necessary in order to better understand the problems, identify the trends and formulate effective countermeasures.

35. For the purpose of this project, *large-scale transnational fraud (LSTF)* includes:-

Fraud involving two or more jurisdictions (in terms of the location of perpetrator, victim, money laundering scheme)

36. In order to identify the key problems that members of the APG encountered and were affected by, four areas were set out in the questionnaires to assist the evaluation [note: jurisdictions could choose more than one area].

(i) Origin jurisdiction – Bases for operation of fraud;

(ii) Victims are residents;

(iii) Transit location for the fraudulent funds; and

(iv) Final destination for the fraudulent funds

All jurisdictions are transit locations

37. Analysis of the jurisdictions' responses revealed that almost all jurisdictions have encountered the same problem, namely being the transit location for the fraudulent funds. This phenomenon illustrated that fraudsters are well organised and able to take advantages to exploit the financial systems / sectors of different jurisdictions in laundering the proceeds where the frauds are perpetuated overseas.

Use of Wire Transfers

38. Wire transfers are commonly used in moving funds between jurisdictions to obscure the origin of funds and give apparent legitimacy of the transactions. Fund travelling through different jurisdictions are also an attempt to slow down LEAs efforts to trace the funds, criminals and organisers of the frauds know that each jurisdiction the funds transit through will require LEAs to make further enquiries which take time, or may prove to be impossible. Such abuses of established financial systems / sectors cause harm to the economies, including the integrity and stability of domestic and global financial systems.

Jurisdictions are source and destination of funds

39. Another major problem is that almost all jurisdictions have residents who are victims of these frauds. However, the prevalence of certain types of fraud vary from jurisdiction to jurisdiction. The most common types of frauds reported by jurisdictions are telephone deception (emergency scam), advanced fee fraud by lottery, internet romance and heritage, investment (Ponzi scheme) and boiler room frauds. The perpetrators in these frauds are mainly overseas / non-local residents. This phenomenon illustrates that fraudsters are adaptive to the local environment and use a wide range of activities to commit frauds. Based on the cases reported by jurisdictions, the victims and perpetrators of telephone deception cases normally belong to the same ethnic group. In cases of boiler room fraud, victims and perpetuators are normally located in different continents. Shell companies are opened in different jurisdictions to facilitate the fund movement and complicate the money trail. The case study provided by Hong Kong of lottery fraud illustrated that the frauds perpetrated are dynamic in nature. The profile of both victims and perpetrators changed over time which suggested that perpetrators are responsive to the enforcement actions and adjusted their operations accordingly.

40. Half of the responding jurisdictions have encountered the problem of both being the origin jurisdiction of the fraud and the final destination of the fraudulent funds.

Origin	Residents are	Fraudulent Funds

	Jurisdiction of Fraud	Victims	Transit Location	Final Destination
No. of Responses	8	14	12	8

Table 1 : Responses for how jurisdictions are affected by LTSF and ML associated with the frauds

ML methods and techniques, vulnerabilities

41. The methods and techniques employed by fraudsters are well known to FIUs, LEAs and financial institutions. Jurisdictions have identified methods and techniques, such as wire transfers, use of shell and overseas companies and the use of money services businesses. From the responses, the money laundering indicators can be sub-divided into four categories: 'Person', 'Product' 'Transaction' and 'Location'. Although these indicators are not unique for transnational frauds, they can be indicators to trigger enhanced CDD, transaction monitoring or further analysis. Details of the money laundering indicators are set out at Annex A.

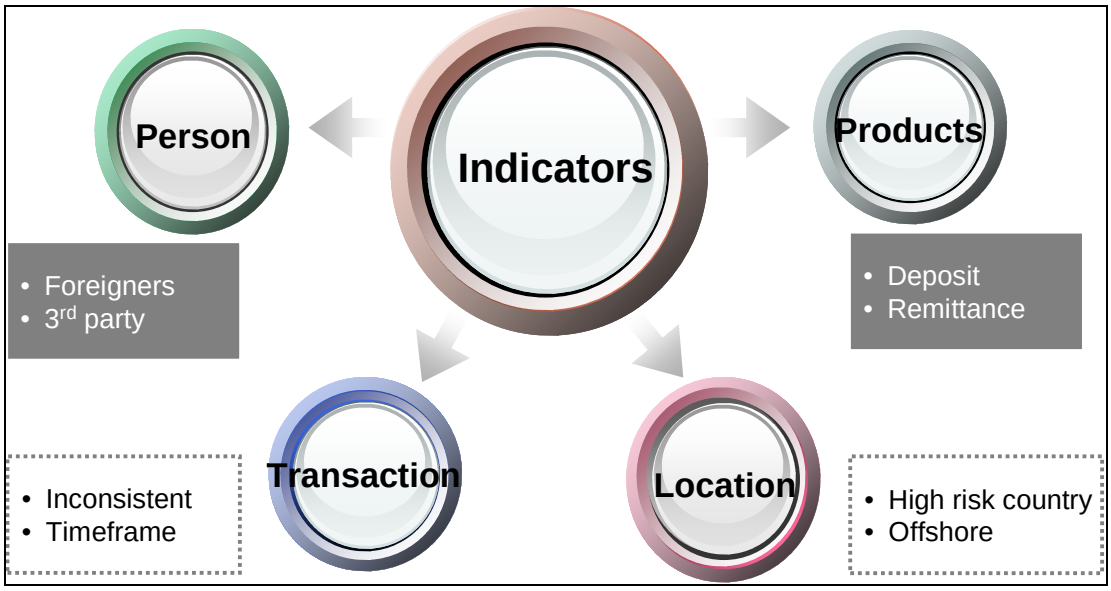


Figure 1: Money laundering indicators

42. Advancement in information technology and increasingly extensive coverage of the internet provide convenient and prompt services. As the internet becomes more prevalent and grows in popularity, so to the ranges of activities performed on-line expands. However, this has also presented new methods for fraudsters to evolve and perpetuate their frauds such as the use of fictitious and bogus websites, social networking, e-commerce and e-auction websites.

43. Fraudsters can register accounts by anonymous e-mail address with fictitious information. Non face-to-face transactions in the cyber world also bring benefits

to fraudsters in the selection of the easiest targets and then moving proceeds via on-line banking services. Remote access to commercial websites and internet payment systems further facilitate the operation anywhere in the world. In addition, the e-crime landscape evolves with the increased internet usage globally where phishing activities occur globally. As internet fraud goes hand in hand with identity theft, jurisdictions should place more emphasis on this shifting battlefield.

44. The identified ML methods and techniques corroborated with the jurisdictions' response where banking, securities, money services business, TSCP and law firms (DNFBPs) are considered as the sectors that have higher risk and vulnerabilities. Although the involvement of TCSPs was somewhat less than the project team anticipated, this may have been due to the quality and number of returns. A review on the Mutual Evaluation Reports (MERs) published in the past three years showed that the ratings of compliance on money services business and DNFBPs in the MERs were generally low. The result of the analysis is also consistent with the five features set out in the FATF Global Threat Assessment (GTA).

> *The GTA recognised that most ML/TF activity must utilise at least one of five features, which are:-*
>
> - *Cash and Bearer Negotiable Instruments.*
> - *Transfer of Value.*
> - *Assets and stores of Value.*
> - *Gatekeepers.*
> - *Jurisdiction/Environmental Aspect.*
>
> *FATF (2010) 'Global Money Laundering & Terrorist Financing Threat Assessment'*

Awareness Raising and Risk Assessment

45. Jurisdictions have different agencies that raise the awareness of the public about the modus operandi of different types of frauds through various means of communication including programs in the mass media, newsletters, news releases, posters and leaflets, community activities, anti-fraud and investor websites. Ongoing training and guidelines are also provided to financial institutions and telecommunication service providers to raise industry awareness and cooperation. It has been observed that there are few awareness programs specifically regarding ML associated with frauds.

46. Jurisdictions should consider conducting risk assessments to determine the nature and extent of the problem; understand the sources and methods; identify the risks and vulnerabilities across various sectors; and evaluate weaknesses in AML/CFT

systems. This will assist in the identification of the likelihood and significance of the problem as well as knowledge and intelligence gaps. Decision makers can be better informed about the problems which in turn should facilitate the formulation of strategy, policy and action plans with appropriate priority and resource allocation to mitigate the risk. LEAs and FIUs are considered the appropriate agencies to contribute information and intelligence in risk assessments; relevant government agencies and the private sector should also participate given the cross sectoral and transnational nature of the issue.

Canada Anti-Fraud Centre (CAFC) is the central agency in Canada created in North Bay, Ontario in 1993 that collects information and criminal intelligence on different types of frauds, including telemarketing, advanced-fee fraud letters, internet fraud and identity theft complaints etc. As a result of the growth of the frauds, CAFC gradually developed and expanded to reflect its role beyond telemarketing fraud and is a key agency in the detection and deterrent of frauds. The data collected by CAFC will be analysed by the Criminal Intelligence Analysis Unit where the unit will further disseminate the information, intelligence brief and statistics to the appropriate law enforcement agencies or regulatory bodies in Canada and the U.S. so that the agencies concerned can keep abreast with the new trends and findings. The unit also works private corporations, financial institutions and internet service providers as well as provides support to investigators and fraud task forces.

Source: www.antifraudcentre.ca

47. Risk assessments provide the basis for a risk based approach to be applied in a manner that would allow resources to be allocated in an efficient way to address the most pressing ML/TF risks.

'A national ML/TF risk assessment is an organised and systematic effort to identify and evaluate the sources and methods of money laundering and terrorist financing and weakness in the AML/CFT systems and other vulnerabilities that have an impact, either direct or indirect, on the country conducting the assessment. Such an assessment may involve multiple public sector offices working together with or without the private sector, or it may involve one or more individual agencies working independently to assess specific aspects of the country's ML/TF situation.

Although depth of coverage may differ, a national ML/TF risk assessment is a process that typically presents information on:-

- *The nature and scale of ML/TF and related predicate crimes. (i.e. the threat).*

- *Weaknesses in AML/CFT systems and controls and other features of a jurisdiction that make it attractive to money launderers and terrorist financiers (i.e. the vulnerability).*

The national risk assessment should be an input to a national strategy, as part of the country's overall AML/CFT risk management process.'

FATF (2008) 'Money Laundering & Terrorist Financing Risk Assessment Strategies'

Continuous Engagement with Financial Institutions

48. As part of the role of an FIU, responding jurisdictions advised that guidance and training related to AML/CFT including seminars and workshops are continuously provided to reporting institutions, including financial institutions. However, the project team noted that no fraud-specific guidance and training, such as emerging trends and red flags are given to financial institutions despite the increasing number of fraud related STRs and number of investigations conducted by LEAs. An exception is AUSTRAC, Australia's FIU, who produce an annual typologies and case studies report that normally includes information related to transnational frauds.

3.2 LEAS / FIUS / LEGAL / PROSECUTING AUTHORITIES

General

49. The responses from members identify that jurisdictions have criminalized ML and penalties for offences include imprisonment and/or fines. Jurisdictions also note that they are able to identify the types of large-scale frauds that generate the most proceeds of crime in their jurisdiction. In general, FIUs and LEAs have been given the necessary powers to freeze or restrain funds which are the proceeds of the predicate offences, and the powers are exercised under various legal frameworks. Primary agencies responsible for the fraud, ML and LSTF are LEAs, both at national and provincial / municipal levels. In some jurisdictions, there are designated financial / economic crime units and proceeds of crime units within the LEAs to investigate fraud and ML. Other agencies involved in combating fraud and ML including tax / revenue authorities, ministry of justice, procuratorate, regulatory authorities including central banks and securities commissions. In some jurisdictions, FIUs are also responsible for the fraud investigation and ML associated with frauds where the primary focus is on the investigation and analysis of STRs relating to fraud or ML. Both FIUs and LEAs have encountered the same obstacles regarding international cooperation, and this issue will be further discussed in the later part of this report.

STR Analysis and Dissemination

50. Jurisdictions have provided statistics regarding the number of STRs received relating to transnational fraud that illustrates a static trend between 2007 and 2009. Among the responses received, FIUs had analysed about 52% of STRs received and about 38% of the analysed STRs were disseminated domestically and internationally. The level of analysis conducted on the STRs by each of the responding FIUs varied according to resource and capability constraints. LEAs did conduct analysis of fraud-related STRs but the actions undertaken are varied.

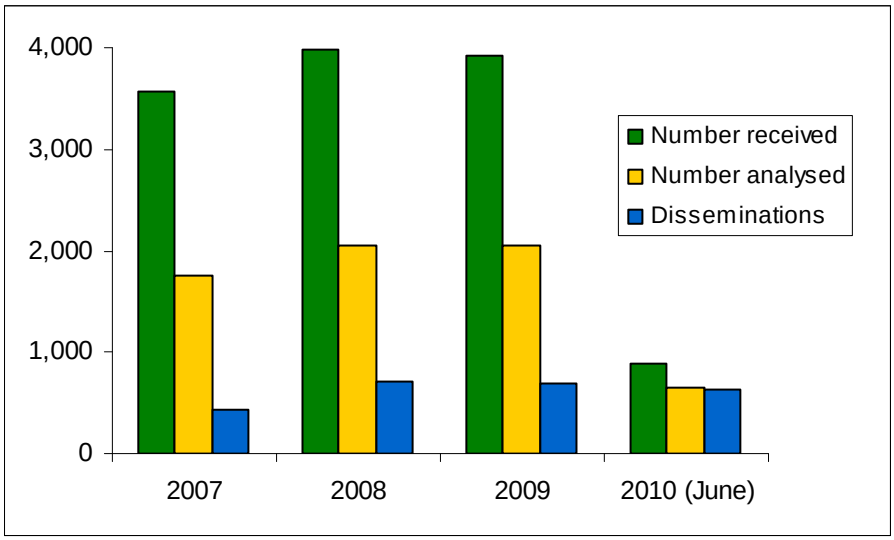


Figure 2 : No. of transnational fraud related STR

51. The types of frauds varied among jurisdictions which affected the enforcement priorities. It is observed that greater emphasis should be made to investigate the financial aspects of the predicate offences, although this is a phenomenon that is relevant to all crime types. In some jurisdictions, it was noted that there are legal constraints that confined the actions of LEAs to the investigation of predicate offences.

52. When a person or account is identified during the analysis of fraud-related STRs, LEAs would share the information with other stakeholders, subject to the provisions of the domestic legislation on the disclosure of the STR information. Some jurisdictions would notify other stakeholders at the conclusion of the investigation. In the event the funds have been transferred to another jurisdiction, some jurisdictions pass that information to the recipient jurisdiction either directly or through FIUs. Resources and operational priority of the originating jurisdiction are factors affecting the timeliness of such dissemination. Consequently LEAs are often left to investigate with only some of the information required which is in some cases outdated.

53. On the other hand, FIUs have other types of information and intelligence that can add value to the analysis and investigation of transnational frauds and ML associated with the frauds. This information includes:-

- ***Cash transaction report (CTR)*** –regardless of the threshold amount specified by the jurisdictions, CTR information provides very useful information to the FIU and LEAs when suspects attempt to break the money trail by conducting cash withdrawals from the accounts. In addition, as a preventive measure in respect of any cash transactions above the threshold, front line staff are required to conduct EDD; which may avoid potential victims from depositing large amount of cash into fraudsters' accounts.
- ***International fund transfer report*** – In meeting international standards, and complementing the AML/CFT regime, certain jurisdictions have implemented a reporting framework for international fund transfers. The reporting requirement, either on a threshold basis, or reported on the basis of the transaction, provides important information or intelligence in the analysis and investigation of frauds especially where the fraud has a transnational element. When CDD is imposed on this kind of transaction, it may create difficulties to the criminal in moving the illegal funds abroad.
- ***Information from Foreign FIUs*** – The financial intelligence that is shared with other FIUs, either on a proactive or formal basis, can provide important leads and intelligence for the FIUs to initiate financial analysis relating to transnational frauds. The information can assist in the fund flow analysis and can result in an investigation and / or the restraint of funds.
- ***Complaint/Queries from Public*** – Most of the non-stand alone FIUs have responded that they do receive reports from the public (mainly victims) related to transnational frauds. This kind of information could be a trigger for the FIU to conduct financial analysis especially when information related to the reported entities (fraudsters) already exists in the FIU's database.

54. In addition to the above information received or collected by the FIUs, there are other types of non-financial information available to FIUs either directly or indirectly. Non-financial information, including land and tax information, criminal records, vehicle registration details and company registration dealing which can add value and support the analysis. It is considered that STR information and the other types of information can form an integral information cycle that could bridge the information and intelligence gaps between FIUs, LEAs and other stakeholders in the analysis and investigation of transnational frauds and ML associated with the frauds.

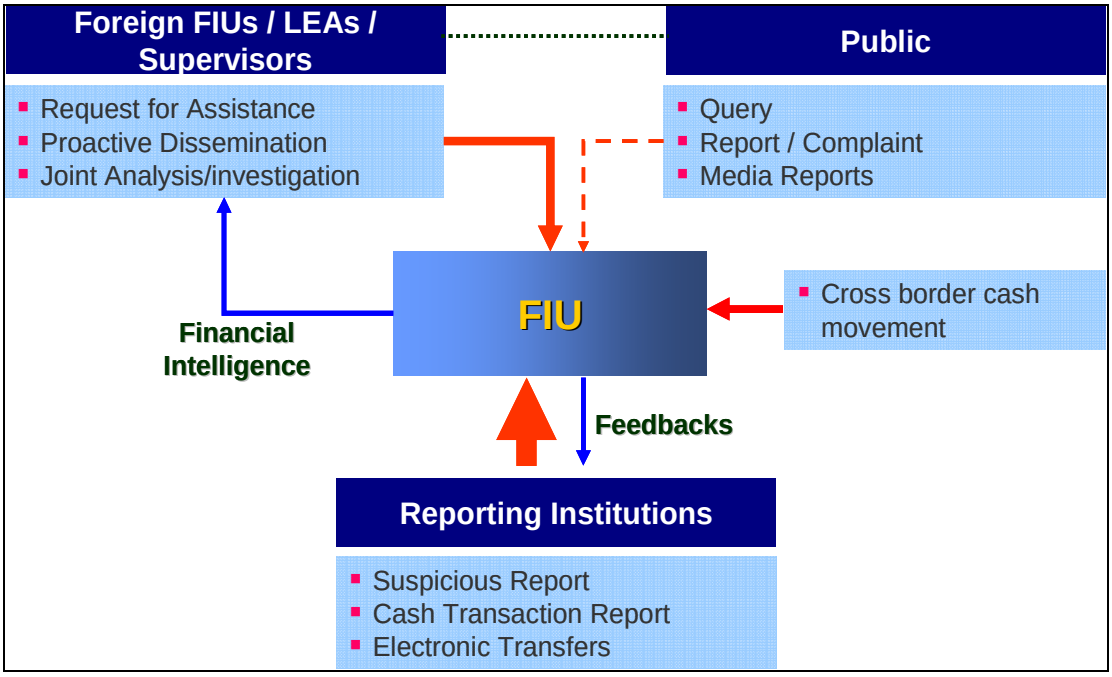


Figure 3 : FIUs' roles to bridge the relationship between LEAs, financial institutions and the public

Proceeds of Crime (ML) Investigation and Prosecution

55. LEAs are the primary agency to investigate ML. Responses from jurisdictions indicated that only a few jurisdictions have statistics on the ML investigations of transnational fraud. In most cases, the ML investigations are conducted in parallel with the predicate fraud where some of the investigations are initiated from STRs. The cross-jurisdiction nature of the fraud may hinder LEAs to commence a local investigation where most of the criminal / fraud activity has occurred abroad. From the case studies, the funds obtained from victims in different jurisdictions would normally be remitted to another jurisdiction where the consolidated funds are quickly disposed of by multiple domestic transfers to other companies (local and offshore) and money services business, multiple wire transfers to overseas companies and cash withdrawals. Offshore companies and their directors have several accounts operating in different jurisdictions to facilitate the wire transfers as well as to give apparent legitimacy of the transactions. The bank accounts used to launder the proceeds are only being operated for a short period of time, especially in telephone deception cases.

56. To avoid detection, criminals also used structured remittances and cash transactions. A case provided by AUSTRAC highlighted a Nigerian syndicate that disposed of the proceeds by structured remittances and cash couriers. The victim was induced to become involved in the money laundering scheme. After the funds have been integrated into the financial system, the proceeds are used to acquire real estate, high value assets, vehicles and boats, investment in legitimate business as well as being kept in cash and offshore bank accounts. The amount of

proceeds recovered / confiscated varied and depended on the ability of LEAs to identify the assets.

57. Compared to the number of STRs being analysed and disseminated (Figure 2), the number of ML investigations conducted is comparatively low, which in part results in low numbers of prosecutions and convictions. The lack of statistical information is one possible reason for this finding. Other possible reasons are the resources and operational priorities of the jurisdictions, legal constraints and the obstacles regarding international cooperation.

Domestic and International Cooperation

58. As the term transnational frauds implies; the fraudster, victims and the proceeds are often located in various jurisdictions. Therefore domestic and international cooperation among parties involved in the investigation is crucial to the successful prosecution of the criminals and recovery of funds.

59. In terms of cooperation in the domestic context, most jurisdictions responded that concerned agencies work well with each other. It was highlighted by one jurisdiction that domestic agencies should have a knowledge and understanding on the roles and powers of other relevant agencies in the same jurisdiction. An increased level of understanding will enhance cooperation and engagement between agencies, especially for those agencies vested with distinct powers. Some jurisdictions highlighted that the privacy laws may restrict the ability of the FIUs and LEAs to share information.[1]

60. For international cooperation, all the responding jurisdictions raised concerns regarding the current situation on international cooperation among jurisdictions, which will be discussed in greater detail in later paragraphs. The concern raised is the disparity between the number of requests for international cooperation and foreign disseminations as compared to the number of STRs received and analysed.

[1] A proposal has been made in the revision of the FATF 40+9 recommendations to amend R4 to include the principle that limitations imposed by data protection and privacy regimes should be reasonable.

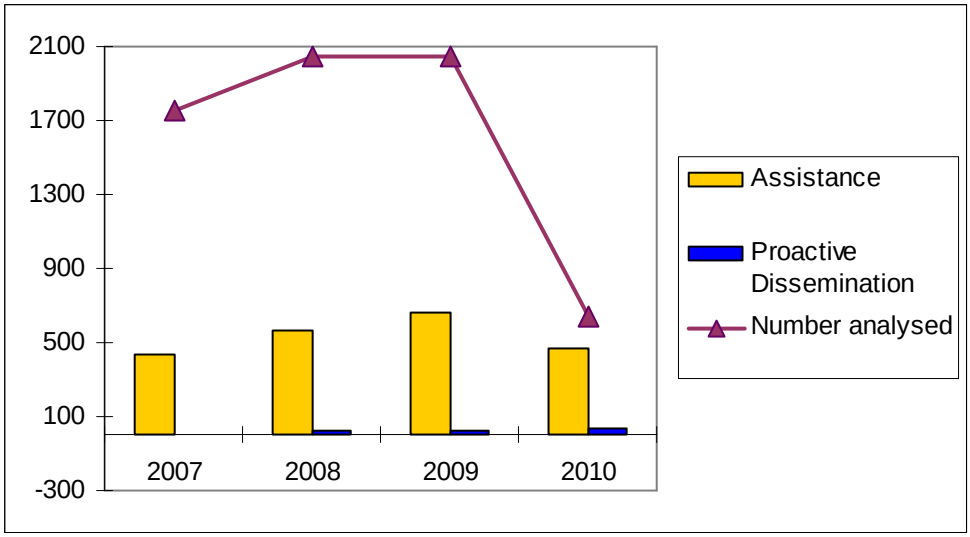


Figure 4 : Comparison – No. of STRs received & analysed and international assistance

61. The major obstacles identified that can hinder international cooperation among the jurisdictions for FIUs and LEAs include the diversified legal requirements such as Memorandum of Understanding (MOU) and treaties for cooperation, sufficiency of information, timeliness of response and capacity and skills of counterparts. It has been raised by one jurisdiction that a better understanding on the difference in capabilities and legal system of other jurisdictions will help to minimize the obstacle in cooperation. The obstacles can be categorized as follows:-

- **Requirement of MOU and Mutual Legal Assistance Treaty (MLAT)** – The level of international cooperation among jurisdictions varied and the lack of MOU and MLAT arrangements between certain jurisdictions can cause difficulties in the exchange of financial intelligence, collection of information and evidence from other jurisdictions for investigation, prosecution or other requests for assistance. The level of cooperation with non-Egmont members may be further limited.
- **Power and authority of FIUs** – The powers and authority of FIUs vary depending on the domestic legislation and the FIU model. For example, domestic legislation may restrict the scope and type of assistance that can be provided to other jurisdictions, such as powers of some provisions only applicable to the predicate offences. Another example is that in some instances the type of request made is beyond the authority of the requested FIU, including requests to interview the subject.
- **Type of data held** – FIUs collect and hold different reports depending on the requirements of the legislation. The types of reports submitted to FIUs include Suspicious Transactions Reports (STRs), Cash Transaction Report (CTRs), International Fund Transfer Reports, Cross Border Cash and Bearer Negotiable Instrument (BNI) Reports. Not all FIUs receive all of these reports. The type of data collected by jurisdictions may affect the level of cooperation provided as the documents sought may not be available.

- **Timeliness of response** – Resource constraints, bureaucratic approval processes, from the authorization to document preparation, may delay the response time to the requesting jurisdiction and thus to the investigation progress.
- **Skills and capacity** – The evolving fraud scheme and its complexity posed challenges in terms of the skills and capacity in dealing with transnational frauds and associated ML. Experience, IT competency and capacity of staff to apply advanced analytical tools in some jurisdictions may affect the ability in the fund tracing process.
- **National interests** – Jurisdictions may consider not responding to a request after taking into consideration its national interests, or where the case is currently of interest to a local LEA where proper approval has to be sought. One jurisdiction has highlighted that a response will be made when there is a clear suspicion that the activity has involved its jurisdiction. This has created difficulties to jurisdictions when the information provided is not complete and does not show the involvement of the jurisdictions in the criminal activities.
- **Sufficiency of information** – It is highlighted that the breadth of the provisions of ML offence has challenged prosecution authorities to guard against the inappropriate use of the provisions. Thus, the availability of sufficient information and evidence is a key to successful cooperation, especially in the application of restraint order to court.

62. Some of the obstacles identified will be resolved in the legal context. However, in the early stage of investigation or intelligence analysis, formal MLA channel is probably not a viable option to gather information / intelligence. It is considered that some form of networking providing "informal assistance" may be a starting point to facilitate jurisdictions in obtaining useful information in the investigation or intelligence analysis, such as the identity information of targets and assets identification, from counterparts. Also, the information can assist the subsequent formal MLA process. One of the examples is the Camden Assets Recovery Inter-Agency Network (CARIN) in the European Union which provides a network for FIUs, LEAs and judicial authorities in sharing of information, asset tracing and confiscation of proceeds.

The Camden Assets Recovery Inter-Agency Network (CARIN)

In October 2002, the Criminal Asset Bureau Ireland and Europol co-hosted a conference in Dublin. The conference was attended by representatives of all Member States of the European Union, some applicants states, Europol and Eurojust. One of the recommendations made was to look at the establishment of an informal network of contacts and a cooperative group in the area of criminal asset identification and recovery. As a result, CARIN was established. The aim of CARIN is to increase the effectiveness of members' efforts, on a multi-agency basis, in the area of cross-border identification, freezing, seizure and confiscation of the proceeds from crime. This is now a major law enforcement tool in targeting organized crime gangs in particular reference to financial deprivation. CARIN has 45 members and observers.

3.3 BANKING / FINANCIAL SUPERVISOR / PRIVATE FINANCIAL INSTITUTION

Preventive measures – Supervisors

63. Jurisdictions have provided consistent responses from both supervisory authorities and financial institutions about the preventive measures applied to their financial institutions. Supervisory authorities issue policy statements and guidelines regarding general AML/CFT measures which includes KYC/CDD procedures, transactions monitoring mechanism, engagement with management information systems and staff training and awareness. The above measures have been defined broadly for ML/TF measures and not specifically to address transnational frauds.

64. However, a few jurisdictions have taken fraud-specific measures to protect the public and the financial institutions from criminal syndicates or criminals conducting frauds. The examples are as follows:

Canada

- The Canadian Banking Association maintains a grid warning system through the Bank Crime Prevention and Investigation Office (BCPIO). The BCPIO coordinates investigation and prevention activities in an effort to protect banks and their customers from financial crime. The grid warning is a message sent to all FI's that provides information to warn of suspected criminal activity, the modus operandi of the scam and the information of suspect. These systems increases the likelihood that fraudulent activity will be identified and makes it difficult for fraud perpetrators to bank in Canada.

Malaysia

- Banking institutions are required to report incidences of fraud and defalcations, attempted frauds, cases of staff misconduct and robberies to the Central Bank through a dedicated frauds repository system. Supervisors are able to generate fraud analytical reports and perform trend analysis which will later be communicated back to the financial institutions.
- The establishment of a financial fraud alert section in the central bank's website to alert the public on fraud schemes, enforcement action taken and reporting mechanism. This initiative alerts the public on the latest modus operandi of frauds.

65. Further, continuous engagement with the industry associations in sharing the latest fraud activities and methodologies can inform the supervisors and the financial institutions on any emerging fraud trends.

Information Sharing Among Financial Institutions

66. Analysis on jurisdictions' responses revealed that almost half of the jurisdictions have indicated that their financial institutions do not share information on ML/TF activities including transnational frauds either with domestic banks or within their own group internationally due to restrictions under domestic laws. One of the key features of transnational fraud is the speed at which funds can be transferred between jurisdictions. Any limitation in information sharing will put transnational fraud investigation and proceeds of crime action at a disadvantage. An Enterprise-wide STR Sharing Paper by the Egmont Group has highlighted the potential benefits for financial institutions and LEAs if the sharing of information among financial institutions and groups can be enhanced. If financial groups are able to share information on fraudsters, it will assist to enhance the overall effectiveness and efficiency in the detection and prevention of transnational frauds as well as the filing and the quality of STRs in general.

67. Meanwhile, Malaysia's financial institutions share information on modus operandi and typologies among domestic banks via Compliance Officer Networking Group (CONG) and within the financial institution's group internationally. But the information on customers is not being shared due to banking secrecy restrictions. As some of the financial groups share the same database, a few jurisdictions indicated that their financial institutions shared the information within the financial groups as the law allowed.

Financial Institutions as the Gatekeeper in Protecting the Misuse of Financial Sectors

68. As FIUs have taken the initiatives to guide and regulate financial institutions from abuse by ML/TF activities, including transnational frauds, and supported by the requirement and close supervision from the supervisory authorities, the balance of the effort lies in the hand of financial institutions. Full implementation of the requirement, from CDD to staff training, including keeping abreast of the latest trends of transnational fraud methodologies is important for financial institutions in eliminating the possibilities, or reducing the risks, of their institutions of being abused for transnational fraud activities.

69. Financial institutions have a crucial role to play as gatekeepers in protecting their institutions from the criminal activities. Besides the preventive measure requirements imposed by the authority (FIU and supervisory authorities), financial institutions have also taken their own initiatives to prevent them from being vehicles in transacting illegal proceeds.

70. As a gatekeeper, financial institutions can deter transnational fraud activities through preventive measures; by asking the right questions of possible fraudsters, conducting comprehensive due diligence processes, and the timely submission of STRs which may keep the authority appraised of possible fraudulent activities.

71. Financial institutions, as part of their social responsibility and also in order to ensure reputational protection, have issued numerous reminders to customers to prevent them from becoming victims of fraud. Notices, especially in the banking halls and at ATMs, together with promotion of safe internet banking activities, have been proven to reduce the risk of customers from being deceived. Understanding the customer's normal pattern of transactions and seeking information from the customer when transactions deviate from the known pattern may save them from falling victim to fraudulent activities.

4 CASE STUDIES

72. Jurisdictions have faced a wide range of fraudulent activities of differing scales in terms of the numbers of reports, number of victims and the amount of losses. Although the prevalent types of frauds varied from one jurisdiction to another, there are similarities in terms of the way the frauds operate and how the proceeds are transferred. The common features observed in the case studies can facilitate jurisdictions in understanding some of the modus operandi, in particular, those areas that jurisdictions are not familiar with.

73. The cases of transnational frauds reported by the jurisdictions are mainly mass-marketing frauds against individuals. The most common types of frauds reported are telephone deception (emergency scam), advanced fee fraud by lottery, internet romance and heritage, investment (Ponzi Scheme) and boiler room fraud.

Type of Fraud	Reporting Jurisdiction	No. of Report / Victim	Fraud Victim Location	Nationality / Location of Perpetrator	Reported Losses (USD)	Location of Money Laundering
Lottery Fraud	Hong Kong	515 reports (in 2009)	27 jurisdictions	Overseas	9.21M	Hong Kong
Telephone Deception	Thailand	2 reports (500 victims)	Overseas	Overseas	65M	Thailand
	Malaysia	496 reports (in 2009)	Malaysia	Overseas	1M	Malaysia
	Hong Kong	1,495 reports (in 2009)	Hong Kong	Hong Kong and overseas	3.78M	Hong Kong and overseas
Investment Fraud	Philippines	1 report	Philippines	Philippines	250M	Philippines and overseas
	Canada	130 victims	Canada and overseas	Canada and overseas	10.3M	Canada and overseas
Advance Fee Fraud	Canada	253 victims	Canada and overseas	Canada and overseas	4.78M	Canada and overseas
Boiler Room Fraud	Macao	1 report (22 victims)	Overseas	Overseas	1.7M	Macao and overseas

Table 2: Major Types of Fraud – Responses from Jurisdictions

Advanced Fee Fraud

74. Advanced fee fraud ('AFF') is a general term to describe a fraud, which usually involves an up-front fee paid by victim who is offered or guaranteed a financial gain by the perpetrator of the frauds. Victims are often solicited through emails, cold calls, text messages, and false documents are used in order to convince the victim to participate in various schemes that appeared to be genuine or in existence.

75. AFF appears in different guises varying its styles and approaches, but all with the same goal: to deceive money from victims. Questionnaires collected from

responding jurisdictions reported that AFF can be categorized mainly into the following types: -

- Lottery scam / heritage scam
- Nigerian scam (or known as 419 scam)
- Internet romance scam

76. Lottery, heritage and Nigerian scams are the most common types of AFF. Lottery and heritage scams usually involve unsolicited e-mails, text messages or faxes sent to potential victims claiming that they have either won a prize or come into an inheritance. In order to collect the cash award or the inheritance, victims have to pay certain fees in advance under the guise of gambling taxes, processing fees, membership fees and administrative fees. It is usual that once the victims respond and advance the required fee, they will either not be able to contact the perpetrators of the frauds, or further funds will be requested to release the prize or heritage.

77. In cases reported relating to the Nigerian scam, swindlers often claim they hold high ranking positions in government in West Africa. They will who allege that large amounts of money from prior regimes needs to be laundered and that they need to transfer the money to a foreign account. A favourable response to the solicitation is followed by excuses why the funds cannot be remitted readily and eventually the victim is required to provide up-front or advance fee for various taxes, fees or bribes to facilitate the processing and remittance of the alleged funds. When the perpetrators of the fraud receive the money, inevitably victims will receive no further contact, or further funds will be requested.

78. Internet romance scams have become more and more popular over the years, which are considered as an evolution of lottery and Nigerian scam. Instead of sending unsolicited emails or letters, swindlers 'fish' for their prey from on-line dating websites and pretend to look for a partner with a view to a long term relationship. They use psychological ploys to lure the victims with a view to forming a relationship and gaining their trust. Once an on-line relationship is formed, the perpetrators then make use of various excuses to obtain money from the victims, including sudden financial difficulties in meeting hospital bills of family members, falling ill or being involved in a serious accident, being robbed, require money for airfares, visas, passports so that they can meet victim, for the payment of phone bills or fines, ongoing living expenses or to sponsor charity or orphanage.

Telephone Deception (or emergency scam)

79. This scam involves the culprit calling the victim by telephone and assuming the identity of one of the victim's relatives, friends or business associates. The culprit

claims that he/she is experiencing some troubles and in need of money urgently. Common excuses used are to pay for bail money or medical expenses overseas due to an arrest or accident, to pay gambling debts or to pay for an investment. The victim is asked to deposit or transfer money into a designated bank account provided by the offender. The offender would open the bank account by using either a bogus or stolen ID card to receive the funds. Alternatively, the offender would use a stooge account or money service business. If they are successful in their initial attempts, the offender will make further contact to the same victim and demand more money. In most cases, reports are made subsequent to the transfer of fund when the victim discovers the call to be a scam.

Boiler Room Fraud / Investment Fraud

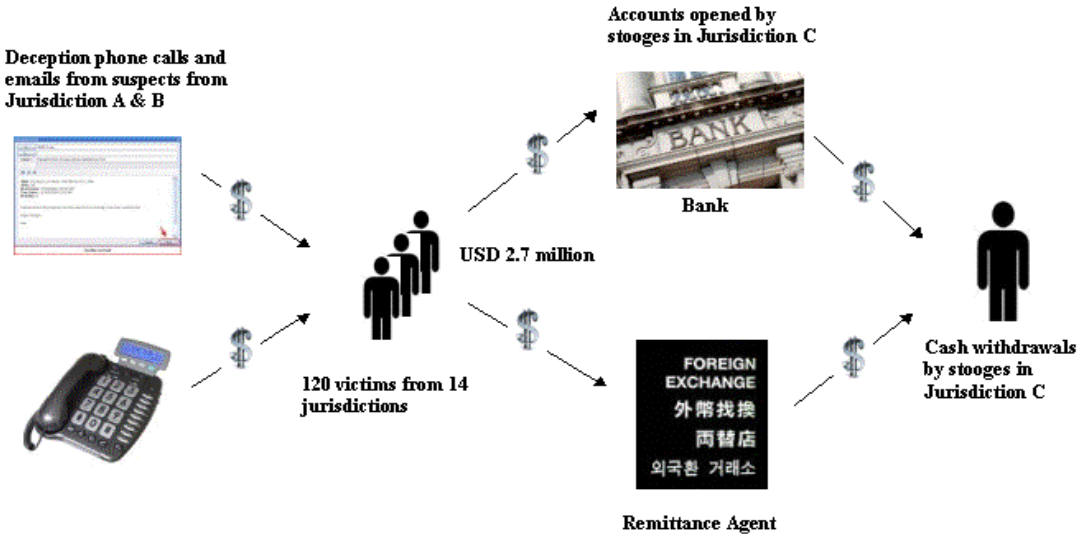
80. These frauds are typically packaged to look like genuine investment schemes with promising returns and the investment opportunities aligned with the contemporary economic climate such as green or new technology and natural resources.

81. Boiler room fraud is a scam involving the sale of shares that are either worthless or non-existent using high-pressure tactics during telephone calls. Salespeople / brokers are hired to call unsuspecting individuals and recommend investment opportunities. In recent years, brokers have made good use of the internet by contacting potential investors via e-mail and falsely representing their businesses with the use of bogus websites to support their legitimacy. Very often, the names adopted are similar to legitimate financial institutions to confuse investors. Alternatively, such entities may provide financial investment trading platforms on the internet. Investors usually receive the monthly statements of their 'investment' through e-mails and they will never have any face-to-face contact with the brokers. Shares are sold at vastly inflated price and also with exorbitant dealing or brokerage charges. They are generally are well-trained, aggressive and determined salespeople continuously on the phone canvassing potential investors to buy the same stock. If an investor does not succumb on the first call, the boiler room operators will call again and again often at inconvenient times, urging them to buy.

82. A Ponzi scheme is an investment fraud where withdrawals are financed by subsequent investors, rather than profit obtained through legitimate investment activities. The Ponzi scheme usually entices new investors by offering investment opportunities claimed to generate high returns with little or no risk. Payments from new investors are used to make "interest payments" to existing investors or "referral fees" to those who recruit new investors. The scheme will collapse when new investors can not be enticed to invest, and the interest payments to existing investors will no longer be able to be met, as the funds 'invested' have been siphoned off for personal use, or paid to existing investors as interest.

Case Study 1: Use of Overseas Stooge Account

83. Between January and April 2010, 24 overseas victims respectively received telephone calls or emails purporting that they had won grand prizes in lucky draws or had made significant profits on investments. To release the funds, these victims were lured to pay advance fees to cover administration charges. The victims were asked to transfer / remit funds, which amounted to a total of USD600,000, to Jurisdiction C where the monies were subsequently withdrawn from a remittance agency. Most of the cold calls or internet messages originated from Jurisdiction A and B. Upon conducting a fund flow analysis, it was estimated that at least 160 overseas victims from 14 different jurisdictions have been defrauded for about USD2.7 million. The proceeds were transferred / remitted to Jurisdiction C between April 2009 and June 2010. Enforcement actions in Jurisdiction C led to the arrest of 13 persons including 2 middle men and 11 stooge account holders who admitted to be employed by others to operate the accounts and coordinate the transfer of funds.



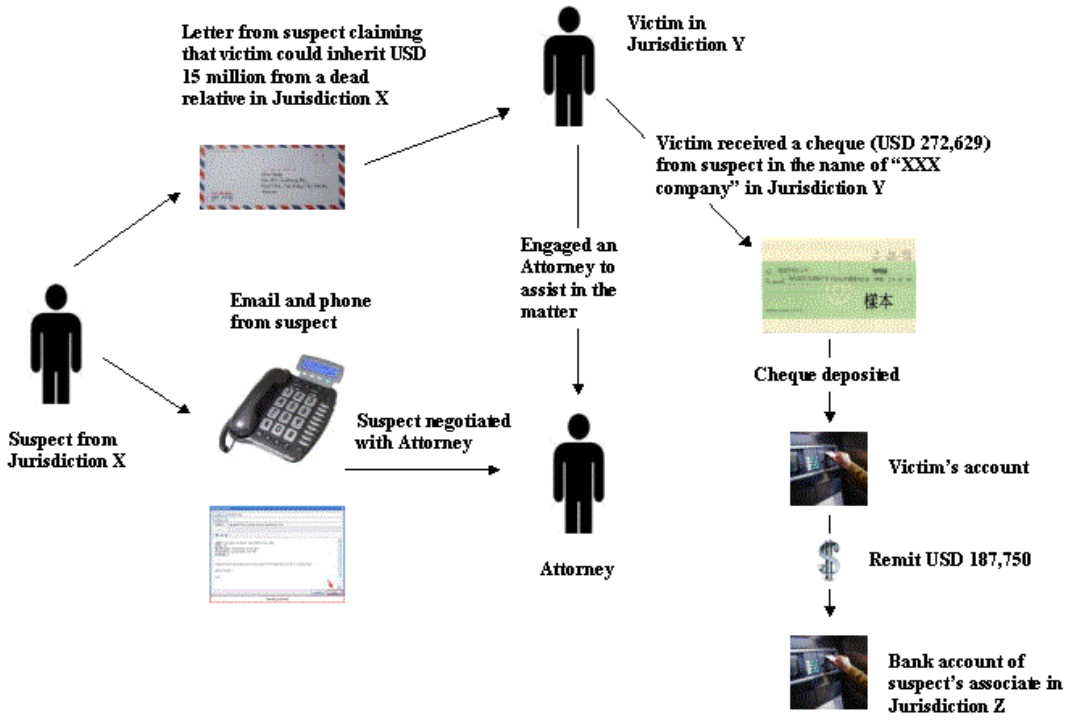
Points to note:

- Targeting overseas victims with no connection or limited knowledge of Jurisdiction C.
- Use of reputable companies and organizations in another jurisdiction to cover the fraud.
- Use of pre-paid phone cards and false identity information to open email accounts and to cover the true identity.
- Use of overseas and local stooges to open accounts and to withdraw the fraudulent funds from banks and remittance agents in Jurisdiction C.
- Syndicate members would collect the cash from the stooges.
- To break the audit trail, fraudulent funds would be withdrawn in cash.

Source: Hong Kong

Case Study 2 : Use of Innocent Parties

84. A victim in Jurisdiction Y received a letter from a suspect in Jurisdiction X purporting that he could inherit US$15 million from his dead relative. The victim engaged an attorney to negotiate with the suspect who was deceived to believe that victim was the official heir. The suspect then communicated with the victim and told the victim that he was required to settle a tax payment in Jurisdiction X before the inheritance could be released. The suspect told the victim that he would arrange the fund transfers. Subsequently the victim received a check for USD 272,629 issued by a company in Jurisdiction Y. The suspect then instructed the victim to deposit the check to his attorney's account. After the check was cleared, the suspect asked the victim to instruct his attorney to remit part of the funds to a tax consultant in Jurisdiction Z due to foreign currency exchange problem in Jurisdiction X. After the remittance to Jurisdiction Z, the bank informed the victim and the attorney that the check was a stolen check. Investigations revealed that the tax consultant was in fact an associate who was a local resident of Jurisdiction Z.



Points to note :

- Use of innocent parties to cover the money laundering activities.
- Use of attorney account to avoid the detection by financial institutions.
- Use of overseas account to complicate the audit trail.

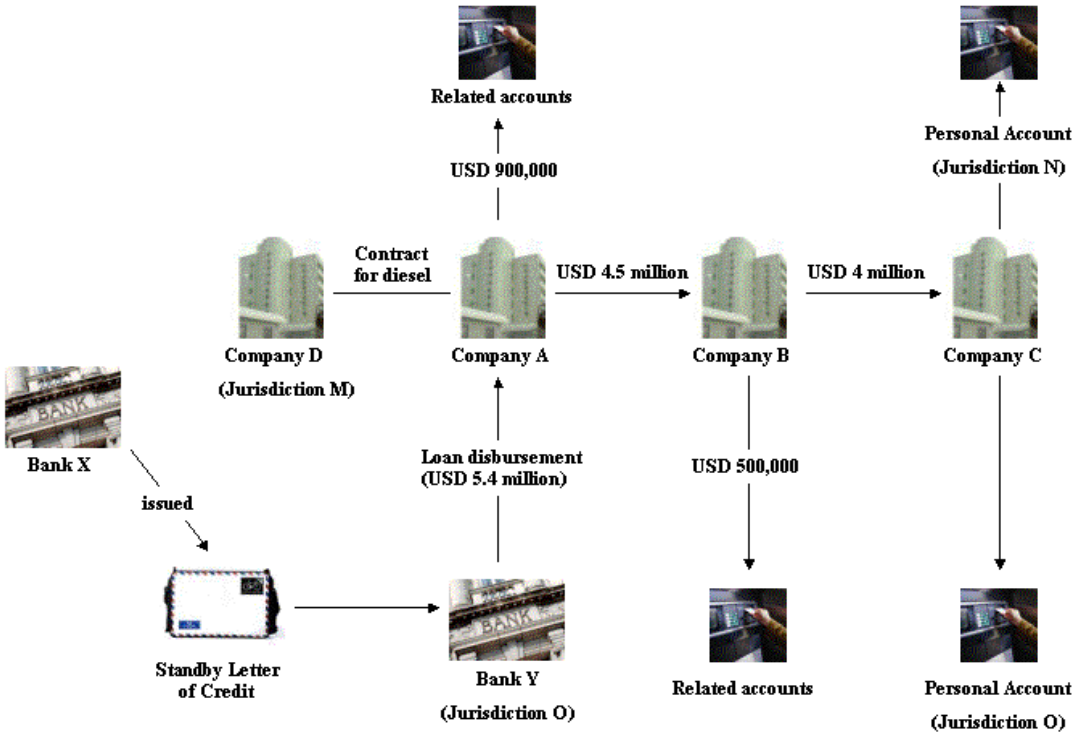
Source: Japan

Case study 3 : Standby Letter of Credit Fraud

85. Company A entered into a contract with Company D (based in Jurisdiction M) to supply diesel fuel. Company A then applied for a loan from a local Bank Y using a Standby Letter of Credit issued by Bank X in Jurisdiction M on behalf of Company D to support the loan application. Bank Y then disbursed a loan of USD 5.4 million to Company A. Company A agreed to receive the documents at a later time.

86. Although the loan funds were disbursed, Company A did not supply the diesel fuel to Company D. Company B was appointed by Company A to supply the diesel fuel but Company B subsequently paid Company C USD 4 million to supply the diesel fuel to Company D. The director of Company C, however, transferred the funds into his personal accounts in Jurisdiction N and Jurisdiction O. Company C failed to fulfil its contract.

87. Company A eventually provided the documents to Bank Y. Bank Y discovered that the documents were forged and the companies involved were all shell companies.



Points to note :

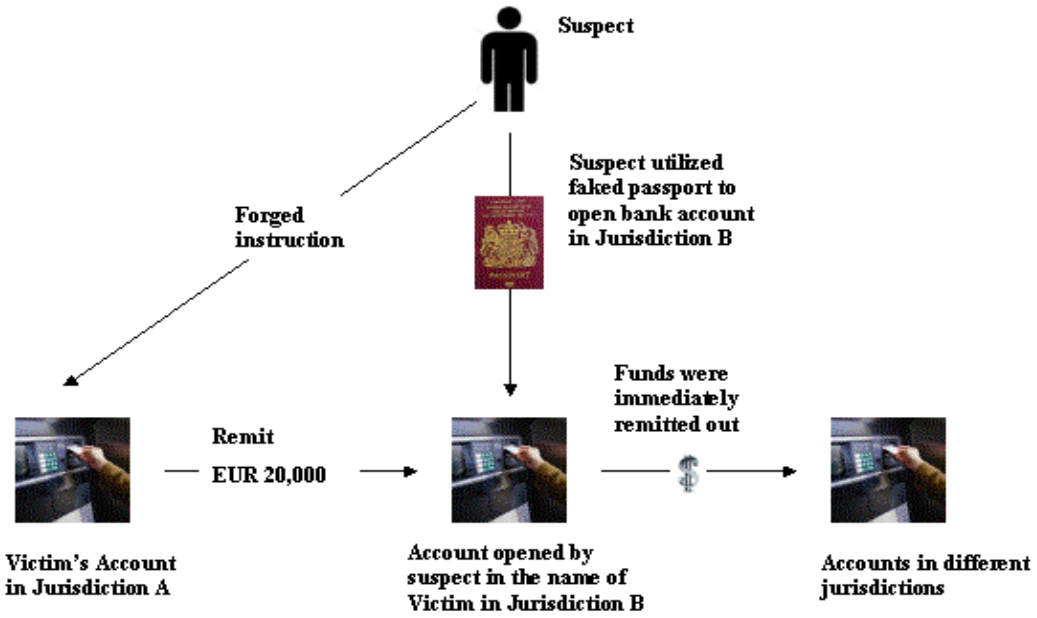
- Use of forged documents to deceive the bank.
- Use of shell companies in various jurisdictions.
- Use of different companies to complicate the transactions.

Source: Malaysia

Case Study 4 : Identity Theft

88. A victim lodged a complaint to his bank in Jurisdiction A for theft of identity and fraudulent wire transfer of money from his account to an account in Jurisdiction B also in the name of victim. The account in Jurisdiction B was opened with the support of a fake passport printed with victim's particulars but a different photo. After the account was opened, forged instructions were made to bank in Jurisdiction A to remit money from victim's account to the account in Jurisdiction B. Upon receipt of the remittance, the funds would be immediately disposed by further remittance to bank accounts in other jurisdictions.

89. Investigations showed that the syndicate committed identity theft in one jurisdiction and used the particulars to open bank account in another jurisdiction. The transnational nature of the operation suggested syndicated work and sophisticated planning in perpetuating the crime.



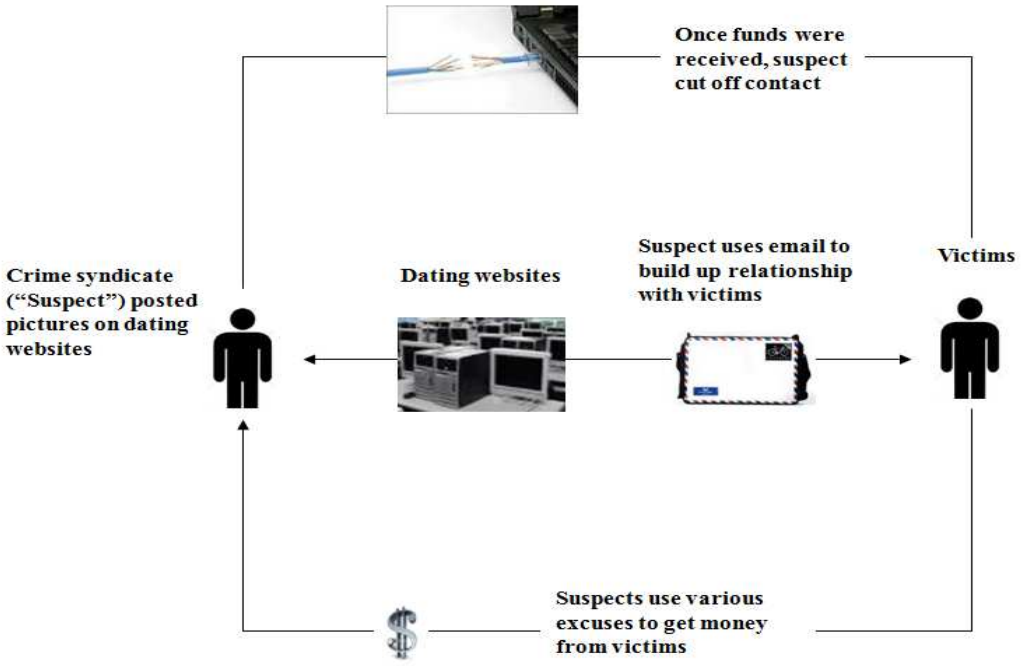
Points to note

- Theft of identity in one jurisdiction through illegal means.
- Use of fake passports with victim's particulars to open bank account in another jurisdiction.
- Transfer of victim's fund by forged instructions to bank to the overseas account.
- Disposal of the fund by ATM withdrawals in other jurisdictions and create difficulties to the investigations.

Source: Hong Kong

Case Study 5 : Advanced Fee Fraud through Internet

90. A crime syndicate posted pictures of foreign females on the dating websites to lure males who intended to find girlfriends or partners on the internet. After establishing emails conversation with the victims, scammers would usually request money for various reasons, such as to offer bribes to officials for the payment of air tickets to the victim's jurisdiction, sudden financial and life crisis, and then requested the victims to send money, ranging from USD1,000 to 10,000. Once the funds were transferred, the scammers would discontinue all contact with the victims and disappeared from the website.



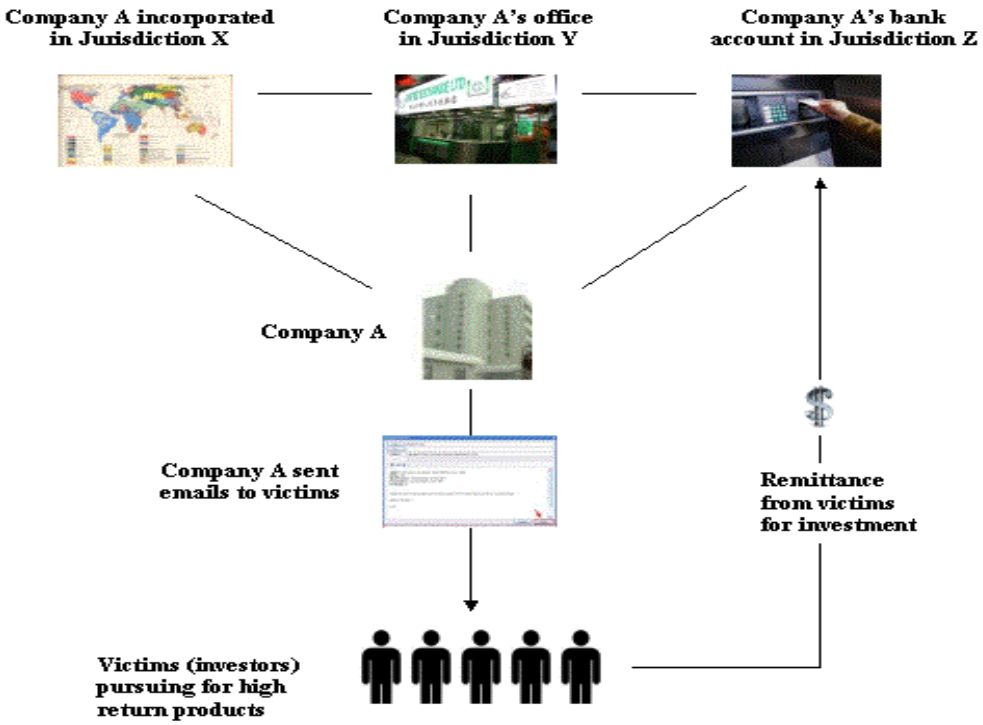
Points to note:

- Make use of social websites (on-line dating) pretending to look for a long term partner.
- Use romance emails and attractive photos to lure victims.
- Use psychological tricks to establish relationship and gain trust from victims.
- Make use of various excuses to get money from victims once a relationship is formed.

Source: Australia

Case Study 6 : Ponzi Scheme (High Yield Investment Product)

91. Company A (an unauthorized brokerage firm) was incorporated in Jurisdiction X (offshore centre) which claimed that it was specialized in stock and futures investment and maintained an office in Jurisdiction Y. The suspects posed as staff of Company A in Jurisdiction Z and contacted potential investors by emails and cold calls offering high return investment products which were non-existent. The website appeared to be a genuine investment company. Investors were asked to remit funds to the bank account of Company A held in Jurisdiction Y. In a one-year period, the account in Jurisdiction Y recorded a total deposit and withdrawal of USD7.9 million respectively. Multiple inward remittances from various individuals of different jurisdictions were recorded. Immediate outward remittances to other jurisdictions were made via e-banking after the inward remittances were received to the account.



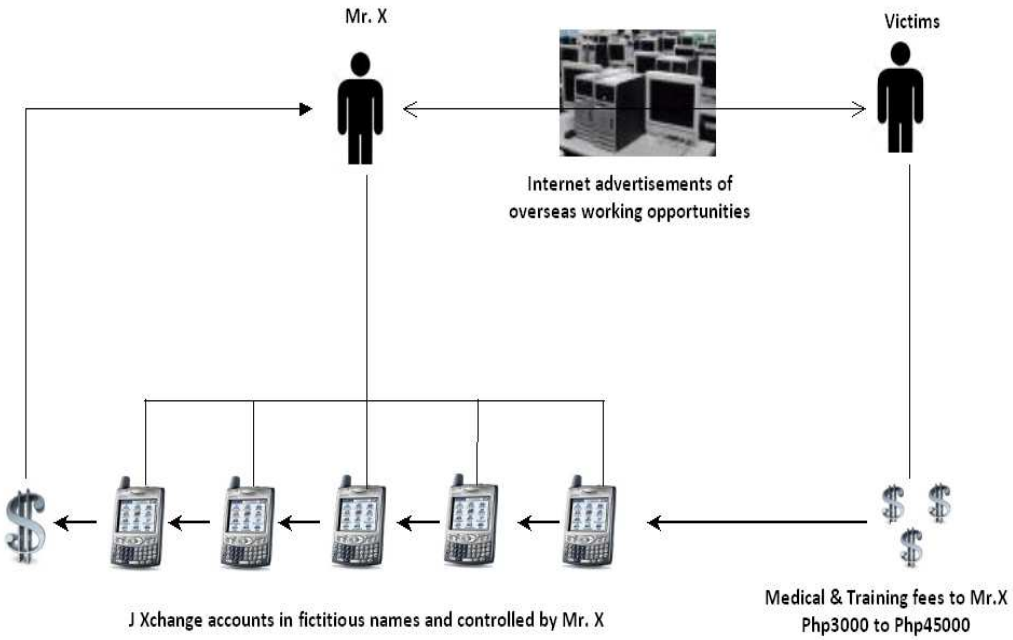
Points to note:

- Use of offshore shell company and fictitious website to promote high yield investment products.
- Investors remitted investment funds to offshore bank account.
- Investment funds were further disposed by remittances to other jurisdictions.
- Immediate withdrawal of the funds remitted to the account.

Source: Malaysia

Case Study 7 : Use of Mobile Payment System

92. Mr. X posted advertisements of overseas working opportunities in the Internet. By using several aliases and fictitious names, he pretended to be the legitimate recruiter or foreign employer. Applicants were misled that they were offered overseas employment and they were required to pay medical and training fees, ranged from Php3,000 to Php45,000. Payments were made through a mobile phone payment system known as 'J Xchange'. Mr. X had opened different J Xchange accounts under fictitious names and victims were instructed to send money to one of the accounts. Upon receiving the deposits, Mr. X transferred the funds to other accounts several times and eventually withdrew the funds in cash.



Points to note from Case Study 7

- Use of Internet to entice victims.
- Use of mobile payment system.
- Use of false identification information to open mobile payment accounts for concealment of the true identity.
- Use of multiple payment accounts to complicate the fund flow.

Source: Philippines

5 CONCLUSIONS AND RECOMMENDATIONS FOR FURTHER WORK

5.1 KEY FINDINGS

93. LSTF and ML associated with the frauds affect jurisdictions in different degrees. Clearly, the problem has transformed into a global crime threat as the operation of the frauds and ML techniques have evolved. Law enforcement, regulatory authorities and financial institutions acknowledge the increasingly complex and transnational nature of the crime and associated ML activities. The key findings of the project can be summarized as follows:

- From the information available to the project team, it is apparent that certain jurisdictions have conducted surveys or studies on certain frauds, mainly related to mass marketing fraud. Unfortunately, from the analysis of the questionnaires, there is a lack of comprehensive and authoritative statistical data to allow the project team to assess the magnitude of the proceeds of LSTF with any degree of accuracy;
- There are challenges in following the money trail of the crime proceeds of LSTF because of cross-jurisdictional nature. The proceeds tended to move quickly by means of the advance in, and availability of, information technology. More importantly, the money trail is broken once the money is withdrawn in cash during the laundering process;
- The techniques used to launder the crime proceeds of LSTF are fairly well known to LEAs, FIUs, financial institutions, DNFBPs and regulators, especially in jurisdictions with more mature AML/CFT regimes. Such techniques include the use of cash, stooge bank accounts, false identity documents to gain access to financial services; money services providers; new payment methods, shell companies and complex corporate structures;
- While the money laundering techniques are known to the authorities and institutions, criminals are still able to exploit the loopholes and avoid detection. There appears to be some capacity issues in terms of understanding and detecting the underlying suspicious transactions / activities and / or the investigation of money laundering activities;
- It is invariably the case that the jurisdiction where the fraud takes place and where the money is laundered are different. Owing to legal constraints or law enforcement agencies being pre-occupied with investigating the predicate crime, the money laundering aspect tend to be the second priority if not completely ignored;
- As mentioned above, there are difficulties in following the money trail of the crime proceeds from jurisdiction to jurisdiction. This being the case, recovering the funds for the victims is not always possible and is normally done when the offenders are arrested or the victims have alerted the banks concerned to recall the remittances;

- The most effective way of tackling the problem of LSTF is raising the awareness of potential victims through well-coordinated publicity / education programmes by both government agencies and NGOs. Moreover, front-line employees of financial institutions should also receive training so that they can identify potential fraudulent activities;
- Apart from actions at a domestic level to prevent and combat the LSTF and associated ML activities, international cooperation is also another key area that needs some attention so that jurisdictions could share information / intelligence in a timely and effective manner. Enforcement and regulatory actions could then be taken with better results.

5.2 ISSUES FOR CONSIDERATION

- There is a requirement for authorities to [better] understand and identify the fraud and the level of threat/risk of associated money laundering poses to their jurisdiction.
- There is a requirement for jurisdictions to further categorise and publicise/share such risk profiles and trends in terms of broad types of fraud.
- This typology complements previous research that acknowledges the fact that such threat/risk should be broken down in terms of fraud types and ML methods, because considerable variations exist.
- Significantly closer interaction between the regulated sector, law enforcement, financial intelligence units and competent authorities needs to be pursued.
- There is an ever increasing requirement to better understand the risk and involvement of NPMs, which the case studies indicate are becoming increasingly central to money laundering associated with LSTF.
- It is important to explore further ways FIUs and LEAs can enhance the exchange of information and data pertaining to trends in money laundering associated with fraud; there exists an appetite for greater information exchange which is currently not being met.
- International cooperation is a key factor. Fast and efficient exchange of information are key to the detection of money laundering associated with fraud and there is still a great deal more that can be done in this area, as currently recognized in the discussions that are taking place in the FATF in respect of R.40 and the Egmont Group in respect of information sharing.
- Although information is available in the public domain, jurisdictions should be more proactively involved in the sharing of trends and profiles internationally. This is particularly true across the Asia Pacific Region as increasing numbers of jurisdictions are exposed to threats associated with NPMs as economies and financial infrastructure develop.
- Increasing level of mutual co-operation to help identify money flows, information for which is currently deficient in some areas.

- Besides compliance with regulations and guidelines, the financial institutions may consider taking their own initiatives to prevent their institutions from being used as a conduit in the transnational frauds.
- A dedicated sharing platform could be initiated for sharing of emerging trends and modus operandi among the institutions.
- Investigative agencies should place greater emphasis on investigating the financial aspects of the predicate offences. Those LEAs that are mandated to investigate ML should develop a culture of "follow the money".

5.3 RECOMMENDATIONS FOR FUTURE WORK

94. It seems clear that the prevention and detection of the LSTF and ML associated with the frauds could be improved by more cohesive and coordinated efforts nationally and internationally in the following areas:-

Risk Assessment

95. Jurisdictions should conduct a risk assessment in order to critically review and assess the problem in terms of the nature, scope and impact. By conducting a risk assessment a jurisdiction will have a better understanding of the fraud risks and areas that are most vulnerable to fraud and ML. This will assist each jurisdiction in the formulation of comprehensive strategy, policy and the creation of an action plan which will ensure that operational priorities and resources can be allocated in the most efficient and effective manner. Intelligence gathering, enforcement action and preventive measures can then be achieved though a coordinated platform.

International Cooperation

96. Jurisdictions should make continuous efforts in enhancing the understanding and cooperation among domestic agencies. Cooperation is essential in the coordinated fight against the risks of transnational frauds and ML. It is appreciated that there exist legal constraints and obstacles where international cooperation is required that takes time to resolve and jurisdictions should aware of the difficulties encountered by their counterparts. Yet, jurisdictions can enhance the level of cooperation in terms of the quality and timeliness of information exchange. Request and reply should contain sufficient identification information of the victims, suspects and related entities, details of the frauds or suspicions, details of any restraint/freeze order and contact points of LEAs. Apart from assisting the counterparts in the investigation and asset tracing process, jurisdiction can also obtain information of the latest trends and methods of the transnational fraud and the ML methods by making request to the LEAs and FIUs, referencing to the reports make by other jurisdictions such as status report, typologies report and research reports.

Regional Task Force

97. The present mode and structure of international cooperation cannot provide jurisdictions with a quick channel to conduct enquiries or to pass information. To address this deficiency, a Regional Task Force where each jurisdiction has a designated point of contact to provide prompt operational support may be a viable option in bridging the gaps.

Intelligence Exchange

98. There is a lack of coordinated efforts to identify the ultimate beneficiaries and uses of the proceeds of the frauds. The complex voyage of the funds by different payment methods through multiple jurisdictions complicates the intelligence analysis process by both LEAs and FIUs. The absence of timely and proactive flows of information, including STR information, clearly demonstrates the deficiency in the present information sharing regime where most jurisdictions stop acquiring more information of the money trail. Experience shows that following the money trail can lead to the identification of new information, can identify further criminal offences or identify further suspects and subsequently lead to the prosecution of the organisers of these frauds. The financial intelligence can facilitate LEAs in the investigation and the subsequent MLA process in obtaining information for evidential purpose.

Central Database

99. Jurisdiction has published Alert List about the information of the entities suspected of fraud activities. This is a valuable source of information that can be shared between jurisdictions. However, there is lack of common platform to collate and publish the information internationally. To optimize the use of the information, a central database should be devised to capture and collate the information from jurisdictions.

Enforcement Action

100. There seems to be misconception in some jurisdictions of the distinction between the predicate offence / crime and ML offence. This is truly reflected from the responses of the jurisdictions that almost all jurisdictions have identified the problem of being the transit location for the fraudulent funds but have taken limited actions or been reactive in the proceeds aspect. Obviously, fraudsters are taking advantage of the differences between jurisdictions that has resulted in lack of adequate responses by some jurisdictions. On the other hand, there may be strong indications from the STR or other information about a fraud scheme and the movement of the proceeds. However, FIUs and LEAs cannot simply take

enforcement action based on the indications and may require further information from other jurisdictions in order to establish a prima facie case and to satisfy the relevant judicial requirements. It is a typical response of the fraudster to challenge the propriety of the enforcement action undertaken by FIUs and LEAs.

Awareness Raising / Capacity Building

101. Jurisdictions should expand the public awareness and education programs in a targeted manner so that individuals (especially the vulnerable groups such as senior citizens) and businesses can recognize the key features of various fraud schemes as well as the most frequently reported schemes. Besides, jurisdictions should make use of the existing studies and reports as guides for action in this regard. It is essential for concerned agencies to enhance the capacity building efforts by preparing 'red flag indicators', statistics, typologies and specific training materials focusing on raising the awareness of both the public and employee of agencies concerned.

Preventive measures

102. Continuous engagement among the FIUs, LEAs and FIs is crucial in providing the synergy in preventing the abuse of financial system by the fraudsters. Feedback mechanism among the stakeholders will enhance the cooperation, and at the same time updating them on the emerging trends and modus operandi of transnational frauds. Since the proceeds of fraud normally originate and then go through FIs, they play a crucial role in preventing and detecting both the fraud and associated ML activities.

ANNEX A : MONEY LAUNDERING INDICATORS

Transaction Pattern / Indicators Identified	Sectors Involved	Instruments / Products Involved	Type of Fraud*				
			AFF	BRF	HYIP	TD	IF
1. Use of accounts of shell companies	Banking	• Wire transfer • Cheque • Money order / bank draft • On-line banking services • Cash deposit / withdrawal • ATM withdrawal	X	X	X		
2. Use of stooge accounts			X			X	X
3. Multiple inward remittances from different senders			X	X	X	X	X
4. Incoming funds transferred to overseas company or personal accounts within a short period of time			X	X	X	X	X
5. Destination of transfer not commensurate with the customer profile			X	X	X	X	X
6. Structured remittances			X	X	X		
7. Temporary repository of funds			X	X	X	X	X
8. No apparent business related activities			X	X	X		X
9. Payment of "consultancy fees" or multiple intercompany loan transactions			X	X	X		
10. Lack of normal personal banking activities			X			X	X
11. Cash / ATM transaction			X			X	X
12. Small balance left in account			X	X	X	X	X
13. Incoming remittances re-directed to third party accounts, another remittance agent and offshore company	MSB	• Wire transfer • On-line services	X	X	X	X	X
14. Multiple remittances through different remittance agents without apparent reason			X	X	X	X	
15. Frequent inward or outward remittances from different senders to same beneficiary or sender			X	X	X	X	X
16. Cash withdrawals			X			X	X

Transaction Pattern / Indicators Identified	Sectors Involved	Instruments / Products Involved	Type of Fraud*				
			AFF	BRF	HYIP	TD	IF
17. Incorporation of shell companies	TCSP	• Company formation and secretarial services	X	X	X		
18. Use of trust account		• TSCP as nominee director or power of attorney of account • TCSP as registered or correspondence business address • TCSP acting as trustee or providing administration services		X	X		
19. Use of Internet / mobile payment system	Internet services provider	• Multiple registrations • Deposit taking and payment services • Sales / purchase of fictitious goods • Email or SMS message • On-line / mobile services	X			X	X
20. Use of bogus or fictitious websites	Securities	• Unlicensed investment products • Unlicensed entities in selling investment products		X	X		
21. Cross-border cash smuggling		• Cash courier	X	X	X	X	

AFF – Advanced Fee Fraud (lottery, heritage, Nigerian 419)
BRF – Boiler Room Fraud
HYIP – High Yield Investment Product / Investment Fraud (Ponzi Scheme)
TD – Telephone Deception
IF – Internet related Fraud (e-Commerce, e-Auction etc)

ANNEX B : QUESTIONNAIRE AND RESPONDING JURISDICTIONS

1. Australia
2. Cambodia
3. Canada
4. China
5. Cook Islands
6. Fiji
7. Hong Kong, China
8. Indonesia
9. Japan
10. Macao, China
11. Malaysia
12. Philippines
13. Russia
14. Chinese Taipei
15. Thailand
16. Vietnam

Note: Jurisdiction responded to the questionnaire but may not have answered each question.

ANNEX C : REFERENCES

Egmont Group of Financial Intelligence Units (2011) *'Enterprise-wide STR Sharing: Issues and Approaches'*.

AUSTRAC (2010) *'Typologies and Case Studies Report 2010'*.

International Mass-Marketing Fraud Working Group (2010) *'Mass-Marketing Fraud: A Threat Assessment'*.

FATF (2008) *'Report on Money Laundering and Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment Systems'*.

FATF (2010) *'Money Laundering using Trust and Company Service Providers'*.

FATF (2010) *'Report on Money Laundering and Terrorist Financing through New Payment Methods'*.

FATF (2010) '*Report on Money Laundering through Money Services Businesses'*.

FATF Working Group on Typologies (2010) *'Operational Issues: Recommendation 27&28'*.

FATF (2010) '*Global Money Laundering & Terrorist Financing Threat Assessment'*

FATF (2008) '*Money Laundering & Terrorist Financing Risk Assessment Strategies'*

ABBREVIATIONS AND ACRONYMS

APG - Asia/Pacific Group on Money Laundering

AFF – Advanced Fee Fraud

AML/CFT- Anti-Money Laundering / Combating the Financing of Terrorism

ATM – Automatic Teller Machine

AUSTRAC – Australian Transaction Reports and Analysis Centre

BCPIO – Bank Crime Prevention and Investigation Office

CAFC – Canada Anti-Fraud Centre

CARIN - Camden Assets Recovery Inter-Agency Network

CDD - Customer Due Diligence

CONG – Compliance Officers Network Group

CTR – Cash Transaction Report

DNFBPs - Designated Non-Financial Business and Professions

EDD – Enhanced Due Diligence

FATF- Financial Action task Force

FI – Financial Institution

FIU – Financial Intelligence Unit

FSRB – FATF Style Regional Body

GTA – Global Threat Assessment

KYC – Know Your Customer

LEA – Law Enforcement Agency

LSTF – Large Scale Transnational Fraud

MER – Mutual Evaluation Report

ML - Money Laundering

MLAT – Mutual Legal Assistance Treaty

MoU – Memorandum of Understanding

MSB – Money Service Business

NGO – Non Government Organisation

NPM – New Payment Method

STR - Suspicious Transaction Report

TCSP – Trust Company Service Provider

TF – Terrorist Financing

USD – United States Dollar

VAT – Value Added Tax

WGEI – Working Group on Evaluations and Interpretation

WGTYP Working Group on Typologies