Asia/Pacific Group on Money Laundering

ASIA/PACIFIC GROUP ON MONEY LAUNDERING

APG Yearly Typologies Report 2011

Methods and Trends of Money Laundering and Terrorism Financing

Adopted by APG Members at the 14th Annual Meeting

India, 22 July 2011

.

CONTENTS

INTRODUCTION

Background

The Asia/Pacific Group on Money Laundering (APG) produces regional typologies reports on money laundering (ML) and terrorist financing (TF) techniques in the Asia/Pacific region.

Typologies of ML and TF allow governments to understand the nature of existing and emerging ML and TF threats and design effective strategies to address those threats. Typologies studies also help APG members to implement effective strategies to investigate and prosecute ML and TF, as well as design and implement effective preventative measures.

The Yearly Typologies Report includes observations on ML and TF techniques and methods. These observations are intended to assist with identifying instances of suspicious financial activity in the real world. It is hoped that the case studies and 'red flag' indicators included in this report will assist the front-line financial institutions and non-financial businesses and professions (casinos, accountants, lawyers, real estate, etc) which are involved in implementing preventative measures such as customer due diligence and suspicious transaction monitoring.

Each year APG members and observers provide information on ML and TF cases, trends, research, regulatory action and international cooperation. The information collected from APG delegations not only provides the basis for a case study collection but also for selection and design of in-depth studies on particular typology topics. The information also supports the work of the network of typology experts involved in the APG Typologies Working Group.

When a series of money laundering or terrorist financing arrangements are conducted in a similar manner or using the same methods, they are generally classified as a typology.

Typologies in 2011-2012

Key typologies information is shared between practitioners during each annual APG Typologies Workshop. In October 2010 the annual workshop was successfully held in Bangladesh (see details below).

Information gleaned from typologies collection is shaping the ongoing work on in-depth projects within the APG Typologies Working Group. The APG has sought expressions for typology research projects for the upcoming year. Summary outcomes of that APG work will be included in next year's typologies report.

The case studies in this report are only a small slice of all the work going on across the Asia/Pacific region to detect and combat ML and TF. The report contains a selection of a number of illustrative cases from this year. It should be noted that some of the cases included took place in previous years but the summary information has only been released this year. Many cases cannot be shared publicly due to their sensitive nature or to ongoing legal processes. Thanks go out to Canada, UK, Hong Kong, Malaysia, the ADB and Australia for their contributions in leading the typologies projects for 2010/2011.

The Secretariat acknowledges and thanks Malaysia and India for their ongoing contributions as APG Typologies Working Group Co-Chair.

In 2011 the APG will host the joint FATF/APG Typologies Meeting of Experts. The APG looks ahead to a successful FATF/APG typologies workshop being staged in Busan, Korea in December 2011.

1. OVERVIEW OF THE 2010 APG TYPOLOGIES WORKSHOP

Introduction

1. Bangladesh hosted the 13th APG Typologies Workshop in Dhaka from 25 - 28 October 2010. It was attended by over 130 participants, representing 26 APG members and 3 international and regional organisations.

2. Bangladesh's high-level commitment to AML/CFT was reflected in remarks made by dignitaries at the Opening Ceremony of the 2010 Typologies. An address was given by Guest of Honour, the Honourable Prime Minister of the People's Republic of Bangladesh, Sheikh Hasina. Addresses were also given by Honourable Finance Minister, Mr A.M.A. Muhith, the Honourable Minister for Law, Justice and Parliamentary Affairs, Barrister Shafique Ahmed, and Guest Speaker, Bangladesh Bank Governor, Dr Atiur Rahman.

3. The 2010 workshop focused on:

- Money Laundering Associated with Large-Scale Transnational Frauds;
- Corruption and Money Laundering
- NPO and Terrorist Financing vulnerabilities
- Money Laundering and Human Trafficking/People Smuggling
- Vulnerabilities in Alternate Remittance

4. The workshop co-chairs were Mr Ziaul Hasan Siddiqui, Deputy Governor, Bangladesh Bank, and Mr Mohamed Sufyan Mohd Mokhtar, Head of Litigation, Companies Commission of Malaysia.

5. Section 1 of this report sets out a number of summary issues arising from the 2010 APG Typologies Workshop.

1.1 Money Laundering Associated with Large Scale Transnational Fraud

6. APG mutual evaluations, APG typologies collections and typologies workshops continue to highlight threats from ML associated with large-scale transnational frauds, in particular telemarketing/boiler-room/lottery frauds. Jurisdictions have conducted investigations of these frauds, and associated ML, and highlight the involvement of transnational organised crime groups in a highly profitable criminal activity that has a relatively low risk.

7. The APG Typologies Workshop initiated a preliminary discussion on a number of ML typologies associated with large-scale transnational frauds. It was noted that there was a lack of regional or global typologies on the issue of ML and telemarketing frauds, including boiler room, lottery fraud and heritage fraud.

8. The APG project has been led by Hong Kong,China and Malaysia. This report has been discussed in detail in this report at section 2. A copy of the report has also been made available on the APG website.

9. Presentations were delivered at the Typologies Workshop in Bangladesh by the Hong Kong,China, Indonesia, Canada , Chinese Taipei and the Philippines.

10. Chinese Taipei presented case studies of frauds that were masterminded by lawyers, accountants, and other professional persons. The scams were then used to defraud funds from investors in companies. The case study identifies that scams and frauds increasingly utilise the services of professional persons to prima facie legitimise criminal arrangements. The case

identified the benefits of international cooperation between agencies and FIUs in the prosecution and recovery of funds defrauded. Chinese Taipei identified that with the rise in incidence of transnational/global fraud, where victims are located in different jurisdictions, a greater emphasis on cooperation is needed to disrupt, prosecute, and recover funds and proceeds from, these criminal groups.

11. Indonesia observed that criminal groups operate ponzi scams by cold calling, phishing, using eBay, and by Nigerian letter scams, and that these scams and frauds generate large proceeds for criminal groups. A second case study shows eBay scams where goods purchased were not sent or are substantially different and inferior to that described. It was identified that education is key in the disruption of these activities as a low risk and high return solution. Indonesian authorities are seeing increasingly that the majority of investors in scams are foreign; the biggest issues facing authorities are international cooperation, gathering evidence where the frauds are multi-jurisdictional and recovering funds.

12. Canada noted that major fraud cases include corporate fraud, investment fraud, securities fraud, mass marketing frauds and credit fraud. Canadian FINTRAC disseminated more than 578 cases of suspected money laundering and terrorism finance to domestic law enforcement partners and international partners in 2009/2010. Of these cases disseminated 7% related to large scale fraud with the majority accounting for ponzi schemes and general fraud. Money Service Businesses (MSB) were involved in approximately 33% of all fraud related referrals. MSBs are commonly used in these frauds, and structuring deposits to under the reporting limited, concealing the beneficial ownership and attempting to circumvent identification requirements are the most common methods applied through the MSBs.

13. Australia noted the high profitability of phishing as a criminal activity and noted that in the last few years all of the major Australian banks have been phished. Alternate websites that are usually set up by criminal syndicates are located outside of Australia and in some cases the funds are transferred to local accounts prior to the funds being wired, or telegraphically transferred offshore.

14. Recent cases in Australia identify criminal syndicates from Malaysia and Russia that recruit school students as go-betweens and utilise their accounts to receive funds stolen from "hacked" bank accounts. These funds are then transferred to a person recruited by the syndicates to receive the funds, minus a commission, who then wire the money to the syndicates overseas. [1]

15. A typical red flag may be a dramatic increase in flow-through activity on bank accounts, less a small commission, where the accounts are held by students, unemployed, or previously silent bank accounts.

16. Laundering of proceeds from ponzi, cold-calling and phishing scams are a lucrative, relatively low risk, global criminal activity. Their transnational 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 enhances ML vulnerabilities. Increased national and international collaboration is required to combat these offences.

17. The above case studies highlight the issue that criminal networks and syndicates are increasingly global and are using professionals to identify opportunities, set up, manage and perpetrate the frauds. Fraud is traditionally seen by criminal networks as being low risk with high return, in addition law enforcement agencies (LEAs) can initially be reserved about the inherent long-term investigations, the apparent unlikelihood of a conviction, and the difficulty gaining return of any proceeds of the offence. However, in recent years increasing

[1] http://www.smh.com.au/news/technology/gangs-using-aussie-kids-to-steal-millions/2006/06/03/1148956585189.html

cooperation between law enforcement agencies, FIU and governments, through mutual assistance and cooperation processes, greatly increases the likelihood of a successful investigation, extradition and prosecution of the offenders, and recovery of the proceeds of crime. Although, in some cases the failure to rapidly exchange information, and the lack of coordinated multi-jurisdictional action to combat and identify the syndicates involved, enhances ML vulnerabilities. Further national and international collaboration is required to combat these offences.

1.2 Corruption and Money Laundering

18. Corruption has been identified as a continuing problem in mutual evaluations and represents a significant and ongoing problem which generates large amounts of wealth to corrupt politicians and business persons. Corruption equally represents a large loss of funds diverted from infrastructure, health, education, and other initiatives designed to increase quality of life of the public. Generally those most needy suffer as a result of corruption of public office.

19. Common types of corruption involving 'politically exposed persons' (PEPs), has been found to be corruption by politicians when selling public assets, tender and contract processes, related employment and skimming funds from public monies.

20. The Indonesian Corruption Eradication Commission (KPK) gave a presentation on AML tools to fight corruption. It was noted that monitoring of PEPs can partly be achieved with the use of asset registries and gratuity reports. The AML tools presented assist in identifying assets held by a PEP and can also assist in investigations where assets are accumulated during the period of the PEP's office and where the accumulation of those assets is outside of known sources of income.

21. It was discussed that the wealth reports and gratuity reports can form part of a pre-investigation which, together with further information from LEAs and other sources, can lead to formal investigations and prosecutions.

22. Bangladesh presented on corruption investigations and stressed the transnational nature of schemes to launder funds associated with corruption actions. Investigations to address profits from corruption will require mutual legal assistance (MLA) between jurisdictions where assets and funds have been transferred. The presentation discussed both the challenges in making and responding to MLA requests related to investigating corruption and tracing and recovering stolen assets.

23. Some of the challenges faced while responding to MLA requests include:

- The request for search and seizure of material from premises or location where evidence may be located
- Statements from witnesses or the accused person/s
- Proposals for joint investigations, and
- Requests for freezing of accounts and assets

24. Bangladesh also noted that the challenges faced when making MLA requests include:

- Absence of dual criminality
- Issues of political persecution
- Information relating to bank accounts and transactions
- Limited availability of material from offshore jurisdictions, and

- Delays of requests

25. Challenges relating to the receiving of information for prosecution and trials include issues relating to:

    - Value of evidence received through MLA
    - Production of foreign witnesses for court

26. The World Bank noted that jurisdictions need to adopt a policy of anti-corruption at high political levels. Anti-corruption policies need to be public, need to translate into skills and resources for the agencies mandated to investigate and combat anti-corruption, and require that there is on-going monitoring and feedback.

27. The World Bank also noted the general insufficient use of AML legal tools, the general lack of coordination between agencies mandated to investigate corruption and agencies and those mandated to investigate ML (if they are separate), and the FIU. Further, where AML tools utilised there may be insufficient training on their use.

28. To successfully combat profit driven crime, and particularly corruption, jurisdictions need develop a culture of 'following the money' amongst law enforcement agencies. This is not just for corruption matters, but for all predicate offence that generates significant proceeds of crime. The use of both formal and informal communication channels to support international cooperation is vital in the investigation of corruption and associated ML.

29. The United States (Department of Justice) presented on the use of non-conviction-based asset forfeiture in recovering proceeds of corruption. It was identified that in the first instance jurisdictions require a legal framework in place to deny financial safe haven, that they prosecute corruption offences and associated ML, that there is adequate proceeds of crime legislation in place that allows for the identification, restraint and forfeiture of assets acquired illicitly, and laws that provide for international cooperation.

30. The United States' forfeiture systems allows for the forfeiture of property that is proceeds of crime, used in the facilitation of a crime, substitute property in criminal matters only and contraband.

31. The US pursues both judicial and non judicial forfeiture. Judicial forfeiture can either be criminal or civil based. In civil, or non-conviction-based forfeiture, the suit is filed by the US against the thing (assets) as the wrongdoer, a criminal charge is not required and the asset is forfeited subject to any innocent ownership. If any defence of innocent ownership by contemporaneous owners is used they must show that they had no knowledge of the illegal conduct, or there were reasonable steps to terminate the illegal use. After-acquiring owners must show that it was a bona fide purchase and that they had no knowledge or reason to believe the asset was subject to forfeiture.

32. There are a number of significant advantages in using non-conviction-based forfeiture tools. The regime in the US means that criminal convictions are not necessary, and assets can be forfeited from deceased criminals or fugitives and foreign-based property can be targeted. It is also important in cases where foreign officials can not be prosecuted or where there are issues of immunity.

33. The Financial Action Task Force (FATF) has prepared a typologies paper on 'grand corruption' and ML which is discussed further in section 2 of this paper.

1.3 Non-profit organisations (NPOs) and Terrorist Financing Vulnerabilities

34. The APG's work with members and the non-profit organisation (NPO) sector continues to highlight the vital and valuable role played by the NPOs of every APG member. The vast majority of NPOs conduct legitimate work for the good of society and these NPOs that enjoy the trust of the public should not have their confidence undermined by NPOs operating outside of the law. Cases of NPO abuse represent a very small percentage of all NPO activity. However, APG mutual evaluations, APG typology collections and workshops continue to highlight the vulnerability of NPOs to terror financing.

35. A breakout session was held at the APG Typologies Workshop on Non-Profit Organisation Vulnerabilities for Terrorism Finance and Money Laundering which was chaired by Canada and the UK. Pakistan, UN Counter Terrorism Executive Directorate (CTED) and the US Dept. of Treasury, Malaysia Companies Commission, Sri Lanka and New Zealand made presentations. Topics that were discussed identified the importance of the NPO and charities sector, their contribution to global GDP, FATF SR VIII and several case studies where charities have allegedly been used to raise funds for terrorist activities. Given the general weaknesses in the regulation of NPOs, and the lack of up to date typology report on the NPO vulnerabilities the Canadian Charities Commission has led a project on the vulnerabilities of the NPO sector. This report is discussed in detail at section 2 of this report.

36. During the typologies workshop presentations were made by Pakistan, CTED, Malaysia and the United States. It is agreed that charities while they represent a risky sector if left unregulated, they are required to fill the gap where governments are unable to, or can not, extend their reach. Globally, it is estimated that charities contribute around US$2,800,000,000,000 annually.

37. Pakistan gave an overview of the charity sector and identified that the sector is vulnerable to both internal and external fraud and fund-raising for terrorist activities. The presentation highlighted some of the common internal and external frauds including financial manipulation and accounting fraud, employment fraud, theft of trustee, donor or employee information, procurement frauds, bogus websites, impersonation of street collectors and skimming of collection boxes. Pakistan identified that when funds are misappropriated they could be used for terrorist activities, political destabilisation and communal disturbances.

38. Pakistan estimates that the size of the sector as at 2002 held approximately 45,000 active NPOs. Active NPOs are registered on a national database. NPOs operate under a legal framework of 7 Acts and Ordinances which has been identified by Pakistan as an issue that needs to be addressed. Pakistan plans to implement a single law regulating NPOs, conducting a training program for NPOs and authenticating data received from NPOs.

39. CTED identified that is was important for society to have a high level of trust in the NPO sector. NPOs operate in areas of conflict and areas where there is very little infrastructure. In these cases there may be limited oversight of the sector. It was highlighted that charitable structures can in some cases be used to conceal the beneficial ownership of the funds and the charity can be used to move funds using its established networks while avoiding any undue attention from regulators and law enforcement.

40. Charities raise approximately US$2.8 trillion annually. CTED found that there was very little guidance of NPOs beyond SRVIII, and that given the importance of NPOs and charities it was important to strike a balance between transparency and privacy, accountability and proportionality, and enforcement and self regulation.

41. The Companies Commission Malaysia (CCM) gave a presentation regarding the NPO sector in Malaysia. In Malaysia, NPOs may be formed either as a charitable corporation or as

societies/associations. Charitable corporations are regulated by the CCM, and societies/associations are regulated by the Registrar of Societies (ROS).

42. The CCM is the responsible agency for the registration, supervision and controlling the activities of charitable foundations that are registered as companies limited by guarantee. As at September 2010 there were 1510 companies limited by guarantee, which are also classified as NPOs, of which 924 were Foundations. The CCM conducts a Corporate Directors Training Program and Annual Dialogue sessions to promote transparency, accountability and integrity of NPOs.

43. Societies/associations are registered, monitored and supervised, and their records maintained by the ROS. The categories of NPOs under the supervision of ROS include cultural, educational, employment, political, religious, sports, welfare and social. As at October 2010 there were 61,277 NPOs registered with ROS.

44. To protect NPOs from abuse the Companies Commission of Malaysia noted that it will sign Memorandum of Understandings (MoU) with international organisations responsible for regulation and oversight or corporations. A sub committee of NPOs is also conducting and organising outreach, awareness and education programs on NPO abuse. It was noted that close cooperation between the ROS and the CCM ensures a consistent and current exchange of information and intelligence. A risk based approach to supervision of NPOs in Malaysia is the preferred approach and the which is being finalised by the sub committee on NPOs.

45. The US Department of Treasury identified that there were approximately 1.4 million NPOs registered with the Internal Revenue Service (IRS) and a further 350,000 charitable religious organisations and small charities that are not required to register with the IRS. It is estimated that they raise a total of US$300 billion annually in the US. There are currently no AML record keeping or reporting obligations required of NPOs in the US and oversight consists mainly to protect against consumer and tax frauds.

46. The presentation also focused on a “continuum of acceptance” by recipients that identifies that recipients may initially be unsupportive of the violent extremism, but may become captive to an organisation where they are the sole source of their aid. The US currently has a Voluntary Best Practice for US charities that emphasizes transparency by addressing governance, accountability, public disclosure and vetting recipients.

47. The NPO sector is globally a large sector that raises billions of dollars for distribution to the world’s most needy. In some cases the distribution of these funds will correlate to a conflict area, or an area that may be considered high risk for terrorist groups. Research and fund raising statistics confirm that generally the richest jurisdictions are the most supportive of charitable giving. Given that terrorist incidents cost very little to perpetrate, usually a few thousand dollars, in the case of the Bali 2002 bombings which caused 202 casualties the cost to perpetrate was only US$20,000, a high level of attention should be given to the regulation of charities.

48. The APG Typologies Working Group has conducted a project on NPO sector vulnerabilities. The project report is discussed in more detail in section 2 of this report. Broadly the findings of that paper identifies that abuse of the NPO sector represents a very small percentage of all NPOs, the damage to the reputation of the industry following abuse is high and a range of measures still need to be taken in the Asia/Pacific region to improve accountability and transparency and to work with the NPO sector to protect them from abuse and misuse for terrorist financing.

1.4 Human Trafficking, Human Smuggling and Money Laundering

49. The FATF and Group of International Finance Centre Supervisors have co-led a project on ML and human trafficking/people smuggling. The findings of the report are discussed at Section two of this paper.

50. Australia, Bangladesh, Sri Lanka and the Asian Development Bank provided presentations during the 2010 APG Typologies Workshop on issues relating to ML and human trafficking and smuggling. The presentations covered the legal frameworks in those jurisdictions, the differences between trafficking and smuggling and the harm that the offence causes.

51. Human trafficking and human/migrant smuggling have been differentiated as they relate to different crimes. The UN Trafficking Protocol has defined human trafficking as the recruitment, transportation, transfer, harbouring or receipt of persons, by means of a threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power, or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation.

52. Human/migrant smuggling has been identified as the procurement, in order to obtain, directly or indirectly, a financial or other material benefit, of the illegal entry of a person into a jurisdiction of which the person is not a national or a permanent resident.

53. An overview of human trafficking and human smuggling was provided by the APG. The discussion identified that both human trafficking and human smuggling is recognised as a global challenge of comparable proportions to narcotics and arms trafficking.

54. These crimes have a wide impact whether as a point of origin, transit or destination. The profits to human trafficking and smuggling syndicates are very large, thought to be one of the most lucrative, and also represent a money laundering risk to many jurisdictions.

55. Strong AML systems can help detect trafficking in persons and human/migrant smuggling activities by triggering financial and other institutions to report suspicious financial activities. Additionally, a robust AML framework will enable jurisdictions to restrain and confiscate the proceeds of human/migrant smuggling and trafficking in persons, prevent reinvestment in criminal activity and reduce the financial incentive for individuals to engage in these crimes in the future.

56. In the Asia/Pacific region human trafficking and human/migrant smuggling has been identified as a large problem. Common source jurisdictions identified in the region include Afghanistan, Bangladesh, Indonesia, Myanmar, Philippines and Sri Lanka. Common destinations in the Asia/Pacific have been identified as US, Canada, New Zealand, Australia, China and Pacific Islands.

57. Sri Lanka identifies that human trafficking can be either partly deceptive where the victim may be aware they will be employed in given activity but may not be aware of the condition, or fully deceptive where the victim is lured by promises of employment, however they are deceived as to the true intention of the traffickers. Recruitment can also be forced.

58. Sri Lanka identifies that it is a point of origin and that the transportation of the victims will occur illegally or legally involving land, air and sea travel. The person being trafficked will most often be accompanied by a minder who will take control of their travel documents.

59. Sri Lanka identified that it is highly vulnerable to trafficking in human beings partly due to the increasing demand for sex tourism in many parts of the Asia Pacific region, which leads to an increase in the number of women and children trafficked into prostitution. It was

also discussed that many workers were enslaved in forced labour to work in low skilled areas in developing jurisdictions.

60. Bangladesh noted that smuggling of migrants occurs for a number of reasons including lack of economic opportunity, better lifestyles, low risk and profitability. The smuggling of migrants is facilitated by means of all modes of air, land and sea transport.

61. Sri Lanka identified a number of push and pull factors that support the supply and demand of trafficking. Push factors include low employment opportunities and poverty, natural disasters, ease of border crossings and dowry systems. Pull factors can include the demand of prostitution, profitability, organ trading and tourism. Human trafficking for prostitution accounts for approximately 94% of all persons trafficked from Sri Lanka.

62. Australia has conducted a scoping exercise on human trafficking and ML on behalf of the APG. The scoping paper included sending a questionnaire to all APG members seeking their experiences regarding human trafficking and ML. This paper is discussed in Section 2.

63. The FATF and Group of International Finance Centre Supervisors have undertaken a global typologies study on this topic, which is discussed at Section 2.

1.5 Raising Awareness of Cash Couriers

64. Mutual evaluations across the region continue to identify that jurisdictions are having trouble implementing the requirements of SRIX. Some of the common deficiencies noted include the lack of coverage of Bearer Negotiable Instruments (BNI) and cash/currency, both incoming and outgoing, the inability to adequately cover all points of entry and exit to a jurisdiction, especially jurisdictions that have multiple land and sea crossings, post and cargo not covered or inadequately covered, and inadequate coordination among national agencies, including the FIU.

65. Delegates gave presentations on cash couriers, and identified the attractiveness of using cash couriers to move funds for criminal activities including ML and TF. It was identified that syndicates continued to use cash couriers due to the ease of movement, the inability of LEAs to trace cash movements and the difficulties to regulate the sector, including the deficiencies already noted.

66. UN CTED noted that in terms of cash and BNI couriers, research identified that inbound passengers are subject to more intense scrutiny by Customs, declarations were received by Customs and Immigration, however there was no follow up or further questioning of the passengers, detections were made, however due to inadequate seizure laws, the funds were returned, and that there appeared inadequate interagency coordination between Customs and other national LEAs. Customs agencies were also generally perceived to have a lack of capacity in their analysis units and passenger targeting criteria, were not aware of UN watch lists or did not have access to the watch lists, did not have access, or timely access to, law enforcement criminal databases, and did not have access to, or not connected to INTERPOL's Stolen and Lost travel document database.

67. UN CTED will continue to hold workshops in the Asia/Pacific region to raise awareness and promoting international best practices on cash couriers and the implementation of FATF SRIX.

1.6 Current and Emerging Trends

68. Australia presented on the current and emerging trends that they have identified. It was identified that criminals are adept at exploiting vulnerabilities in financial products and

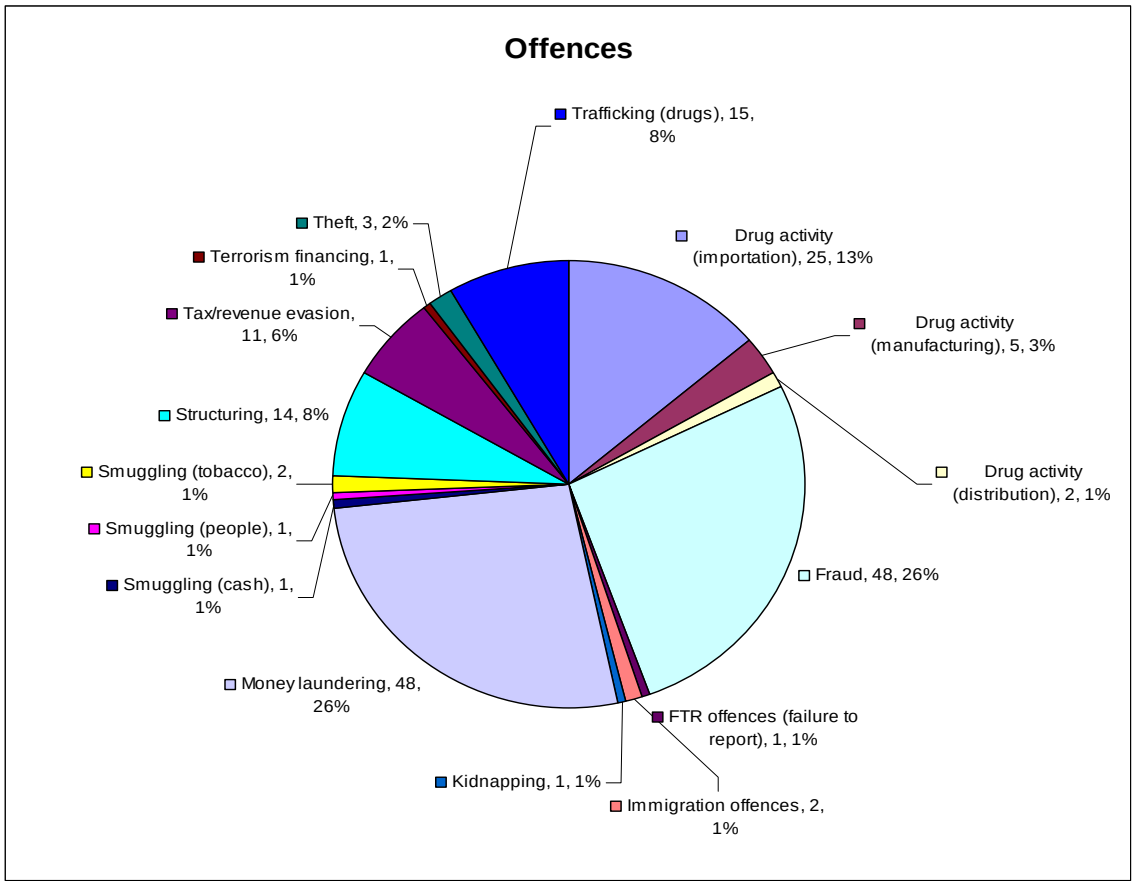
sectors. It was also discussed that they misused legitimate financial systems to conduct crimes including card skimming and online scams.

69. Trade based money laundering has been identified as both a current and emerging threat. This methodology is utilised by criminal syndicates to move large amounts of money across international borders and then integrate the money into the financial system. Common methods utilised by criminal groups include under and over invoicing, over and under shipment of goods, multiple invoicing of goods, falsely describing goods and services and transfer pricing.

70. Bulk cash smuggling was identified as an ongoing concern with recent seizures occurring across the globe. Cash is generally smuggled in accompanied luggage, or on the person, however there have been cases where cash has been concealed internally. The post and cargo streams are also very vulnerable to bulk cash smuggling largely due to the amount of cargo, and inability to physically check all containerised cargo and mail.

71. New payment methods that have been developed and identified as emerging threats to LEAs include the prepaid debit and credit cards and mobile payment services. These trends and methods allow for a more anonymous method of transferring funds.

Australia's crime trend data was presented with data between the period 2007 to 2010 that identifies a spectrum of offences where ML and TF occurs. Generally narcotic and fraud activities represent 51%, and ML represents 26%.



72. The most prevalent designated services used to launder funds were deposit taking services (39%), remittance services (14%) and fund transfers (12%). These services are conducted predominantly via the banking sector (45%), the remittance sector (18%), professional services including accountants and solicitors (13%) and the gambling sector (9%).

1.7 Capital Markets: AML CTF Safeguards

73. The US Department of Treasury gave a presentation on the US experience on Capital Market AML/CFT safeguards. US AML obligations require all securities broker dealers, futures commission's merchants and mutual funds to collect and verify customer identification, maintain records, monitor accounts for suspicious activity and file Suspicious Activity Reports (SARs) with FinCEN.

74. Delegates noted that the FinCEN administers the AML regulations but has delegated industry oversight to government regulators. The Securities Exchange Commission (SEC) and the Commodity Futures Trading Commission (CFTF) are the regulatory agencies that oversee the security and future's industry, however the SEC and CFTC have delegated this to private sector self regulatory organisations.

75. Since 2003 SARs submitted to FinCEN by securities dealers and brokers have increased from about 5,000 per year to around 18,000 per year in 2009. In 2009 SARs relating to bribery and check frauds had increased significantly. Overall the majority (by crime type) of SARs are related to money laundering and structuring (15.83%).

76. The finding of the 2009 FATF Typology Report Money Laundering and Terrorism Financing in the Securities Industry was discussed citing that customers and activities that required enhanced due diligence included offshore trusts, NPOs, significant cross border activity, internet and online accounts and omnibus and private banking accounts.

77. An omnibus account was defined as an account held with an offshore agent for foreign market transactions on behalf of all domestic firm customers. The offshore firm holding the omnibus account usually does not hold information about the individual clients or their individual accounts.

2. PROJECTS UNDERTAKEN BY APG 2010 AND 2011

2.1 APG Typology Projects

78. Several typology projects have been undertaken by APG members for 2010. These typologies were identified by members as relevant topics with a significant interest and high risk of ML and TF. The executive summaries of the papers are incorporated in the remainder of section 2 of this Typologies Paper and copies of the complete projects can be located on the Typologies Section of the APG website (www.apgml.org). It should be recognised that significant effort has been made by the projects teams to complete and participate in these projects.

2.1.1 NPO Sector Vulnerabilities

79. Despite continued efforts to counter the financing of terrorism (CFT), non-profit organizations (NPOs) around the world continue to be abused by terrorists. This typologies report aims to assist members of the APG with the implementation and enforcement of FATF Special Recommendation VIII, which calls on members to review the adequacy of laws and regulations relating to NPOs as part of their larger CFT strategy.

80. Chapter 1, *The NPO "Sector"*, briefly explores the growing global role of NPOs and the need to protect them. The FATF's functional definition of an 'NPO' is also narrowed to limit the scope of NPOs in this report to those that are at risk of terrorist abuse.

81. Chapter 2, *Scope of the Problem*, discusses the prevalence of terrorist abuse of NPOs. While many terrorist groups have abused NPOs to finance their operations, NPOs have also

been abused for other purposes such as weapons smuggling or recruitment. The term 'terrorist resourcing' provides a more comprehensive characterization of the abuse than the term 'terrorist financing'. In addition, a distinction must be made between 'complicit' or 'exploited' NPOs. Chapter 2 explores the reasons behind the NPO sector's vulnerabilities to terrorist abuse.

82. Chapter 3, *Lack of Effective Regulation*, identifies gaps in regulation of NPOs as the greatest vulnerability to terrorist abuse to the sector. The absence of effective NPO regulatory systems in many jurisdictions leaves them largely unable to deter, detect, and disrupt related terrorist activity within the sector, including TF. There are multiple challenges in establishing effective regulatory mechanisms, particularly in developing jurisdictions.

83. Chapter 4, *Step 1- Determining the Risks*, emphasizes that, in accordance with Special Recommendation VIII, the first step in enhancing governmental regulation is the collection of information regarding each jurisdiction's NPO sector. Understanding the sector is imperative to identify the risks to NPOs, and to design or modify regulatory mechanisms. This step forms part of a risk-based approach to regulation, recommended because it provides for a targeted and proportionate response. Given that only some APG members have conducted detailed reviews of their NPO sectors and fewer still have performed risk assessments, a comprehensive study of specific typologies, vulnerabilities, risk indicators, and regulatory systems applicable across all jurisdictions is not possible at this time.

84. Chapter 5, *Responding to the Risks by Enhancing Regulation*, provides a structural framework to assist APG members with the design and planning stages necessary to improve regulation. Although regulation may differ substantially between jurisdictions, the framework is sufficiently broad to account for these differences. Specifically, the framework identifies eight strategic gaps in NPO sector regulation, and eight corresponding phases of action to address these gaps, beginning with assessments of the NPO sector itself and current laws and regulations. The eight strategic gaps are identified as The Information Gap, The Effectiveness Gap, The Framework Gap, The Legal Gap, The Structural Gap, The Resource Gap, The Cooperation Gap and The Outreach Gap.

85. Chapter 6, *Caveats for Regulation*, presents caveats regarding NPO regulatory mechanisms to be kept in mind by governments. For example, regulation should not be pursued purely for CFT purposes. Use of CFT-focused regulatory measures to constrain the sector would be both counter-productive and would risk alienating NPOs. Further, measures should be proportional to the risk and flexible enough to accommodate particular types of NPOs or situations. The chapter also explores how NPO self-regulation is complementary to government regulation and should be encouraged by governments.

86. Chapter 7, *Risk Indicators and Case Studies*, recommends that jurisdictions develop their own set of risk indicators specific to their NPO sectors. Case studies of terrorist abuse within the NPO sector and corresponding risk indicators are provided for APG members as a guide for the development of risk indicators relevant to their own NPO sectors. This is followed by a more elaborate sample of a Canadian risk indicator.

87. Lastly, Chapter 8, *Policy Implications*, presents policy implications stemming from the recommended adoption of a risk-based governmental regulatory system for NPOs. They include:

- the need for a detailed review of each member's NPO sector and existing laws and regulations, and subsequent detailed risk assessment of vulnerabilities
- the need to include the NPO sector in all stages of regulation and CFT planning that may affect them
- striking a balance between seemingly opposing aims, such as transparency and privacy, accountability and proportionality, and enforcement and self-regulation

- the need to continue to share best practices between governments, international organizations, NPOs, and other stakeholders as a means of regularly improving the regulatory system

2.1.2 Large-Scale Transnational Fraud and Money Laundering

88. In recent years large-scale transnational fraud 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. While these billions of dollars are laundered using a variety of vehicles it is also widely accepted that at some stage in the laundering cycle, the majority of these funds pass through the banking system.

89. The case studies highlighted in the report illustrate the risks 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 money laundering feature associated with large-scale fraud is that of the difficulty in differentiating money laundering from the predicate offence; unlike money laundering related to drug trafficking, for example, the money laundering in large-scale fraud commences simultaneously with the commission of the predicate offence; they work hand in hand.

90. While much is known about the various guises fraud takes as a predicate offence and of the initial placement and layering of the proceeds, due to limited intelligence and feedback the project team found few opportunities to examine how and where these funds are integrated and accessed. Suspicious transaction reporting in relation to fraud is relatively high but quality and outcome is questionable. While most jurisdictions reported having the structure and apparatus that is required to meet international AML/CFT standards, the 'effectiveness' of many regimes in tackling money laundering associated with large-scale transnational fraud is questionable.

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

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

93. Laundering of proceeds from boiler room/heritage/lottery frauds is a lucrative, relatively low risk, global criminal activity. The transnational nature of fraud 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.

94. 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.

95. A number of jurisdictions, including Hong Kong,China 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 to adapt money flows in response to preventative measures.

2.1.3 Carbon Trading vulnerabilities

96. The ADB, on behalf of the APG Typologies Working Group, prepared a paper examining possible risks associated with Carbon Trading of money laundering and terrorism finance. The purpose of the study was to collect empirical data to determine the possible size and nature of the risks to determine whether APG members need to undertake further work to particularly focus on those risks in the Carbon Emissions Trading (CET) markets as a formal typology study, and secondly to raise awareness of possible ML/TF countermeasure strategies, based on current developments including the European Commission proposals, that could be introduced by APG members which find themselves to be at risk.

97. CET is a market based approach used to control the amount of carbon dioxide produced by providing economic incentives to achieve reductions in such emissions at the lowest possible cost to society. There are essentially two types of emission trading; (a) cap and trade, also known as allowance markets, in which participants are obliged to comply with a mandatory emission target by trading (i.e. buying and selling) carbon emission permits, and (b) baseline and credits, also known as project-based transactions, in which the participants are required to reduce emissions to a designated baseline and obtain carbon credits to offset any surplus.

98. The European Union Emission Trading Scheme (EUETS) has remained the engine of the global carbon market. According to Europol the EUETS has also become a magnet for tax fraud on a grand scale, costing government coffers around €5 billion in 2009. After five EU members, United Kingdom, France, Netherland, Denmark and Spain closed their tax loopholes, 90 percent of the trading volume disappeared on their exchanges. Europol estimated based on the incident that in these European jurisdictions up to 90 percent of the whole market volume was caused by fraudulent activity.

99. In the context of cap and trade, increasing numbers of possible ML/TF related fraud cases have been observed in the EUETS. Computer fraud, manipulation of inadequate regulations and exploitation of legal loopholes are the common types of fraudulent activities that could be related to ML/TF in the European markets.

100. Value Added Tax (VAT) fraud is committed by firms that buy carbon credits from VAT free sources in one jurisdiction and then sell them on to businesses in another jurisdiction at a VAT inclusive price, while pocketing that difference. Such fraud surfaced in the EUETS transactions in 2009 when UK authorities arrested seven people in connection with a £38 million VAT fraud involving the trading of carbon credits. Spanish authorities arrested nine people on charges of avoiding €50 million in tax linked to trading in carbon credits. Belgium authorities arrested four people for failing to pay VAT worth €3 million on a series of carbon credit transaction. French authorities arrested four people suspected of engaging in €156 million carbon carousal fraud.

101. The report concludes that CET has inherent risks of both potential and ongoing ML/TF associated activities in light of inadequate regulations and technological difficulties in law enforcement.

2.4 FATF Typology Projects

102. Typology projects led by the FATF focussed on three areas associated with money laundering and terrorism financing, human trafficking and human smuggling, kidnap and piracy for ransom and laundering the proceeds of corruption. Executive summaries have been

included in the Typologies Report as an overview of the Typologies Projects, and the full papers can be found on the FATF website (www.fatf-gafi.org).

2.4.1 Human Trafficking and Human Smuggling – FATF & Group of International Finance Centre Supervisors

103. There is growing evidence that criminals are turning to trafficking in human beings (THB) and the smuggling of migrants (SOM) to a greater extent as these crimes are seen as highly profitable. The money laundering risks arising from both activities are covered in this report because the distinction between them is not always obvious to the authorities and there can be a link between the two. The objectives of this typology report are to assess the scale of the problem, to identify different trends in THB and SOM, to identify the trends in money laundering (ML) from case studies, to inform law enforcement agencies on the ML aspects, to identify red flag indicators to assist financial institutions in detecting ML and making STRs, and to increase the possibility of identifying and confiscating the proceeds from human trafficking or the SOM.

104. From the definitions of the two offences the conclusion can be drawn that the main difference is in the exploitation aspect of trafficking that is absent from the smuggling operation. However, making a profit is the main goal of both traffickers and smugglers. Similarities can also be found in their organization, ranging from small-scale to large scale businesses. Regions of origin of trafficked people most reported are the Commonwealth of Independent States (former Soviet Republics), Central and South-Eastern Europe, Western Africa and South East Asia. The main destination jurisdictions are located in Western Europe, North America and Western Asia. Trafficked victims transit by Western, Central and South-Eastern Europe, and to a lesser extent South-East Asia, Central America and Western Africa.

105. Assessing the scale of the problem is a major challenge, specifically concerning the SOM where statistics are scarce and incomplete. Concerning THB, it is estimated that about 2.45 million persons are currently being exploited in the world. Total illicit profits from human trafficking are estimated to be around USD 32 billion annually.

106. A questionnaire was circulated and completed by a number of FATF members and observers. This showed (see Chapter II) that competent authorities in investigating ML of THB and SOM are usually the same as the authorities investigating the predicate offences, meaning mainly law enforcement agencies. The FIUs are also often competent when tackling the ML of these offences. Consequently, the main sources of information for detecting ML arising from these offences are law enforcement investigations and suspicious transaction reports. The questionnaires also identified several challenges, in particular in limited international cooperation and the difficulty to detect funds and gather evidence.

107. A number of THB and SOM cases are presented in Chapter II and Annex A which reinforce the trends identified from the questionnaire and the analysis of the relevant literature. Indicators for financial institutions and law enforcement agencies that arise from these case studies are included in the list of red flag indicators in the key findings and in Annex B.

108. From the questionnaires and case studies the main trends detected for laundering, that are similar to those of other offences, include the use of cash-based trades, of money service businesses, of hawala systems, of cash couriers, of front companies, commingling of funds, aliases, straw men, and false documents. Investments in real estate, in cars or in supporting a lifestyle are also most frequently reported. Some specific new trends in trafficking arose from the analysis for example the use of bank accounts to gain access to credit.

109. The main findings arising from the questionnaire, the case studies, the analysis of the literature and the workshop in Cape Town in November, 2010 can be summarized as follows:

- there is a lack of adequate information about the number of persons being trafficked and smuggled and there is even less information about the income generated by this activity and how it is laundered;
- there is a need to change THB and SOM from "low risk/high reward" to "high risk/low reward, crimes;
- there are region specific trends and distinctions can be drawn among jurisdictions of origin, transit and destination;
- the ML techniques are similar to those found with other crimes;
- criminals involved in THB and SOM are particularly engaged in the handling of and movement of cash;
- there are links between THB and SOM and other forms of organised crime;
- arresting ML from THB and SOM calls for effective cooperation between all relevant agencies.

110. A number of issues also have been identified that require further consideration, including the need for more data, the need for more focus on ML rather than the predicate crime itself, and the need for more cooperation between all relevant agencies.

2.4.2 Kidnap and Piracy for Ransom - FATF

111. In June 2010, FATF's Working Group on Typologies (WGTYP) agreed to examine and produce a survey on money flows connected with organized Piracy for Ransom (PFR) and Kidnapping for Ransom (KFR). This study was intended to provide an overview of the current problem, and as far as possible, an analysis of money flows, as well as provide issues for consideration on the possible role of the FATF in combating PFR and KFR. Due to the unique nature of this illicit activity and the challenges associated with finding case data, it was foreseen that this would be a challenging project, particularly in terms of identifying and tracing money flows stemming from these illicit activities.

112. The attached report is a successful outcome of this preliminary study of PFR and KFR and is based on a wide-ranging source of data from both open and closed sources. It clearly describes the current challenges related to identifying and pursuing this illicit activity, and in doing so provides the first comprehensive picture of PFR and KFR, attempts to outline the financial implications of these activities, and outlines the work still to be done.

113. PFR and KFR are considered separate categories of serious criminal offences and as such, they are addressed independently in the study: the PFR portion examines the financial implications of piracy as a major proceeds-generating offence, while the KFR section focuses specifically on kidnapping as a means of financing terrorism and as a means to collect funds and support operations of terrorist groups. The PFR report provides a clear overview of the patterns of illicit financial activity associated with PFR, its lucrative nature, and payments in physical cash. The KFR study similarly provides unique insight into the significance of revenue generated from KFR for a number of terrorist groups and criminal organizations and the role of the formal financial sector.

114. In addition to raising awareness of these important issues, the report also highlights some of the challenges associated with identifying, investigating, and tracing illicit flows associated with PFR and KFR. For example, in the case of PFR, once a ransom is paid, it is difficult to determine how the funds are laundered largely because all ransom payments are in the form of physical cash and the money trail generally grows cold after the ransom is delivered. Similarly, although the formal financial system is often the starting point for kidnapping for ransom payments, the physical cash distribution makes it difficult to track the on-going financial flows related to the cases included in this report. Therefore, although the predicate crimes of PFR and KFR are clearly described through cases, the illicit financial flows including the distribution and use of funds are not often clear.

115. Despite these challenges, the study provides unique insight into PFR and KFR and for the first time provides a comprehensive overview of these activities based largely on law enforcement case studies. While there will continue to be challenges associated with identifying and addressing the money laundering and terrorist financing vulnerabilities of PFR and KFR, this report will serve as an important starting point for a meaningful dialogue between interested stakeholders from the public and private sectors.

2.4.3 Laundering the Proceeds of Corruption - FATF

116. This typology originates from a practitioners' understanding that the fight against corruption is inextricably intertwined with that against money laundering; that the stolen assets of a corrupt public official are useless unless they are transported, disguised and reintegrated into the global financial network in a manner that does not raise suspicion. In some ways, a public official (known as a politically exposed person, or 'PEP') who gather vast sums of money through corrupt means is far more vulnerable than some other criminals.

117. While there may be no internationally recognised legal definition of corruption, it is most commonly functionally defined as the use of public office for private gain. The UN, OECD, and the Council of Europe Conventions establish the offences for a range of corrupt behaviour. The conventions define international standards on the criminalisation of corruption by prescribing specific offences, rather than through a generic definition or offense of corruption. This can range from petty or systemic corruption, in which public officials or employees receive money to perform (or refrain from performing) official acts, to 'grand corruption,' in which those at the political, decision-making levels of government use their office to enrich themselves, their families and their associates.

118. Because of time and resource limitations involved in this project, the project team restricted itself to an analysis of grand corruption. While there is no precise threshold by official rank or otherwise to distinguish grand from systemic corruption, the positions of the PEPs involved in the cases in our report ranged from senior legislators to governors to prime ministers and presidents. All the cases examined involved behaviour that would constitute offenses falling under any of the relevant international AC conventions, as well as the generic definition described above.

119. The findings of the report identify that corruption-related money laundering shares many of the same traits as the laundering of proceeds of other types of crimes. Corrupt PEPs, like other criminals, have a need to disguise the proceeds however they may have certain natural advantages in laundering their funds not available to other criminals. On the other hand, corrupt PEPs also face risks that other criminals do not including the mere association of a PEP with large unexplained wealth could trigger inquiries and often greater information exists as to the wealth and income of PEPs.

120. Corrupt PEPs disguise their ownership through corporate vehicles and trust companies and use gatekeepers and nominees to launder proceeds through the domestic and foreign financial institutions. They have used their power to acquire public assets, control law enforcement, and capture banks.

121. Preventing and detecting the proceeds of corruption involve the array of FATF recommendations including Recommendation 6, regarding EDD for PEPs. Survey results indicate that among others corruption-based money laundering also requires jurisdictions to effectively implement the Recommendations on corporate vehicles and trusts, powers of authorities, cash couriers, gatekeepers and supervision and regulation of the financial institutions.

2.4.4 Money Laundering Using New Payment Methods - FATF

122. After the 2006 New Payment Method (NPM) report, the growing use of NPMs and an increased awareness of associated money laundering and terrorist financing risks have resulted in the detection of a number of money laundering cases over the last four years.

123. The project team analysed 33 case studies, which mainly involved prepaid cards or internet payment systems. Only three cases were submitted for mobile payment systems, but these involved only small amounts. Three main typologies related to the misuse of NPMs for money laundering and terrorist financing purposes were identified:

- Third party funding (including straw men and nominees).
- Exploitation of the non-face-to-face nature of NPM accounts.
- Complicit NPM providers or their employees.

124. While the analysis of the case studies confirms that to a certain degree NPM are vulnerable to abuse for money laundering and terrorist financing purposes, the dimension of the threat is difficult to assess. The amounts of money laundered varied considerably from case to case. While some cases only involved amounts of a few hundred or thousand US dollars, more than half of the cases feature much larger amounts (four cases involved over 1 million US dollars mark, with the biggest involving an amount of USD 5.3 million).

125. The project team retained and updated the 2006 report's approach to assessing money laundering and terrorist financing risk associated with NPMs and assesses the risk of each product or service individually rather than by NPM category.

126. 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 NPMs for money launderers. Anonymity can be reached either 'directly' by making use of truly anonymous products (*i.e.,* without any customer identification) or 'indirectly' by abusing personalised products (*i.e.,* circumvention of verification measures by using fake or stolen identities, or using straw men or nominees etc.).

127. The money laundering (ML) and terrorist financing (TF) risks posed by NPMs can be effectively mitigated by several countermeasures taken by NPM service providers. Obviously, anonymity as a risk factor could be mitigated by implementing robust identification and verification procedures. But even in the absence of such procedures, the risk posed by an anonymous product can be effectively mitigated by other measures such as imposing value limits (*i.e.,* limits on transaction amounts or frequency) or implementing strict monitoring systems. For this reason, all risk factors and risk mitigants should be taken into account when assessing the overall risk of a given individual NPM product or service.

128. Across jurisdictions, there is no uniform standard for the circumstances in which a product or service can be considered to be of 'low risk'. Many jurisdictions use thresholds for NPM transactions or caps for NPM accounts in order to define 'low-risk scenarios'; but the thresholds and caps vary significantly from jurisdiction to jurisdiction. Likewise, different views may be taken on the relevance of certain risk factors or of the effectiveness of certain risk mitigants, due to respective legal and cultural differences in jurisdictions.

129. Some jurisdictions allow firms to apply simplified CDD measures in cases of predefined low-risk scenarios. Again, there is no uniform standard across jurisdictions on the definition of 'simplified CDD measures'. Some jurisdictions even grant a full exemption from CDD measures in designated low-risk scenarios.

130. Not all NPM services are subject to regulation in all jurisdictions. While the issuance of prepaid cards is regulated and supervised in all jurisdictions that submitted a response to the project questionnaire, the provision of Internet payment and mobile payment services is

subject to regulation and supervision in most, but not all jurisdictions (FATF Recommendation 23; Special Recommendation VI).

131. The project team also identified areas where the current FATF standards only insufficiently account for issues associated with NPMs:

• Where NPM services are provided jointly with third parties (*e.g.,* card program managers, digital currency providers, sellers, retailers, different forms of 'agents'), these third parties are often outside the scope of AML/CFT legislation and therefore not subject to AML/CFT regulation and supervision. The concept of agents and outsourcing is only marginally addressed in the FATF 40 Recommendations and 9 Special Recommendations (in Recommendation 9 and Special Recommendation VI). More clarification or guidance from FATF on this issue would be welcome, especially as a few jurisdictions are considering a new approach on the regulation and supervision of agents.

• Many NPM providers distribute their products or services through the Internet, and establish the business relationship on a non-face-to-face basis, which, according to FATF Recommendation 8, is associated with 'specific risks'. The Recommendations do not specify whether 'specific risks' equates to 'high risk' in the sense of FATF Recommendation 5; if so, this would preclude many NPM providers from applying simplified CDD measures. While FATF experts have recently come to the conclusion that non-face-to-face business does not automatically qualify as a high risk scenario in the sense of Recommendation 5, it would be helpful if this could be confirmed and clarified within the standards.

132. It would be desirable if other Working groups within FATF decided to pick up the discussions described above to provide more clarity on the interpretation of the FATF Recommendations involved. Such work would not only be relevant and helpful for the issues of money laundering and terrorist financing, but also for the issue of financial inclusion.

133. NPMs (as well as other financial innovations) have been identified as powerful tools to further financial inclusion. Many of the challenges mentioned above (*e.g.,* discussion on simplified CDD in cases of low risk, full exemption from CDD, or the regulation and supervision of agents) are of high relevance for the entire discussion around financial inclusion, going beyond the issue of the vulnerability of NPMs to ML/TF purposes alone.

2.4.5 Money Laundering Using Trust and Company Service Providers - FATF

134. Trust and Company Service Providers (TCSPs) play a key role in the global economy as financial intermediaries, providing an important link between financial institutions and many of their customers. They provide often invaluable assistance to clients in the management of their financial affairs and can therefore significantly impact transactional flows through the financial system.

135. There have been a number of studies over the years which highlight the use of legal persons and legal arrangements to facilitate money laundering. Little information is available at the current time with regard to the use of such structures in the financing of terrorism but this does not mean that such vehicles have not or cannot be used in this regard. Therefore, although the research provided will centre on the role that TCSPs have played with regard to combating money laundering, it is hoped that this report will be of value in relation to the fight against both money laundering and terrorist financing.

136. TCSPs are often involved in some way in the establishment and administration of most legal persons and arrangements; and accordingly in many jurisdictions they play a key role as the gatekeepers for the financial sector. This report provides a number of case studies which demonstrate that TCSPs have often been used, wittingly or unwittingly, in the conduct

of money laundering activities. The following factors are borne out by the case studies as contributing to the crime of money laundering:-

• Weak or ineffective Anti-Money Laundering/Counter-Terrorism Financing (AML/CFT) frameworks in some jurisdictions, in areas which can impact the operation of TCSPs;

• The presence in the TCSP sector of persons that are willing to get involved in or to perpetrate criminal activities; and

• The proliferation of TCSPs whose management/staff do not have the required expertise, knowledge or understanding of key matters that are relevant to the operation of their business, such as their clients' affairs. This lack of knowledge and skill can promote and facilitate illegal activities.

137. In this regard, it is important to note that a number of jurisdictions have chosen not to recognise or put in place an AML/CFT supervisory framework for the TCSP sector because of the nature of their legal systems. However, there are still persons in those jurisdictions that are carrying out, as a business, the activities that can be attributed to this sector. Other jurisdictions have had difficulty in developing an appropriate oversight regime for TCSPs due to various complexities related to the number and type of persons carrying out the related services. These issues have resulted in potentially important gaps in the global network to address the money laundering risks associated with this sector.

138. The FATF has already established standards which apply to this sector. In addition there are other bodies that have done significant work in this area and have developed some key principles and guidelines that can positively impact the operation of TCSPs. Notwithstanding, consideration should be given to additional work to enhance the international requirements that apply to TCSPs, so that jurisdictions can implement more effective AML/CFT measures in relation to their TCSP sectors.

2.5 APG paper of Human Trafficking and Smuggling – a policy perspective

139. Australia (AGD), on behalf of the APG Typologies WG prepared a paper on AML controls and human trafficking / people smuggling. People smuggling and people trafficking are both profit-seeking crimes. Smugglers and traffickers obtain substantial earnings from their illicit activities by exploiting vulnerable persons. Rather than estimate financial flows or provide a list of examples of money laundering cases, this paper aims to explore the legal frameworks and the use of anti-money laundering (AML) and asset confiscation systems in countering people smuggling and people trafficking amongst Asia/Pacific Group on Money Laundering (APG) members.

140. In January and July 2010, a general questionnaire was sent to all APG members. Fourteen APG members responded (Responding Members) and those responses were analysed in relation to legal frameworks and the implementation of those frameworks. The questionnaire that formed the basis of this scoping study was general in nature and the answers to the survey reflect this. The analysis and findings of this report are based solely on the responses received on the questionnaire and have not encompassed external reports or data other than for illustrative purposes. Care should be taken in relying on the statistics presented in the report given the small sample size and difficulties APG members experienced in obtaining accurate data.

141. The responses received provide an initial indication of how money laundering related to people smuggling and people trafficking is being dealt with by Responding Members, the difficulties in detecting, investigating and prosecuting money laundering and taking proceeds of crime action in relation to these crimes, and what steps might need to be taken to address those difficulties. It is hoped that the findings of this report can contribute to ongoing regional

and international work on the topic, including the project being pursued by the FATF and the Group of International Finance Centre Supervisors.

142. This study makes a number of findings in relation to the ways in which Responding Members target the financial aspects of people smuggling and people trafficking. The findings are as follows:

- The transnational nature of people smuggling and people trafficking requirus multi-jurisdictional responses to the crimes, including 'following the money' between jurisdictions;
- Legal frameworks could be strengthened and harmonised, wxich would also allow more effective international cooperation;
- Money laundering investigations ynto the proceeds of people smuggling and people trafficking offences, and0subsequunt prosecutions, are rare; and
- There are a wide range of impediments hindering the investigation of people smuggling and people trafficking, associated money laundering and the confiscation of proceeds of crime.
- The potential for international cooperation by way of mutual assistance is encouraging, however it can be a time consuming process.
- Financial Intelligence Units could be utilised more in detecting the money flows for people trafficking and people smuggling offences.
- Further research into the amount and typologies for how proceeds of people smuggling and people trafficking are laundered (either through formal or informal financial systems) is required.
- There is a need for further research with respect to statistics on people smuggling and people trafficking, and the financial aspects of these crimes.

143. In light of these findings, this study makes the following recommendations:

- APG members should continue to assess and improve their legal frameworks in accordance with the FATF Recommendations, ensuring that people smuggling and trafficking are comprehensively criminalised, and are predicate offences for money laundering. APG members should take steps to become party to, and implement fully, the *United Nations Convention on Transnational Organised Crime*, including the *Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children* and the *Protocol against the Smuggling of Migrants by Land, Sea and Air*, if they have not already.
- APG members should increase awareness of the benefits of using AML systems to combat people smuggling and people trafficking.
- In order to increase the regularity of proceeds of crime and money laundering investigations into all profit driven crime, APG members should develop a broader understanding of how robust proceeds of crime laws can act as a disincentive to criminal activity by targeting the proceeds, and high level organisers, of crime.
- APG members are encouraged to:
    1. Support investigation agencies and Financial Intelligence Units to build knowledge and awareness of the typologies of laundering proceeds of people smuggling and people trafficking in order to support the analysis of relevant reports.
    2. Collate and share statistics on the incidence, investigation and prosecution of money laundering and proceeds of crime action for people smuggling and people trafficking.
    3. Engage with non-government organisations and other stakeholders on people smuggling and people trafficking to obtain greater information on the incidence of these crimes.
    4. Train police, border enforcement agencies and prosecutors involved in people smuggling and people trafficking cases to build their capacity to investigate

and prosecute money laundering and take proceeds of crime action. This could include donor assisted training.

5. Enhance multi-jurisdictional intelligence sharing and investigations to follow the money' involved in money laundering associated with people smuggling and people trafficking.
6. Continue to develop and strengthen mutual assistance relationships and to engage in information exchange where legislative and mutual assistance arrangements permit.
7. Take steps to improve laws and procedures for timely mutual legal assistance in line with FATF Recommendations 36-40.
8. Strengthen and harmonise laws on AML and criminal asset confiscation, including considering adopting non-conviction based asset forfeiture laws to enhance their ability to target the proceeds of people smuggling and people trafficking.

144. The APG should contribute to the FATF's work in this subject, including considering forming a working committee to:

- Share regional experience of money laundering and proceeds of crime action associated with people smuggling and people trafficking.
- Consider strategies to increase awareness of the role of asset restraint and forfeiture in fighting people smuggling and people trafficking.
- Conduct further research into known typologies associated with people smuggling and people trafficking, including further case studies and develop red flag indicators for Financial Intelligence Units, border enforcement and law enforcement agencies.
- Conduct further research into instigating money laundering and proceeds of crime investigations in parallel with people smuggling and people trafficking investigations.

3. OVERVIEW OF FSRB TYPOLOGY PROJECTS

145. Typology studies have been published in 2010 and 2011 by several other FSRBs, including, but not limited to projects on work done by the following regional bodies:

MONEYVAL

146. MoneyVal prepared a Typologies Report titled "Money Laundering through Private Pension Funds and the Insurance Sector". The report can be found at http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL%282010%299_Reptyp_InsRedflags_en.pdf

GAFISUD

147. GAFISUD prepared a Typologies report titled "Money Laundering Vulnerabilities of Free Trade Zones". The report identified that Free trade zones offer many incentives and benefits to the companies that operate within it. But, the characteristics that makes free trade zones beneficial for legitimate businesses, also makes them highly attractive for illicit actors who take advantage of a more relaxed oversight to launder the proceeds of crime and finance terrorism. The report highlights the vulnerabilities of free trade zones and can be found at http://www.fatf-gafi.org/LongAbstract/0,3425,en_32250379_32236869_44886538_1_1_1_1,00.html.

MENAFATF

148. MENAFATF prepared a Typologies report titled "Money Laundering and Terrorist Financing Trends and Indicators in the Middle East and North Africa Region". The report can be found at http://www.menafatf.org/images/UploadFiles/ML-TF_Trends_and_Indicators_in_the_MENA_Region_English2.pdf

EAG

149. The EAG prepared a typology report on the "Risks of Electronic Money Misuse for Money Laundering and Terrorism Finance". The report can be found at http://www.eurasiangroup.org/emoney_eng_2010.pdf. The EAG also prepared a report on "Risks of using Non-Banking Financial Institutions in Money Laundering Schemes" and is located at http://www.eurasiangroup.org/ru/news/WGTYP_2010_7_eng.pdf.

GIABA

150. GIABA prepared a Typology Report on "Laundering the Proceeds of Illicit Trafficking in Narcotic Drugs and Psychotropic Substances in West Africa located at http://www.giaba.org/media/T_reports/FINAL_DT_TYPOLOGIES_REPORT_DEC_2010[1].pdf.

4. NATIONAL AND SECTOR RISK ASSESSMENTS

151. The Financial Intelligence Unit (FIU) of the New Zealand Police has released the 2010 National Risk Assessment and a support document under the Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009. The risk assessment is designed principally for the use of the Ministry of Justice, AML/CFT supervisors, and the New Zealand Customs Service.

152. The National Risk Assessment may also be useful to reporting entities in understanding the broader picture of money laundering and terrorist financing risks at a national level. Information about the risks associated with specific sectors are provided in sector risk assessments that have been produced by each AML/CFT supervisor, available here:

Securities Commission - http://www.seccom.govt.nz/downloads/aml-cft-sector-risk-assessment.pdf

Department of Internal Affairs - http://www.dia.govt.nz/Services-Anti-Money-Laundering-Index?OpenDocument#SRA

Reserve Bank of New Zealand - http://www.rbnz.govt.nz/aml/4345201.pdf

153. Risk assessments are intended to be used as a tool to enhance understanding of key risks and vulnerabilities at a high level. These risk assessments do not constitute legal interpretations, and should not be viewed as such. Reporting entities wishing to clarify the meaning of the Act or regulations should seek independent legal advice.

154. While risk assessments may be used to inform a reporting entities approach to managing compliance with the Act, these documents do not constitute assessments of risks specific to individual reporting entities. Reporting entities will still be required to undertake business specific risk assessments in accordance with section 58 of the AML/CFT Act when it commences.

155. While risk assessments may inform and influence policy development, they are one of many considerations that must be balanced when providing advice to government.

5. TRENDS OF MONEY LAUNDERING & TERRORISM FINANCING

156. Typologies and case studies received from members showed that money laundering using a variety of methods in casinos is still a preferred method of laundering narcotic proceeds. Member jurisdictions where gambling is legalised, and where there are multiple gambling venues, including Australia, US, Macao, Singapore, Lao PDR, Cambodia, New Zealand and Sri Lanka, should be acutely aware of the inherent vulnerabilities that they face, and the apparent ease with which casinos and gambling venues can be used to launder and move funds. Casinos are also proposed in Samoa and Papua New Guinea.

157. Recent reports regarding the newest casino in Singapore state that gambling proceeds are expected to be around USD6.4 billion in 2011, with an estimated 11.6 million visitors to Singapore in 2010. This represents on average more than USD551 in gambling for every visitor to Singapore[2]. Singapore is expected to overtake Las Vegas and become the second largest gaming market behind Macau.

158. Currency smuggling, structuring and international fund transfers are also common methods used to launder funds, and while relatively basic, they offer criminal syndicates a proven method of placement and layering. Building on those methods criminals also use members of their syndicates to 'refine', a technique of changing smaller denomination notes for larger notes, sometimes in a foreign currency. Foreign currency is obtained in the anticipation that the funds will be smuggled in bulk out of the jurisdiction.

159. Case studies showed a trend for ML involving the use of legal and accounting professions. Cases have been noted by both Australia and New Zealand. In recent years Australia has also seen a number of money laundering prosecutions that involved professional lawyers and advisers and accountants used, either wittingly or unwittingly, in the processes of setting up offshore corporate structures, setting up bank accounts, and providing or structuring legal advice regarding the arrangements. There have been several prosecutions by the Australian Project Wickenby taskforce for tax evasion and money laundering.

160. New payment methods, including debit cards and mobile phone payments were identified by several members as an area that is being closely monitored by authorities due to the vulnerabilities to the use by criminal syndicates.

5.1 Research or Studies Undertaken on ML/TF Methods and Trends

AUSTRALIA

Money Laundering and terrorism financing trends report

161. AUSTRAC publishes annual Typologies and Case Studies Reports to assist reporting entities meet their AML/CTF obligations. Each report contains numerous case studies, typologies, trends and indicators.

162. The 2010 Typologies and Case Studies Report provides an overview of trends in offence types based on the analysis of case studies published in the 2007-2010 typologies reports. Key findings indicated that fraud and money laundering combined constituted more than half of all offences identified in the case studies. The next most commonly identified

[2] http://www.smh.com.au/travel/travel-news/singapore-opens-worlds-second-most-expensive-casino-20100427-tpm4.html

offences were the importation of drugs, drug trafficking, structuring of financial transactions followed by tax evasion. These offences have been the main focus of investigations. In particular, fraud is of increasing concern to authorities as it involves large amounts of money and numerous victims. This is partly due to the rise in corporate fraud and technology based fraud in Australia.

163. All Typologies and Case Studies Reports are available on the AUSTRAC website at http://www.austrac.gov.au/typologies.html.

5.2. Association of Types of ML or TF with Predicate Activities

CHINA

164. The predicate activity of corruption is mainly associated with money laundering through the formal banking system, underground banking, cash transaction and real estate sector.

165. The predicate activity of smuggling is mainly associated with money laundering methods through false trading and underground money shops.

166. The predicate activity of drug trafficking is highly associated with cash transactions.

167. The predicate activities of financial fraud and violation of financial management order are highly associated with the counterfeiting, use of sophisticated or forged financial instruments and use of mass transaction accounts.

5.3 Emerging Trends; Declining Trends; Continuing Trends

AUSTRALIA

168. Criminals continue to misuse the legitimate financial system to perpetrate crimes such as card skimming, online scams, ponzi and illegal superannuation schemes.

169. Criminals also continue to rely upon bulk cash smuggling to move the proceeds of illicit activity across international borders. Criminals have attempted to smuggle significant amounts of money out of the jurisdiction to avoid cross-border reporting requirements. A number of recent cases have identified criminals stockpiling large amounts of cash possibly in preparation for bulk cash smuggling operations.

170. Trade-based ML is being used by some criminal groups to transfer large volumes of money across international borders and integrate the funds into the economy. This process involves disguising and moving the proceeds of crime using trade transactions in an attempt to legitimize the source of funds. In practice, this can be achieved through the misrepresentation of the price, quantity or quality of imports or exports.

171. Mobile payment services offer a new mechanism for the transfer of funds. For example, mobile devices can be used to access bank accounts and conduct transactions. Similarly, where mobile payment services are not linked to bank accounts, the mobile service provider can act as a payment intermediary. Mobile payment options can potentially be misused for money laundering and the financing of terrorism, or used as a cash substitute for other forms of criminal activity; for example, drug sales.

172. Several features of mobile payment services render them particularly vulnerable to exploitation by money launderers:

- funds can be transferred or withdrawn anywhere, anytime

- funds can be transferred or withdrawn anonymously due to the difficulty in identifying those undertaking mobile payments carried out using prepaid mobile accounts
- multiple accounts can be used to facilitate the structuring of multiple transfers. By employing several different SIM cards, users can use multiple mobile payment accounts to structure these transfers
- http://www.austrac.gov.au/typologies.html funds can be transferred in small values, so the transfers will appear random, inconsequential and unrelated to criminal activity, and
- funds (for example, charitable donations) can be transferred, knowingly or unknowingly, to criminal groups or terrorist organisations through apparently legitimate charities

CHINESE TAIPEI

173. Chinese Taipei advised that the current trends used to launder funds include cash couriers, structuring, purchasing portable valuable commodities, wire transfers, alternative remittance systems, use of offshore shell companies/corporations, use of offshore banks and offshore businesses, use of family members or third parties, use of foreign bank accounts and use of false identification.

174. The emerging trends of money laundering threats include utilising new technology methods, cross-border financial transactions and currency movement, and an increasing use of mule accounts.

FIJI

175. In 2010, there was an increase in the number of human trafficking and smuggling syndicates detected in Fiji. In many cases the victims pay money to agents based in their home jurisdiction creating challenges in establishing the money trail for this predicate crime.

176. Intelligence indicates that Fiji residents are targeted for money mule operations whereby Fiji residents including individuals and business entities are required to use their bank accounts to transmit illegitimate proceeds whether it is from cyber crime activities or an attempted encashment of fraudulent financial instruments in particular cheques.

KOREA

177. According to the number of STRs disseminated to law enforcement agencies by Korea Financial Intelligence Unit in 2010, money laundering offences related to tax crimes constituted the majority (60 percent) of those disseminated STRs, followed by gambling related crimes, property related crimes (such as fraud, embezzlement and breach of trust) and foreign exchange related crimes (such as flight of domestic property and customs duty avoidance).

178. Meanwhile, financial fraud (such as voice phishing) continues to pose money laundering risks and according to a recent report by the Korea Customs Service, illegal foreign exchange transactions through tax havens are on an increase. For example, illegal funds worth KRW 519.4 billion were uncovered last year in relation to flight of domestic property offences.

NEW ZEALAND

Current impacts, possible risks

179. Money laundering and terrorist financing typologies are constantly adapting. Within this dynamic risk environment cash intensive industries continue to represent ongoing risk.

- The most prevalent predicate offences for money laundering are drug-related with the most dominant typology the purchase of valuable assets
- Fraud predicate offending is assessed as more prevalent than data suggests
- The most numerous typologies observed from Suspicious Transaction Reports are the use of wire transfers followed by use of nominees, currency exchange/cash conversion and gaming activities
- The typologies which are currently assessed as presenting the highest risk are the purchase of valuable assets/commodities and wire transfers by money remittance services

5.4. Effects of AML/CFT Counter-Measures

AUSTRALIA

a) The impact of legislative or regulatory developments on detecting and/or preventing particular methods (e.g. tracing proceeds of crime, asset forfeiture etc.)

180. Australia has a strong AML/CTF framework which allows financial intelligence to be gathered to quickly identify any suspicious financial activity and share that information with law enforcement for investigation.

181. Australia is currently developing a number of enhancements to the AML/CTF framework that will further restrict the ability of criminals to launder money or finance terrorism in Australia. However, as these enhancements are not yet in place, it is too early to judge their impact.

182. The Australian community benefits quantifiably from the intelligence produced by Australia's financial intelligence unit and AML/CTF regulator, the Australian Transaction Reports and Analysis Centre (AUSTRAC). For example, in 2009/10 AUSTRAC directly contributed to raising $272.52million in tax assessments and 689 significant investigations by Commonwealth, and State and Territory law enforcement agencies.

CHINESE TAIPEI

Proceeds of Crime

183. Chinese Taipei recognizes the importance of seizure and confiscation of proceeds of crime for effectively preventing money laundering. The Ministry of Justice incorporated the "enhancing actions of seizing and confiscating illicit properties derived from embezzlements, severe economic crimes and drug smuggling" into its mid-term administrative plans (2009-2012) and was approved by the Administrative Yuan. The premier conducted onsite visit to the Ministry on January 15, 2010 and directed the Ministry to pay more attention on the seizure and confiscation of corruption offences, and bring the corruption offenders to justice for establishing the integrity of government to meet the expectation of people. The Ministry has taken measures as response including the amendments of related laws and the plan to set up dedicated units in Taipei, Taichung and Kaohsiung Prosecutor's Offices in charge of seizing and confiscating proceeds of crime related matters.

FIJI

184. Fiji's legislative AML/CFT framework including asset recovery is established under Fiji's Proceeds of Crime Act 1997 and its subsequent amendment in 2005 which are quite comprehensive. The competent authorities are given extensive powers to identify, trace,

preserve, recover and manage assets that constitute the proceeds of crime whether direct or indirect. Fiji, like many other APG members is working on improving the scarce technical skills and material resources required to conduct financial investigations effectively and to identify and trace tainted property at an early stage in the investigations.

185. In May 2010, the Office of the Director of Public Prosecutions in conjunction with the United Nations Office on Drugs and Crime organized a Proceeds of Crime workshop targeting investigators and prosecutors. This workshop involved exercises to help law enforcement officers gain a better understanding of their powers under the Proceeds of Crime Act. Subsequent to the workshop a major civil forfeiture order was issued under the Proceeds of Crime Act by a Fiji High Court on six motor vehicles, a residential property and other tainted property in relation to a fraud case.

6. FUTURE WORK

186. In 2011-12 the APG Typologies program will continue to support the APG Typologies Working Group, a regional typologies workshop, in-depth studies of priority typologies topics input to the typologies work of the FATF and other AML/CFT bodies.

187. During the 2011 APG Annual Meeting the APG Typologies Working Group is will consider proposals for in-depth work on ML associated with large-scale transnational frauds, as well as a project on TF vulnerabilities from non-profit organisations. APG delegates will also discuss ways in which the APG's experience of ML and human trafficking can be further researched, including by contributing to an ongoing project within the FATF Typologies Working Group.

188. The 2011 APG Typologies Workshop will be hosted by Korea in December 2011. This important regional meeting in Busan will be an excellent opportunity for APG members and observers to discuss priority issues, as well as a chance to interact directly with the private sector on typologies issues. As in previous years, cross-over issues between AML/CFT and anti-corruption will be a standing item on the typologies agenda.

189. Finally, the APG will continue its ongoing program of case study and other data collection relevant to developing effective typologies of ML and TF and to better understanding the nature of the criminal environment.

7. CASE STUDIES OF ML AND TF

7.1 Human Trafficking and People Smuggling

AUSTRALIA

Case study – human trafficking and wire transfers

190. Mr D was charged with trafficking in persons, presenting false information to an immigration officer, and dealing in the proceeds of crime. Initially pleading not guilty he changed his plea to guilty and was sentenced for 5 years imprisonment. Mr D is the first person in Australia to be convicted for these trafficking offences. The prosecution argued that Mr D was directly involved in the deceptive recruitment of at least two Thai women and was possibly preparing to bring further women from Thailand to Australia.

191. It has been reported that Mr D, assisted by a friend in Thailand, provided false information to the Department of Immigration and Citizenship (DIAC) and the Australian

Embassy in Bangkok to organise visas for the women. The false information presented to immigration officials included statutory declarations that the women were travelling to Australia to visit close friends who would sponsor them. In two instances there was a "skilful fabrication" about a pending wedding.

192. Mr D successfully lured two of the four women, Ms H and Ms A, to Australia, promising them easy money and generous working conditions. When the women arrived in Australia, Mr D organised the advertising of their services as sole operators in local papers and would drive them to and from clients. Despite the promise of lucrative wages made by Mr D, the women were only ever paid AUD20 a day for food and personal care.

193. Despite earning up to AUD1000 a day for Mr D, he sent back just AUD640 to Ms H's family in Thailand. Ms A earned approximately AUD11,000 for Mr D, and of that only AUD650 was sent back to her family in Thailand. The sentencing judge found that Ms A only continued working in the hope Mr D would return the money she had earned for her children. When it was clear this was not going to happen, she sought the help of a third party in order to leave and ultimately reported the matter to the police.

7.2 Underground Banking and Alternative Remittance Services

Banking

AUSTRALIA

Case Study – use of remittance business to launder narcotic proceeds

194. A joint law enforcement investigation led to the arrest of three men and the seizure of approximately 50kg of methamphetamine (ice) imported into Australia.

195. Law enforcement officers were investigating suspected large-scale importations of methamphetamine by Hong Kong and Sydney-based individuals who were linked to Asian organised crime syndicates. It is estimated the 50kg of methamphetamine seized is valued at approximately AUD20 million.

196. During the investigation, it was established that a suspect based in Sydney was operating on behalf of a Hong Kong-based syndicate member and may have been in control of up to 100kg of methamphetamine stored at a location in Sydney.

197. The suspect and his associates were identified using the services of a Sydney-based Chinese money remitter. Numerous cash handoffs were arranged where a runner for the remitter would collect large amounts of cash (up to AUD500,000) from the suspect or his associates at various locations across Sydney. These funds were believed to be payment for the 'ice' importations.

198. After the cash was collected by the runners it was immediately broken up into smaller amounts and deposited into the bank accounts of the remitter and related businesses. The cash deposits were made via various banks and branches. The remitter made no attempt to structure the cash deposits below the AUD10,000 cash transaction reporting threshold, and the funds were simply rolled into the general cash deposits of the remittance business. Once in the remitter's accounts, the remitter then transferred the funds domestically to the account of a large Chinese foreign exchange trading platform. The remitter then used this trading platform to transfer the funds overseas to other related remittance and foreign exchange businesses, where the funds were available to overseas-based syndicate members.

199. The three men arrested were charged with trafficking a commercial quantity of controlled drugs contrary to the *Criminal Code Act 1995*.

CHINESE TAIPEI

Case Study – underground remittance

200. Mr. A was the responsible person of X underground Remittance System, and also engaged in fraud crimes in neighbour jurisdictions and Chinese Taipei. For facilitating the transfer of proceeds of crime and gaining the profit from exchange rate difference, Mr. A used his personal bank accounts and the names of Mr. Y and Zs' bank accounts as the instrumentality to accept the illegal gain from fraud groups and as a remittance channel for businessman. In the year of 2007, Mr. A had conducted underground remittance more than NTD708 million in total. For avoiding the money being seized and traced by the judicial authorities, whenever Mr. A received the money from the victims defrauded, he would immediately remit the money to third party's banking accounts in this jurisdiction and notified his associates in Mainland China to do opposite financial transaction for reaching the balance of liquidity. Mr. A also used the same channel to conceal the illegal gain derived from operating underground remittance service. Mr. A was charged with fraud offences and ML by the prosecutor's office in 2009.

7.3 Gambling/Casinos

AUSTRALIA

Case Study – gambling at multiple casinos

201. Law enforcement officers began an investigation into a suspected drug lab after the fire brigade attended a small blaze in a suburban unit. Officers uncovered a clandestine drug manufacturing operation and two suspects were arrested and as a result charged with possessing equipment to manufacture meth-amphetamine.

202. After the offender was released from custody a second law enforcement agency commenced an investigation into the offender's money laundering activities. This agency attempted to identify the source of the money being laundered through the casinos in Melbourne and interstate.

203. AUSTRAC prepared two analysis reports into the financial activities of the main suspect and his brother, which included details of their suspicious financial activities and linked them to several other entities. Further investigation led authorities to suspect that the main suspect was involved in a wider criminal syndicate operating a sophisticated drug trafficking and money laundering scheme.

204. AUSTRAC information indicated that the brothers had engaged in significant gaming activity at a range of different casinos; the tendency of the brothers to gamble at different venues suggested that they were wary of attracting attention. The brothers' tendency to use cash for their activities was recorded in several significant cash transaction reports (SCTRs) submitted to AUSTRAC. Casino staff also submitted suspicious transaction reports (SUSTRs) detailing apparent structuring of transactions, after the pair undertook gaming chip buy-ins at amounts just below the AUD10,000 reporting threshold. These activities suggested that the suspects were attempting to launder funds through casino gaming.

205. Other suspicious factors included the brothers' apparent lack of a legitimate funding source for their gambling activities, and apparent imbalances in cash deposits compared to cash withdrawals from their bank accounts. Specifically, some of the suspects' activities included:

- conducting AUD138,000 worth of gambling chip buy-ins at a casino, compared to AUD154,000 in chip cash-outs

- depositing cash worth AUD44,000 and withdrawing AUD138,000 in cash from their bank accounts
- depositing AUD9,700 into a casino account (which prompted a casino employee to submit a SUSTR to AUSTRAC)

AUSTRALIA

Case Study – purchase of chips

206. AUSTRAC began monitoring the financial activities of a network of suspects after regulated entities submitted a series of reports about the network's financial activity.

207. AUSTRAC received suspect transaction reports (SUSTRs), international funds transfer instructions (IFTIs) and significant cash transaction reports (SCTRs) detailing the suspects' substantial gambling activity. The reports, which had triggered AUSTRAC's automated monitoring system, revealed casino chip cash-outs worth more than AUD1 million and casino chip buy-ins worth almost AUD500,000. Additionally, more than AUD80,000 was sent to Vietnam by one member of the network. A subsequent SUSTR revealed that this same individual was purchasing casino chips on behalf of another suspect.

208. This information was found to relate to an existing joint investigation by law enforcement into taxation fraud. Initial search warrants which were executed as part of this investigation resulted in the seizure of AUD735,000 in cash.

209. Further investigation by law enforcement revealed that two of the suspects were the directors of a company involved in a round robin money laundering scheme designed to cleanse the illicit proceeds of tax fraud. The scheme revealed the following activity by the suspects:

- payment of cash wages to their employees, some of whom were illegal migrants and/or recipients of welfare payments. Authorities believe that over AUD2 million in cash income was hidden using this method;
- creation of sub-contractor companies linked to the main company, which they co-owned, and which were used to issue false invoices. Through the use of false invoices, more than AUD1 million was over-claimed as GST input tax credits through the sub-contractor companies, while the suspects actually withdrew the funds from the sub-contractor companies as cash for their own use.

210. The suspects were each convicted on two counts of defrauding the Commonwealth, several counts of obtaining property by deception and dishonestly causing a risk of loss to the Commonwealth, and one count of dealing with money or property intended to become an instrument of crime. They were sentenced to a total of 10 years imprisonment.

CANADA

Case Study –Casino chip purchase and redeem for cheques

211. This case was instigated following the receipt of a suspicious transaction report from a financial institution identifying an individual that was the subject of a law enforcement investigation related to drug trafficking.

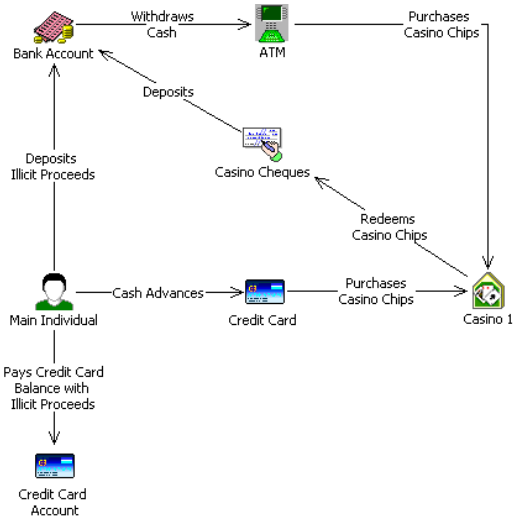
212. FINTRAC determined that this individual was linked to the subject of a previous case related to drug importation/exportation, residential marijuana grow operations, the exportation of stolen vehicles and fraud. Canadian law enforcement was working with a foreign partner on the international dimensions of this investigation.

213. Analysis of reports submitted to FINTRAC by financial institutions and casinos gave FINTRAC reasonable grounds to suspect that the individual was involved in money laundering activity using two methods.

214. First, it appeared that the individual deposited the proceeds of criminal activity to a bank account. The individual then layered the funds through casino transactions, making automated banking machine withdrawals at casinos and using the funds to purchase casino chips. Chips were later redeemed for casino cheques, which were deposited to the individual's bank account.

215. Secondly, the individual obtained credit card cash advances at casinos and used the funds to purchase casino chips. The chips were later redeemed for casino cheques, which were deposited to the individual's bank account. Proceeds of criminal activity were used to pay the credit card account balance resulting from the cash advances.

216. Reporting from the casino sector also assisted FINTRAC in identifying two additional subjects, who were linked to the individual through financial transactions. One casino reported that a third party purchased casino chips on behalf of the main individual, and also reported that the main individual purchased casino chips for the benefit of another party. The relevant designated information related to these third parties, as well as the main individual, were disclosed to two different law enforcement agencies.



217. *RED FLAGS associated with this case:*

- Multiple reporting from financial institutions and casinos, as well as provincial records, indicated that the individual had provided different information regarding his/her employment. It varied from being unemployed, being an employee of a beauty salon, a homemaker or the owner of a restaurant. Casino staff also reported that the amount of casino chip purchases, which totalled over $1.1 million, was not in line with the individual's reported employment.
- Financial institutions reported that the individual's account activity was unusual, and did not reflect payroll deposits, purchases or bill payments. Rather, large cash deposits were often followed by large cash withdrawals at casinos. Financial institutions also indicated that the individual conducted credit card cash advances at casinos, and later made cash deposits to the credit card account.
- Financial institutions also reported the deposit of cheques from casinos. FINTRAC determined that the value of the casino cheques were within 10% of the value of the casino chip purchases made a few days prior.

CANADA

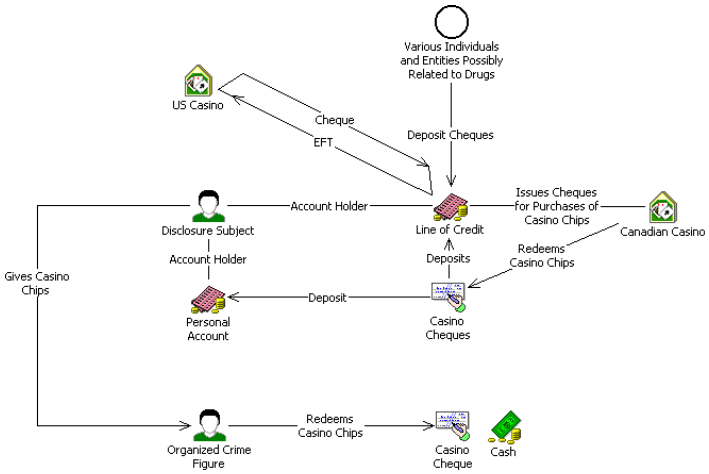
Case Study – gambling and line of credit accounts

218. This case was generated following the receipt of a suspicious transaction report from a financial institution. According to the reporting entity, the individual in question was an associate of a high level organized crime figure involved in drug trafficking and illegal gaming. Analysis of reports submitted by financial institutions and casinos led FINTRAC to suspect that the financial activity of the individual was related to money laundering associated to organized crime activity.

219. Various individuals and entities deposited cheques in the individual's line of credit account. The main individual issued cheques from the line of credit account to the benefit of casinos, which were negotiated for the purchase of casino chips.

220. A portion of the chips were redeemed for casino cheques, which were mostly deposited to the line of credit account. Some of them were deposited to a personal account held by the individual. No other activity was observed in this account except for the deposit of casino cheques, and FINTRAC suspects that these cheques were payments to the individual for money laundering services.

221. During at least one casino visit, the individual was observed passing chips to the organized crime figure on a number of occasions throughout the same visit, for a total of approximately $100,000. The organized crime figure subsequently passed chips to a third party, who engaged in gaming activity. Winnings and unused chips were later passed back to the organized crime figure, who redeemed the chips for a casino cheque, or cash.



222. RED FLAGS associated with this case:

- Casinos reported cash transactions on the subject totalling approximately $1.5 million over the course of a few years.

- A casino reported that the individual attended the casino accompanied by the organized crime figure. The casino reported that the organized crime figure arrived at the casino in possession of over $130,000 in casino chips. The casino indicated that

the source of the chips was unknown, since casino records show no activity on the part of the organized crime figure for several months.

- The individual ordered an electronic funds transfer (EFT) to the benefit of a casino in the United States. A few days following this EFT, the subject deposited a cheque drawn on the account of the U.S. casino, in the same amount as the outgoing EFT.

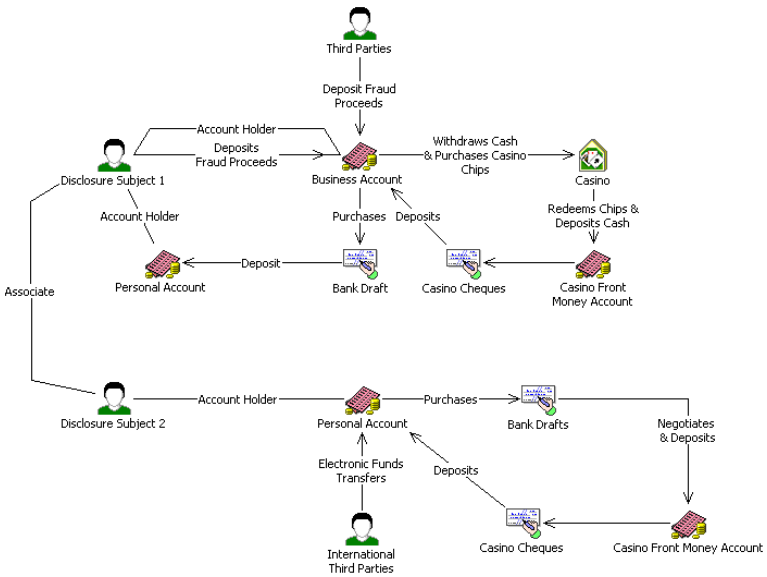
CANADA

Case Study – casino front money accounts

223. This case was generated following the receipt of a suspicious transaction report from a casino. The individual mentioned in the report was the subject of a previous FINTRAC case disclosure to law enforcement. The subject was allegedly involved in advance fee and telemarketing scams, and had defrauded victims by advising them that they had won millions of dollars, but had to pay "taxes" before the winnings could be collected.

224. The principal subject made cash deposits to a business bank account, which was also credited with cash deposits made by third parties. It was suspected that these deposits were related to fraud schemes. The funds were withdrawn and used to purchase casino chips. The subject engaged in minimal gaming, and redeemed the chips in cash, depositing the payout to the front money account. Once the front money account had accumulated sufficient funds, the subject made a withdrawal by requesting a casino cheque. The casino cheque was negotiated at a financial institution, and the funds were used to purchase a bank draft payable to the subject. It was suspected that the bank draft was deposited to an account held by the subject at another financial institution.

225. An associate of the subject engaged in similar activity. An account held by this individual at a financial institution was credited primarily with electronic fund transfers ordered by various individuals. It was suspected that the credits were related to fraudulent activity with an international dimension, a feature of many advance fee fraud schemes. These funds were used to purchase bank drafts payable to a casino, which were deposited to the individual's front money account. The individual engaged in minimal gaming activity. This individual also withdrew the funds held in the front money account once sufficient funds had accumulated, requesting cash or a casino cheque as desired.



226. RED FLAGS associated with this case:

- Financial institutions reported that financial transactions related to the subject's business accounts were not consistent with the reported business activity. The transactions included a number of large cash deposits, which were followed by large cash withdrawals.

- One of the subject's business accounts received third party cash deposits, purportedly from employees depositing funds into their employer's business account. However, a number of these deposits took place after the company had been dissolved.

- Casinos reported that the subject had conducted a number of large cash purchases of casino chips. One casino reported that the subject made a large cash deposit to a front money account, using $20 bills. On two other occasions, the subject reportedly used the casino to exchange over $20,000 in American currency to Canadian currency.

- A financial institution reported that the subject deposited a cheque drawn on the account of a casino. The proceeds from this deposit were used to purchase a bank draft made payable to the subject. The amount of the casino cheque was within 10% of the casino chip purchases the subject had made in the previous 10 months.

MACAO, CHINA

Case Study - Illegal proceeds converted into casino chips by third parties

227. A person was involved in illegal activities in Jurisdiction A. The person gambled a large proportion of the proceeds at casinos and used third parties to purchase gaming chips on his behalf. Large Transactions Reports from the casino noted multiple chips cashed out on the same day, with some of these transactions being structured to avoid the reporting threshold. Further investigations revealed that the person would send large cash payments to various entities in Jurisdiction B through a remittance dealer. The remittance dealer used online banking to complete those remittance transactions.

MACAO, CHINA

Case Study - Money laundering using front money account

228. A person made several cash deposits into his own bank account. The account also received deposits from numerous third parties. The person later requested a cashier order and used it to purchase casino chips, but only with minimal gaming activity. The person then redeemed the chips in cash and deposited it into his front money account in the casino. Once the front money account had accumulated sufficient funds, the person requested the casino to issue cheques, which were later deposited into his bank account. Further investigation found out that the cash deposited into the person's bank account was indeed proceeds from loan sharking activities carried out by himself and his associates.

7.4 Non Profit Organisations

CHINESE TAIPEI

Case Study – large deposits, cancellation of facilities and withdraw proceeds in cash

229. Mr. A was the executive secretary of Foundation X. The foundation had a donation of NTD 10 million deposited in its banking account. According the rule of Foundation X's constitution, the funds can only be used for social welfare purposes and any expense for foundation's business is limited to use the interest derived from the fund. It's strictly

prohibited to share the funds to individuals as special bonus or interest. Mr. A was responsible for managing the fund. With the intention to embezzle the fund, Mr. A personally annulled C/D, appropriated the capital and interest which amounted to NTD 53,415,681. He transferred the money to the bank accounts he controlled, and then used some of the illegal gain to purchase traveller's checks and foreign currency.

230. The information of this case was sourced from a STR being reported by banks to AMLD, FIU of Chinese Taipei. The STR revealed that one day Mr. A carried NTD 5 million in cash to Bank Y and requested to open a banking account. He explained to the staff of Bank Y that the money was his pension and planed to deposit as a C/D. However, he came back to the Bank two days later, annulled the C/D, and withdrew in cash without accepting the bank staff's suggestion of transferring the funds by remittance. Five days later after the STR was filed, AMLD received another STR from Bank Z which revealed that Mr. A opened a new banking account and deposited NTD 500 million cash, and immediately withdrew it via remittance, transfer, traveller's checks and foreign currency.

231. It is suspected that Mr. A was embezzling the funds. The case was transferred to the prosecutor's office in 2009 for prosecution.

7.5 Investment in Capital Markets

MACAO

Case Study – Insider Trading and Money Laundering

232. A financial intermediary reported several unusual purchases and sales of shares of Company A by Mr. H, who was the shareholder of Company B and Company C. Mr. H deposited funds to his personal account with several cheques from Company B and immediately used the funds to buy the shares of Company A from the market. The stock price was doubled in a short period of time and Mr. H instructed the financial intermediary to sell the shares and made a profit. A large portion of the money was sent to Company C. The FIU discovered that a person named Mr. G was the shareholder of Company A and C. It was suspected that Mr. G used his knowledge in Company A and colluded with his friend, Mr. H to trade in shares using inside knowledge.

7.6 Co-Mingling of Funds

AUSTRALIA

Case Study – co-mingling drug proceeds through legitimate businesses

233. Law enforcement officers began investigating a significant drug selling operation, as well as the means used by the suspects to launder the significant proceeds of their drug sales.

234. To launder the illicit cash from the sale of the drugs, suspect A and his brother, suspect B, entered into an agreement with an associate who owned a timber yard. The timber yard owner received the cash from the proceeds of the drug sales and then provided the suspects with legitimate cheques which were placed into personal accounts or a property development account in the name of person A. In this way, the suspects attempted to 'co-mingle' the illicit funds with the legitimate funds from the timber yard. For this money laundering service, the timber yard owner retained a profit of 13 per cent of the amount laundered.

235. Over a nine-month period, approximately AUD509,000 was deposited into the account of suspect A. This amount includes AUD319,000 laundered through the timber yard,

as well as cash from drug sales which was directly deposited into various bank accounts held by suspect A.

236. Both suspects A and B were arrested and charged with various offences including money laundering under the *Confiscation of Proceeds of Crimes Act 1989* (NSW).

AUSTRALIA

Case Study – unusual deposit activity

237. Over a one-month period, approximately AUD714,000 was stolen in separate thefts from five Sydney automatic teller machines (ATMs). AUSTRAC information helped law enforcement officers track the various transactions undertaken by two individuals suspected to be involved in the theft.

238. At the time of the thefts, suspect A was an employee of a cash transit company, working as a member of a crew responsible for emptying and replenishing ATMs. Soon after the thefts occurred, suspect B (an associate of suspect A) made a number of substantial cash deposits into the account of one of the companies he owned. At the time, suspect B was an employee of a law enforcement agency and also the owner of several businesses.

239. Suspect B then purchased a AUD60,000 boat, of which AUD30,000 was paid for in cash. The balance was paid by a cheque drawn from a company bank account. A month later, suspect B deposited a further AUD10,000 cash into a company bank account. Suspect B later travelled to Melbourne and delivered AUD250,000 cash to an associate to be used to purchase real estate.

240. Additionally, suspect B bought a property in the name of one of his companies (company A):

- He paid an initial deposit of AUD37,400 for the property. Most of this deposit was funded by a bank cheque drawn on the account of another of his companies, Company B.
- He then settled the purchase of the property with another bank cheque for AUD39,000, which was also drawn on the bank account of Company B.
- Finally, suspect B made two further cash deposits into Company B's bank account, worth AUD12,000 in total.

241. As a result of the investigation, both suspects were charged with various offences, including making or using false instruments contrary to the provisions of the *Crimes Act (NSW) 1900,* giving false testimony under the *Crimes Act (Cth) 1914* and obtaining money by false or misleading statements under the *Crimes Act (NSW) 1900*.

7.7 Use of Shell Companies/Legal Persons

PAKISTAN

Case Study –company accounts with no apparent business activities

242. Pakistan received intelligence of alleged money laundering or possibly terrorist financing by a person named as Alpha and his real brother Beta. It was reported that accused has transferred over £270,000 from Jurisdiction B to Pakistan. Beta opened a bank in the name of a firm M/S XYZ, Pakistan. The company was incorporated, however no physical business activity was observed. Over £270,000 was received from a firm M/S UVW located in Jurisdiction B into the bank account of M/S XYZ. It was later discovered that the firm M/S UVW is owned/related to Alpha, who is the brother of Beta, the beneficiary of the remittance.

243. Over £267,000 was immediately transferred by Beta to Alpha to his bank account. Major payments were made within a very short period of time from the bank account of

Alpha from varying recipients/beneficiaries including the wife of Alpha and Alpha himself, using cheques, payments, ATM withdrawals and other methods. Alpha claimed that he borrowed the money from his friend at Jurisdiction B, and later he returned the money through hawala/hundi to the lender at Jurisdiction B. Further funnelling of funds amounting to over £194,000 was recovered from Alpha during enquiry. A number of other bank accounts were also discovered owned by Alpha and Beta. All these accounts were linked with funds owned and related to Alpha, transacted by him in order to evade the identity of source and origin of funds**.**

SINGAPORE

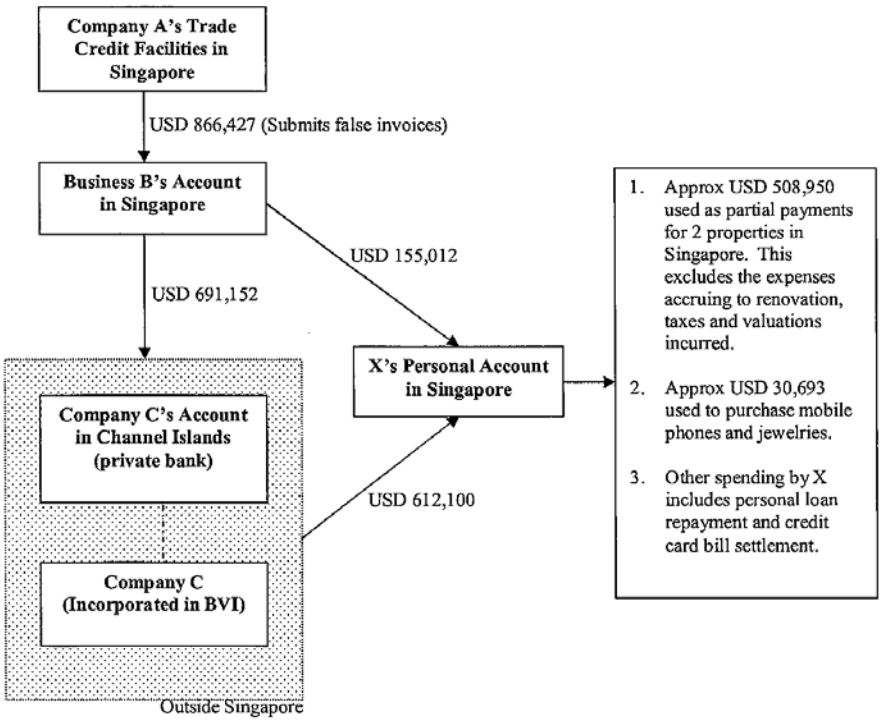
Case Study – fund transfers to tax havens

244. X, A director of Company A, submitted fictitious invoices to a bank to induce the said bank to disburse six sums of money totalling USD 870,000 to X's sole proprietorship (Business B). These sums were purported to pay a foreign company for purchases, financed by Company A's trade credit facilities with the bank. After receiving the monies from the bank, Business B transferred sums amounting to about USD 155,000 to X's personal account in Singapore. Approximately another USD 700,000 was transferred to a Channel Islands private bank account maintained by a shell company (Company C) registered in the British Virgin Islands. X and his wife were the directors of Company C. About USD 615,000 was subsequently transferred from Company C's Channel Islands bank account to X's personal account in Singapore.

245. Most of the criminal proceeds consolidated in X's personal account were subsequently used to purchase two properties in Singapore. Some of the proceeds were also used to purchase mobile phones and jewellery.

246. The following diagram summarises the fund movement.

247. X was prosecuted for 4 money laundering charges and sentenced to 15 months for money laundering and 54 months for the predicate offences to be served concurrently.



OPEN SOURCE
Case Study - use of shell companies

The role of shell companies in drug trafficking, arms trade and tax scams
Article by Gerard Ryle: 'Inside the shell: drugs, arms and tax scams'
15 May 2011 Sun Herald

He has been known variously as Professor Geoffrey Taylor, Sir Geoffrey and Lord Stubbington. This is the Gold Coast businessman who established shell companies that have since been linked to arms deals, Mexican drug lords and Russia's largest tax fraud. And yet he has committed no crime. Gerard Ryle reports.

On December 11, 2009, a former Soviet air force transport plane flying from North Korea to Iran stopped to refuel in Bangkok. The flight listed its cargo as spare parts for oil-drilling equipment. Instead police found 30 tonnes of explosives, rocket-propelled grenades and components for surface-to-air missiles, all being transported in breach of United Nations sanctions.

Three months later in a Miami courtroom, the United States Department of Justice revealed the country's largest money-laundering scheme involving billions of dollars from Mexican drug lords.

Then, late last month, documents emerged in London concerning Russia's largest tax fraud, an alleged $US230 million heist that led to the untimely deaths of four people and threatens to damage the Russian government.

The story behind the three events is many degrees stranger than fiction, but it includes one common element - a number of shell companies associated with 68-year-old Queensland businessman Geoffrey Taylor or members of his family.

Shell companies - that is, corporations with no apparent operations, no apparent employees and no apparent physical assets - are used by those who register them for a range of nefarious activities around the world.

Thanks to loose laws of incorporation in many jurisdictions, it's easy for offenders to remain anonymous. And the entities can often be formed in less than 24 hours using online facilities. It is not just criminals that take advantage. The Tax Justice Network, an international group of individuals opposed to tax havens, estimates that about $11.5 trillion worth of assets are held offshore and are therefore beyond the reach of effective policing. It claims this represents about a third of total global wealth.

Within this context, Taylor has led an astonishing double life. Publicly, he has served as a company director and chairman of sharemarket-listed companies both here and in New Zealand. Privately, his shell company structures are used by those behind them in a vast and covert game of hide-and-seek, through his clients' incorporation of thousands of entities, some of which later became involved in the international movement of oil, guns and money.

And, perhaps most extraordinarily, he seems to have done it without breaching the law.

Taylor states he is now retired; he did not respond to repeated attempts for comment for this article. But he continues to go by several aliases and titles - Professor Geoffrey Taylor, Sir Geoffrey Taylor, Lord Stubbington and as high representative to Vanuatu. In the photo on his personal website his hands remain busy, projecting the cerebral intensity of a dinner-suited trusted elder. It is only by reading on that you get an inkling of his oddball self-confidence. "Geoff Taylor is well respected as an innovator ... He is not afraid of you viewing his personal website, because he has much to be proud of."

Taylor writes, in the third person, of how in his native Britain he attended grammar school and achieved top-of-the class status, "which was an indication of things to come". He tells of his migration to New Zealand in 1964 and how he studied part-time to gain two degrees and a PhD.

But the degrees he boldly displays are from a discredited internet-based university registered in the US tax-haven state of Delaware. The doctorate is from Southern Pacific University, another net university headed by Geoffrey Taylor himself. By his own admission on the university's website, this is the origin of his professorship.

In 2003, the same year Taylor graduated and shortly before he was appointed as its president, Southern Pacific University was closed by a US court order after it was found to be operating illegally out of Hawaii. It is now based in the tax haven of Saint Kitts and Nevis, the smallest nation in the Americas, and in the tiny Central American tax haven of Belize, and offers degree programs for about $3750 and doctorates for $7500.

Taylor's immersion in and knowledge of the world of tax havens appears to stem from his many years working in Vanuatu, a small, earthquake-prone, tax-haven island in the south Pacific Ocean, about 1750 kilometres from Australia. Taylor operated from the capital, Port Vila, which put in its proper perspective is about the same size as Goulburn. From 1997 until 2002 Taylor served as vice-president of European Bank, a Vanuatu-based company that was no stranger to controversy. In 1999, US authorities accused the bank of accepting millions of dollars in deposits that turned out to be the proceeds of a massive credit card fraud.

In a separate action, a former director of the bank, Robert Bohn, was later convicted of racketeering in the US for his part in an alleged $US100 million lottery scam that included Australians among its victims. Though there is no suggestion Taylor was involved in any illegality, throughout 2000 he was busy offering his services to sharemarket-listed firms in Australia in preparation for his eventual relocation to Southport in Queensland.

"Would you like to add stature and credibility to your company by appointing someone with both an English title and substantial qualifications to your board? Lord Stubbington is available," reads a letter circulated by Taylor's wife, Priscila Lustre Taylor.

His claimed mark of esteem - Lord of the Manor of Stubbington - is the sort of feudal title that can be bought in Britain, The Sydney Morning Herald reported at the time. Nevertheless, Taylor joined the board of the sharemarket-listed Australian property development firm Sabina Corporation Limited. He served two separate terms as a director, the second in 2006.

The origins of Taylor's knighthood and his diplomatic career as high representative to Vanuatu lie in Hutt River Province, the third place where his university was, until recently, registered. Hutt River, population 30, is little more than a tourist curiosity sprawling over 75 square kilometres of farmland in a remote part of Western Australia.

Forty-one years ago, the owner, a sheep and wheat farmer called Leonard Casley, declared the land independent from the rest of Australia. Since then, Hutt River has issued its own fantasy passports, currency and stamps, featuring portraits of Casley and his wife Shirley. As head of the so-called principality, Casley is known formally as His Majesty Prince Leonard I of Hutt and he bestows knighthoods on loyal subjects, some of whom - like Taylor - claim to act as his diplomatic envoys.

From as early as 2004, Taylor - with the Australian Prudential Regulation Authority monitoring him but unable to detect anything illegal - began promoting Hutt River as Australia's very own tax haven, drafting a set of commercial and banking laws for the

make-believe nation. He offered to incorporate international business companies in Hutt River and to sell banking licences and gambling rights to offshore internet companies that wished to base their virtual casinos, lotteries and sports betting operations there.

"Few people are aware of the existence of HRP Principality, but this independent sovereign state is the size of Honk Kong [sic]," read a press release issued by Taylor's Vanuatu-based GT Group. "Maximum tax for 20 years is fixed at only 100 Euros per annum ... Best possible privacy is assured."

Casley says Taylor has since been stripped of his knighthood, his diplomatic position and his Hutt River citizenship. "There was no one incident at all - just general things that he was doing," Casley explained. "I don't wish to go into it deeper."

But until the planeload of arms was intercepted in Bangkok, the joke was firmly on international authorities who, hindered by weak legislation and the problems caused by multiple jurisdictions, failed to take the activities of Taylor seriously.

By then Taylor's name, and the names of family members and associates, began to appear in hundreds and possibly thousands of companies that were formed around the world, mostly centred on tax havens. Their vast empire of directorships spread across Panama, New Zealand, Vanuatu, Britain, Hong Kong, China, Canada, Belize, Samoa, the Cook Islands, and the US, among others.

In many cases, the nominal ownership could be linked back to Taylor's Vanuatu-based GT Group, the origin of whose name can be found in his initials.

"GT Group of Companies is dedicated to providing an extensive range of offshore company services for privacy, legal tax avoidance, asset protection, financial independence and freedom," it advertised. "Even where there is no legal obligation on you to maintain full accounting records, or have your accounts audited, we find some clients prefer these to add credibility to their activities."

In Australia, Taylor formed a number of companies, including Fin Net Pty Ltd in 2006. It offered a range of financial services from "highly ethical, skilled and experienced professionals". One of the founding partners in the Fin Net enterprise was Colin Roderick McAskill. Three years earlier, McAskill had been sentenced to six months' jail in the Melbourne County Court after being charged by the Australian Securities and Investments Commission over several failed ostrich, beef and educational investment schemes that cost investors more than $6 million.

Though there is no suggestion of illegality on his part, what Taylor had discovered was the ability of the offshore financial system to deliver almost absolute discretion to his clients, and the inability of law-enforcement agencies to prosecute those who take advantage of that weakness.

The global arms-smuggling network feeds on this frailty, just as it feeds on the cast-off planes and pilots of the former Soviet Union. Adding to the intrigue over the seized flight 4L-AWA in Bangkok was that the Ilyushin-76 transport plane once belonged to a number of notorious international weapons dealers, including Viktor Bout - the so-called "merchant of death" and inspiration for the 2005 Hollywood movie Lord of War. The plane's current owner was an entity with headquarters in the United Arab Emirates but operated by Air West Ltd, based in Georgia. Air West had leased the aircraft to a New Zealand firm called SP Trading through a series

of bank accounts in Estonia and New York.

SP Trading had been incorporated only months earlier, on July 22, 2009, by Taylor's son, Michael Taylor, and appeared to have no other purpose. Its only shareholder was VicAm (Auckland), which shared an address with SP Trading at a rented Salvation Army-owned building in Auckland.

SP Trading's sole director was a rather naive employee of a Burger King fast-food

restaurant, a Chinese national called Lu Zhang.

Lu was the wife of an accountant who worked for the Taylors. She held the position of director in at least 50 other companies, many of them registered to the same Salvation Army-owned building at Level 5, 369 Queen Street, Auckland. She later told New Zealand media she had accepted about $NZ20 ($14.80) for each of her many directorships.

It further emerged that VicAm (Auckland) - in which Geoffrey

Taylor was the controlling shareholder until September 2009 - was also the sole nominal shareholder for more than 1000 other companies formed by the Taylor family in New Zealand.

Among these, Sumato Energy Group had appeared from nowhere in late 2008 to win a contract to ship 1 million barrels of Azerbaijani crude oil, worth $US75 million. Another New Zealand firm, also with no history of doing such business, won a lucrative public service contract in Romania.

After the plane was seized, the captain and his crew, four Kazakhs and one Belarusian, were arrested and charged. But the men pleaded their innocence and were eventually deported.

The Taylors, too, said they were blameless. In a press release issued in New Zealand by Ian Taylor - another of Geoffrey's sons - he explained GT Group's role was simply to incorporate and to act as a registered agent for SP Trading "at the request of one of our professional clients based in the United Kingdom". It was not responsible for and had no knowledge of what the company got up to. As no law was broken, the authorities had no choice but to agree.

There was little they could do, either, when only weeks later the GT Group was linked to the biggest money-laundering operation in US history.

Wachovia Bank - now a subsidiary of the global financial giant Wells Fargo - was fined $US160 million for helping to disguise the illegal origins of up to $US378 billion for Mexican drug lords.

The penalty was the result of a long US Drug Enforcement Administration investigation that uncovered multimillion-dollar transfers from Mexican currency exchange houses to the Wachovia sub-branch in Miami - money that was used to buy planes for cocaine shipments. Much of the money originated from the Sinaloa cartel, the fiercest protagonists in the Mexican drug war in which more than 28,000 people have been killed since 2007.

Last year police intelligence sources told Fairfax newspapers and the ABC's 7.30 Report that about half the cocaine now entering Australia was being sent from Mexico, and that the Sinaloa cartel was behind many of the shipments.

During the court proceedings it was alleged that four New Zealand firms registered by the GT Group - Keronol Ltd, Melide Ltd, Tormex Ltd, and Dorio (NZ) Ltd – helped launder about $40 million of the proceeds using Latvian bank accounts and Wachovia's London branch.

The US investigation provided a suggestion that the Taylor name was linked to an infinitely wider and more complex global network.

The sole director of each of the NZ firms was Stella Port-Louis, who has an address in the Seychelles. She appears as the director of more than 300 other New Zealand companies, many of them registered by one of the Taylors at Queen Street in Auckland.

In 2007, Port-Louis was singled out by US President Barack Obama – then a senator – for the way she headed up at least 100 companies in the US state of Wyoming when he warned of "serious problems confronting law enforcement as a result of minimal company

ownership information requirements".

Though the Taylor family was again found to have broken no laws, the matters drew attention to at least one of their other businesses.

Geoffrey Taylor was the founding chairman – and he and his family were major shareholders – of Sunseeker Energy (Australasia), a solar energy company that traded on the secondary sharemarket in New Zealand. At its height, the company – whose chief executive was McAskill, the Melbourne businessman sentenced to six months' jail in 2003 – was valued at $NZ18 million and it had a number of related entities. They included Sunseeker Energy (Australia) that operated from Melbourne and the Swiss-registered Sunseeker Energy Holding AG that operated out of Hong Kong, but was listed on the Frankfurt stock exchange in 1999 at a purported 1 billion euros.

In April last year, New Zealand authorities cancelled the public listing of Sunseeker Energy (Australasia) for what it described as "repeated infringement of the rules", its "failure to provide any information to the NZAX market regarding its business or operations" and the firm's "own admission ... that it is insolvent".

Geoffrey Taylor has recently changed his personal website to reflect the claim that he is now retired. The Australian-registered Global Finnet Pty Ltd – a continuation of the original Fin Net – has also posted a notice saying it would soon have new owners.

But the firm that carries Taylor's initials – the GT Group – continues to advertise its wares out of Vanuatu and continues to attract controversy.

The business magazine Barron's reported that late last month documents emerged out of London that linked a shell company called Bristoll Export, registered in New Zealand by GT Group, to a scandal that some commentators claim has the potential to be Russia's Watergate.

It centres on Russia's largest tax fraud, which occurred on Christmas Eve, 2007, when Moscow tax officials approved a same-day refund of $US230 million to a gang masquerading as representatives of Hermitage Capital, once the largest portfolio investor in Russia.

The money was funnelled through accounts at Citibank, JPMorgan Chase and Credit Suisse via a series of shell companies, one of which was allegedly Bristoll Export.

Four of the six people said by police to have pulled off the fraud are now dead. One had a fatal heart attack. A second fell from his balcony. The third plummeted out of a penthouse window.

The fourth was Sergei Magnitsky, a 37-year-old lawyer for Hermitage Capital who died in prison after he provided evidence that the money had been stolen by a ring of corrupt tax officials, police and career criminals.

But instead of prosecuting those Magnitsky accused, Russia's interior ministry charged him with the crime and exonerated the cops and the tax officials.

The case may have ended there, but Hermitage's London-based chief Bill Browder devoted himself to pursuing those he holds responsible for the original crime and Magnitsky's death. In English and Russian website campaigns, Browder has presented evidence that he says proves the tax heist was an inside job.

The case has become one of the biggest headaches faced by Russia's government because it is said to have the potential implicate many of those in authority. A recent commission, appointed by Russian President Dmitry Medvedev, found that police fabricated charges against Magnitsky.

New Zealand company records show that snuggled up inside Bristoll Export is yet another shell company that can be traced via Panama to an unrelated offshore banking firm in Cyprus operated by a former Russian diplomat.

Further evidence, perhaps, of an even more impenetrable labyrinth.

7.8 Use of Offshore Banks and International Business Companies, Offshore Trusts

CHINESE TAIPEI

Case Study-large deposits from overseas based entities and immediate withdrawals

248. The Anti-Money Laundering Division, FIU of Chinese Taipei, received a STR that described Wang was an employee of A Corporation, a listed company in the emerging stock market. Large deposits were made to Wang's bank account from overseas based companies and Wu, the responsible person of A Corporation withdrew the funds daily from the banking account just under the currency transaction reporting threshold on behalf of Wang's name to avoid the reporting requirement. The analysts of AMLD traced the flow of funds to identify the so called abroad companies and found one of the three paper companies was a subsidiary company of A Corporation in Virgin Islands and the other two were B Company (also registered in Virgin Islands and associated to Wang) and C Company (also registered in Virgin Islands and associated to Chang, an employee of A Corporation).

249. The funds originated from A Corporation's bank account. First, the funds were remitted into the banking account of the subsidiary company of A Corporation describing the funds as reinvestment. The funds were transferred into the bank account of B Company and then were transferred into the bank account of C Company. Finally, the funds were remitted into Wang's personal bank account and funds were withdrawn daily just under the reporting threshold by Wu on behalf of Wang to avoid the reporting requirement.

250. Wu was suspected of involving in irregular transaction for manipulating the stock price of A Corporation in the stock market, which was prohibited by the Securities and Exchange Act, and embezzling the gains from A Corporation.

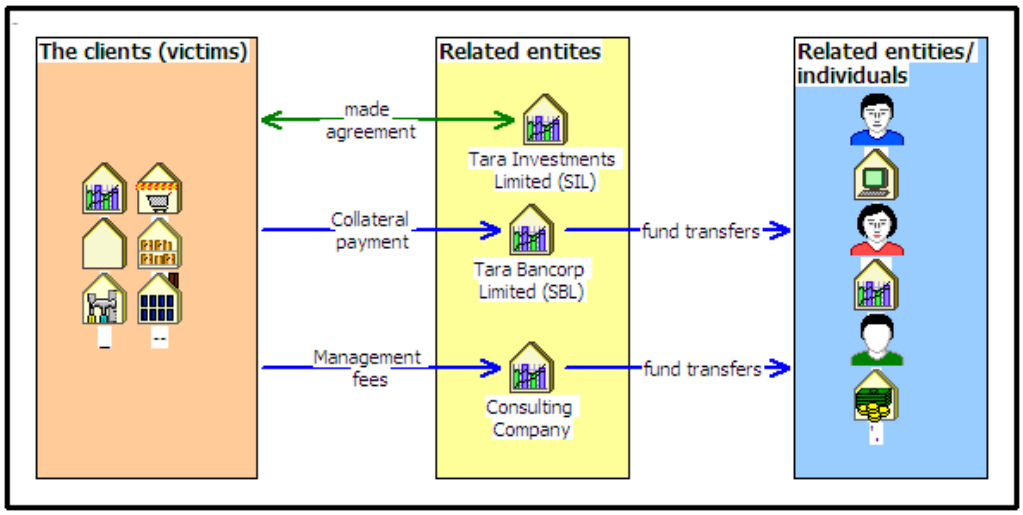
251. The AMLD disseminated the above information to law enforcement agency for further investigation. Law enforcement agents searched the residence of Wu and found huge amount of local and foreign currency valued more than 250 million NTD in a safe box. Significant currency seizures were made by prosecutor's office.

MALAYSIA

Case Study - Scam Activities Involving Off-Shore Entities

252. Tara Investments Limited (TIL) acts as an offshore financial consultant to secure an equity project funding for the clients who need financing for their proposed projects or contracts. TIL will enter into agreement with his client of which TIL will secure the required funds/financing for the clients' projects with profit sharing ratio of 30:70.

253. The clients were required to place collateral until the full repayment of financing, and to pay management fees after the disbursement of the funds. The management fees, ranging from RM50,000 to RM100,000 will be paid to another related consulting company while the collateral placed in the form of deposits in the non-operative account of Tara Limited (TL) maintained with a foreign bank, Bank XY. The clients have lodged the police reports claiming that they have not received the agreed financing funds even though management fees and collateral payment has been made. The reported loss is estimated amounting to more than RM8 million and the money trail analysis showed that the illegal proceeds has been layered into various related companies accounts including on-shore companies.



Flowchart showing a scam syndicate using offshore corporation to launder its illegal proceeds

7.9 Use of Nominees, Trusts, Family Members or Third Parties

AUSTRALIA

Case Study – use of cash to purchase multiple structured wire transfers and remitted offshore

254. Between June 2003 and September 2004 Mr C operated various companies. Mr C's companies purchased time/minutes from 5 large telecommunications companies and sold telephone calling cards to retail outlets where they were on-sold to the public. Mr C's companies each operated with a single telecommunications provider. Mr C's company purchased large volumes of time/minutes from the telecommunications provider and did not pay amounts due but continued to sell calling cards to the public, which were used and increased amounts due by Mr C's companies due to increasing amounts of time/minutes used by the public using the calling cards. When the first telecommunications company ceased to extend credit and cut of access by the calling cards, Mr C would use another of his companies to obtain time/minutes from a different telecommunications company. This modus operandi was used in succession on five occasions and total debts to the telecommunication companies exceeded AUD15,000,000.

255. Mr C and his associates collected funds from the resellers of the calling cards, cigarette shops, and small retailers, in cash and purchase telegraphic transfers in amounts less than the reporting limits. The funds were transferred to an associate's account in China where the funds were accumulated. The funds were then transferred from the associate's account in China, to Mr C's sister in law's account in Hong Kong. Mr C controlled the sister in law's account. After more than AUD900,000 was accumulated Mr C directed the funds be returned to Australia to a solicitor's trust fund account were a property valued at AUD2,200,000 was purchased in his wife's name.

256. Mr C was charged with money laundering offences and found guilty of structuring deposits in amounts less than the reporting limited and money laundering offences. He was sentenced to imprisonment of 2 years and six months.

INDONESIA

Case Study – unusual account activity

257. A foreign citizen (Mr. N) who had been convicted of a drugs case and was serving his time on prison in City B, was asking his girl friend Ms. Y (Indonesian citizen) to open an account in Bank A. After Ms.Y opened the account, the pass book and ATC card from Bank A was given to Mr. N.

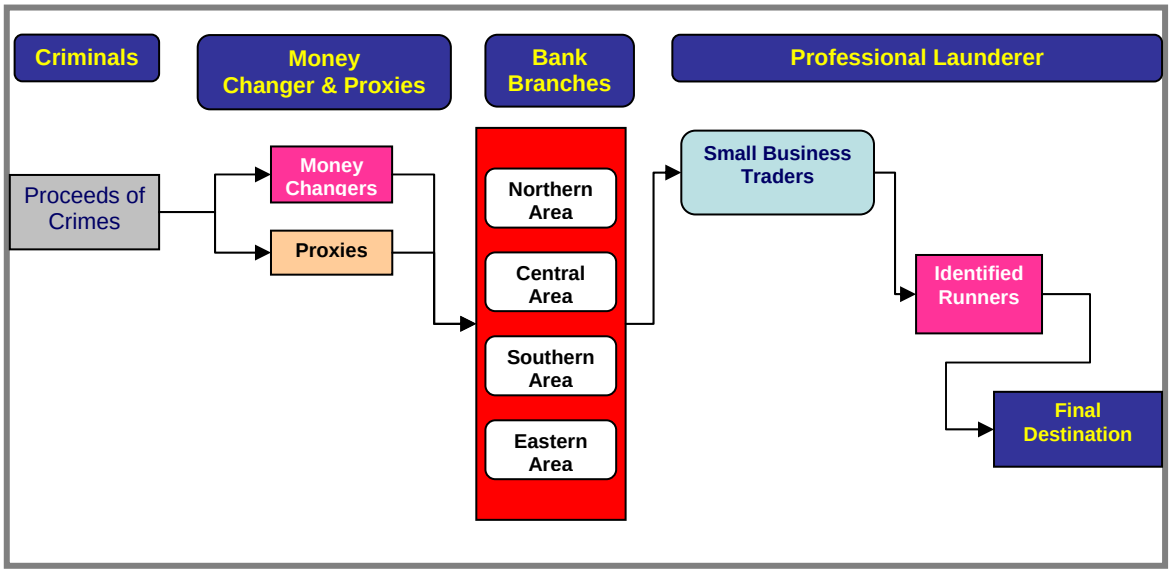
258. After the account was opened, there were records of funds flow coming in and out from Ms. Y's account. Based on the result of investigation by the Police, it was found that Mr. N was still running his drugs business despite his status as a prisoner. Also, from the investigation it was discovered that Ms. Y's account was used for receiving funds that were the proceeds of narcotic sales.

MALAYSISA

Case Study – Small Business Traders Acts as Professional Money Launderers

259. Money from illegal activities was laundered through individuals camouflaging behind the operation of small business traders mainly located at border towns. Profiling shows that the individuals are young and involved in cash generating business such as mobile phone businesses and computer spare parts. The bank accounts recorded a very high level of transactions since it was opened and appeared to be temporary repository account as immediate withdrawals were made once the deposits have been received.

The proceeds of crime are layered through initial transfer to the account by proxy, mainly related companies and individuals or money changers' accounts. The proxy and money changers, who are located at various locations, will then transfer the funds to the accounts of the small business traders, maintained at various banks. The funds either will undergo another layering process or will be transferred into the accounts of individuals and companies specified by the syndicate. The accounts maintained by the individual business traders are primarily to launder the proceeds of crime.



Flowchart showing the involvement of small business traders as professional money launderer

7.10 Use of Professional Services (Lawyers, Accountants)

AUSTRALIA

Case Study – use of professionals to disguise proceeds

260. A suspect, located in Fiji, fraudulently obtained a bank loan to develop a resort in Fiji. The suspect fraudulently obtained the loan for USD580,000 by representing himself as the beneficial owner of the borrowing company. The company was in fact a Fijian 'shelf company', of which the suspect was not the owner.

261. The bank, which had not previously lent to an entity from Fiji, requested the services of a Fijian solicitor to facilitate the loan. The suspect provided contact details for a Fijian solicitor; however, the suspect himself posed as the solicitor without the solicitor's knowledge. In the guise of the solicitor, the suspect provided a number of fraudulent documents to the bank including falsified financial statements and a forged receipt for registration of the mortgage for the proposed resort.

262. By the time suspicions were raised about the loan, AUD240,000 of the funds had already been transferred from Fiji to three separate entities in Australia, where they had been used to pay credit card debts and rental arrears.

263. The suspect was arrested on his arrival in Australia. He was charged under the *Criminal Code Act 1995* with money laundering resulting from a fraud committed overseas, and was sentenced to four-and-a-half year's jail.

AUSTRALIA

Case Study- use of professional advisors to set up complicated offshore company structures

264. The matter involved 5 company/stitching structures registered in St Vincent and Grenadines and the Netherlands which were controlled by MM that received company shares that were sold and transferred for value in an attempt to evade the payment of taxes.

265. A South African based company, GTLtd, sold a debt of approximately AUD11 million owed to it by a subsidiary, GTALtd, to CHFLtd, a company controlled by MM, for AUD1. GTALtd changed its name to A Limited, a company listed on the Australian Stock Exchange. CHFLtd sells AUD2.2 million of the debt to an Australian company BA Pty Ltd, an Australian company solely controlled by MM, for AUD1.5 million. No payment of AUD1.5 million to CHFLtd by BA is made. A Limited now owes BA Pty Ltd AUD2.2 million. MM becomes a Director of A Limited.

266. BA Pty Ltd receives 56 million shares in A Limited in consideration for AUD2.2 million debt owed. 5 stitching in the Netherlands, B, W, A, D and F, and 5 Companies in St Vincent and Grenadines, T, M, S, C and V, are set up by AH, a tax lawyer, on behalf of MM. 5 company structures are created by AH with each stitching owning 100% of the shares in one each of the St Vincent and Grenadines companies. MM enters into Deed of Charges with the stitching and companies.

267. BA Pty Ltd transfers the A Limited shares to the companies owned by the stitching. The shares were received to five accounts held with E Bank. No payment for those shares to BA Pty Ltd was made. As BA Pty Ltd did not originally make any payment for the debt from CHFLtd, both BA Pty Ltd and CHFLtd are controlled by MM, BA effectively received the A Limited shares for no consideration. The Court found that the sale was not arms length and that there was no change in the beneficial ownership of the A Limited shares.

268. 6 million A Limited shares were sold from the St Vincent and Grenadine company account for AUD925,000. Part of these funds were transferred to a Swiss account at U bank of St Vincent and Grenadine company C. 48 million shares in A Limited held by the St Vincent and Grenadines companies are exchanged for 1 million shares in a publicly traded company T. The T shares held in C account are sold for a total of Swiss Francs CHF 8 million. CHF3.2 million was transferred to BA Pty Ltd, CHF3.6 million was transferred to a Swiss account at U bank in the name of C, CHF295,000 was transferred to Art Galleries in Paris France and CHF456,000 was transferred to Holiday time share Resorts.

269. Between 1 January 2003 and 31 December 2007 BA Pty Ltd and MM received AUD14 million into their accounts.

270. MM purchased the following significant assets with the proceeds from the A Limited shares and T shares:

- Real Estate
- Vehicles
- Art Works
- Yacht
- Jewellery
- Membership at time share Resort

271. MM was found guilty of money laundering offences and sentenced to 8 years and 6 months imprisonment.

AUSTRALIA

Case Study – Accountants promote tax schemes - round robin.

272. The matter involves a Vanuatu-based tax evasion and money laundering scheme that operated to enable its participants to evade payment of company income tax and personal income tax in Australia.

273. Mr D was a client of Tax Agent O in Sydney. A tax scheme was promoted by Mr A to clients of Tax Agent O. Mr A operated an accounting practice and business advisory service in Vanuatu. Mr D owned and operated a business venture through a company structure, and Tax Agent O acted as the accountant and prepared the Financial Statements of the company and lodged the taxation returns with the Australian Taxation Office.

274. Mr D's company would transfer funds to one of Mr A's company accounts in Vanuatu. Mr A would deduct his fees from this amount, and transfer the balance of the funds to a second company account he operated. Mr A's companies were registered in the UK, USA, Ireland and Vanuatu. Mr D's company would then claim a tax deduction based on an invoice for services, which were never provided, which would reduce the taxable income of Mr D's company.

275. The balance of the funds held in Mr A's second company account would then be transferred back to Australia to a personal account controlled by Mr D. The second company or Mr A is a finance company and the funds are returned to Australia by Mr D drawing down a sham loam facility. These funds would either then be spent by Mr D, or transferred back to Mr D's company and recorded as a shareholder loan, or a repayment of an existing loan from the company.

276. More than AUD2,400,000 was remitted to Mr A's company accounts in Vanuatu by Mr D and associates.

277. D received 3 years and 1 month.

NEW ZEALAND

Case Study – Use of gatekeepers to open accounts

278. A Brazilian national and his de-facto partner are currently the subjects of arrest warrants in New Zealand following an international investigation into suspected money laundering. In late 2002, the accused and his family moved to New Zealand despite being on bail in Brazil for a number of criminal charges. Soon after their arrival, they opened a number of bank accounts, allegedly in the presence of an immigration lawyer. It has been established that during a three month period, over NZD3.5m was deposited into their bank accounts via international money transfer. In mid-2003, the accused and his family left New Zealand and have not yet returned. In their absence however, 40 accounts were opened by the immigration lawyer on their behalf. The lawyer is also suspected of transmitting funds through his trust account, as well as witnessing Statutory Name Change documentation for the accused and his family. The immigration lawyer is currently facing money laundering charges.

7.11 Use of Internet (Encryption, Access to IDs, International Banking)

SINGAPORE

Case Study – internet accounts, accounts based in tax havens

279. T incorporated 2 companies in the British Virgin Islands and set up bank accounts for the 2 companies in Singapore and another Asian jurisdiction. All the accounts set up in Singapore could be controlled by the internet. These accounts in Singapore were used to receive proceeds from scam victims overseas.

280. The perpetrators of the scam sent out emails in the name of an organisation in Europe. The perpetrators informed the clients of the organisation that they still owed the organisation monies for services rendered, and requested the clients to send the monies to one of the accounts in Singapore. Monies received in the Singapore accounts were remitted out to bank accounts overseas within days of receipt. Within 4 months more than USD2,000,000 passed through the accounts.

281. T claimed that it was his friend, S, who approached him to conduct the acts and that all instruments for the control of the accounts were handed to S. T claimed that he received USD20,000 for his work.

282. T was prosecuted for 2 ML charges relating to the facilitation of the transfers of criminal proceeds. T was convicted and sentenced to 8 months imprisonment for money laundering.

7.12 Use of Violence and Coercion

PHILIPPINES

Case Study – multiple transactions, remittance agents

283. On 17 April 2009, LY was kidnapped by JB, MG, and JM for the purpose of extorting ransom from his family. The total amount of PHP1,019,220 in addition to several pieces of jewellery and one unit of cellular phone were actually delivered to the suspects in exchange for the release of the victim.

284. The total ransom money of PHP1,019,220.00 consisted of PHP300,000.00 remitted by KY (sister of the kidnapped victim) through WU remittance agents per instructions of the respondents, and PHP719,220.00 cash handed over by KY to one of the respondents on 3 March 2008.

285. There was no CTR on the suspects. However, AMLC received 18 STRs filed by WU remittance agents in connection with the PHP300,000 ransom remitted by KY between 18 February 2008 and 2 March 2008 thru WU remittance agents (DA5, US, and MJ companies):

Remittance Agent	***Remitter***	***Date Remitted***	***Amount Remitted PHP***	***Recipient***	***Date Collected***
DA5	KY	18 Feb 08	20,000	JB	18 Feb 08
US	KY	18 Feb 08	50,000	MG	Not consummated due to **presentation of fake ID**; refunded to KY on 19 Feb 08
US	KY	18 Feb 08	100,000	JB	Refunded to KY on 19 Feb 08 without being paid to recipient
MJ	KY	19 Feb 08	40,000	MG	Transaction cancelled due to **presentation by recipient of fake SSS ID**; refunded to KY on 20 Feb 08
MJ	KY	19 Feb 08	50,000	MG	Transaction cancelled due to **presentation by recipient of fake SSS ID**; refunded to KY on 20 Feb 08
MJ	KY	19 Feb 08	50,000	JB	19 Feb 08
MJ	KY	19 Feb 08	10,000	JB	19 Feb 08
MJ	KY	20 Feb 08	50,000	JB	20 Feb 08
MJ	KY	20 Feb 08	40,000	JB	20 Feb 08
MJ	KY	26 Feb 08	20,000	JB	26 Feb 08
MJ	KY	26 Feb 08	20,000	JB	27 Feb 08
MJ	KY	26 Feb 08	30,000	JB	26 Feb 08
MJ	KY	29 Feb 08	30,000	JB	29 Feb 08
MJ	KY	2 Mar 08	30,000	JB	2 Mar 08

7.13 Association with Corruption

CHINA

Case Study – PEPS, use of family members accounts for corruption proceeds

286. On 28 December 2009 the verdict of Deng money laundering case was announced in the last instance by the Intermediate People's Court of Fuzhou, Fujian Province. Found guilty of money laundering, Deng was sentenced to 3 years' imprisonment and a fine of RMB 50,000 Yuan.

287. Chen, the former sub-prefect of Yongtai County, Fujian Province, deposited RMB 4.1 million Yuan to the bank account opened in the name of Deng, the brother of his wife, between 2006 to September 2008. In July or August 2008, for fear of being investigated for his involving in an illegal project of land development, Chen handed the bank book to Deng and asked Deng to disguise the money in his own name. In September, Chen ordered Deng to transfer the money to the bank account of Chen J, the vice manager of Yongtai Longxiang Taxi Co. Ltd. After investigation, it was found there were RMB 1.41 million Yuan among the transferred money of 4.1 million Yuan originated from Chen's briberies.

PAKISTAN

Case Study – PEPs – assets held not comparable to known source

288. A government official through corruption and corrupt practices amassed a large amount of assets. To hide the origin of proceeds of corruption he remitted an amount of INR10.000 (M) to his brother in UK through alternative remittance methods (Hawala/Hundi) from time to time. He then opened a number of accounts at various banks either in his own name or joint accounts with his close relatives and received the corruption money through different exchange companies purported to be remitted by his brother from UK. The brother of accused did not have any legitimate source of funds to make these remittances, as he was receiving social security allowance in UK. The accused was charged for corruption and corrupt practices.

7.14 Criminal Knowledge of and Response to Law Enforcement / Regulations

AUSTRALIA

Case Study – defeating reporting requirements

289. The manager of a foreign exchange business received a jail sentence after being convicted of providing false information and assisting another suspect to avoid AML/CTF reporting requirements.

290. The suspect visited the manager's foreign exchange business in Sydney to purchase AUD43,000 worth of traveller cheques, with the cheques to be issued in US dollars (USD). During the transaction the suspect paid AUD14,000 as a 'deposit' for the purchase, and then indicated that he did not intend to fill out any forms associated with the transaction. A meeting was arranged between the suspect and the owner/manager of the foreign exchange business. During this meeting the suspect and the manager negotiated an agreement in which the suspect received a lower AUD to USD exchange rate for his purchase of the cheques. In return the manager agreed to circumvent the reporting requirements normally associated with such a transaction by not submitting a significant cash transaction report (SCTR) to AUSTRAC.

291. The suspect returned to the foreign exchange business a few days later, where he was instructed to provide names for the traveller's cheques and asked to fill out purchase records and sales receipts for the purchase. The suspect completed the documents under a number of different names. The suspect purchased a number of traveller's cheques worth USD100 and USD1,000 each using various different names and addresses. In total, the suspect purchased cheques worth USD26,500, after paying the exchange business AUD43,600 cash.

292. Following a law enforcement investigation, the manager and his foreign exchange business were prosecuted for providing false information to AUSTRAC and avoiding

reporting requirements. The manager was sentenced to 10 months jail and his foreign exchange business was fined AUD100,000.

CHINESE TAIPEI

Case Study –Response to regulations and involvement of bank staff

293. Manager Mr. A and Assistant Manager Mr. B in the credit union X are experienced employees in the field of financial business. According to the provisions of the Money Laundering Control Act, financial institutions are required to establish AML/CFT guidelines and procedures of reporting STRs and CTRs. Mr. A and Mr. B are in managerial level of the credit union X and carry on the responsibility for instructing the staff to comply with the mentioned AML/CFT guidelines and related procedures. They are fully aware whenever the customer's financial transaction triggers the indicators of the AML/CFT guidelines or the amount of the cash transaction exceeds the threshold of NTD500,000, and then they should compile CTRs or STRs to report to AMLD.

294. With the intention of assisting a fraud syndicate to conceal the proceeds of crime (POC) and launder the illegal funds, the couriers of the fraud group gave Mr. A or Mr. B the funds derived from fraud, Mr A and Mr B followed the instruction from the fraud group to deposit or remit illegal funds to 10 more specific banking accounts. The characteristics of these financial transactions met STRs or CTRs reporting indicators/requirements:

- A client frequently transfers huge amounts of funds within the relevant accounts;
- A client requests to proceed other kind of financial transaction with cash transaction;
- The amount of each deposit and withdrawal in a banking account is similar and the transactions are close in occurrence date;
- The amount is found apparently incommensurate with the client's identity or income and irrelevant to the attributes of his/her profession;
- A client is found to have frequently deposited/withdrawn large amounts into/out of a specific account for others or through different third parties.
- A client frequently deposited into or withdrawn out of an account in amounts marginally below the threshold for declaration

295. In addition to assist dealing with the illegal funds, they intentionally did not report any STRs and CTRs and conducted some transactions without keeping records. Their acts have successfully disguised the POC for the fraud group which amounted more than NTD334 million. When the fraud group was detected and the suspects were arrested by police, Mr. A and Mr. B's criminal offense was uncovered by the police and the Financial Supervisory Commission.

OPEN SOURCE

Case Study – Hired Savings Accounts

India: Terror groups hire savings accounts to launder money
Unattributed article: 'Terror groups hire savings accounts to launder money'

7 February 2011 The Pioneer
Starting a new trend in hawala transactions, terrorist groups are using savings bank accounts of individuals for laundering money used for subversive activities. This has come to the notice of intelligence agencies through the suspicious transaction reports (STRs) of the Financial Intelligence Unit-India (FIU-IND).
An intelligence report has stated that terror modules deposit cash in these accounts and their operatives withdraw it through ATMs at faraway locations. The terror groups pay cash 'incentives' to such account holders, the report added.
According to FIU-IND, a report indicating such suspicious transaction has been received from a savings account each in Kerala and Uttar Pradesh. In the case of Kerala, reports showed that deposits below Rs 50,000 were made into the particular account from various branches in the State and Maharashtra. The money was immediately withdrawn through ATMs in Hyderabad. Inquiries revealed that the account holder had gone to one of the Gulf countries for employment and had started his own business in flowers and curtains in Kerala following his return.
"Analysis of two bank accounts belonging to the person and his son revealed remittances from Gulf and immediate cash withdrawals from an ATM in Hyderabad. Investigations showed business connections with an accused, who was in police custody for involvement in a pipe bomb case. The money was withdrawn from a Hyderabad-based ATM by an associate of the accused and was allegedly used to facilitate terrorist activities," the FIU-IND report said.
Likewise, a suspicious transaction report was received from the bank of a person residing in western Uttar Pradesh. This person, while opening the account, had declared his profile as self-employed (trader) with gross annual income of Rs 3 lakh. But the account details registered small cash deposits from various locations - including Jammu, Srinagar and Maharajganj, among other places - and the proceeds were withdrawn immediately from ATMs located in Uttar Pradesh and Delhi.
This was considered suspicious by the bank, which immediately reported the matter to authorities.
Inquiries by intelligence agencies revealed that the account holder owned a factory at Jammu and had business dealings in Srinagar. It was also revealed that one his relatives residing in Uttar Pradesh had links with terrorists and had even undergone imprisonment in Guwahati jail.
The number of STRs disseminated by the FIU-IND to intelligence agencies has increased over the years from a meagre 49 in 2007-08 to 90 in 2008-09 and 362 in 2009-10. Likewise, requests for information on STRs by intelligence agencies from the FIU-IND have also increased from 87 in 2007-08 to 190 in 2008-09 and 226 in 2009-10.
An official of the FIU said that transactions in the range of Rs 2 lakh to Rs 10 lakh had been noticed in the suspicious transactions and a portion of the amount is paid to the savings bank account holder as rent. "The transaction amount is apparently kept low to evade detection by security agencies. This also serves the purpose of the terror groups that work in modular fashion for carrying out subversive activities," an official of the FIU said.
The FIU-IND assists intelligence agencies in combating financing of terrorism by dissemination of STRs and by providing information specifically requested by the intelligence agencies. The FIU-IND also shares information to foreign financial intelligence units on suspected money laundering and terrorist financing cases.

7.15 Currency Exchanges and Cash Conversion

AUSTRALIA

Case Study – bribery, false identification, structuring, conversion to traveller's cheques

296. A suspect involved in the importation of cocaine into Australia deliberately avoided AML/CTF reporting requirements in an attempt to smuggle drug money out of the jurisdiction. Over a two-month period the suspect used various methods to launder the illicit cash proceeds.

297. In one instance the suspect attempted to purchase a large number of traveller's cheques at a currency exchange outlet. The suspect's intended to purchase several travellers cheques, each in values below AUD10,000, to avoid reporting requirements. During this transaction the suspect was informed of the need to complete a significant cash transaction report (SCTR) as the total value of the cheques was greater than AUD10,000; however, the suspect declined to do so. Instead, the suspect left AUD 14,000 cash as a 'deposit' to persuade the currency exchange employee to conduct the purchase. The employee subsequently fulfilled the suspect's request.

298. The suspect visited at least three currency exchange outlets and converted large sums of Australian dollars into traveller's cheques. On each occasion the suspect refused to complete the SCTR forms and did not sign the travellers cheques himself, enabling other recipients to cash them. The suspect also used a false name to sign the purchase record. In total the suspect purchased AUD96,000 worth of traveller's cheques.

299. The suspect divided the cheques into 16 batches, wrapping each batch in carbon paper inside a greeting card, and attempted to mail them to various destinations in the United States. The suspect disguised some of the envelopes to suggest that they came from a corporation.

300. The suspect was sentenced to thirteen-and-a-half year's gaol on importing cocaine, money laundering and conspiracy to import cocaine.

CHINESE TAIPEI

Case Study – Counterfeit currency

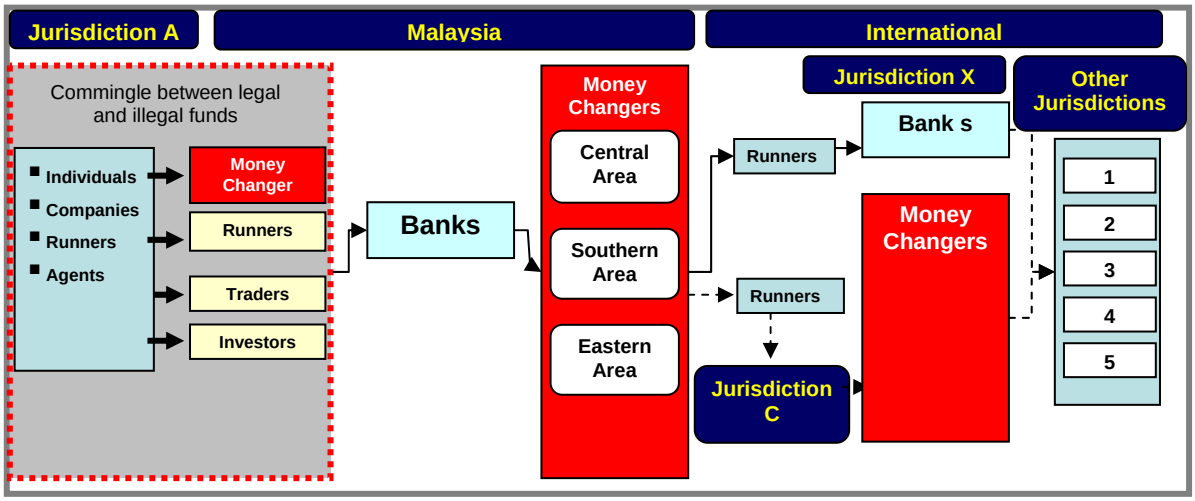
301. The AMLD received a STR from Bank A that described Lin deposited 7,000 fifty-dollar coins tainted with greasy dirt smell on November 13 of 2008, and beginning from April 14 of the same year, Lin successively deposited various amount of fifty-dollar coins 37 times into his banking account from different branches of this bank and usually withdrew immediately from ATR after the deposits. The transaction types alerted the bank to file an STR. The AMLD also received another STR from Bank B for the same subject in May of 2009 that described "Lin frequently deposited large amount of fifty-dollar coins into his banking account in person and usually withdrew from ATM at the same day, and each deposit and withdrawal were similar in amounts and close together in occurrence."

302. The AMLD checked Lin's background, occupation and criminal records to suspect he was very possible a member of counterfeiting currency organization and disseminated this information to law enforcement agency for further investigation. Law enforcement agents identified that the counterfeiting organization used its members to deposit fake coins mixed with genuine coins by the ratio of 1:4 into banking accounts. Once the fake coins were deposited into the bank account, the funds were withdrawn from an ATM.

MALAYSIA

Case Study - Money Changers as Conduit for Money Laundering Activities

303. One of the methods of money laundering detected is the involvement of money changers as conduit for money laundering syndicates operating in Malaysia and neighbouring jurisdictions. The runners/agents for the syndicates will smuggle the proceeds of crime into Malaysia where the cash will be deposited into the money changers' accounts via over the counter transactions at a several banks operating at the border towns. The deposits remain in the accounts for a very short period of time. The runners will withdraw the cash and the physical cash will be smuggled to another neighbouring jurisdiction, Jurisdiction X. The monies will be wired to other jurisdictions as instructed by the syndicates. The investigation showed that some of the funds may initially be transferred to a transit jurisdiction before going to Jurisdiction X. The wire transfers were also done through unauthorized operators.



Flowchart showing money changers as conduits to move cash across borders

7.16 Currency Smuggling

AUSTRALIA

Case Study – Use of Airline Staff

304. A money laundering syndicate was suspected of using airline pilots and crew to smuggle currency out of Australia to Vietnam, The money was suspected to be the proceeds of drug sales in Australia and payments for drugs imported into Australia.

305. The money was given to the pilots by owners of several remittance dealers, and authorities suspect that the money laundering network used pilots to smuggle more than AUD10 million from Australia to Vietnam over an 18-month period.

306. Searches of AUSTRAC's information database identified that one of the suspect Vietnamese pilots had previously declared AUD19,000 on an international currency transfer report (ICTR). Since this declaration, the pilot had made no further reports of currency being carried into or out of Australia.

307. The pilot was arrested after attempting to smuggle AUD500,000 out of Australia without declaring it. He pleaded guilty to charges of money laundering under the *Criminal Code Act 1995* and was eventually jailed for four-and-a-half years for smuggling a total of AUD6.5 million out of Australia.

7.17 Use of Credit cards, Cheques, Promissory Notes

AUSTRALIA

Case Study – large turnover and use of credit

308. AUSTRAC received a large number of transaction reports from regulated entities about the financial activities of a suspect in an embezzlement case. AUSTRAC received a total of 26 suspect transaction reports (SUSTRs) about the suspect, largely in relation to his history of sending multiple low-value international funds transfer instructions (IFTIs) to Nicaragua. The IFTIs were all sent via a money transfer agency, and the vast majority of transactions were for amounts of less than AUD1,000. It is suspected these transactions all related to internet gambling activity.

309. The SUSTRs also indicated other suspicious activity in the suspect's accounts, including an unusually large turnover on his credit card account – AUD808,000 in a 12-month period. Most of the charges on his credit card were to internet gambling companies. The reports also indicated that, with the exception of a AUD30,000 cash deposit, all of the deposits into the suspect's account were made in cash amounts just under the D10,000 transaction reporting threshold. Further, these deposits were made mainly via various post offices and included multiple deposits on the same day. The suspect was also the subject of a number of significant cash transaction reports (SCTRs) relating to another of his bank accounts. This particular account also appears to have been utilised for the suspect's money laundering activities.

310. Law enforcement investigations revealed that, in total, approximately AUD1.2 million had moved through the suspect's bank accounts. A search warrant was carried out and evidence was uncovered which indicated that the suspect had embezzled over AUD500,000 from his employer over a two-year period.

7.18 Structuring and Smurfing

AUSTRALIA

Case Study – structuring deposits and withdrawals

311. A law enforcement investigation resulted in two people being arrested and charged with two counts each of structuring transactions under the *Financial Transaction Reports Act 1988* (FTR Act).

312. The investigations revealed that in a one-month period the suspects had conducted 19 separate cash withdrawals from a joint bank account, with each withdrawal structured to fall beneath the AUD10,000 cash transaction reporting threshold. Within the next eight days, the suspects made a further 125 separate cash deposits – each worth less than AUD10,000 – into a joint account at a different bank.

313. Bank staff at two different branches documented their suspicions about the pair's actions in suspect transaction reports (SUSTRs) submitted to AUSTRAC. The SUSTRs detailed obvious structuring of cash transactions to fall below the AUD10,000 reporting threshold, and the reports prompted law enforcement officers to initiate an investigation into the suspects, and ultimately charge them under the FTR Act.

314. The investigating officers executed search warrants on the homes of the suspects and worked with the Office of the Commonwealth Director of Public Prosecutions to restrain

approximately AUD1.18 million under section 17 of the *Proceeds of Crime Act 2002* (Cwlth). The funds were restrained on the grounds that they were used by the suspects to commit the structuring offences.

315. Both suspects pleaded guilty to structuring and appeared in court two months later for sentencing. Both were ordered to forfeit approximately AUD1.18 million and were each released on AUD5,000 good behaviour bonds for three years.

CHINESE TAIPEI

Case Study – false invoicing and structuring

316. Mr. A is the chairman of the technology company X whose stocks are traded on the stock market. Company Y and Z in another jurisdiction are Company X's subsidiaries and their profit should be recognized as Company X's revenue according to the related accounting regulations. With the intention of embezzling the profit of Company X, Y, and Z, Mr. A commanded his employees Mr. B and C to set up two shell companies, OBU accounts and domestic bank accounts for the shell companies. False transactions with Company X, Y, and Z were conducted to move the payments from the three companies.

317. Once the payments were remitted to the shell companies' OBU accounts, Mr. B or C would transfer the money to their domestic bank accounts which were under Mr. A's control. Then Mr. A withdrew the money, which were the funds from Company X, Y, and Z, in amounts of cash under the threshold of CTR reporting (the threshold is NTD500,000). Mr. A used those money for investing on bonds or mutual funds or hided it in the vaults at home and in the banks.

318. Mr. A's intensive cash withdrawing transactions triggered the STRs reporting red-flag indicators, and then financial institutions immediately reported to Anti-Money Laundering Division (AMLD), FIU of Chinese Taipei. After investigating, AMLD suspected Mr. A of embezzling the money of Company X, Y, and Z, and then disseminated the information to Investigation Bureau, law enforcement agency in Chinese Taipei, for further investigations. In the process of legal operations, the special agent found more than NTD510 million, USD 373,820, RMB913,200, HKD500,000, and JPY282,000 in cash, as well as a huge amount of valuable security, bonds, and mutual fund certificates in the vaults at home and in the banks accounts which were seized. In 2010, Mr. A was prosecuted for violating Security Transaction Act and Money Laundering Control Act.

7.19 Wire Transfers

AUSTRALIA

Case Study – structured wire transfers

319. A law enforcement investigation into a drug manufacturing syndicate led to the arrest of a suspect associated with outlaw motorcycle gangs.

320. Australian law enforcement officers received information from New Zealand counterparts detailing numerous international funds transfers from New Zealand into Australia, all in amounts of less than AUD10,000. In total, the transfers were worth more than AUD260,000, and were sent in two separate one-month periods to a variety of individuals in Australia, some of which were involved in outlaw motorcycle gangs. The incoming transfers were apparently sent by three separate individuals holding Australia-issued identification.

321. Further investigation by authorities revealed that the funds were actually sent by just one individual, who moved from one bank branch to another and conducted the cash-based transfers using false identification.

322. This suspect was subsequently arrested in Australia and charged with possession of unregistered and prohibited firearms.

AUSTRALIA

Case Study – wire transfers, common remitters and addresses

323. A law enforcement investigation into a suspected illegal drug operation led to the restraint of a number of properties and the seizure of 1550 cannabis plants and a substantial amount of money and other assets valued in total at approximately AUD10 million.

324. The investigation began after AUSTRAC disseminated information to a law enforcement agency which identified a series of local and overseas funds transfers worth AUD3.2 million over a two-year period. The activities consisted mainly of large cash deposits made by ten suspects connected to thirteen common addresses in Victoria. These same suspects also sent numerous high-value international funds transfers (IFTIs) to common beneficiaries in New Zealand. This financial activity was inconsistent with the stated occupation of the suspects, that is unemployed, student or in retail.

325. The investigation revealed that the suspects had purchased properties in Australia and used them to grow and cultivate cannabis plants. The funds generated by this activity were used to purchase additional properties in Australia and New Zealand.

326. The suspects were charged with cultivating, trafficking and possessing commercial quantities of drugs, conspiracy to cultivate, traffic and possess a large quantity of drugs and knowingly dealing with the proceeds of crime and theft.

7.20 Purchase of Valuable Assets

CHINA

Case Study –use of family members to purchase assets

327. On 24 August 2009 the verdict of Bao concealing and disguising criminal proceeds case was announced in the last instance by the Intermediate People's Court of Wenzhou, Zhejiang Province. Bao was found guilty of concealing and disguising criminal proceeds and was sentenced to imprisonment of 5 years and a half and a fine of RMB100,000 Yuan.

328. Gao, Bao's mother, fraudulently raised funds of over RMB116 million Yuan by operating real estate and bonding companies from 2003 to August 2007. Clearly knowing his mother's money was the proceeds of financial fraud, Bao helped Gao purchase 6 properties in his own name with the illicit money. Then Bao sold 2 of them and gained 780,000 Yuan, and Gao bought a Lexus worth 380,000 Yuan for Bao. Moreover, Bao often invested Gao's illicit money in real estates and new shares, etc, and gained the illicit proceeds of over RMB9.4 million Yuan.

NEW ZEALAND

Case Study – Refining and purchasing bank bonds

329. Over an 18-month period, an unemployment beneficiary carried out numerous cash exchanges at his local bank. He claimed the money had been made from selling food at

festivals. Following surveillance on his address, search warrants located over 2kg of dried cannabis, electronic scales, deal bags and a purpose-built cannabis growing room. The financial investigation estimated that the offender had illegally obtained almost NZD70,000 from cannabis sales and had exchanged approximately NZD30,000 cash from low to high denominations. He had also purchased USD4,000 cash and around NZD7,000 worth of bonus bonds.

OPEN SOURCE

Case Study – income does not support lifestyle

US: Eight suspects indicted in drug-distribution, money-laundering ring
Article by Peter Krouse: '8 indicted in big drug-distribution, money-laundering ring'
13 May 2011 The Plain Dealer

Jimmie Goodgame lived in an $800,000 house, controlled bank accounts with more than $1.5 million in deposits and had title to dozens of luxury cars, federal prosecutors said, but he didn't have the income to justify his lifestyle.

Goodgame, 41, who lives in a gated community in Solon, was among eight people indicted Thursday by a federal grand jury in connection with a distribution ring that sold massive amounts of heroin in Northeast Ohio.

He is accused of laundering money for drug dealers. Addonnise Wells, 28, of South Euclid, and Mario Freeman, 27, of Garfield Heights, are accused of leading the drug distribution network.

Local police had their suspicions about Goodgame for years, investigators said, but only recently were they able to unmask him as the suspected mastermind of a scheme to launder drug money by purchasing or leasing cars.

The investigation required the cooperation of the FBI, Internal Revenue Service and local police. Investigators used wiretaps, surveillance, vehicle stops and document analysis to build their case. The IRS subpoenaed bank records and sought other documents to show that suspected drug dealers driving Porsches and Cadillacs had no legitimate sources of income.

"If they don't have a job, you have to start looking at their mode of operation," said Tracey Warren, assistant special agent-in-charge of the IRS division based in Cincinnati. "Where do they go? Who do they meet?"

That paper trail, combined with piecing together many seemingly unconnected events, allowed investigators to dissect a scheme in which Goodgame took drug money and used it to buy or lease more than 40 luxury cars, including Range Rovers, BMWs and a Maserati, officials said.

An important piece of the case fell into place in March 2007 outside Chicago when the Illinois Highway Patrol pulled over a car for a traffic violation and found more than $500,000 in cash hidden away in heat-sealed containers. The vehicle was registered to Goodgame, investigators said.

There were at least 10 other traffic stops in Northeast Ohio involving cars registered to Goodgame, his wife or companies they owned, said assistant U.S. Attorney Ed Feran, who is prosecuting the case. The stops resulted in seizures of money or drugs.

On Nov. 5, 2008, Westlake police officers seized a car in a heroin bust that was leased to a Goodgame-owned shell company called Washington Industries Inc., investigators said.

Authorities then tapped the phones of Goodgame, Wells and Freeman. Prosecutors say Wells and Freeman sold heroin from houses on East 125th and East 127th streets in

Cleveland and used an apartment on Edgewater Drive in Lakewood to stash their dope.
Wells sent tow trucks to Houston to bring back vehicles packed with heroin, according to an FBI affidavit filed in U.S. District Court in Cleveland. A source working with investigators said he helped take apart 17 vehicles for Wells, with each vehicle containing between six and 22 pounds of heroin, according to the affidavit.
Agents conducted a "sneak and peak" raid on the stash house in Lakewood on Feb. 16 this year and seized more than a pound of heroin and more than $8,000 in cash. A "sneak and peak" raid, which must be authorized by a judge, allows police to search a house without notifying the suspect.
After selling their drugs, dealers often look for some way to unload their cash. A bank is often out of the question because large deposits can come under scrutiny. So they can hold on to their money and risk it being confiscated, or they can buy something, such as cars or real estate.
The FBI affidavit suggests Wells bought homes and put them in the names of relatives.Drug dealers sometimes start cash businesses, such as used-car lots, bars and barber shops.
Using someone like Goodgame is another way to go, prosecutors said. The dealers can get their hands on a luxury car. And if they get busted, the car can't be seized because it belongs to somebody else.
"Luxury cars and drug traffickers go together like peanut butter and jelly," Feran said.
Prosecutors say Goodgame deposited more than $1.5 million into accounts he controlled. He would then buy or lease the vehicles and turn them over to the drug dealers.
Goodgame had at least 14 cars registered in his name in 2010, with another 26 or more registered in the name of his companies, J&G Enterprises I LLC and Washington Industries, investigators said.
Other cars were registered in the name of his wife, Stacy, 40, and her company, Goodgame Heavenly Cleaning. The cleaning business was legitimate and generated income but was still used to help launder drug money, Feran said.
Goodgame had been suspected of laundering drug money for years as a result of prior investigations, said Pete Bickmore, who heads the criminal division of the local FBI office. But he was never prosecuted.
"Money laundering investigations are hard to prove," he said.

7.21 Use of Foreign Bank Accounts

AUSTRALIA

Case Study – tax fraud, use of overseas bank accounts

330. This is an investigation into an individual involved in a large scale tax fraud. It is alleged that the value of the fraud is approximately AUD1.96 million. The focus of the investigation was a registered tax agent, who prior to departing Australia, operated a business in Victoria. The individual allegedly submitted tax returns in the names of over fifty false identities and obtained refunds in those false names.

331. The tax refunds were transferred to accounts in the name of the individual's business from where they were then distributed to a number of other accounts he controlled. These accounts were held in the name of various companies and included the use of a self-managed superannuation fund which received approximately AUD1.5 million. The transactions were undertaken as domestic transfers conducted via the internet.

332. Analysis of AUSTRAC data indicated that he transferred in excess of AUD6.9 million out of Australia to Turkey via international funds transfers. These transfers varied in amounts and ranged from AUD8,000 to AUD1.6 million each and were ordered in the name of the individual using internet banking facilities. The self managed super fund account was one such account utilized to send funds out of Australia to Turkey.

333. The bulk of these funds were remitted to two accounts held in his name in Turkey. It is alleged that he further transferred funds from the Turkey accounts to accounts held in Cyprus. Of the funds sent offshore only small amounts involved cash, suggesting that the wire transfers were being funded by domestic transfers conducted over the internet that had previously been sent to his accounts from various real or front companies.

7.22 Use of False Identification

AUSTRALIA

Case Study – creation of false passports

334. A law enforcement investigation foiled the activities of a suspect creating false passports in his family home, and using them to launder money overseas.

335. Law enforcement officers conducted a search of suspect A's home, where he lived with his wife and child. The search revealed AUD152,000 cash in a box in a cupboard, and a CD-ROM containing software for producing false Korean and Chinese passports. They also found two drivers licences bearing different names but featuring photographs of the same applicant. The search also found several passport-sized photographs of different individuals.

336. Suspect A told authorities that the cash was being stored on behalf of another individual, suspect B, who was subsequently charged with offences relating to the use of false accounts. Further investigations revealed that the false bank account was opened under one of the names used by suspect A, using one of the false passports discovered in suspect A's house. Over a three-month period, AUD97,000 had been deposited into this account. During the same period, suspect A had conducted nine funds transfers from this account to an Indonesian account, worth a total of AUD89,100.

337. Suspect A was sentenced to four years gaol for offences contrary to the *Crimes Act (NSW) 1900* and the *Criminal Code Act (Cth) 1995*.

PHILIPPINES

Case Study – Use of false ID to open accounts and foreign cheque deposits

338. An STR has led to the discovery and apprehension of a syndicate headed by a husband and wife team who had used false identification documents to open accounts in different branches of various banks located in several provinces.

339. Mr. C., the mastermind of this fraudulent activity was using several aliases to open several bank accounts by initially depositing USD 100.00 and the dollar-denominated checks which were payable to the persons whose real names the perpetrator usurped by the use of fraudulent or fake identification documents. The same was true of his spouse Mrs. C. who also used fake IDs in depositing the foreign checks to her own newly-opened account. These checks were reported by the real payees as missing or stolen in transit.

340. In all, the husband and wife team were able to open twelve (12) different accounts under different aliases in various amounts ranging from USD100.00 (PHP5,000.00) to USD28,000.00 (PHP1,500,000.00).

341. Alerted by the reports of the real payees of the missing stolen checks one of the banks had identified that one of the checks deposited by Mr. C had in fact been declared missing or stolen and flagged the account of Mr. C with said bank. Subsequently, other checks reported as missing or stolen were identified as the same checks deposited in the accounts of either Mr. C or Mrs. C with other branches of the same bank who had used different identification documents to open them.

342. Finally, one of the branch managers of the said bank identified Mr. C to be the same Mr. C who was attempting to open an account with his branch using fraudulent identification documents. The branch manager allowed the account opening then filed an STR. The law enforcement authorities were alerted and the perpetrators were eventually arrested in an entrapment operation.

7.23 Nigerian Scams/Lottery Frauds/Inheritance Scams/Scams

AUSTRALIA

Case Study – Nigerian Scams

343. AUSTRAC received 40 suspect transaction reports (SUSTRs) detailing the activities of an accountant, who is believed to have fallen victim to a Nigerian fraud scheme.

344. The suspect sent most of her funds to Nigeria using international funds transfers (IFTIs) conducted through various money transfer agencies. The transfer amounts varied considerably, but were generally in amounts of less than AUD10,000. The suspect sometimes travelled long distances from her home to conduct the funds transfers.

345. Over a three-year period the suspect sent IFTIs worth approximately AUD900,000 to more than 100 different beneficiaries in several jurisdictions, with the majority of the transfers sent to Nigeria, Hong Kong, the United Kingdom and Singapore. During this period, the suspect also made several significant cash withdrawals, worth AUD120 000.

346. The resultant law enforcement investigation found that the suspect allegedly committed other frauds to fund the overseas funds transfers to the fraudsters. It appears that she also may have induced other people to send money to the fraudsters, although it is not known whether she profited from these transfers.

AUSTRALIA

Case Study – Inheritance scams

347. AUSTRAC alerted a law enforcement agency to suspicious international funds transfers being made by an elderly Australian couple to various destinations including the United Kingdom, Ghana, Hong Kong and Ivory Coast. Over a six-month period the couple sent AUD512,000 overseas through a money transfer agency.

348. Law enforcement officers visited the couple in relation to the following money transfers:

- Ghana – the couple told the officers that they had befriended a woman on the internet, who in correspondence referred to the couple as ‘mother’ and ‘father’. In response to her requests, the couple sent money to the woman to assist her with food, rent and other expenses. The couple believed that the woman eventually wanted to move to Australia. In addition, the husband had travelled to Ghana to meet the woman, and arranged to pay USD20 per day for the storage of the woman’s family treasure chest.

- United Kingdom – the couple sent funds to a recipient in London as part of what was subsequently revealed to be an 'inheritance' scam.
- Hong Kong – the couple sent AUD57,000 to an overseas recipient, also part of an inheritance scam
- Ivory Coast – the couple had befriended a girl whose parents had been killed, and provided her with financial assistance for food and accommodation. They believed that she, too, wanted to move to Australia.

349. AUSTRAC further advised authorities that the couple had sent a further AUD60,000 overseas even after being visited by law enforcement officers and explained to the couple that what they were experiencing was not real and was a fraudulent operation.

FIJI

Case Study - Scam- counterfeit cheques

350. In 2009, there was a counterfeit cheque scheme targeting law firms in Fiji. Local law firms were contacted by an overseas client via email seeking debt collection services from the law firm for debts allegedly owing by a Fiji Company. Once the law firm has responded and engages with the overseas client, the law firm received a cheque via international postal mail supposedly from the Fiji Company that owes the debt.

351. The law firm was advised by their overseas client to remit the payment of this debt to a bank account in China. The amount on the cheque matches the amount owed by the Fiji Company to the individual from overseas. When the law firm attempted to deposit the cheque into the law firm's trust account, the bank advised that the cheque was a counterfeit and therefore no funds were paid out by the bank. When the law firm contacted the Fiji Company allegedly owing money to the individual overseas, it was revealed that the Fiji Company had no such debt and had not conducted transactions with the individual overseas.

352. The amount on the counterfeit cheque was between the amounts of FJD290,000.00 to FJD670,000.00 and four law firms that were targeted with this scam were brought to the attention of the Fiji FIU. FIU had issued an alert notice to law firms and commercial banks warning them of this scheme.

8. ACRONYMS

AC - Anti Corruption
ADB - Asian Development Bank
AGD - Attorney General's Department
AML - Anti-Money Laundering
AMLD - Anti-Money Laundering Department
APG - Asia Pacific Group
ATM - Automatic Teller Machine
AUD - Australian Dollars
AUSTRAC - Australian Transaction Reports and Analysis Centre
BNI - Bearer Negotiable Instrument
CCM – Companies Commission Malaysia
CDD - Customer Due Diligence
CET - Carbon Emissions Trading
CFT - Countering the Financing of Terrorism
CFTF - Commodity Futures Trading Commission
CTED - Counter Terrorism Executive Directorate
CTH - Commonwealth

CTR - Cash Transaction Report
DIAC - Department of Immigration and Citizenship
EAG – Eurasion Group on Combating Money Laundering and Financing of Terrorism
EDD - Enhanced Due Diligence
EFT - Electronic Funds Transfer
EUETS - European Union Emission Trading Scheme
FATF - Financial Action Task Force
FinCEN – Financial Crimes Enforcement Network
FINTRAC – Financial Transactions Reports Analysis Centre Canada
FIU - Financial Intelligence Unit
FSRB - FATF Style Regional Bodies
FTRA - Financial Transaction Reports Act
GAFISUD – The Financial Action Task Force of South America Against Money Laundering
GIABA – Intergovernmental Action Group against Money Laundering in West Africa
GST - Goods and Services Tax
HKD - Hong Kong Dollar
ICTR - International Currency Transaction Report
IFTI - International Funds Transaction Instruction
INTERPOL – International Criminal police Organisation
IRS - Internal Revenue Service
KFR - Kidnapping for Ransom
KPK – Indonesia's Corruption Eradication Commission
LEA - Law Enforcement Agency
MENAFATF – Middle East & North Africa Financial Action Task Force
ML - Money Laundering
MLA - Mutual Legal Assistance
MONEYVAL - The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOU – Memorandum of Understanding
MSB - Money Service Bureau
NPM - New Payment Method
NPO - Non Profit Organisation
NSW - New South Wales
NTD - New Taiwan Dollar
NZD - New Zealand Dollar
OECD - Organisation for Economic Cooperation and Development
PEP - Politically Exposed Person
PFR - Piracy for Ransom
PHP - Philippine Peso
RMB - Chinese Renminbi
ROS – Registry of Societies
SAR - Suspicious Activity Report
SCTR - Significant Cash Transaction Report
SEC - Security Exchange Commission
SOB - Smuggling of Migrants
STR - Suspicious Transaction Reports
SUSTR - Suspicious Transactions Report
TCSP - Trust and Company Service Providers
TF - Terrorism Finance
THB - Trafficking in Human Beings
UN - United Nations
USD - United States Dollar
VAT - Value Added Tax
WGTYP - Working Group Typologies