Asia/Pacific Group on Money Laundering

ASIA/PACIFIC GROUP ON MONEY LAUNDERING

APG Yearly Typologies Report 2012

Methods and Trends of Money Laundering and Terrorism Financing

Adopted by APG Members at the 15th Annual Meeting

20 July 2012

.

(Telephone: +612 9277 0600 Fax: +612 9277 0606 Email: mail@apgml.org)

CONTENTS

INTRODUCTION

Background

1. The Asia/Pacific Group on Money Laundering (APG) is the regional anti-money laundering / combating the financing of terrorism (AML/CFT) regional body for the Asia Pacific. The APG produces regional typologies reports on money laundering (ML) and terrorist financing (TF) techniques to assist governments and other AML/CFT stakeholders to better understand the nature of existing and emerging ML and TF threats and pursue effective strategies to address those threats. Typologies studies assist APG members to implement effective strategies to investigate and prosecute ML and TF, as well as design and implement effective preventative measures. When a series of ML or TF arrangements are conducted in a similar manner or using the same methods, they are generally classified as a typology.

2. 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.) involved in implementing preventative measures including CDD and STR reporting.

3. 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.

Typologies in 2011-2012

4. The APG Typologies Working Group continued its work in 2011-12 under the leadership of India and Malaysia as Co-chairs. In July 2011 the APG Typologies Working Group met to determine the work program for the year, including the in-depth study of trade based money laundering (TBML) in the Asia/Pacific region and the conduct of a joint APG / FATF Typologies Meeting in late 2011 hosted by the Republic of Korea in Busan.

5. The summary of the trade based ML project, précis and references to typologies studies by other AML/CFT bodies and the case studies featured in this report are only a small slice of the work going on across the Asia/Pacific and other regions to detect and combat ML and TF.

6. The report contains a selection of illustrative cases of various typologies gathered from APG members' reports as well as open sources. 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.

7. Thanks go out to Australia and Malaysia for leading the APG Typologies Working Group during 2011/2012.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2011-12

1.1 2011 Joint FATF/APG Typologies Meeting of Experts

8. The Republic of Korea hosted the joint the Financial Action Task Force (FATF) / APG Typologies Meeting of Experts in Busan from 5– 8 December 2011. The APG recognises and thanks the government of the Republic of Korea for their leadership in hosting the global typologies meeting in 2011.

9. The 2011 meeting was a great success and was attended by more than 290 delegates from 73 jurisdictions and 11 organisations. The 2011 joint FATF/APG meeting is the largest typologies event that the APG has ever conducted.

10. The meeting was jointly chaired by the APG and the FATF Working Group co-chairs. The workshop moved forward very significant work on the following topics, which will all result in reports in mid-2012:

    - Trade Based Money Laundering (led by APG);
    - Illicit Tobacco Trade and money laundering
    - Operational Issues
    - Corruption related Money Laundering.

11. Following the APG/FATF Typologies Workshop two additional workshops were held on technical issues with the Egmont Group and separately with ESAAMLG and the generous support of the Commonwealth Secretariat.

1.2 TBML project

12. Trade Based Money Laundering (TBML) has been recognized by the FATF in its landmark study published in 2006, as one of the three main methods by which criminal organizations and terrorist financiers move money for the purpose of disguising its origins and integrating it back into the formal economy. This method of ML is based upon abuse of trade transactions and their financing. The 2006 FATF Study highlighted the increasing attractiveness of TBML as a method for laundering funds, as controls on laundering of funds through misuse of the financial system (both formal and alternate) and through physical movement of cash (cash smuggling) become tighter.

13. The APG TBML study published in July 2012 aims to build on the existing studies and consider the extent of the prevalence of TBML and current methods, techniques and modus operandi for TBML so as to shortlist 'red flags' to detect and respond to TBML. The Paper has sought to clarify and furnish explanations for terms and processes of trade finance to assist ML investigators.

14. The APG's 2012 study focuses on TBML in the course of international trade in goods, but largely excludes the international trade in services and domestic trade.

15. The features of the dynamic environment that distinguish TBML from other forms of ML are its occurrence through intermingling of the trade sector with the trade finance

sector in cross- border transactions. The foreign exchange market and the long supply chain make international trade vulnerable to TBML.

16. The APG study sets out a large number of 'red flags' which are categorised in five broad groups: trade finance, jurisdictions, goods, corporate structure and predicate offences.

17. The case studies included in the paper, besides identifying the elements of trade that facilitate TBML, also bring out the mechanisms of trade finance used in TBML. The case studies highlight the financing of different segments of trade through diverse mechanisms of trade finance that can introduce risks in the trade transactions which are difficult to assess by financial institutions. The mechanisms of financing trade through factoring and through disbursement of trade credit to overseas suppliers are present risks for financial institutions unless due diligence is exercised over the overseas trading partner. Another case study shows how the operations of 'exchange houses' owned and controlled by criminals coupled with 'compromised' working of a bank make trade finance mechanisms means for indulging in TBML. Case studies also demonstrate the use of alternative remittance system and of corporate structure to facilitate TBML. A final case study shows multiple forms of international trade and various mechanisms of trade finance which give inherent flexibility to criminals to adopt those forms and types which suit the demands of a situation.

18. Any strategy to prevent and combat TBML needs to be based on dismantling of the TBML structures yet allowing genuine trade to occur unfettered. A holistic approach, with emphasis on inter-agency coordination and international cooperation, needs to be universally adopted by the policy-makers. A comprehensive strategy which takes into account sectoral peculiarities, agency specialization and jurisdictional frameworks can only address the challenges in tackling TBML.

19. Multiple agencies are associated either directly or indirectly in combating TBML. They may have even achieved professional specialization and competence in such mandated work. However, the strategy to prevent and combat TBML requires expertise created through the combination of all such authorities. One way-forward to combine the respective competencies of relevant authorities for combating TBML is to form domestic task-forces. Task-forces focused on TBML investigations will need to have the ability to utilize the expertise of each agency without compromising its functional skills.

20. There is an urgent need to strengthen the existing bilateral arrangements like Trade Transparency Units (TTUs) and to build multilateral mechanisms for international cooperation. The bilateral arrangements must ensure prompt exchange of information with regular follow-ups which should result in more efficient delivery. The multilateral mechanisms may entail equal commitment of all trading jurisdictions for coordination in matters relating to TBML.

2. OVERVIEW OF TYPOLOGY PROJECTS BY FATF AND FATF-STYLE REGIONAL BODIES

21. A range of typology studies have been published in 2011 and 2012 by several other FSRBs, including, but not limited to projects on work done by the following regional bodies:

2.1 FATF Typology Projects

22. The FATF Working Group on Typologies has produced a paper on the *Specific risk factors in laundering the proceeds of corruption* which was published in June 2012. It was designed as a follow-up of the previous FATF typology report on corruption and is intended to assist reporting entities (financial institutions and DNFBPs) to better analyse and better understand specific risk factors which may assist them in identifying situations where corruption-related ML risk has increased.

23. The report noted, corrupt politically exposed persons (PEPs) try to use a wide array of means to disguise the nature and the source of the funds in order to place corrupt money in the financial system without suspicion (such as corporate vehicles, sophisticated gatekeepers, cash and countries with weak ML controls). Corruption-related transactions often involve an intermediary of some kind, (including family members and close associates), whether within the PEP's jurisdiction or beyond.

24. The analysis is not limited to transactions involving PEPs as that term is defined within the FATF Recommendations but also focuses on officials (including family members and close associates), business relationships, and companies for which transactions may present a heightened risk of corruption-related ML. The report relies on studies and literature written by a number of stakeholders and experts in the field, and the discussion is backed by a large body of case studies.

25. Though the document concludes that corruption-related ML typically uses many of the same techniques as other types of ML, the discussion also makes clear that certain characteristics — customer types, countries and regions, and product/services — when taken together and in the context of corruption-related ML, should also be considered higher risk, regardless of whether a PEP has been identified.

26. The report also provides references to a number of additional sources of relevant information that could be useful for reporting entities when designing their risk management policies.

27. The FATF Working Group on Typologies has also produced a *FATF Guidance On Financial Investigations*.

28. During the FATF's latest revision of its standards, greater attention was given to the operational AML/CFT framework. One goal was to strengthen the law enforcement standards (R.30 and R.31) to enhance the functions, responsibilities, powers and tools of law enforcement to effectively conduct ML, TF and asset-tracing investigations. The revised standards more clearly reflects the central importance of financial investigations amongst the FATF's operational and law enforcement recommendations.

29. The FATF's new guidance on financial investigations is intended to help countries better understand law enforcement's role in the larger AML/CFT context. The guidance can also be useful to future AML/CFT assessments and to assist assessors determine the effectiveness of the operational AML/CFT regime.

2.2 MONEYVAL –Europe's FATF-Style Regional Body

Criminal Money Flows on the Internet: Methods, Trends and Multi-Stakeholder Counter-action (March 2012)[1]

30. In March 2012 MONEYVAL published its report on Criminal Money Flows on the Internet, which reflected a cooperative effort of MONEYVAL, the Council of Europe's Global Project on Cybercrime as well as the joint AML/CFT project of the EU and the Council of Europe in the Russian Federation (MOLI-RU 2).

31. The report notes that though cybercrime appears to be widespread and generates large amounts of criminal proceeds, the data on related ML and evidence of successful law enforcement action is weak. In addition to contributing to raising awareness on current initiatives aimed at preventing and combating cybercrime and ML, as well as on proceeds generating offences on the Internet, the report considers the cyber-laundering risks and vulnerabilities and illustrates identified ML methods, techniques, mechanisms and instruments of criminal proceeds from cybercrime relying on a number of cases received from contributors, setting out typologies that were identified and specific indicators of potential ML activity within this context.

2.3 MENAFATF – The Middle East / North African FATF-Style Regional Body

Illicit Trafficking in Narcotic Drugs and Psychotropic Substances and ML – 2011[2]

32. The MENAFATF's report noted that the ML techniques for proceeds of illicit drug and psychotropic substances trafficking are varied and not necessarily different than ML techniques in general. The most commonly reported in the case studies under review are purchase of real estate, trading in vehicles and use of bank deposits.

33. It was noted that the large scale of drugs-related proceeds makes it difficult to move these funds at the banks without raising suspicion. Criminals may resort to sectors with less supervision to launder funds.

34. The report noted common use of shell companies or the purchase and sale of real estate and cars as a ground to justify bank deposits and funds transfers.

35. The MENAFATF noted an intersection between ML indicators found in ML cases in general (regardless of the predicate offence), and the indicators for laundering proceeds illicit trafficking in narcotic drugs and psychotropic substances. It can be considered that extreme wealth, carrying out transactions with no clear economic justification, or bank transfers from and to persons existing in countries famous in the cultivation, manufacturing, smuggling or trafficking in narcotic drugs and psychotropic substances, are important indicators that should not be ignored.

36. The MENAFATF points out the importance of establishing specialized divisions to combat drugs-related ML and investigating ML offences in parallel to investigations into illicit trafficking in narcotic drugs and psychotropic substances.

[1] http://www.coe.int/t/dghl/monitoring/moneyval/Typologies/MONEYVAL(2012)6_Reptyp_flows_en.pdf
[2] http://www.menafatf.org/images/UploadFiles/Illicit_Trafficking_and_ML_Eng.pdf

37. Member countries should work on raising the awareness level of DNFBPs, in particular real estate agents, about ML techniques and indicators. Countries should ensure that effective coordination exists between bodies concerned with combating illicit trafficking in narcotic drugs and psychotropic substances and AML entities at both the local and international levels.

2.4 The Eurasian Group (EAG)

Organized criminal groups (including those formed along ethnic lines) in operations (transactions) with cash and non-cash assets – December 2011[3]

38. The report highlighted legal and institutional mechanisms for investigating oragnised criminal groups across a number of EAG members and observers. The report noted the importance of using financial investigations to combat organised crime and found that financial transaction and deals related to offences committed by organized crime groups often have distinctive features. Cased of organized crime groups using cash settlements and financial and credit mechanisms were noted.

Preventing Offences Related to Placement of Orders for Supply of Goods, Work and Services for State and Municipal Needs – 2011[4]

39. This EAG report is particularly useful for those agencies involved in combating public sector corruption and fraud in public procurement. The report notes that the public procurement procedure involves a number of steps, each of which may represent risks. The following stages that are most frequently exposed to the risks of offences:

- Order Placement and Contracting Stage;
- Contract Performance Stage.

40. Section 3 of the report sets out indicators of suspicious activities in public procurement. Section 4 of the report summarizes indicators of public procurement-related offences that can be detected by FIUs, as well as references information resources and financial transactions data.

41. The report provides detailed typologies of financial schemes used for public procurement as well as red-flag indicators. Two examples include the use of patents for gaining corruption proceeds; and bribery of government-owned companies' officers by large foreign companies for arranging large-scale procurement of goods.

2.5 ESSAMLG – the Eastern and Southern Africa AML Group

Laundering the Proceeds Of Illicit Trafficking In Narcotic Drugs and Psychotropic Substances (ESAAMLG Region) – September 2011[5]

42. Case studies collected in the ESAAMLG report found that illicit drug cultivation, processing and use are on the increase in the region. In addition to the region's use for transit of drugs, cocaine and heroin are now increasingly being consumed within the region. Laundering of drug proceeds occurs through purchase of real estate, luxury vehicles, front companies, insurance industry and through collusion with bank employees

[3] http://eurasiangroup.org/WGTYP_2011_10_eng.doc
[4] http://eurasiangroup.org/WGTYP_2011_6_eng.doc
[5] http://www.esaamlg.org/userfiles/DRUG-TRAFFICKING-REPORT.pdf

to facilitate both local transactions and international wire transfers to off shore jurisdictions. The study further revealed that no single member of the region has experienced all the above trends however some ML trends are more prominent in some of the member states compared to others.

Vulnerabilities of ML Related to Trafficking in Persons in the ESAAMLG Region" - 2011[6]

43. The general level of implementation of AML measures in the ESAAMLG region remains low which adds to the vulnerability of ML from trafficking in persons in the region. Only six (6) member countries in the region have enacted legislation criminalising trafficking in persons.

44. There is very little formal or informal coordination and cooperation amongst member countries on trafficking in persons. There is little to no empirical data on cases of trafficking in persons, such as statistics and case studies, exist in the region.

45. While there were few substantiated findings from ESAAMLG members in regard to ML from the trafficking in persons, research literature indicates that member countries are vulnerable to syndicate/organised criminal groups involved in trafficking in persons. It is known that the main routes/corridors are through Namibia, Zambia and Tanzania into Malawi, Mozambique, Zimbabwe, Swaziland and then into South Africa as either the final destination or transit to Europe.

[6] http://www.esaamlg.org/userfiles/HUMAN-TRAFFICKING-Report-Mauritius-2011.pdf

3. TRENDS OF MONEY LAUNDERING & TERRORISM FINANCING

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

AUSTRALIA

46. 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.

47. AUSTRAC recently published the 2011 Typologies and Case Studies Report. The 2011 report examines the ways in which criminals misuse banks, casinos and money transfer agencies to commit serious transnational crime, fraud, terrorism financing, and people smuggling and human trafficking. The report includes 20 case studies that were initiated or supported by reports submitted to AUSTRAC by account and deposit-taking, gambling and remittance service businesses. All five Typologies and Case Studies Reports (2007 – 2011) are available on the AUSTRAC website http://www.austrac.gov.au/typologies.html

48. This year, AUSTRAC also launched its first National Threat Assessment (NTA) on ML, outlining the threats to business and government from transnational crime.

49. ML in Australia 2011 (MLA 2011) presents a consolidated picture of ML - the indicators and activities involved, the sectors and professions that are vulnerable, a range of new and emerging threats and the general framework within which business and government operate to identify and prevent this crime.

50. The public report aims to assist businesses to keep up to date with emerging ML threats and assist them to develop appropriate preventative strategies. MLA 2011 also aims to increase wider public awareness of ML threats so that the community can understand why anti-ML measures are in place.

51. The public report is derived from Australia's first classified NTA report led by AUSTRAC, which is available to selected Australian Government agencies. This threat assessment is a priority action of the Commonwealth Organised Crime Response Plan, which is part of the Australian Government's Organised Crime Strategic Framework.

52. Australia's classified NTA on ML establishes a baseline assessment of key ML threats and vulnerabilities, which will inform future policy and legislative change, operational efforts and intelligence targeting.

53. The NTA is a multi-agency effort led by AUSTRAC. The assessment is based on information and intelligence analysis from AUSTRAC and a number of Commonwealth and state Government agencies. ML in Australia 2011 is available via http://www.austrac.gov.au/money_laundering_in_australia_2011.html\

CANADA

FINTRAC Typologies and Trends Reports – October 2011[7]

54. FINTRAC published a second publication on *Trends in Canadian Suspicious Transaction Reporting*. This series of publications is intended to help reporting entities strengthen their efforts to comply with the *Proceeds of Crime (ML) and Terrorist Financing Act*. It is intended to provide strategic financial intelligence and feedback to reporting entities about STRs. These publications also help provide reporting entities with a baseline that can be used in the future to assess changes in STR reporting over time.

ML and TF Trends in FINTRAC Cases Disclosed Between 2007 and 2011 – April 2012[8]

55. The April 2012 report analyzes data from over 2100 FINTRAC cases disclosed to law enforcement and security-intelligence agencies, and observes changing trends and indicators in ML and TF in Canada.

56. In regards to ML, the report shows that investment frauds such as Ponzi schemes were prominent while advance fee schemes have been surpassed by debit and credit card fraud, as well as market fraud. The report also describes key indicators of the movement of terrorist financing, including using multiple institutions and accounts, attempting to avoid the reporting of large cash transactions, and reissuing bank drafts through third parties.

FIJI

57. The Fiji FIU has not engaged in any formal research or studies on ML/TF typologies and trends. However the Fiji FIU continues to develop case studies from possible ML and serious crimes cases that have been disseminated by the Unit to Law Enforcement Agencies. These case studies have been published in the Fiji FIU Annual Report 2010 which can be accessed via its website: www.fijifiu.gov.fj

58. The 3rd National AML Conference was held on 9 November 2011 and consisted of highly experienced personnel from key Law Enforcement Agencies discussing the Legal Framework for AML in Fiji and the highlights of successful ML cases in Fiji. A key component of the program was the presentation of the "Turtle Island Case Study' which was also discussed at the Egmont Plenary in July 2011 where Fiji FIU was one of the finalists for the Best Egmont Case Award (BECA).

59. The Fiji FIU also holds quarterly meetings with AML Compliance Officers of the various financial institutions. In this meeting, reporting institutions are briefed on the ML typologies and trends noted by the Unit. ML typologies are also discussed during the meetings of the AML Law Enforcement Working Group, a sub-committee of Fiji's National AML Council. The Working Group is also working on a ML Typologies document for Law Enforcement Agencies.

[7] http://www.fintrac.gc.ca/publications/typologies/2011-10-eng.pdf
[8] http://www.fintrac.gc.ca/publications/typologies/2012-04-eng.pdf

USA

Identity Theft: Trends, Patterns, and Typologies Based on Suspicious Activity Reports Filed by the Securities and Futures Industries, January 1, 2005 – December 31, 2010 - September 2011. [9]

60. FinCEN is the United State's FIU. FinCEN's report focuses on identity theft in the securities and futures industries. Based on Suspicious Activity Report by the Securities and Futures Industries (SAR-SF) filings, it describes recent patterns and trends of SAR-SF reporting and identifies methods by which identity thieves may access and abuse investment, retirement, and trust accounts to defraud individual account holders and/or securities firms.

61. Two SAR Activity Review: Trends, Tips and Issues – Issues 20 & 21 were published in late 2011 and mid-2012[10]. These reports are a product of collaboration among the USA's financial institutions, law enforcement officials and regulatory agencies regarding SARs and other reports filed by financial institutions under FinCEN's regulations.

62. Issue 20 features articles by two of FinCEN's multi-disciplinary working groups: SAR filings related to international prepaid cards, and the risks associated with the growth in Remote Deposit Capture (RDC) services. FinCEN's Office of Regulatory Analysis shares findings of their assessment of SAR filings prior to and following FinCEN's Advisory on Informal Value Transfer Systems (IVTS) in September, 2010. Also, FinCEN's Office of Outreach Resources provides an update on SAR-related inquiries to our Regulatory Helpline.

63. The *Law Enforcement Cases* section includes cases summaries that demonstrate the importance and value of BSA data to the law enforcement community. Cases in this section highlight how the use of BSA data, particularly SARs, and the detection and analysis of suspicious transactions by financial institutions proved to be of value to law enforcement and prosecutors.

64. In *Issues & Guidance*, articles from the United States Trustees Program on their efforts in combating bankruptcy-related mortgage fraud and mortgage rescue schemes and from Immigration and Customs Enforcement (ICE) on organized retail crime are presented. Also included are several articles from FinCEN staff focusing on a variety of topics of interest for financial institutions: health care fraud and associated red flags; SAR confidentiality; distinguishing between BSA SARs and other suspicious activity reporting initiatives; and, E-filing information for filers of the Registration of Money Services Business form (FinCEN Form 107). Also included in this section is an update to FinCEN's February, 2011 Advisory on Elder Financial Exploitation.

65. In the *Industry Forum* section, an industry viewpoint is provided on the ML risks associated with trading cash for gold.

66. Issue 21 focuses on trends and issues related to Money Services Businesses (MSBs).

[9] http://www.fincen.gov/news_room/rp/files/ID%20Theft%2011_508%20FINAL.pdf
[10] http://www.fincen.gov/news_room/rp/files/sar_tti_20.pdf

Suspicious Activity Reporting in the Gaming Industry January 2004 – June 2011 Based on Filings of Suspicious Activity Reports by Casinos and Card Clubs from January 1, 2004, through June 30, 2011 (In March 2012)[11]

67. Gaming institutions covered by FinCEN's regulations submitted 74,816 Suspicious Activity Report by Casinos and Card Clubs (SAR-C) filings from 2004 through June 2011. Dollar amounts reported in these filings totalled $1.77 billion. Annual filings consistently increased, while total dollar amounts fluctuated from year to year. The steady increase in SAR-C filings during the study period paralleled a significant expansion of gaming operations across the United States.

68. More than 40% of the filings reported suspicious activities characterized as structuring. The reports frequently described activities involving chip, jackpot and token redemptions, which customers may have structured to avoid currency transaction reporting requirements.

3.2 Association of Types of ML or TF with Predicate Activities

AUSTRALIA

69. Through an Australian Crime Commission (ACC) Board approved special investigation, July 2010 – June 2011, the ACC worked with partners to identify, detect and disrupt ML activities, minimise criminal exploitation of vulnerabilities and enhance national understanding of ML methods. During the year, the ACC contributed to Australia's National Threat Assessment on ML and joined the newly formed Australian Federal Police-led Criminal Assets Confiscation Taskforce. The ACC uncovered several ML syndicates, identified vulnerabilities in the finance sector, and exposed links between organised crime and casino high rollers involved in Commonwealth fraud. The ACC also provided a major contribution to proposed amendments to the AML/CTF Act 2006, with findings from its work informing the proposed changes to strengthen and increase reporting requirements.

70. Working with partner agencies, the ACC restrained $29.88 million worth of cash and assets including cars, jewellery and property this year. The bulk of this was the result of the *Sethra investigation*, a joint ACC / Victoria Police investigation that targeted a significant drug and organised crime syndicate and culminated in one of the largest single proceeds of crime restraints made in Victoria.

71. This joint Victoria Police/ACC investigation was prompted by ongoing monitoring of ML targets identified in a previous operation. In August 2010, Victoria Police and ACC members executed search warrants at 12 Melbourne premises. During the searches, police located an estimated 2.25 kilograms of heroin, two kilograms of cannabis, 100 grams of amphetamine, 200 MDMA (ecstasy) tablets, A$1,433,485 cash and A$524,930 in casino chips. It is also alleged that the principal targets of this investigation trafficked 12 kilograms of heroin. An estimated $20 million in property was also restrained, A$900,000 in jewellery and five vehicles with an estimated value of A$120, 000 were also seized as proceeds of crime. A total of 25 people were charged in relation to trafficking a drug of dependence (principally heroin) and dealing in proceeds of crime.

72. Between July and October 2010: The NSW Police Force seized more than 28 kilograms of heroin, with an estimated street value of AU$19.4 million, as well as AU$395,050 in cash. Follow up searches by ACC and the NSW Police Force located mobile phones,

[11] http://www.fincen.gov/news_room/rp/files/GamingIndustry508March2012.pdf

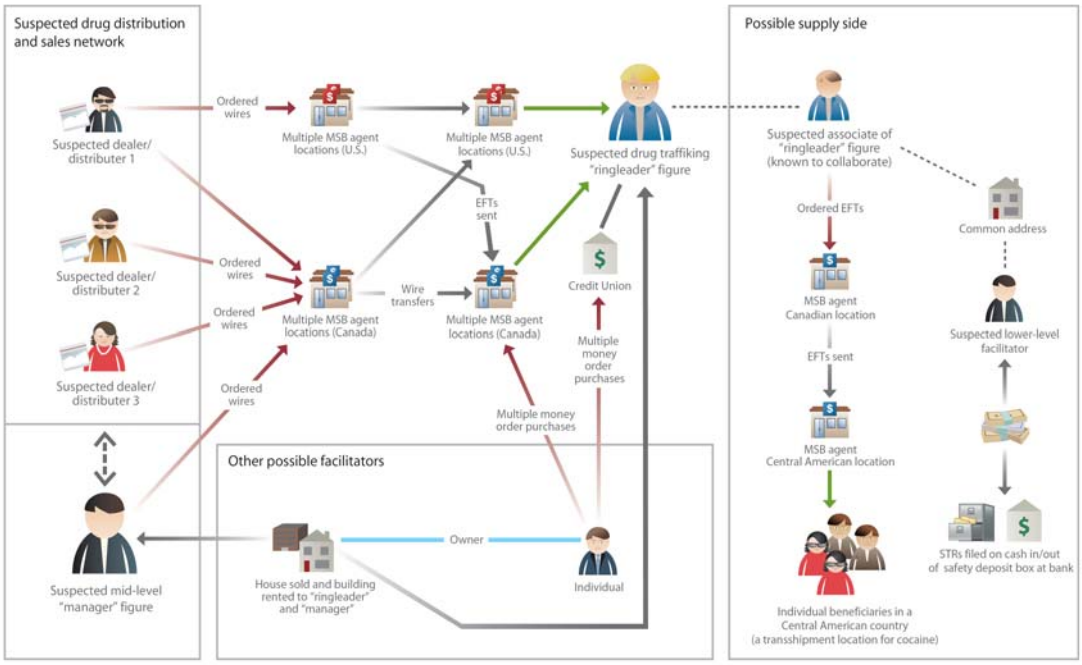
ledgers, an automatic money counter, scales and suspected drug packaging. Three people were charged with drug offences. A senior Western Australian outlaw motorcycle gang member was charged with drug offences related to the previous attempted shipment of four kilograms of methylamphetamine seized in 2009 and a similar shipment identified as having taken place earlier.

73. Hong Kong Police located and arrested the subject of an Australian provisional arrest warrant in Kowloon City, in relation to two seizures of methylamphetamine (ice) in December 2009 and January 2010. It is alleged this man was a significant link to Asian organised crime syndicates providing drugs to Australian criminals on a large scale. His extradition remains subject to appeal before Hong Kong courts. The Sydney Joint Organised Crime Group arrested another person who had been hiding since the January 2010 ice seizure and who is alleged to have played a significant role on behalf of Hong Kong entities organising and distributing drug importations. The New South Wales Crime Commission began proceeds of crime action against the key syndicate members, including a well publicised outlaw motorcycle gang member suspected to be hiding overseas to avoid arrest in relation to the seizures and criminal activities identified during this investigation.

74. The ACC-led Financial Intelligence Assessment Team (FIAT) identified over A$2.4 million being sent to bank accounts in China, suspected to be undeclared income. In September 2010, the Australian Federal Police charged a Sydney woman with dealing in proceeds of crime greater than A$1 million. Again working with the Australian Federal Police, in February 2011, FIAT intelligence was used to shut down another Sydney-based ML syndicate involved in tax avoidance. Two women were arrested and more than A$800,000 was seized. The FIAT also identified vulnerabilities in the finance sector, involving bank employees allegedly colluding with organised crime.

CANADA

Suspected laundering of drug proceeds by exploiting electronic funds transfer (EFT) services to send funds to the ringleader of a drug trafficking operation.



75. This case was initiated following the receipt of law enforcement information about one senior suspected drug trafficking "ringleader" and three individual subordinates who acted as "middle-managers" between several drug suppliers, and also coordinated street-level drug sellers. According to law enforcement, the suspected ringleader, and his principal "middle-managers", had long histories of criminal charges and convictions for drug trafficking and possession of the proceeds of crime. Law enforcement suspected that the ringleader bought cocaine himself, or through his middle-managers. The "managers" then sold the cocaine themselves, and also dealt with other lower-level individuals as part of a "dial-a-dope" operation. Financial transactions for these individuals show that they used dozens of MSB locations/agents across a wide geographic area in North America, and sent over $70,000 in drug proceeds to the suspected ringleader through hundreds of below threshold international EFTs and domestic wire transfers.

76. The ringleader also collected the proceeds at different agent locations, including one in a casino. Most of those involved in the trafficking operation reported employment at a restaurant or were on social assistance.

77. MSB STRs indicated that both the ringleader and the "middle-managers" were sending wires/EFTs at a very high frequency, were suspected of splitting transactions, were travelling across jurisdictions to different MSB agent locations to either send or receive wires/EFTs, and were consistently providing multiple names or different spelling to MSB agents.

78. Police information also identified an individual with suspected links to the ringleader. Financial transactions for this suspected associate showed that he/she sent thousands of dollars worth of international EFTs to a Central American country with a known history of being a transhipment point for cocaine trafficking – suggesting a possible connection to the supply side of the drug operations. Another individual who shared an address with the ringleader's suspected associate was also flagged in bank STRs for suspicious financial activity related to the use of a safety deposit box, and to what appeared to be "refining" through small denomination cash deposits, followed by cash withdrawals.

79. STRs and law enforcement information also identified other suspected facilitators who were positioned to assist the ringleader with trafficking-related operations. One such suspected facilitator was reported in MSB and bank STRs as having purchased a number of non-sequential money orders, payable to himself/herself, and then deposited these into his/her account at a financial institution. This individual also apparently sold one property to the ringleader and a middle-manager figure, and also rented out another building to them as well.

80. This case highlights how MSBs can be used as a central part of the financial activity of a drug trafficking operation. In this case, MSB agents in a wide range of geographic locations were used by a group suspected drug traffickers to "repatriate" drug money back to an individual suspected to be the operation's ringleader.

RED FLAGS associated with this case

- Clients appeared to split their transactions to avoid reporting requirements.
- The transaction frequency was high, combined with the use of multiple agent locations (sometimes on the same day).

- Subjects used various spellings of their names and/or misled reporting entities regarding their names.
- International electronic funds transfers (EFTs) were sent to a country which is frequently exploited by drug trafficking organizations (DTOs) for cocaine transhipment and ML purposes.
- The value of transactions did not appear to be commensurate with stated employment.

CHINA

81. China indicated that the predicate offences of public-related crimes and corruption are growing in number. The early ML crimes most related to economic crimes, drug crimes and smuggling crimes. However, as the statistics showed, the following two kinds of crimes increased recently: one was the public-related crime, such as pyramid selling, illegal fund-raising and various underground funds, the other was corruption, mainly occurred in banking, securities and transportations sectors and related to government officials and senior managers in state-owned enterprises.

FIJI

82. The National AML Council established under Section 35 of the FTR Act and is responsible for coordinating national AML efforts and advising the Government and the FIU on AML related matters. The AML Law Enforcement Working Group which reports to the National AML Council held 5 meetings in 2011 and had joint presentations from partner agencies discussing law enforcement issues such as border currency and immigration related issues, investment and monitoring of investors, challenges in investigation and prosecuting ML crimes.

83. Fiji's AML Law Enforcement Working Group is currently compiling case studies relating to predicate offences and the proposed Typologies Report for Fiji is expected to be released in 2012.

INDIA

84. TBML has generally been found associated with fraud, smuggling and narcotic trafficking.

THAILAND

85. Thailand reported that the most common criminal activity is drug trafficking. This is also one of the main sources of funding for insurgent groups in Southern Thailand.

86. Thai insurgent groups are also involved in goods smuggling, usually cigarettes, liquor, pirated DVDs, small arms trafficking and human trafficking.

3.3 Emerging Trends; Declining Trends; Continuing Trends

AUSTRALIA

87. In Australia, syndicates have been identified laundering funds by storing large amounts of cash in secure locations, gambling at casinos and other venues or online, intermingling criminal and legitimate activities, investing in a range of high-value assets such as cars, motorcycles, marine craft, racehorses, works of art, jewellery and real estate, investing in securities, shares and stocks, operating bank accounts in false names and transferring assets to non-criminal associates.

88. Australia continues to see sophisticated and well-organised criminal syndicates exploit weaknesses in business products and services to launder the proceeds of illicit activity and to commit financial and other serious crime. Organised crime is becoming more diversified, sophisticated and transnational.

89. Advances in technology and increased globalisation, combined with the diversification, sophistication and transnational nature of organised crime, are some of the issues that shape current and emerging threats to the Australian financial environment.

90. The 2011 AUSTRAC Typologies and Case Studies Report provides details about continuing and emerging trends. Criminals continue to exploit legitimate services offered by reporting entities to perpetrate scams and frauds, for example, boiler room scams and advanced fee fraud.

91. **Boiler room scams** - involve the illegal and/or aggressive selling of worthless or overpriced shares, or shares traded in limited volumes or markets. Boiler room fraud is generally highly organised, spanning multiple jurisdictions and can involve the use of sophisticated technology and identity fraud.

92. **Advance fee fraud** - Advance fee fraud involves an unsolicited invitation to potential victims to invest funds, usually with the promise of significant financial returns. The scams lure potential victims by offering them a range of benefits. These may include money, prizes, gifts or employment – none of which actually exist.

93. Advance fee frauds are evolving and the methodologies used by scammers reflect advances in technology and global communication.

94. **Terrorism financing** - Law enforcement and intelligence agencies have observed further patterns and activities relating to terrorism financing, including:

- individuals, often from the same cultural background, using their personal bank accounts to transfer funds offshore to provide support for terrorism activities overseas

- individuals using false names to undertake international funds transfers, particularly to high-risk jurisdictions8 This may include an individual of one gender giving instructions that an international funds transfer be carried out in the name of an individual of the opposite gender foreign nationals coming to Australia for a specific time frame to raise funds to support overseas terrorist organisations. Typically, these individuals only stay in Australia for short period of time – usually no longer than one month offenders undertaking card ‘skimming’ on EFTPOS and automatic teller machines (ATMs) to generate funds to support terrorist organisations or activities.

95. **People smuggling** - Australian law enforcement agencies have identified a number of indicators associated with people smuggling.

96. People-smuggling ventures may be funded through several low-value international funds transfers, often to a common overseas beneficiary. These transfers may be sent by (apparently) unrelated customers, who may share the same ethnic background.

97. Funds transfers related to people smuggling may be sent to countries with no apparent commercial connection to the activities of the customer transferring the funds.

98. People smuggling facilitators may insist that the identification documents of those being smuggled are destroyed to prevent them being used to trace their source country. Consequently, identification documentation used by these individuals to establish accounts or transfer funds offshore after their arrival in Australia may be fraudulent or not represent their true identity. Reporting entities should be vigilant when individuals who have recently arrived in Australia report that their identification documentation has been destroyed or lost.

99. **Human trafficking** - Australia is a destination country for victims of trafficking from at least Thailand, Malaysia, and the Republic of Korea. AUSTRAC and partner agencies have identified indicators which may suggest to reporting entities the misuse of their services to fund human trafficking operations and launder the profits of these operations:

100. The ACC's unclassified report Organised Crime in Australia 2011outlines trends in the international environment, serious and organised crime activities in Australia and the resulting harms to the Australian community. The overall risk to Australia from organised crime is assessed as high. Organised criminal activity is increasingly diverse and is evolving rapidly.

101. Organised crime in Australia generates billions of dollars of illicit proceeds and direct and indirect costs to governments, the private sector and the community of similar magnitude.

102. Superannuation and Investment Fraud—Examples of organised criminal activity in the superannuation sector have been identified and there is potential for this activity to increase, despite the level of regulation and enforcement.

103. In April 2011, the ACC established the multi-agency Task Force Galilee to combat and prevent serious organised investment fraud (scams that use sophisticated techniques to solicit investment in non-existent or worthless shares and other securities).

104. ML is an extremely diverse activity carried out in Australia at all levels of sophistication by most, if not all, organised crime groups, with or without the assistance of professional advisers. Alternative remittance services continue to be widely used by organised crime groups. International trade provides criminal syndicates with the opportunity to launder money. Organised crime will consistently seek to exploit areas that receive less regulatory attention.

CANADA

Trends in FINTRAC's ML cases related to Corruption

105. From April 1st, 2010 to March 31st, 2011, 34 ML cases related to corruption activity, within Canada and abroad, were disclosed by FINTRAC to law enforcement agencies in Canada and foreign financial intelligence units.

106. The most common corruption activity related to the ML cases were bribes or kickbacks given to labour unions, government officials or other involved businesses in order to win municipal contracts. In addition to this activity, embezzlement of corporate funds was also commonly suspected by law enforcement agencies. This corruption activity targeted several industries, both domestically and internationally. These included the construction industry, government sector and natural resources or mining industry.

107. More than half of FINTRAC's disclosed cases (56%) involved Politically Exposed Persons (PEPs), where they were either subjects of disclosures or the beneficiaries of the funds. The remainder of the cases involved organized crime groups or individuals and businesses not associated to any organized crime group. In addition to corruption, offences related to fraud, drugs and illegal import/export activities were also suspected.

108. FINTRAC observed that with international cases, most financial transactions involved electronic fund transfers (EFTs) to and from various individuals or businesses in other countries. Domestic ML cases related to corruption also involved several EFTs but the main financial transactions conducted were large cash deposits and withdrawals, purchases of bank drafts, currency exchanges and casino transactions.

109. Furthermore, almost all of the financial transactions were conducted through financial deposit-taking institutions (such as banks or credit unions) while the rest were conducted through either casinos or money services businesses (MSBs) such as currency exchange dealers or remittance/funds transmitters.

110. A number of services or organizations were also suspected to be used in the laundering of criminal proceeds. More specifically, lawyers, trust accounts or trust companies, and non-profit organizations such as charities or foundations were used in schemes. A lawyer or law office was involved in at least 10 cases.

111. Twenty-eight of the ML corruption cases involved a business or multiple businesses that were used in the criminal scheme. FINTRAC observed that next to construction companies, financial businesses such as holding companies or investment companies were the second most commonly used type of business in corruption and ML activity. Other businesses used in the schemes included import/export companies, consumer goods businesses, and mining/excavation businesses.

Trends in FINTRAC's ML Cases related to Mass Marketing Fraud

112. Between April 1st, 2009 and March 31st, 2011, FINTRAC disclosed 31 ML cases related to mass marketing fraud to law enforcement agencies in Canada as well as foreign financial intelligence units (FIUs) supporting the investigation of nearly 90 individuals and 100 businesses.

113. Twenty-three percent of the mass marketing fraud schemes were orchestrated by criminal organizations, while the remainder by individuals. These fraudsters primarily

targeted either victims in the United States, Canada, or both. In other cases, targeted victims were in the United Kingdom or Spain, or the victims were unspecified.

114. The most frequently suspected schemes were advanced fee scams, mail order frauds, pyramid schemes, boiler room schemes and "Grandson" scams*. In all of FINTRAC's cases, information from law enforcement or foreign FIUs indicated that victims were contacted by fraudsters either by mail, telephone or via the Internet.

115. In the 31 disclosed cases, all but one case involved the use of a deposit taking institution such as a bank or a credit union. Furthermore, 18 cases involved the use of MSBs, such as currency exchange dealers or remittance/funds transmitters. These sectors were also the main entities that reported large cash transaction reports or suspicious transactions activities to FINTRAC.

116. Not surprisingly, casinos were used in only two cases, mainly because mass marketing fraud cases rarely involve cash proceeds and more commonly involve cheques or electronic wire transfers.

117. In terms of the types of transactions these subjects were conducting, over 4000 international EFTs were sent to and from various individuals or businesses in other countries. Following the international EFTs, deposits of cash, cheques and bank drafts were frequently observed. The purchase of bank drafts, money orders and in some cases precious metals were the next most common transactions conducted. Currency exchanges and the importation of currency were also conducted.

118. In addition to suspicious financial activity, many of these cases involved the use of businesses to help launder criminal proceeds. In assessing our disclosures, 24 cases included a business as a subject of investigation or a beneficiary of a transaction.

119. The most observed business types included:

- Telemarketing business/call centre;
- Financial services company;
- Management consultants business;
- Real estate business/real estate investment firm;
- IT services business;
- Investment company; and
- Holding company.

* *Grandson scams involve seniors who receive a phone call from someone posing as a police officer or law enforcement official from another country, claiming that the senior's grandchild is in custody and they need to wire funds to bail them out of jail.*

CHINA

120. ML crimes in China are extending from the developed coastal areas to undeveloped areas. ML crimes appeared early in the southeast coastal areas, represented by those of underground money shops in Guangdong and Fujian Province. Recently it appears that ML crimes were spreading to the underdeveloped inland regions.

121. As for typologies, the technologies of ML are various and complicated. The traditional laundering methods, such as cash smuggling, were usually used in the past. However, the technologies of ML are becoming more and more diversified and complicated. The ML cases discovered with the help of the PBC mainly involve underground money shops, tax fraud, financial fraud, drug trafficking, smuggle and

corruption, among which, those related underground money shops and illegal foreign exchanges took the most proportion, while corruption cases mainly happened in state-owned enterprises and financial sectors.

The main ML/TF methods reported by China in 2011/12 include:

122. *To transfer the illicit money through overseas or domestic bank accounts.* Taking Pan' gang ML case in Shanghai for example, Pan took advantage of tens of domestic bank accounts to assist "Ayuan", a swindler lived in Chinese Taipei, to transfer and disguise the illicit money of online fraud. In another example of Ding embezzlement case in Beijing, Ding went to Hong Kong to open a personal account for transferring the illicit kickback from another company, avoiding the concern of domestic regulators and disguising his illicit money with the financial circumstance of Hong Kong.

123. *To remit the illicit money abroad though underground money shops.* By means of balancing their overseas or domestic bank accounts, underground money shops could provide cross-border remittance services without real cross-border fund flows, thus avoiding the anti-ML monitoring on foreign exchanges. Taking Cai ML case in Quanzhou, Fujian for example, Cai secretly remitted his proceeds of drug crime from Philippines to China through underground money shops.

124. *To disguise the illicit money with cash transactions and developed circumstance.* Cash transactions separated the origins and the whereabouts of money flow, which handicapped the investigation badly. In Huang ML case in Beihai, Guangxi, for instance, Huang controlled lots of bank accounts in Guangzhou and Shenzhen and was used to laundering money with cash transactions, clearing up the trace of ML. Meanwhile, it was normal that there were tens of millions of RMB in and out of one bank account in the developed areas such as Guangzhou and Shenzhen, which concealed Huang's ML.

125. *To take advantage of various financial services to avoid bank's concerns.* The financial services, such as online banking, telephone banking, facilitated the financial affairs of the public, as well as the money launderer. Taking the Luo underground money shop case in Shanghai for example, Luo and his fellows made full use of the cashier's check, telephone banking and other services to transfer money, and separated the transactions around different tellers in different banks in order to avoid the concern of banks.

126. *To register shell companies as "transit stations" for illicit money.* In order to launder criminal proceeds, criminals could place the illicit money into the lawful operations of registered companies, or registered lots of shell companies to disguise the illicit money with frequent and complicated transactions. Taking "10.20" case in Kaiping, Guangdong Province for example, Xu's criminal group registered a overseas company as the base of ML, then registered more than 20 companies and opened lots of bank accounts for depositing the embezzlement money and other illicit proceeds.

127. *To invest the illicit money in lawful sectors.* Not only could criminals launder the illicit money through investments, but also gain more proceeds. The investments here, including financial investments and real investments, involved various sectors such as banking, securities, futures, funds, insurances, real estates, noble metals, artworks and collections. Taking the Yang ML case in Chengdu, Sichuan Province for example, the criminal gang controlled several bank accounts of shell companies and other companies, and invested the illicit money of financial fraud in real estates, gas stations, securities, mines and power stations, gaining illicit proceeds of over tens of million yuan.

128. *To gamble with illicit money.* Not only was gambling one of the extravagant lifestyles of badger hats, but also one of the key ways to launder money. Taking Li embezzlement and net-gambling case for example, Li took advantage of his post to embezzle the traffic fees of RMB 118.5 billion Yuan into net-gambling, causing heavy losses to the public interests.

129. *To disguise illicit money with import and export trade.* This technology of ML always connected with smuggling crime. Operating import and export trades, criminals declared lower prices to the Customs for tax evasion and ML. Taking Duan smuggling and ML case in Wuxi, Jiangsu Province for example, the vendor sold tens of thousands tons waste plastic by declaring lower prices to the Customs, and asked the buyers to separate the payments in two parts: one is the payment according to the declared price, which would be paid according to the right procedure after applying to customs; the other is the balance between the declared price and the real trade price, which would be transferred to the appointed domestic bank accounts and laundered abroad to pay for the vendor.

130. *To launder money through the third-party payment platforms.* The third-party payment platforms gave facilities for the payment of e-commerce, but blocked the identification of banks on money flow, which might be misused by criminals to launder money. Taking a pyramid selling case in Shanghai for example, the suspects opened 36 accounts in one of the third-party payment platforms and misused to collect, transfer illicit money and return criminal proceeds, involving over 184 million Yuan.

131. *To smuggle the cash of criminal proceeds***.** Cash smuggling was one of the most original ML technologies, and was still used in the border areas at present. Criminals employed others to carry, transport or post cash in and out of the border to make cross-border transfers for the illicit money. For example, after gained the proceeds of drug crimes, the drug dealers in Yunnan Province employed the local villagers to carry the cash to the appointed person in Burma. Moreover, there were lots of “shuikes” at the Shenzhen Luohu Port and Zhuhai Gongbei Port, who made a living by means of carrying small-value cash through the ports and assisting the cross-border transactions for underground money shops and overseas casinos.

CHINESE TAIPEI

132. The usual methods to launder money in Chinese Taipei include cash couriers, structuring, purchasing portable valuable commodities, wire transfers, alternative remittance systems, using offshore shell companies/corporations, using offshore banks and offshore businesses, using family members or third parties, using foreign bank accounts and using false identification etc.

133. The emerging trends of ML threats include utilising new technological methods, cross border financial transactions and currency movement, and increasing use of mule accounts.

134. Recent customs detection have shown some false reporting and interception of packages with a lot of banking cards (such as UNION PAY). Those suspicious packages were sent from China and south-east Asian countries, and also listed false receivers’ addresses. Once the packages arrive in the shipping companies and were identified safety, the real holders would assign ignorant persons to draw for the packages. After investigations, we found those foreign banking cards were exploited by fraud syndicates as the ML tool of withdrawing the proceeds of fraud crimes in China which also caused the awareness of financial institutions in here. So far, the involved money amounted to billions NT dollars.

135. Information about the cards is shared with the related foreign counterparts. Those cards still could work in Chinese Taipei due to the issuing countries have no legislations to block the suspicious money and revoke the banking cards to stop the card's functions. These kinds of cases have caused threats of ML to the financial system in Chinese Taipei.

FIJI

Emerging Trends

136. Cybercrime has now become one of the emerging trends and threats for Fiji. The Fiji FIU has noted the use of internet banking facility portals at local commercial banks for cybercrime related activities such as phishing, hacking, identity theft and advance fee fraud.

137. Human trafficking and smuggling syndicates – In 2011, there was an increase in the number of human trafficking and smuggling syndicates detected in Fiji. In most cases, the modus operandi was the use of travel agents and massage parlors as front companies to facilitate such activities.

Declining Trends

138. Use of minor's bank accounts – there has been a general decrease in the number of minor's bank accounts used for tax evasion activities. The Fiji Government in 2010 introduced compulsory tax identification number (TIN) registration for all individuals and this may have addressed the use of minor's accounts for tax evasion purposes.

Continuing Trends

139. Advance Fee Fraud - The Fiji FIU issued a press release dated 23 September 2011 to the local media advising members of the public to exercise extreme caution when receiving unsolicited emails promising attractive job opportunities, payment of lottery awards, inheritance of large amounts of funds, lucrative investment opportunities and other "get-rich-quick" schemes. This was due to the large increase in advance fee fraud and cybercrime related activities.

140. Tax Evasion – the Fiji FIU continues to note typologies related to possible tax evasion such as the use of family members and the use of personal bank accounts to hide business proceeds.

HONG KONG, CHINA

141. No significant changes have been observed in ML trends in Hong Kong. The primary sources of laundered funds in Hong Kong continue to be illegal gambling, fraud and financial crimes, loan sharking, smuggling activities and vice. The ML methods range from cash transactions, wire transfers, use of stooge account, use of non-resident account, use of corporate account, etc. to complicate the transactions and to conceal the ultimate beneficiaries.

INDIA

142. With financial transactions coming under enhanced monitoring, TBML is being looked as a safer mode of transfer of value by criminal syndicates. Thus TBML is emerging as a threat. The inherent difficulties in determining correct transaction values of goods being traded and the sheer volume of trade make it convenient for the criminals to use trade as a vehicle and as a safe camouflage for movement of tainted funds. Misuse of export promotion schemes and zero duty commodities are emerging as the favourite avenues of TBML.

SRI LANKA

Emerging & Continuing Trends

- Submission of fraudulent documents in the form of bank drafts or cheques with larger values for encashment.
- Use of accounts for third party deposits where depositors were requested to deposit money into account as job application registration fees, investment schemes or lottery contribution. Such deposits were immediately withdrawn through ATMs.
- Remitting money out of Sri Lanka purported as payment for imports where no actual imports were taken place.
- Frequent transactions just below the reporting cash threshold.
- Large value deposits and immediate withdrawals.

Declining Trends

- Use of bank accounts to collect ransom
- Use of non-profit organizations for terrorist financing activities.

THAILAND

143. Insurgent groups continue to use cash couriers to move money because of easy access to air and land borders. Other means to move money is unregulated hawala which is operated through a money exchange business.

144. The rampant use of the ATM cards is emerging. Insurgent groups recruit students to open bank accounts. ATMs are then used for frequent transactions involving small amounts.

3.4. Effects of AML/CFT Counter-Measures

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

AUSTRALIA

145. 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.

146. In 2010–11, a number of new pieces of legislation relevant to AML/CTF were enacted, including:

- the *Law and Justice Legislation Amendment (Identity Crimes and Other Measures) Act 2011*, which amended a number of Acts including the *AML/CTF Act* in relation to certain written notices and the disclosure of information held by AUSTRAC

- the *Autonomous Sanctions Act 2011*, which came into effect on 26 May 2011 creating a comprehensive regime to apply targeted sanctions against countries or proscribed persons or entities of those countries, consistent with Australia's foreign policy objectives.

147. Additionally, the *Combating the Financing of People Smuggling and Other Measures Act 2011*, which is part of the suite of measures announced by the Australian Government in April 2010 to combat people smuggling, received Royal Assent on 28 June 2011. This Act amends the *AML/CTF Act* to strengthen AUSTRAC's regulatory regime for the money remittance sector. Under the reforms, remittance service providers are required to demonstrate their suitability for registration prior to being registered with AUSTRAC and their ongoing suitability to maintain registration. They also have to reapply for registration on a regular basis. Additionally, the new laws give us more flexibility to take enforcement action against remitters who do not comply with the requirements of Australia's AML/CTF regime.

148. On 10 March 2011, the Attorney-General, Minister for Home Affairs and Justice and the Commissioner of the Australian Federal Police launched the Criminal Asset Confiscation Task Force (CACT). The CACT brought together agencies with a key role in the investigation and litigation of proceeds of crime matters. The Taskforce is led by the AFP and includes the ACC, the Commonwealth Director of Public Prosecutions (CDPP) and the Australian Taxation Office.

149. The ACC plays an important role in identifying criminal proceeds and its intelligence and investigation capability has been integral in the confiscation of proceeds of crime cash and assets. The value of proceeds of crime assets that have been restrained as a result of operations that involved ACC so this financial year totalled almost A$30m. However the ACC continues to work with the Australian Commonwealth government and its partners to strengthen this and supporting legislation such as the Unexplained Wealth Legislation.

150. As these measures above have only recently been established, it is too early to judge their impact.

151. In 2010–11, AUSTRAC disseminated thousands of individual transaction and analytical reports to partner agencies. Among the most significant results attributable to the use of FIU intelligence were the 1,619 cases investigated by the Australian Taxation Office during 2010–11, which resulted in A$241.11 million in additional tax assessments being raised.

CHINESE TAIPEI

152. In furtherance of implementation of the politically exposed persons (PEPs) measures, the FSC has continually encouraged the Bankers Association to coordinate with the Joint Credit Information Center (JCIC) to establish a database of PEPs. The PEPs database will be set up by banks in order to implement FATF recommendation on PEPs.

153. Chinese Taipei recognizes the importance of seizure and confiscation of proceeds of crime for effectively preventing ML. The MOJ 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 Body. From June 1, 2011, dedicated units have been established under the Special Investigation Division in the Supreme Prosecutor's Office, Taipei, Taichung and Kaohsiung District Prosecutors Offices which are in charge of seizing and confiscating proceeds of crime related matters.

HONG KONG, CHINA

154. The newly enacted Anti-ML and Counter-Terrorist Financing (Financial Institutions) Ordinance (AMLO) will take effect on 1 April 2012. The AMLO seeks to codify the preventive AML measures, including the customer due diligence (CDD) and record keeping requirements for financial institutions with the attendant provisions for sanctions, and to put in place a licensing regime for remittance agents and money changers (RAMCs). The AMLO will strengthen the overall preventive AML/CFT measures / regimes in Hong Kong.

INDIA

155. The Indian Law which deals with ML (The Prevention of ML Act, 2002) was amended in 2009 and among large number of other offences included as predicate ***offences;*** the Customs Act was also included as a predicate offence. This has enabled TBML investigations into Customs Frauds also. Other major changes included delegation of powers of search, seizure & ***survey;*** legislative changes to increase the number of Investigating Officers under the Prevention of ML ***Act;*** modifications of certain legal provisions to bring clarity and to make them unambiguous. All these legislative changes have resulted in a sharp increase of number of cases booked, value of assets attached (frozen), number of arrests made and number of prosecutions filed, since 2009. The regulators too have issued directions to the stakeholders of their respective sector to report transactions which are suspected from AML/TF perspective. This too has also started yielding results.

SRI LANKA

156. Two main pieces of legislation relating to the AML/CFT regime in Sri Lanka were amended during the year providing more powers to Law Enforcement Agencies on tracing proceeds of crimes and broadening the criminalisation of terrorist financing with new definitions for individual terrorist, terrorist organisation and terrorist act. The amended legislation is referred to as the Prevention of ML (amendment) Act No 40 of 2011 and Convention on the Suppression of Terrorist Financing (amendment) Act No 41 of 2011.

4. CASE STUDIES OF ML AND TF

4.1 Trade Based ML and Transfer Pricing

CHINESE TAIPEI

157. Mr Lu was the chairman of a stock exchange listed company, X. With the intention of falsely boosting sales he instructed Mr Mon, the person in charge of his re-investment company Y to set up more than 10 paper companies in Hong Kong through the company service provider's assistance. Mr Lu divided those paper companies into buyers and sellers. He and Mr Mon exploited the titles of those companies to undertake false cyclic trades of the same goods (electronic components and parts). Mr Lu ordered Mr Mon to repeatedly import and export the same goods and declare them at Customs at a higher and higher price, which was many times as much as the original value of the goods, in order to quickly increase the false deals among Company X and the related paper companies. Company X accumulated the turnover over NTD 65.8 billion (approx. USD2.2 million) through these measures of multiple in money and paying for goods over two years.

158. Meanwhile, Mr Lu instructed his subordinates to use the above exaggerated sales/accounts receivable to apply to the banks for gaining operational funds. The exaggerated sales was also stated on the financial statements of Company X, and then it was filed to the Authority for permission of issuing the overseas exchangeable commercial bond (ECB) in amount of USD 157 million. Mr Lu used the USD 157 million to falsely make payments with those paper companies for covering their purposely deals to decorate the records in the accounting documents and financial statements and to convince the investor and bank. The money from banks' financing and ECB was partly appropriated as Mr Lu's personal fund to manipulate the stock price of Company X under dummy accounts. Mr Lu gained the proceeds of crime over 1 billion NT.

159. In the end Company X lost all assets estimated over tens billion NTD.

160. Mr Lu and his associates were prosecuted for breaching the Securities and Exchange Act and Business Entity Accounting Act, etc. In September 2011 Mr Lu was fined and sentenced to 12 years imprisonment.

FIJI

161. Company A (Fiji) imported spare parts from Company B in Japan and sold the parts locally. It is believed that Company A and Company B are related. Analysis found that there were some difference in the value of imports by Company A and remittances sent to Company B for the imports.

162. Mr X is the director for Company A. Mr X is an Asian national who is reportedly a resident of Japan and frequently travels between Fiji and Japan. Company A deals with automobile and machine spare parts. Company A imported used motor vehicle parts from Japan between January 2008 and March 2011. The used motor vehicle parts included used engines, car radios, seatbelts, jacks, seats, rear-view mirrors, wheels fitted with tyres, silencers, radiators, steering clutches, windscreens, and wipers used pneumatic tyres.

163. It was established that Company A had been electronically remitting funds to an account maintained at Mxxxxx Bank in Japan. The beneficiary of the funds remitted was stated to be Company B. Company B bears the same name as Company A. Company B is listed as a Japanese automobile business.

164. This case was referred to Customs Authority and a copy sent to Fiji Police-Counter Terrorism Unit for further investigation.

HONG KONG, CHINA

165. A syndicate in Jurisdiction A established two trading companies in the British Virgin Islands and Belize (both are well known offshore jurisdictions) to operate in Hong Kong. Two bank accounts were opened by the two trading companies.

166. Between 2005 and 2008, numerous victims all over the world were deceived into remitting money (totalling about US$30 million) into the two bank accounts of these two trading companies. Acting on information provided by overseas LEAs, Police raided the two companies and arrested two persons-in-charge. The accused claimed to be exporters of electronic products with shipments destined for an African country. The two companies engaged some remittance agents to remit the "sales proceeds" via Hong Kong back to Jurisdiction A. They also produced various trading documents, including Letters of Credit to support their claim. They blamed the remittance agents for substituting their business income with crime proceeds and they pleaded their innocence of the advance fee fraud. Upon further enquiries by Police they were subsequently charged for ML offence(s) in Hong Kong.

INDIA

Case 1

167. Company L located in India entered into an arrangement of merchanting trade with Company F located in a foreign jurisdiction and Company G located in another foreign jurisdiction. The arrangement entailed exports of goods from F to G. However, the trade finance arrangement made by L required on paper, goods to be exported from F in the name of L and then goods to be further exported to G, even though physically the goods were shipped from F to G. The Company L entered into an agreement with an underwriter U so that on the guarantee of the genuineness of the transactions by L, the underwriter U got irrevocable letters of credit opened in favour of F. The company F on shipment of goods to G got such letters of credit discounted with the bank. Initially company G accepted the goods and made payments to the underwriter U, who in the process received a commission. After successful completion of initial rounds of transactions, Company G defaulted on payments to U even though the letters of credit opened by it in favour of F had already been discounted by F. Thus merchanting trade finance mechanism failed. On investigation it was found that L was in league with F and G. The underwriter U was left with heavy losses. The predicate offences of cheating, criminal conspiracy and corruption were involved and merchanting trade finance was used to launder the criminal proceeds.

Case 2

168. Individual (A) located in foreign administration laundered the proceeds from narcotics trafficking. To remit part of the proceeds of crime to his home in India, he colluded with Indian exporters (B, C & D). The Indian exporters (B, C & D) overvalued the exports to earn export incentives. Individual A opened letters of credit abroad for the Indian exporters in the name of bogus firms (P, Q & R). The actual importers (X, Y & Z) situated in the same country as A collected the goods exported from India and gave to A the actual cost of the goods imported. A in turn remitted the inflated proceeds of exports

against the LCs opened by A in the name of P, Q & R. Thus the exporters B, C & D after receiving the higher remittances retained the actual costs and conveyed the additional amounts to the family members of A in India. The exporters B, C & D gained the exports incentive on overvalued exports and the actual importers X, Y & Z gained by avoiding the costs of opening the letters of credit. The individual A succeeded to launder the narcotic proceeds into India through trade finance.

Case 3

169. A STR received by the FIU identified suspicious advance inward remittance against exports by XYZ Ltd. Analysis by FIU-IND identified four additional bank accounts of XYZ Ltd. having substantial cash transactions with other banks. This intelligence was shared with the Enforcement Directorate and Customs.

170. Customs conducted verification of export records and found that XYZ Ltd. had not undertaken any export. The verification report was shared by Customs with the Enforcement Directorate.

171. The Enforcement Directorate conducted searches resulting in recovery and seizure of incriminating documents, and Indian currency equivalent to USD 138,000. Investigation conducted revealed that XYZ Ltd. had defrauded members of the public in attracting deposits from them on false promises of high returns. These deposits had generated substantial cash transactions in the bank accounts.

172. Subsequent large numbers of STRs submitted by banks to the FIU revealed information that XYZ Ltd. had indulged in real estate transactions and diamond trading and opened foreign bank accounts.

173. Investigation revealed that the proceeds of crime were invested in real estate as well as illegally transferred out of India. The money amassed abroad was brought back to India as advance payments against fake exports. Investigation also revealed that XYZ Ltd., fabricated invoices to show the local purchase of diamonds whereas no purchase of diamonds had taken place.

174. Important contributions were received on the basis of spontaneous exchange by a foreign FIU which identified related foreign corporate entities used as conduits for accumulation of funds abroad.

175. A case of ML has been registered and laundered properties of the value of USD 22.64 Million have been attached / frozen. International co-operation helped in identifying overseas assets of nearly USD 35 Million.

MACAO, CHINA

176. A criminal syndicate, XYZ, with its regional base in Country A, registered a shell company B in a country that is a tax haven. XYZ opened bank accounts at more than 10 banks in Country A and applied for high value loans.

177. Members of XYZ also set up a number of ‘supplier’ shell companies in Country C and Country D. The person in charge of shell company B claimed that the company dealt with cross-border trading activities, and thus purchased goods from Country C and Country D. Shell company B issued fake invoices as supporting documentation for obtaining loans from the banks in Country A, which could directly credit the funds to the bank accounts in Country C and Country D.

178. Once the "suppliers" shell companies received the remitted funds, they would immediately transfer the funds through a circuitous route back to shell company B or other controlled accounts. Some of the funds were used by shell company B as its banks' collateral and used to repay loans.

179. This fake transaction cycle caused huge damage to the banking system and resulted in a huge amount of outstanding non-performing loans for the banks. The person in charge of shell company B is believed to have escaped arrest.

180. From this incident, the banks reported a total loss of HKD70 million (approx. USD9 million) and the amount of remittance made by shell company B recorded was up to HKD250 million (approx. USD32 million).

MALAYSIA

Case I: Tax evasion through trade transactions with related entities

Methods used:

Use of nominees, trusts, family members or third parties etc.
Use of shell companies/corporations
Wire transfers
Currency exchanges/cash conversion

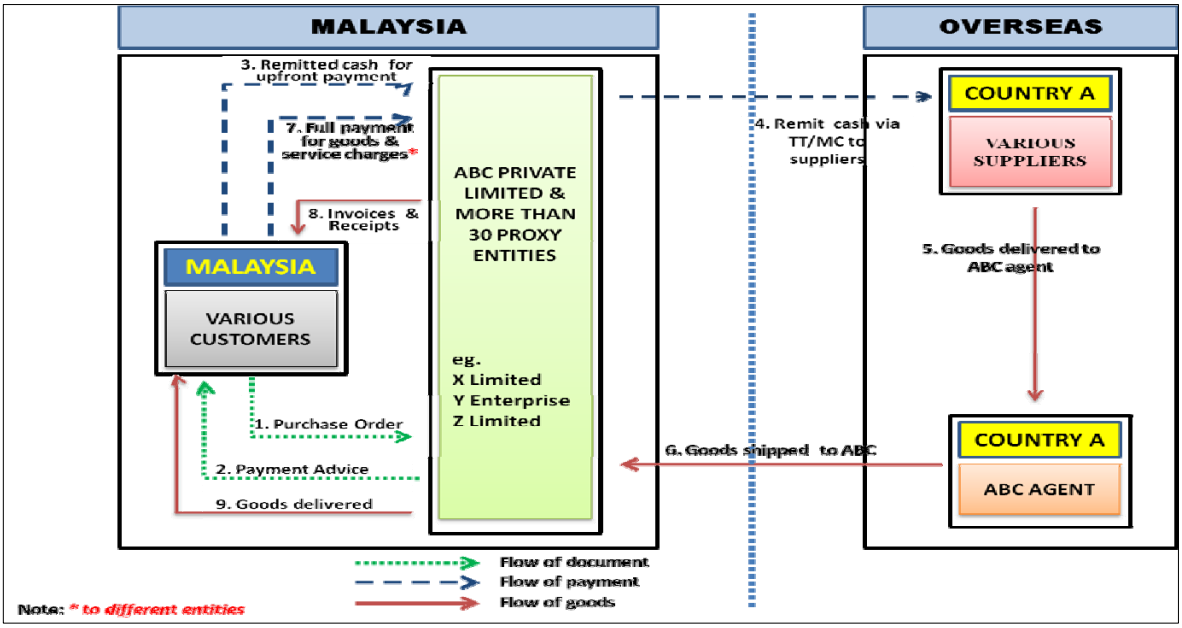
181. A family controls more than 30 business entities (sole proprietorships and private limited companies). ABC Private Limited (ABC) acts as the main company which is registered with the Inland Revenue Board of Malaysia (IRBM), however most of the other entities did not register themselves with the IRBM.

182. The organisation operated as a wholesaler agent dealing with imported goods of various types including clothes, electrical appliances, shoes, handbags, etc. ABC set up agents in other countries to manage the goods for storage and shipment purposes. The organisation used any of the business entities to communicate with their customers in terms of documentation, payments and delivery of goods.

183. ABC received orders from customers located in Malaysia to import goods from Country A. ABC would issue payment advice stating the price of goods, service charges for 'door-to-door' goods delivery as well as naming which entities will communicate with the customers. The customers would have to make upfront payments to the named entities (e.g. X limited). Upon receiving the partial payments, ABC would place orders to suppliers/manufacturers in Country A using different entities (e.g. Y Enterprise). Y Enterprise would remit cash via telegraphic transfer or money changers to suppliers/manufacturers in Country A.

184. Prior to the delivery of goods by ABC the customers would have to settle the balance of payments to Y Enterprise. ABC would also tell the customers to pay the service charges to different entities (e.g. Z Limited). Z Limited is not registered with the IRBM and as such the income is not reported to the IRBM. Y Enterprise also reported understated profits to the IRBM by submitting false documentation.

185. The investigation of this case is a joint effort between the IRBM with other LEAs. Subsequently, the IRBM agreed upon civil settlement with ABC and did not pursue the case to the court of law. However, other LEAs may pursue a different course of action.



Case II: Custom duties evasion through agents

Methods used:

Use of nominees, trusts, family members or third parties etc.
Use of shell companies/corporations
Wire transfers
Association with corruption

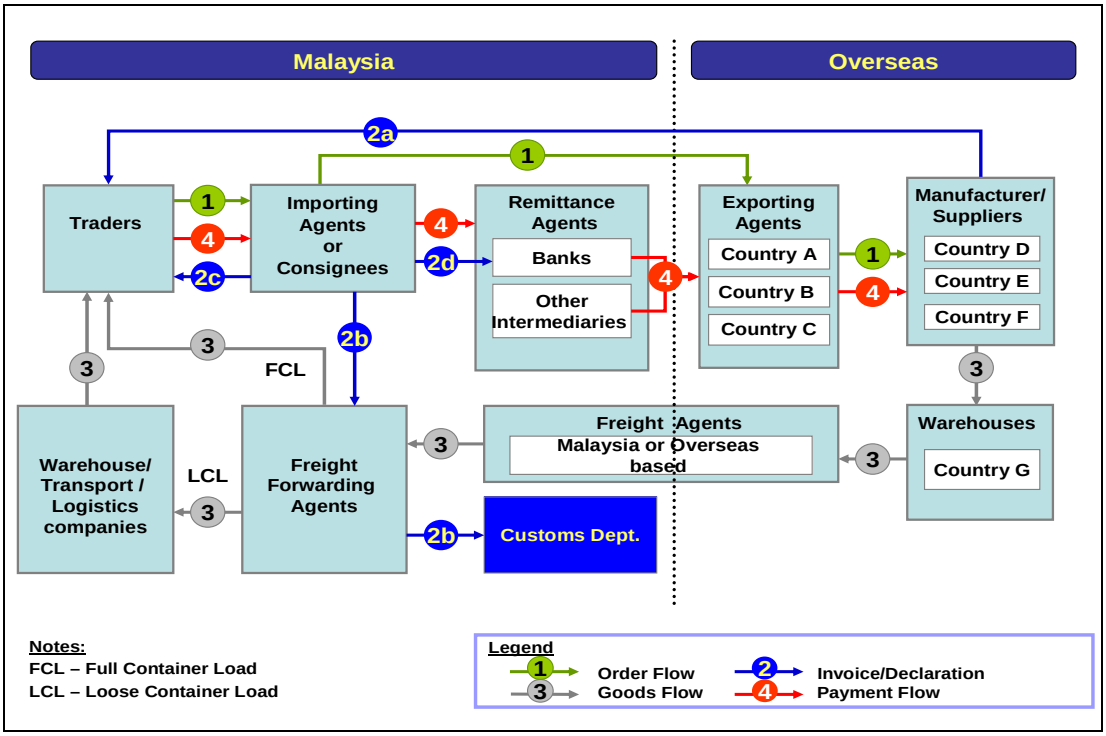
186. A group of entities (i.e. sole proprietorships and private limited companies) were established by several individuals to act as importing agents or consignees for the importation of goods. An importing agent was assigned to provide services to a number of traders (i.e. receive order/payment and issuance of invoice).

187. An order made by a trader would be sent to the manufacturer/supplier through the agents. A pro-forma invoice (2a) to confirm the order would be sent directly to the trader by the manufacturer/supplier. Depending on the arrangement between trader and the group, an initial payment would be made before goods were delivered to the warehouse, owned by this group. Goods were checked and packed at the warehouse to confirm that they met specifications.

188. A fictitious invoice (2b) with a lower amount is issued to the consignee and would be submitted for Customs declaration through the forwarding agents when the shipment arrived in Malaysia. Upon Customs clearance, goods would be delivered directly to the trader or sent to a warehouse for distribution.

189. The importing agent would issue an invoice (2c) to the trader based on the actual cost of goods sold. The balance of the invoice amount would be deposited by the trader into the agent's account plus the service fees charged for the importation. Another set of fictitious invoice (2d) would be prepared by the importing agent to support the remittance made to the exporting agent overseas. Payment would then be made to the manufacturer/supplier.

190. This modus operandi is used to disguise the fact that trader is the actual consignee for the imported goods and minimal amount is paid as customs duty. While investigation has discovered that payments made are for goods shipped into Malaysia, it has yet to establish that there are illegal funds remitted overseas supported by a fictitious invoice.



Case III: Mislead the banks in approving banking instruments to a corporation

Methods used:

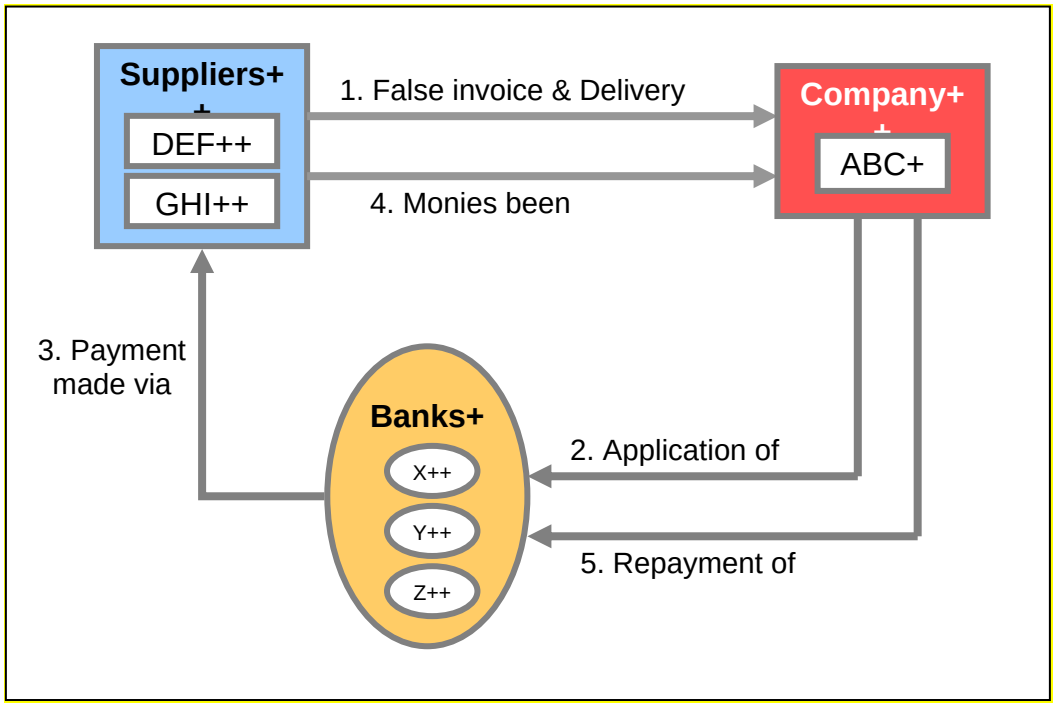
Use of companies / corporations
Use of banking facilities (i.e. Bankers Acceptance)
Use of false invoices / delivery notes / payment vouchers

191. By using its listed holding company as Corporate Guarantor, Company ABC has been granted with Bankers Acceptance (BA) by a few reputable banks. The limit for each BA is approximately RM50 million (approx. USD16.25 million) of which in order for the bank to pay in advance directly to the selected supplier for every goods supplied, Company ABC need to submit to the bank all relevant documents issued by the suppliers as agreed in a common trading.

192. The external auditor of Company ABC noticed something amiss when they detected that although Bank X had made payments as requested to the suppliers (as utilization of BA facility by Company ABC), the monies were transferred back by the supplier to Company ABC without conclusive documentation and explanation. This was done by submission of false documents (invoices and delivery notes issued by suppliers) to the banks.

193. An investigation revealed that the transactions were created by the directors of Company ABC with the knowledge and consent of the supplier. They managed to convince the banks in approving the amount requested for financing the purchase of the nonexistence goods. Investigation also revealed that there were 37 submissions of invoices and delivery notes by supplier DEF dated between December 2008 and April 2009 amounting to RM37.8 million (approx. USD12.3 million) to Bank X. There was no delivery of goods or services rendered to Company ABC.

194. Based on the investigation, prosecution of the directors of Company ABC for the offence under the provisions of section 368(a) of Companies Acts 1965 will be undertaken.



PAKISTAN

195. Mr X is engaged in the textile business in Peshawar. He had been operating a USD account at a commercial bank in Peshawar for business purposes.

196. The account details suggest that funds were being credited in cash mode followed by foreign remittances to textile companies in China with the purpose of importing cloth. These remittances were made against the pro-forma invoices of Chinese companies presented by Mr X. It is imperative to note that Mr X has not used any conventional banking facilities like a letter of credit for the importation of cloth. Hence, in the absence of proper documentation, the account activities created a suspicion that goods were being smuggled against which funds were remitted to the Chinese companies. The case has been referred to LEA.

SRI LANKA

197. Sri Lanka Customs filled an STR relating to activities of several individuals and entities that have violated a Customs Ordinance by defrauding a large amount of foreign exchange approximately USD 7.5m in the guise of outward remittances meant for imports.

198. Individuals and entities involved and their relationships can be summarized as follows:

Company	Proprietor/Director	Introduced to Bank by
"PS"	Proprietor - Mr. "S"	Mr. "S" has been introduced to the Bank by Mr. "A"
"BM"	Proprietor - Mr. "B",	Mr. "B" has been introduced to the

		Bank by Mr. “S”.
“SUM”	Directors - Mr “SO” and Mr “MR”	
“AC”	Directors - Mr “SO”, Mr “MI” and Mr “A”	Introduced to the bank by Companies “SUN” and “MT”.
“SUN”	Director - Mr “A”	
“MT”	Director - Mr “SO”	

199. All above companies are engaged in importation of fabric from country “U”.

200. Bank “H” has been identified as the main bank and supported the activities of above companies where they maintain accounts.

201. Preliminary investigation by the Department of Customs, revealed that Company “PS” and “BM” are non-existent and the import documents submitted to the banks for remitting money were forged. Furthermore, individuals identified as proprietors are also non-existent and forged national identification documents were presented to the bank to open bank accounts.

202. Bulk cash deposits were made into the accounts of Company “PS” and “BM”. All deposits were in amounts below the FIU threshold limit. It was also observed that most of these deposits were made during evening banking hours (from 3.00 pm to 6.00 pm).

203. Unusually large cash deposits to the above mentioned accounts were noted since the accounts were opened. However, from mid October 2010, it has significantly increased. Deposited cash has been remitted to an importer in Country “U” on the same day or the subsequent day, in favour of one of the main companies.

204. Investigations further revealed that other companies involved, “SUM”, “AC”, “SUN” and “MT” are engaged in the importation of fabric and they understated the value of the import consignment for customs purposes.

205. The mastermind behind the fraudulent activities involving all the above mentioned companies is the individual identified as Mr SO. He has given instructions to deposit cash into the accounts of Company “PS” and “BM”.

206. Several import consignments were seized by Customs as some of the suspects were absconding investigations and goods have not been claimed.

207. All related accounts of the above mentioned individuals and entities have been suspended by the FIU pending further investigation.

208. The FIU has referred the matter to the Criminal Investigations Department to further investigate the ML offence and to Exchange Control Department to investigate violation of Exchange Control regulations. Furthermore, the Department of Customs imposed penalties on individuals and entities relating who violated the Customs Ordinance.

4.2 Human Trafficking and People Smuggling

AUSTRALIA

Case Study – human trafficking

209. Authorities received an allegation that three foreign nationals were being forced to work in sexual servitude at a registered brothel. A search warrant of the premises found that a number of foreign women were working at the brothel. Investigations resulted in two persons each being charged of three counts of possessing a slave and three counts of exercising the rights of ownership over a slave.

210. While full details of payments and transactions made in association with the three women remain unknown, AUSTRAC financial transaction data indicated that the manager of the brothel had made a number of low-value international funds transfer instructions (IFTIs) to Hong Kong and Malaysia. These international transfers were made through banks and authorities suspected to be in connection with the three victims.

211. In addition, AUSTRAC information assisted authorities to identify a number of women linked to common addresses. These addresses were also linked to the manager of the brothel. The women made a number of structured international transfers to Hong Kong and Malaysia, which authorities suspect may have been for the purposes of facilitating the movement of trafficked individuals to Australia.

Case Study – Use of remitters to facilitate people smuggling

212. Australian law enforcement agencies cooperated with foreign law enforcement counterparts to investigate international people smuggling networks. The investigation identified the use of remittance dealers for financing people smuggling. Foreign law enforcement agencies subsequently brought charges against remitters in their jurisdiction in relation to people smuggling, ML, and providing financial services without appropriate licensing.

213. The investigations identified that people smugglers use funds held by Middle East-based remitters for staged transfer to people smuggling facilitators. The stages of funds transfers were linked to the progress of individuals being smuggled through transit countries.

214. The methodology has a number of benefits for those involved in people smuggling:

- The people *smuggler* can be confident that the funds exist to pay for the individual's passage to Australia.
- The Middle East-based *remitter*, located in the source country, has access to funds to use in the operation of their business. Their business cash flow is assisted through the staged release of funds to the people smuggling facilitators.
- The *individuals being smuggled* make payments to the Middle East-based remitter and effectively have their funds held in trust. The funds are safe-guarded while they progress through transit countries, avoiding the need for them to carry cash, with its associated risks.

215. The methodology uses a three-part process which relies upon international funds transfer instructions and funds deposited with Middle East and Australian-based remitters:

Part 1: Funds transfer instructions from Australia

216. An Australian-based remittance dealer accepts instructions from customers to send money to beneficiaries in the Middle East. The Australian-based customers provide funds to the remitter by:

- depositing funds directly into the remitter's bank account; or
- providing funds directly to the remitter.

217. Where funds are provided directly to the Australian-based remitter it results in limited information being available for authorities to identify the original owner of the funds, because:

- the deposit made directly to the remitter's bank account may be less than the AUD10,000 threshold transaction reporting limit; or
- the remitter may accumulate cash payments from numerous customers and then deposit the funds into their bank account in one amount.

218. The Australian-based remitter maintains a record of individual payments made by Australian customers intended for beneficiaries in the Middle East. The remitter uses these records to balance transactions with their counterpart remitter in the Middle East.

Part 2: Imports from Asia by entrepreneurs in the Middle East

(i) The counterpart remitter in the Middle East receives payments from local businesses to pay for imported goods from suppliers in Asia.

(ii) The remittance dealer facilitates funds transfers to the Asian suppliers by instructing an associated Australian-based remitter to transfer funds from Australia using the deposits from Australian-based customers (refer Part 1), avoiding official reporting of the transaction in relation to import tax and excise duty payable in the Middle Eastern country.

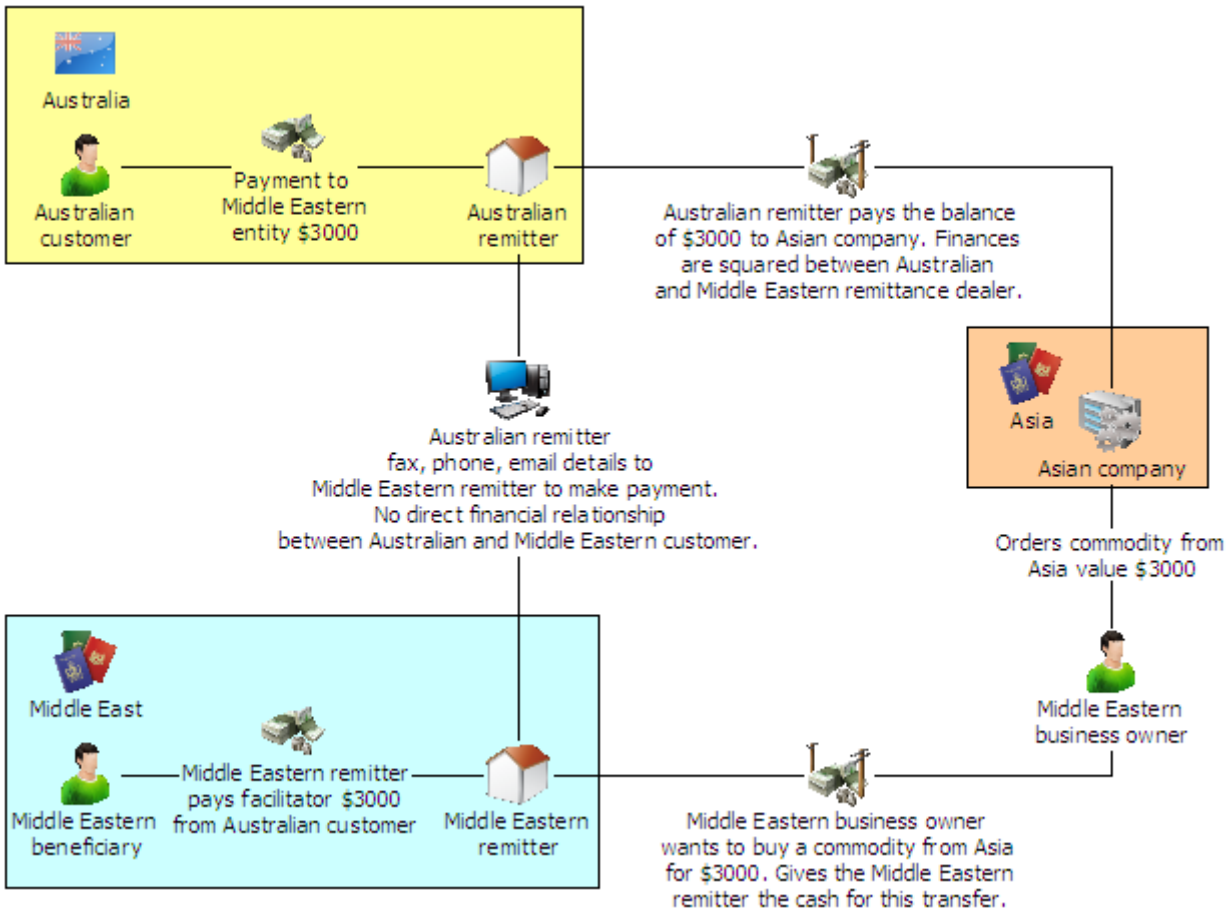
219. At this stage, funds provided by the local businesses can be used by the Middle East-based remitter to facilitate people smuggling by making payments to people smuggling syndicates at specific points in a person's passage from their country of origin.

220. To confirm payment has been effected for the goods being imported from Asia, the Australia-based remitter sends a copy of the funds transfer instruction to their counterpart.

Part 3: Payments to effect funds transfer instructions from Australia

(i) The Middle East-based remitter will arrange for payments to be made to the intended recipients as per the instructions from the Australian-based customers (refer Part 1).

221. The financial methodology is complete when the export company in Asia has received its payment and the funds have been released to the intended recipients in the Middle East.



222. In practice, it is likely that the methodology would involve an even more complex series of payments which could vary in value and take place over a longer timeframe before all parties involved are 'in balance' and all funds are with their intended beneficiaries.

223. Of significance to this methodology is the fact that where funds are transferred overseas:

- international funds transfer instructions may not identify the sender or the ultimate beneficiary
- some international funds transfers may not be reported at all.

FIJI

224. From December 2010 the Fiji FIU and Fiji Police Force (FPF) were taking cooperative steps to proactively target high risk local businesses such as massage parlours and travel agents.

225. The Fiji FIU received an STR from a local commercial bank in January 2011 on a local Asian businessman Mr B, who was reportedly the director of one of the travel agencies. Subsequent FIU analysis established that Mr B did not hold a work permit in Fiji, and that several inward remittances from an Asian country were made into his personal account with a local commercial bank in Fiji. The Fiji FIU established that several cash withdrawals were made by Mr B from ATMs in New Zealand, Indonesia, Thailand, Japan, Netherlands, Spain and Australia.

226. There are strong suspicious indicators suggesting that the local Asian businessman Mr B may have used the travel agency as a front" business to facilitate human trafficking related activities.

THAILAND

227. Thai Police arrested Mrs A and charged her for "procuring, seducing or taking away for an indecent act women and a child for sexual gratification of others". The victims were lured to work in Japan, but instead forced into prostitution. Authorities were informed that the perpetrator's proceeds of crime were transferred via cash couriers from Japan to Thailand. Police seized Mrs A's property valued at 12 million Baht in foreign bank notes and deposit totaling 9 million Baht and a Mercedes valued at 3 million Baht. Almost all properties seized were in the possession of her mother or registered by her mother's name. Finally, the court ordered forfeiting all seized property.

4.3 Underground Banking and Alternative Remittance Services Banking

AUSTRALIA

228. A joint Australian Federal Police (AFP) Australian Crime investigation identified individuals who were part of a well organised international ML scheme responsible for the laundering of millions of dollars through cash deposits and international funds transfers.

229. The investigation into the activities of a remittance business network and its agents in Sydney and other major Australian cities identified that large amounts of cash were being deposited into Australian bank accounts operated by the network.

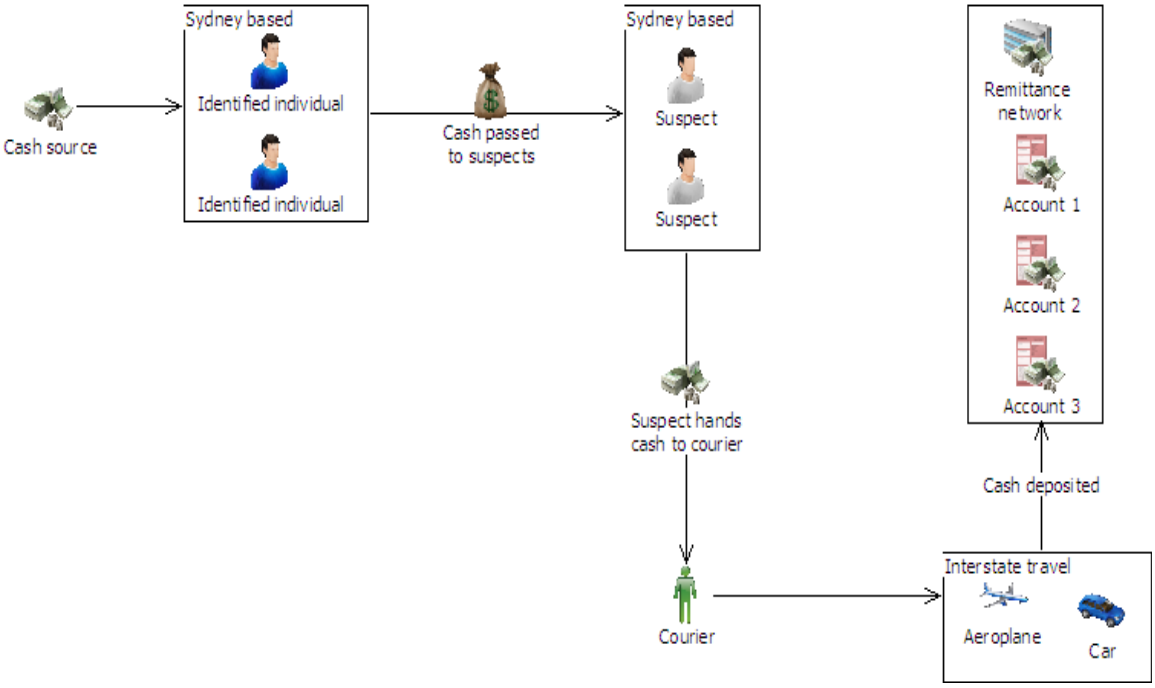
230. The investigation found that the bank accounts had received multiple large cash deposits in denominations of AUD50 or AUD100 notes. Some of the deposits were worth AUD100,000 and, altogether, these cash deposits totalled millions of dollars. Investigators identified that the majority of the deposited funds were subsequently transferred overseas.

231. The investigation also revealed that previously unidentified individuals from Sydney had been depositing large amounts of cash into three Australian bank accounts linked to a remittance business network operating in Australia.

232. The investigation focused on the identified members of the Sydney-based network and two suspects responsible for the cash deposits. The identified members of the remittance network would take delivery of the cash in Sydney and then pass it on to the other suspects. These suspects would either deposit the money in Sydney into the bank accounts linked to the remittance network, or give the money to a courier for it to be physically transported interstate by road or air for depositing into the same, linked bank accounts.

233. During the resolution of this matter, investigators searched vehicles, businesses and residential premises in Sydney and ultimately seized more than AUD9 million cash.

234. The investigation led to three people being charged with recklessly dealing in the proceeds of crime (that is, money or property) to the value of AUD1 million or more. A fourth person was charged with possession of money or property reasonably suspected of being proceeds of crime. One of the offenders received a sentence of 14 months imprisonment, while another received a sentence of seven years.



Case Study

235. AUSTRAC's monitoring systems identified a substantial increase in cash activity undertaken by a remittance dealer. Further analysis identified inconsistencies between the information the remitter had reported to AUSTRAC, and the information reported by the financial institutions where the remitter was a customer.

236. The Australian Crime Commission's (ACC) and AFP undertook further investigations. As a result of the investigation two suspects were charged with ML offences under the *Criminal Code Act 1995*. One of the suspects was the remittance dealer, while the second suspect, an associate of the first suspect, allegedly acted on behalf of third parties to deposit large amounts of cash into accounts owned by the remittance dealer.

237. This investigation was triggered by recognised ML indicators. AUSTRAC data revealed significant discrepancies between the transactions reported by the remittance dealer from its own 'business' perspective, and the transactions reported to AUSTRAC by the financial institutions which dealt with the suspect remittance dealer as a customer (that is, transactions reported from a 'customer' perspective).

238. In a typical remittance business, authorities would reasonably expect that, over time, a high proportion of the cash paid by customers to the remittance dealer to pay for international funds transfers would eventually be deposited into a bank account held by the remitter. This 'balancing' of money received by the remitter against money ultimately deposited with financial institutions should be recorded in various AUSTRAC transaction reports, as per the below example:

Step 1

239. A remittance dealer receives a total of AUD100,000 cash from various customers as payments for international funds transfer instructions. The remitter, reporting from a 'business' perspective, should submit to AUSTRAC:

- threshold transaction reports (TTRs) recording any cash payments of AUD10,000 or more they have received from their customers; and
- international funds transfer instruction (IFTI) reports detailing all international transactions.

Step 2

240. Over time, the remitter would normally be expected to deposit some, if not all, of the AUD100,000 cash with a financial institution. The financial institution would in turn report these cash deposits to AUSTRAC in TTRs – in these reports, the remitter would be recorded as a 'customer' of the financial institution.

241. If the remittance dealer operates in the manner described above, it is comparatively straightforward for AUSTRAC to follow the flow and volume of money through its business. This is because the amounts reported from both 'business' and 'customer' perspectives are relatively consistent with each other.

242. However, certain business practices by the remittance dealer may lead to discrepancies between the transaction amounts reported by the remitter and the deposit amounts reported by financial institutions.

243. For example, the remitter may decide not to deposit the entire AUD100,000 cash into a bank account to pay for the outgoing international transfers, instead using some of the cash to pay for incoming funds transfers sent to Australian-based customers. This is consistent with the 'hawala' method of transferring funds. The remitter may also utilise hawala for international transfers by arranging for an overseas associate to pay an overseas beneficiary directly.

244. Authorities recognise that the use of hawala by remitters may lead to some discrepancies between a remitter's turnover as reported from the 'business' and 'customer' perspectives. However, the effect of hawala alone seldom explains larger discrepancies. Where significant discrepancies do occur, AUSTRAC is more likely to suspect a remittance business to be handling and moving proceeds of crime, and escalate such matters to law enforcement.

245. This investigation foiled a major ML operation. Transaction reporting information received by AUSTRAC revealed a number of significant and suspicious changes in the financial transaction patterns of the remittance dealer involved:

- The remittance dealer's activities changed from facilitating small outgoing international funds transfer instructions (IFTIs), to accepting large cash deposits and facilitating large IFTIs. This spike in financial transaction activity was clearly inconsistent with the remitter's previous profile and history.

- Shortly after this increase in the size of IFTIs, business bank accounts held by the remittance business stopped receiving deposits. However, AUSTRAC analysts identified additional accounts operated by the remittance business, which had been opened under a new company name. Under this new company name, the remitter's business practices appeared to change. While the remitter continued to report to AUSTRAC that the majority of its remittances were being sent to Iran, information received from institutions dealing with the remitter as a customer reported that a significant proportion of the business's outgoing IFTIs were now being sent to the United Arab Emirates (UAE).

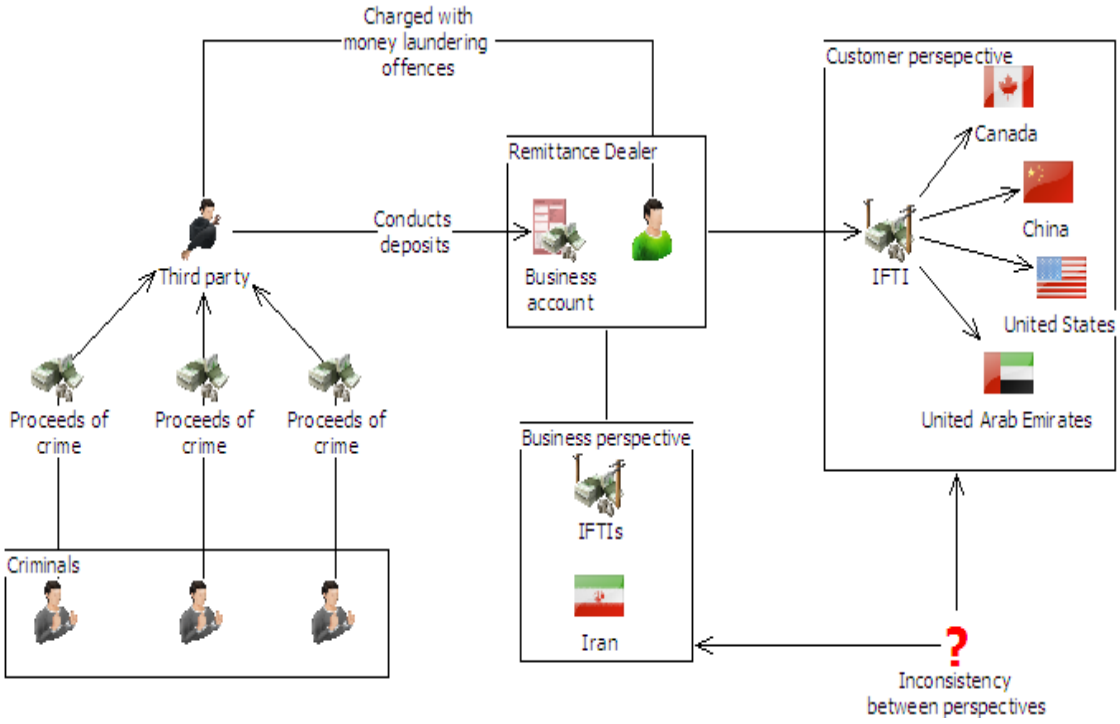
- The remitter's transaction activity continued to escalate while operating under the new company name. Over a three-month period the remitter recorded cash deposits totalling AUD34 million and outgoing IFTIs totalling AUD33 million. At the peak of activity, the remitter was receiving cash deposits into its bank account of AUD1 million each day, and on one occasion received almost AUD4 million in two days. The third party making these large cash deposits made no attempt to conceal them, and they were conducted at the same bank branch.

- Information provided by reporting entities was also invaluable in highlighting discrepancies in the remitter's activities. The value of the remittance dealer's business activity as reported to AUSTRAC was significantly less than that reported by the financial institutions that dealt with the remitter as a customer. This discrepancy in reporting strongly suggested to authorities that the remittance dealer was dealing with proceeds of crime, rather than funds generated by legitimate business activities.

246. The following table highlights the discrepancies in the remitter's transaction activities as reported from customer and business perspectives, over a 10-month period:

Transaction types	**Value as reported by the remittance business**	**Value as reported by reporting entities dealing with the remittance business**	**Difference**
Cash deposits recorded in TTRs	AUD48 million	AUD92 million	AUD44 million
Outgoing IFTIs	AUD55 million	AUD95 million	AUD40 million

247. As the remitter's cash activity escalated, law enforcement agencies executed warrants against the syndicate and stopped its operations. The AFP arrested two individuals, and restrained AUD1.2 million. While the original source of the funds could not be established, the large amount of cash involved led authorities to suspect that the funds were the proceeds of crime.



HONG KONG, CHINA

Case 1

248. In October 2010, a cross-boundary telephone deception was reported in which a victim of Jurisdiction A was deceived into remitting USD100,000 to a bank account in Hong Kong. These funds were further remitted through a remittance agent in Hong Kong into two bank accounts in Jurisdiction B and distributed elsewhere. After investigation, the bank account holder and the remittance agent were arrested and charged with ML offence(s) in Hong Kong.

Case 2

249. In 2008, Customs smashed a syndicate distributing counterfeit and illicit cigarettes to street-level peddlers. Eight (8) bank accounts held by the masterminds had received cash or transfer deposits amounting to HK$114 million (approx. US$14.7 million) from 16 peddlers over 2 years. It was also found that HK$35.8 million (approx. US$4.6 million) of which had been transferred out from the said accounts to an unregistered remittance agent. However, the final destination of the transferred money could not be ascertained.

250. The core syndicate members were respectively convicted of ML offence(s) and sentenced to 5.5 years imprisonment at maximum. Assets of HK$9.5 million (approx. US$1.2 million) were restrained. The unregistered remittance agent was also convicted of the offence of non-registration and fined HK$8,000 (approx. US$1,000).

INDIA

251. Person 'X', a practicing Medical Doctor, was moving funds between India and abroad through illicit channels by use of Alternate Remittance System (Hawala). He was in contact with certain persons in a number of foreign countries including Canada, UAE, USA & UK, who used to give instructions to 'X' for delivery of funds to various persons in India, as well as they used to transfer funds in the Accounts of certain exporters from India as remittances against exports on the instructions of 'X'.

252. Searches were carried out at the premises of 'X' and documentary evidence indicating receipt and distribution of funds by 'X' were recovered and seized, which revealed that more than 1,000 recipients had availed of the network established by 'X' for receipt of money from abroad through an Alternate Remittance System (Hawala). These 1,000 recipients included a sizeable number of exporters. Investigations revealed that these exporters had either exported cheap goods or had fabricated export documents to account for the large remittances received in their accounts.

253. On conclusion of the investigations, 'X' has been charged for illegal movement of funds amounting to Rs.727 Million (US$16 Million).

4.4 Commodity Exchanges (barter – e.g. reinvestment in illicit drugs)

THAILAND

254. A syndicate operated its trafficking business in the southern parts of Thailand, including illicit cross-border trade with a neighboring country. The authorities found out that the gang had opened a luxury car dealer enterprise in Bangkok as place to launder their drugs proceeds and used it for direct exchange of drugs payment. Four suspects were arrested and 134,000 amphetamine tablets, three cars, jewellery, luxurious

electrical appliances and 6,000,000 Baht in cash was seized (approx. USD192,000). Assets including one house and three condominiums were also frozen. Authorities also seized their 17 sport cars, valued at 120 million Baht (approx. USD3.8 million).

4.5 Gambling/Casinos

AUSTRALIA

Case Study 1

255. Casino staff lodged two suspicious matter reports (SMRs) with AUSTRAC detailing suspicious deposits of foreign currency into casino gambling accounts. These reports assisted border protection authorities to detect and apprehend two Japanese nationals who were attempting to leave Australia without declaring physical currency worth more than AUD10,000.

256. Over a seven-year period the pair had made a number of trips to Australia, bringing with them substantial amounts of Japanese Yen, which they deposited into casino gaming accounts. The source of these funds is unknown.

257. Throughout this period, the pair had regularly submitted cross-border movement of physical currency (CBM-PC) reports indicating they were carrying physical currency worth AUD10,000 or more. CBM-PC reports must be submitted by travellers arriving in and departing from Australia when carrying physical currency worth AUD10,000 or more (or the foreign currency equivalent).

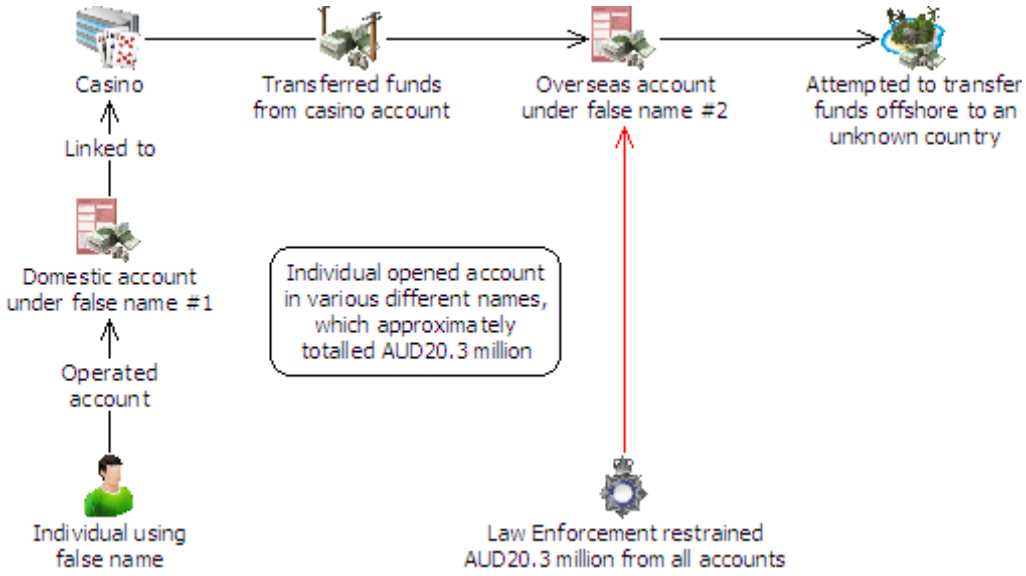
258. However, during more recent visits to Australia, the pair had not submitted any CBM-PC reports, even though they were undertaking similar levels of casino gaming activity, involving large amounts of cash. This was assessed as an indication that the pair may still have been carrying, but not declaring, significant amounts of cash during more recent visits.

259. Analysis of AUSTRAC information over a seven-year period revealed that the pair had deposited more than AUD11 million cash into gaming accounts in Australia. However, over that same period the pair had only reported bringing into Australia the equivalent of AUD7 million cash.

260. AUSTRAC alerted border protection authorities about the discrepancy and authorities stopped the pair as they attempted to leave Australia. It was discovered that they were carrying foreign currency worth almost AUD30,000 – none of which had been declared. The pair were each issued with an infringement notice and fined for failing to report movements of physical currency valued at AUD10,000 or more.

Case Study 2

261. A law enforcement agency identified an individual who was operating a bank account under a false name. The bank account had a balance of in excess of AUD300,000, and was linked to a casino account. The individual attempted to transfer funds from the casino account to an overseas account, which was also operating under a false name. Further investigations revealed that the same individual had opened two accounts under false names. As the investigation progressed, a total of approximately AUD20.3 million was uncovered in a number of different accounts, and these funds were restrained by law enforcement officers.



.

JAPAN

262. As media has reported recently, it is alleged that an ex-chairman of a major paper manufacturing company, who 'borrowed' approximately USD 140.8million from the company for his personal spending, has kept the money in offshore casino accounts.

263. Media coverage of the case report that the Daio Paper Corp indicated that Ikawa squandered his personal fortune, he took out more than 10 billion yen ($130 million) in loans in 26 installments from the company's seven subsidiaries to cover his losses. It was reported that Ikawa repeatedly lost in high-stakes casino games in Macao and Singapore.

264. Ikawa, the grandson of the firm's founder, was arrested on suspicion of having committed aggravated breach of trust and violating the Companies Law.

4.6 Non Profit Organisations

NEW ZEALAND

265. Reporting by media and NZ Police in March 2011 highlighted a variation on an old theme; the abuse of a non-profit organization (NPO) via the internet. In this case it was a Mexican charity that was used to fool New Zealanders into laundering money inadvertently through a personal banking account. NZ Police report that the targets in the fraud received an unsolicited email that had a link to a genuine United States charity working to eradicate poverty in Mexico.

266. However, there was a link further down the email with a request to set up a bank account to receive donations. The email recipient was told to keep 10% of the donation as an administration fee and to forward the remainder through a money wiring service. In essence, after this process the 'donated' money becomes virtually untraceable and targets are caught up in an off-shore ML scheme.

267. NOTE: It is debateable whether or not the targets of the fraud can be seen as assisting in ML. Although the targets maybe 'unwitting' participants they may be considered as being 'reckless as to the intent' of the offence if they turn blind eye to the suspicious nature of the transactions. As such they may be considered as committing the offence of ML.

PAKISTAN

Case 1

268. Mr A declared that he was involved in a real estate advisory business. He had been maintaining USD and PKR accounts at a commercial bank in Faisalabad.

269. A significant amount of foreign remittances were received from international NGOs in the USD account of Mr A followed by cash withdrawals. The foreign currency cash was converted into PKR in the open market and then equivalent amounts were deposited in the PKR account of Mr A followed by cash withdrawals in tranches. Upon further investigation, it was discovered that Mr A was also serving as the Executive Director of an NGO. It was discovered that Mr A had urged international donors (NGOs) through different websites to remit funds for disaster relief and church plantation in Pakistan. Hence, the aforementioned unusual pattern of transactions highlight the suspicion that the funds received from international NGOs could have been utilized for purposes alternative by using suspects own foreign currency accounts.

Case 2

270. It was reported that a US NGO M/s. ABC Associates working in Pakistan is under investigation of LEA of the charge of embezzlement of funds of projects. As per details, the intelligence aid agency gave a contract to M/s. ABC Associates, a foreign based NGO, of significant amount for the construction of a road. Later on, the aid agency found something fishy in the project and approached the NAB, which had already identified an embezzlement of funds. Further, Mr A, an authorized signatory of cheques of all suspicious accounts, was also investigated by the LEA for fraud and embezzlement. A detail analysis of accounts revealed a scheme of ML. The relevant scheme appears as below:

Stage 1: Mr A embezzled funds of M/s. ABC Associates and sent them abroad to his family members and friends;

Stage 2: The counter-parties who received the funds sent them back home to Pakistan to Mr A's personal accounts and Mr A explained to the bank that funds are his salary/income.

Stage 3: Again Mr A withdrew the same funds in cash and got them converted in PKR currency and transferred them to his personal PKR accounts where he again withdrew the same funds in cash mode to avoid an audit trail of embezzled funds.

271. The overall pattern of activities suggests layering and integration of corruption money. The case has been disseminated to LEA.

4.7 Investment in Capital Markets

CHINESE TAIPEI

272. Duan Fa Technology Corporation was registered to engage in computer software and hardware selling and buying, maintenance and system service. Mr Ten was the president

of the corporation in charge of the technology department. Mr Chan was the General Manager in charge of administrative department. Mr Chan Gin was the Vice General Manager in charge of the finance department.

273. During 2003 to 2004, the corporation's meetings of shareholders made a resolution to publicly offer shares with the price of 10 NT dollars each share to raise capital of 43.4 million NT dollars (approx. USD1.48 million). However, the three persons mentioned above colluded for their personal gain, by falsely releasing the capital increase announcement to the public with different prices of 15, 20 and 22 NT dollars per share which was over the agreed price. Then they appropriated the over collected stock payment in amount of NTD 7,912,388 (approx. USD 268,400). For disguising and concealing the proceeds of crime and criminal behaviours, they used third parties as nominees to buy the shares with the appropriated funds. After that, they sold the shares to the new investors for laundering the appropriated money.

274. They were suspected of violating the provisions of Company Act, Securities and Exchange Act, Criminal Code, ML Control Act and Commercial Accounting Act. The case was referred by the Investigation Bureau to the Prosecutor's Office for prosecution.

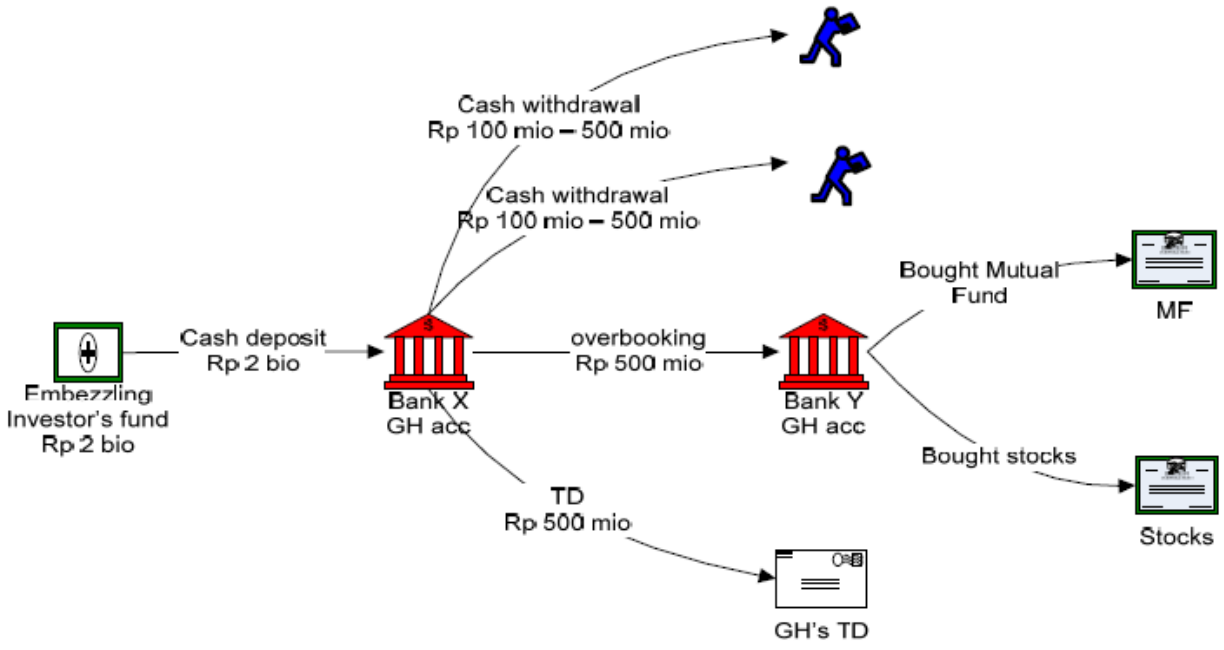
INDONESIA

Case 1:

275. GH who was a branch manager of Securities X had traded stock using his client's portfolio/money without the customer's authorisation.

276. GH transferred the stock to various securities accounts. The profits from embezzling investor's funds were transferred to GH's account. The fund then overbooked to many different accounts and reinvested in mutual funds, TD and stocks.

Flow of Funds:



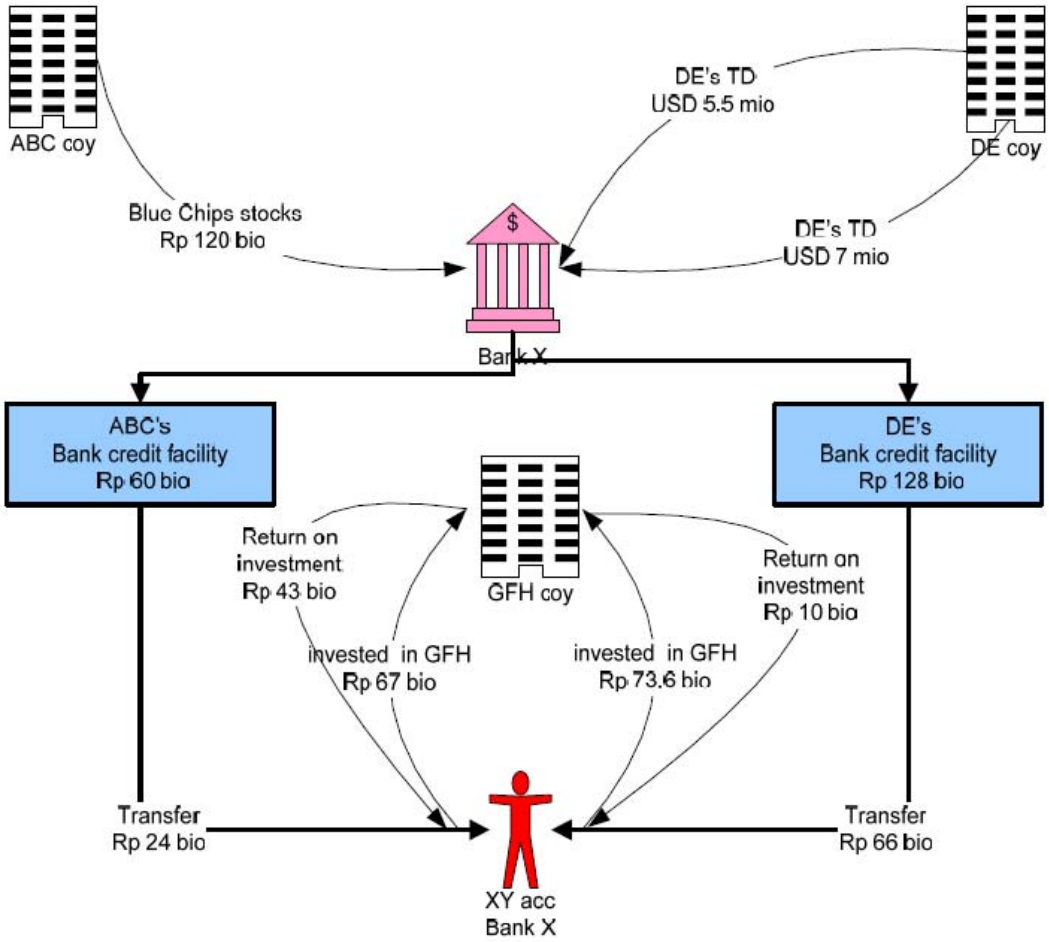
Case 2:

277. Bank S sold its marketable securities amounting to USD41Million. Part of the result amounted to USD 34Million was transferred to Bank X account and the rest amounted to USD7Million was converted into Time Deposit on behalf of DE Company. This TD was recorded as receivable in Bank X's bookkeeping.

278. DE company used the TD for obtaining a credit facility amounting to Rp 128 bio from Bank X. ABC company also obtained bank credit amounting Rp. 60 billion. This facility was guaranteed by blue chip stocks which were fraudulent.

279. The money from credit was transferred to XY's account amounting to Rp 66 bio (from DE company) and Rp 24 bio (from ABC company). XY transferred the money to GFH's account. GFH was company involving in embezzling investor's money through selling fraudulent mutual fund.

Flow of Funds:



4.8 Co-Mingling of Funds

INDONESIA
Case 1 – terrorist financing through an internet business

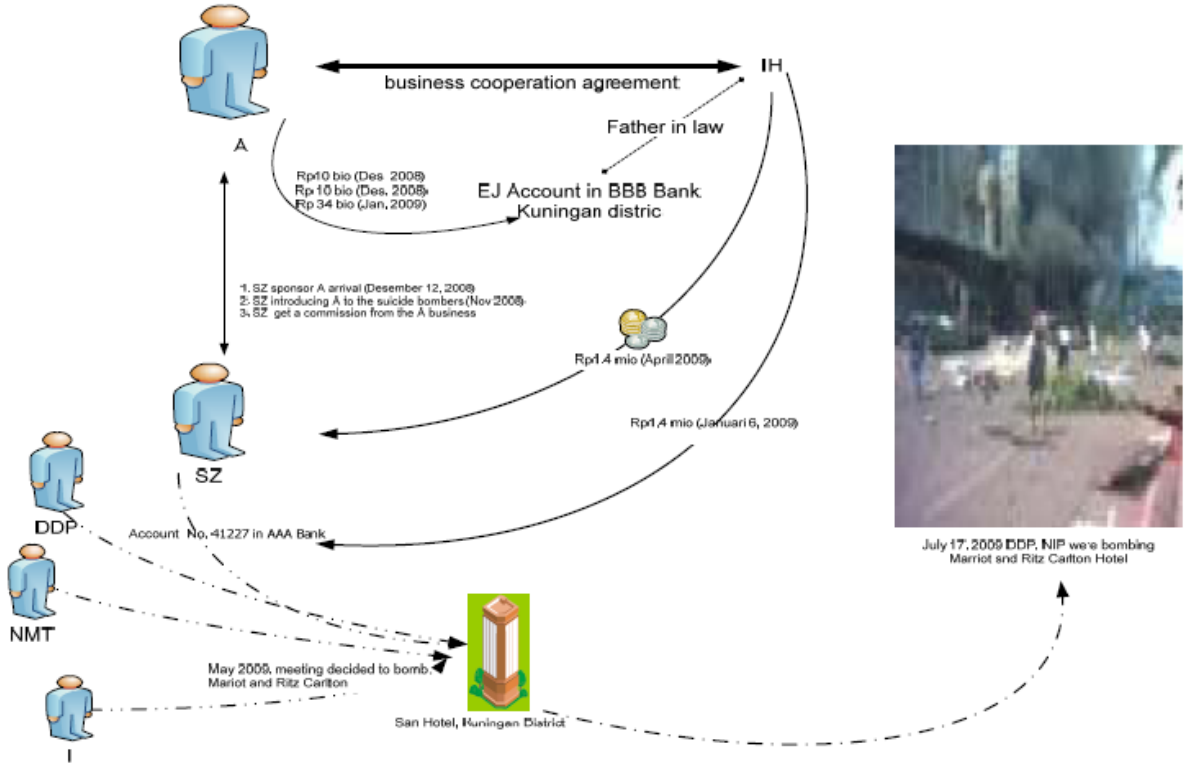
280. SZ is one of the participants in the J.W. Marriot and Ritz Carlton hotel bombing in July 2009.

281. It is known that A has a close relationship with SZ. The relationship can be seen that the SZ is a sponsor of the arrival of A in Indonesia and SZ also introduced A to suicide potential.

282. SZ helped A to develop an internet business with IH in Kuningan, West Java. SZ obtained a certain percentage of the trade agreement. The fee for SZ amounted to Rp2.8 mio was sent by A using IH bank account in January and The money was used by SZ to fund for J.W. Marriot and Ritz Carlton hotel bombing.

283. SZ was shot dead in October 2009.

Flow of Funds:

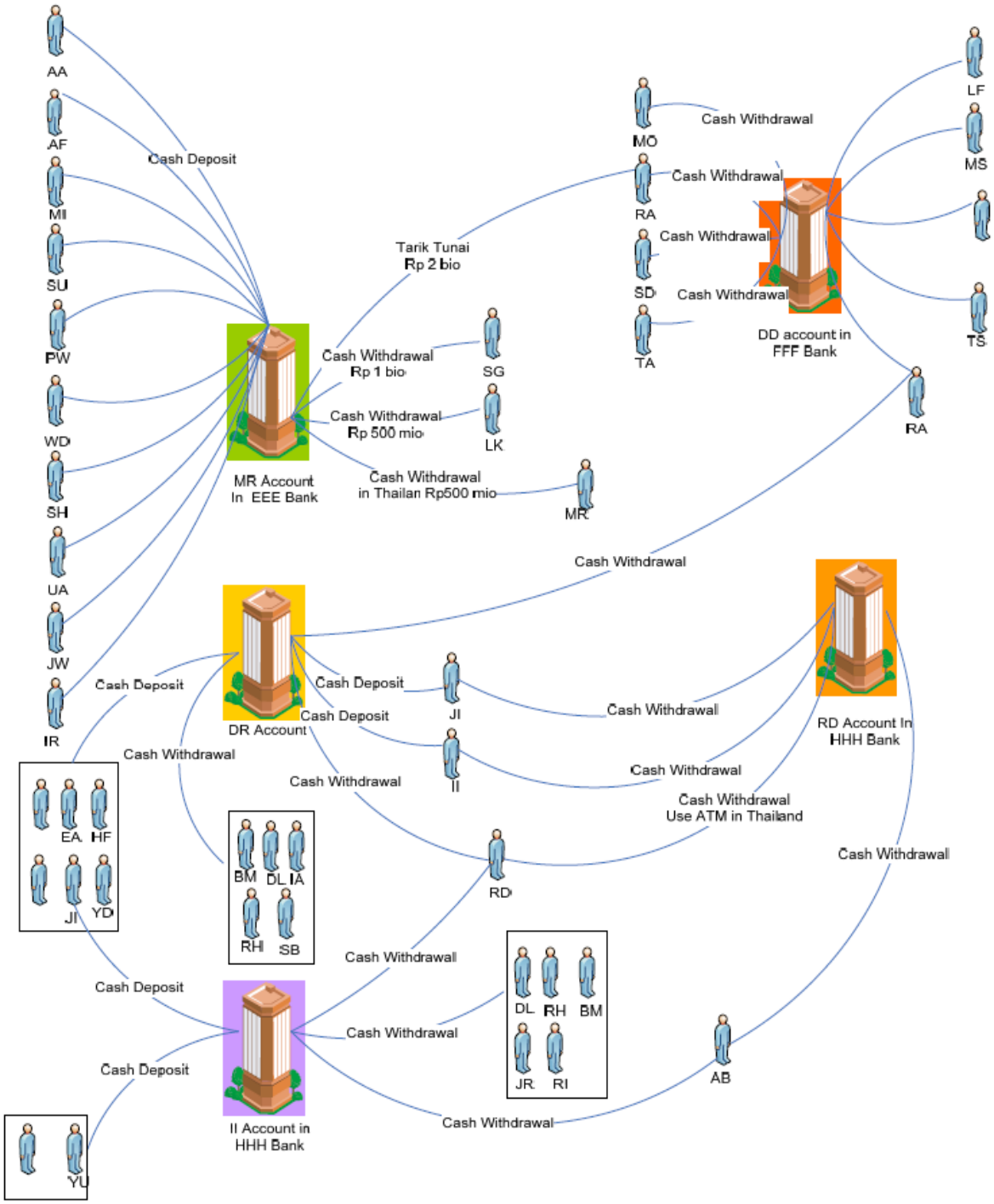


Case 2:

284. SM, a Nigerian national living in Thailand is suspected of using an Indonesian bank account for drug trafficking. Parties involved in this case were MR (entrepreneur/clothing shop owner), DD (owner of cell phone voucher shop), DR (clothes store owner), RD (clothing store manager).

285. Based on RD's bank accounts, it was identified that there were many cash transactions and withdrawals via ATMs. ATM withdrawals were often conducted in Thailand. Depositors' of the funds were DR and other parties (the relationship with DR is unknown).

Flow of Funds:



THAILAND

Bandidos Case

286. In early July, 2006, after receiving information from Liaison Officers in Bangkok that members of the Bandidos motorcycle gang in Thailand had colluded with British mafia to buy extensive commercial interests in Samui Island (a world-famous beach resort destination) the police and the DSI arrested four people, two Britons, one Dane, and one Thai. They were charged with extortion and ML offences. An early investigation found that they allegedly ran many businesses on the island, including property developments, restaurants, and entertainment and tourist enterprises, as fronts for unlawful activities. In addition, they were also accused of laundering criminal proceeds from the British mafia and converting them to legitimate assets. They were also believed to be members of a transnational criminal organization. At the time of writing, further investigation is still in progress.

287. Thai authorities provided the following summary from press reports of the case (Bangkok Post, July 3 2010).

- A former land official has been sentenced to 2 years and 3 months in prison for document forgery and malfeasance in connection with the Bandidos criminal syndicate and plots of land on the resort island of Samui.
- Pramual was arrested in 2006 along with 3 members of the Bandidos, an international motorcycle gang operating on Samui.
- As a land surveyor attached to Surat Thani land office, Pramual was found to have provided the foreign suspects with forged land documents.
- Gang members had allegedly extorted money from local businesses, laundered money and bribed local officials to issue illegal land ownership documents for public land.
- The foreign suspects allegedly ran many businesses on the island as fronts for illegal activities, including property development firms, restaurants, entertainment and tourist enterprises.
- The arrested foreigners were identified as British nationals Peter Watkin Jones, 40, Crispin John Granville PatonSmith, 43, and Danish national Kim Lindegaard Nielsen, 36.

4.9 Use of Shell Companies/Legal Persons

THAILAND

Terrorist financing case

288. An Asian man, aged 38, transferred money from a subprime system to Mr Q who paid to bomb makers in southern Thailand many times. He registered 999 Travelling & Sightseeing Co. Ltd. established in Bangkok for the purpose of air ticket distribution as shell company.

289. An Asian man (Pakistani), aged 38, transferred money from subprime system to Mr. Q (Thai muslim living in the southern most of Thailand) who paid to bomb makers and car-bombers (Terrorists) in the deep south of Thailand many times. He registered 999 Travelling & Sightseeing Co. Ltd. established in Bangkok for the purpose of air ticket distribution as a shell company. He also facilitated underground banking system to the

human trafficking gangsters who sell the fraudulent passports to the migrants from South Asia. These gangsters use Thailand as a hub for producing fraudulent passports and sometimes give a safe haven for illegal migrants before moving to the third country.

AUSTRALIA

Case Study

290. Authorities investigated three suspects for their involvement in the use of an offshore scheme to defraud the Commonwealth and avoid paying almost AUD4 million in tax.

291. The suspects allegedly used an offshore scheme promoted by an overseas accounting firm to avoid paying the tax:

- A fictitious intermediary company was set up by the overseas accounting firm, which charged the main company, owned by the suspects, for inflated business expenses on 44 separate occasions.
- By artificially inflating their business expenses, the suspects reduced their company's taxable income and therefore the amount of income tax they were required to pay.
- After the main company paid the inflated invoices issued by the intermediary company, the funds used to pay the invoices were diverted into offshore trust funds held in each of the suspects' names.
- These undeclared company profits were subsequently channelled through the trust funds and bank accounts, and finally withdrawn by the suspects as cash from automatic teller machines in Australia.

292. Ultimately, two of the suspects were found guilty of conspiring to dishonestly cause a loss to the Commonwealth and sentenced to six-and-a-half year's imprisonment.

CHINA

Liu Underground Money Shop in Nanchang, Jiangxi, Province

293. On 4 June 2009, the verdict of Liu underground money shop case was announced in the first instance by the People's Court of Nanchang County, Jiangxi Province. Liu was found guilty of illegal business operations and was sentenced to 1 year imprisonment and fined RMB 110,000 Yuan (approx. USD17,500). This was the first "illegal-settlement-service" underground money shop case sentenced.

294. The Nanchang Branch of PBC received an anonymous phone report that a children's wear store in Xihu District, Nanchang, was suspected of ML. After investigations, three stores (a grocery store and a stationery sports goods store in Qingshanhu District and a children's wear store in Xihu District), were found to have opened bank accounts in two banks and frequently operated suspicious transactions involving RMB 2.7 billion Yuan (approx. USD 427,301,992), which was obviously out of accord with their scope and size of business. The PBC suspected the three stores of ML and reported the matter to the local police.

295. The special investigation group carried out an unified action both in Shenzhen and Nanchang on 21 May 2008, and successfully arrested Liu and other 7 suspects, with a large number of bankcards, bankbooks, Digital Certificates, computers, mobile phones and register materials, seals of the companies captured, and 71 bank accounts with RMB 22.95 million Yuan frozen (approx. USD3.6 million).

296. Liu had registered over 10 shell companies since 2007. She opened bank accounts for these shell companies and applied for online banking services; meanwhile, she opened personal accounts with the ID cards of others or her own and also applied for online banking service; with these bank accounts, she illegally operated a settlement service without any real business background and made illicit proceeds. From May 2007 to May 2008, she received the money of RMB 8.97 billion Yuan (approx. USD 1.42 billion) from nearly 600 companies in Shenzhen with the controlled companies' accounts and transferred to the controlled personal accounts in complicated laundering technologies.

MACAO, CHINA

297. An overseas scam syndicate assigned three of its members (X, Y and Z) to Country A and planned to commit crimes. Member X and Y each set up 2 shell companies (4 companies in total) in Country A and opened bank accounts under these shell companies' names as a channel to commit scams. Member Z was the main operator, controlling the illegal activities behind the scenes.

298. These members stated on the Internet that they could help clients to invest in stocks with a high return, as a result a number of clients from different parts of the world remitted funds to the 4 shell companies' bank accounts, total funds received approximately amounted to HKD15 million (approx. USD1.9 million). After receipt of funds, these scam members immediately withdrew all the funds in cash. After investigation, two of the members were arrested for further criminal charges.

4.10 Offshore Banks, International Business Companies, Offshore Trusts

NEW ZEALAND

299. In December 2010 Mrs A and Mrs B were sentenced in relation to helping launder an estimated NZ$4.5 million (approx. US$3.6 million). They worked for Mr C, an Auckland based drug importer. Mr C, who had claimed unemployment benefit for 20 years, had earlier pleaded guilty to various charges (including importing Class A drugs and ML) and received an 11 year sentence. The Crown case against Mr C involved the laundering of NZ$4.5m, of which NZ$2.5m was transferred overseas to Mr C's European accomplice, Mr D, who escaped NZ in 1999 after being charged with conspiracy to import cocaine.

300. Mrs A, through a company she set up (of which Mr C was the sole shareholder), transferred money to bank accounts in Liechtenstein that Mr D could access. Mrs A also ran a nightclub owned by Mr C and operated a safe deposit box which contained several hundred thousand dollars; the proceeds from the sale of imported ecstasy and cocaine. Mrs B banked money for Mr C, converting some of it into Euros and withdrawing other amounts when instructed. Two Lithuanian money launderers were also involved and travelled to NZ to act as cash couriers carrying NZ$880,000 (approx. US$708,017) back to Europe.

301. Whilst reports indicated that neither woman lived a lavish lifestyle nor were they paid large sums for their work, Mrs A had a NZ$275,000 Porsche (bought for cash) registered in her name as well as NZ$40,000 VW vehicle. Mrs A and Mrs B both denied knowing the money was illicit and were acquitted of conspiring to import drugs. Mrs B received 10 months home detention and Mrs a 12 months, with 160 hours' community work.

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

AUSTRALIA

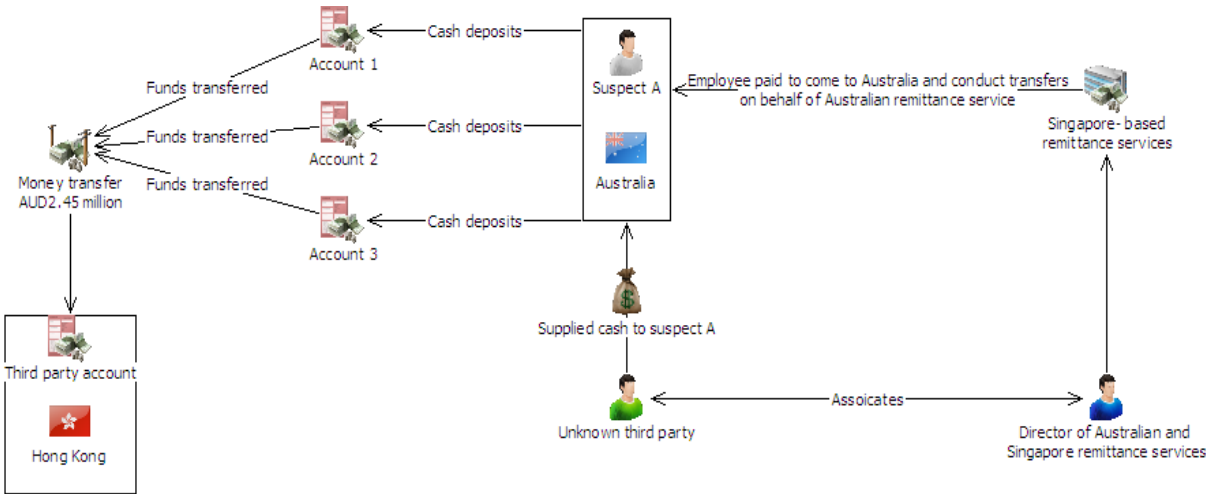
Case Study

302. Law enforcement officers commenced an investigation into an Australian money remittance service provider who was suspected of laundering illicit funds. Authorities alleged that the director of the money remittance business, before departing Australia, sent more than AUD7 million of suspected illicit funds to accounts, some held in his own name. Authorities established that the director also operated a remittance business in Singapore.

303. Authorities subsequently began investigating the activities of Suspect A, who was a Malaysian national. Suspect A arrived in Australia from Singapore on a temporary visa, claiming to be visiting friends and family. It was established that Suspect A had previously been employed by the director to work at his remittance business in Singapore. Authorities believed that the director paid for Suspect A to come to Australia for approximately one month to conduct international funds transfers on behalf of the Australian remittance business. Further investigations revealed the following:

- Upon arriving in Australia, Suspect A established three accounts at three separate leading financial institutions. All three accounts were established in Suspect A's own name.
- Over an 11-day period, Suspect A made cash deposits worth AUD2.45 million into the three accounts. On each occasion the deposited funds were subsequently remitted to third-party accounts in Hong Kong on the same day of the deposit.
- Prior to attending the branches to make the deposits, Suspect A collected the cash and instructions about transferring the cash from a third party.
- Authorities established that this third party was also linked to the Australian money remittance business.
- During the period in which these cash deposits were being made, AUSTRAC received two suspect matter reports (SMRs) from reporting entities. The SMRs detailed the substantial amounts of money involved in the deposits and subsequent international funds transfers.

304. Suspect A was arrested and charged with two counts of ML, and sentenced to one year's imprisonment with a non-parole period of seven. After serving this sentence, Suspect A was also deported from Australia.



CHINESE TAIPEI

305. Since Mr A had debts piling up, he plotted a scheme to use third party's name to set up a company named "LG Display Co. Ltd" and falsely claimed that the business was to sell LG LCD products. In 2009, Mr A made use of the opportunity of the short supply and high demand for LCD panels. He falsely claimed that he could supply every model of "LG" LCD products but buyers would have to pre-pay 30% of the cost for the goods. Mr A hired some unknowing staff to promote the business and successfully got 4 orders. He asked those 4 buyers to pay the down payment of NTD 48,630,939 (approx. USD 1.7 million) in total to "LG Display Co. Ltd" but always postponed delivering products. Mr A went into hiding and evaded dealing with the orders. His fraud scheme was disclosed to the Police by those buyers. After investigation, the Police found that after Mr A got the proceeds of crime, he used USD 370,000 and NTD 1,440,000 (approx. USD 48,450) to repay his overseas and domestic debts respectively. Moreover, with the intention to conceal the rest of the proceeds of crime, Mr A instructed his sister, Ms B, to deposit NTD 17,880,000 (approx. USD 600,000) into her unknowing friend Mr C's account and kept NTD 7,000,000 (approx. USD 237,000) in Ms B's house. Those proceeds of crime were seized during the investigation. This case was referred to the Prosecutor's office by the Police and Mr A was accused of fraud and laundering money.

FIJI

306. A number of suspicious transaction reports were received from a local commercial bank on an Asian businessman operating a local seafood business. The business is reportedly engaged in the wholesaling and retailing of fish. Suspicious transaction reports on his wife who is engaged in "domestic duties" but reportedly carrying out business transactions from her personal bank account were also received.

307. In June 2011, suspicious transaction reports were received on 4 employees of the same seafood business who are of different ethnic origins. The four employees were receiving large amounts ranging from FJ$100,000 (approx. USD 55,000) to FJ$800,000 (approx. USD 440,000) being deposited into their personal bank accounts within a period of 4-8 months.

308. The questionable deposits were reportedly derived from business income. It was alleged that the business owner was trying to divert business proceeds through the use of third parties and family members (wife) in order to evade tax.

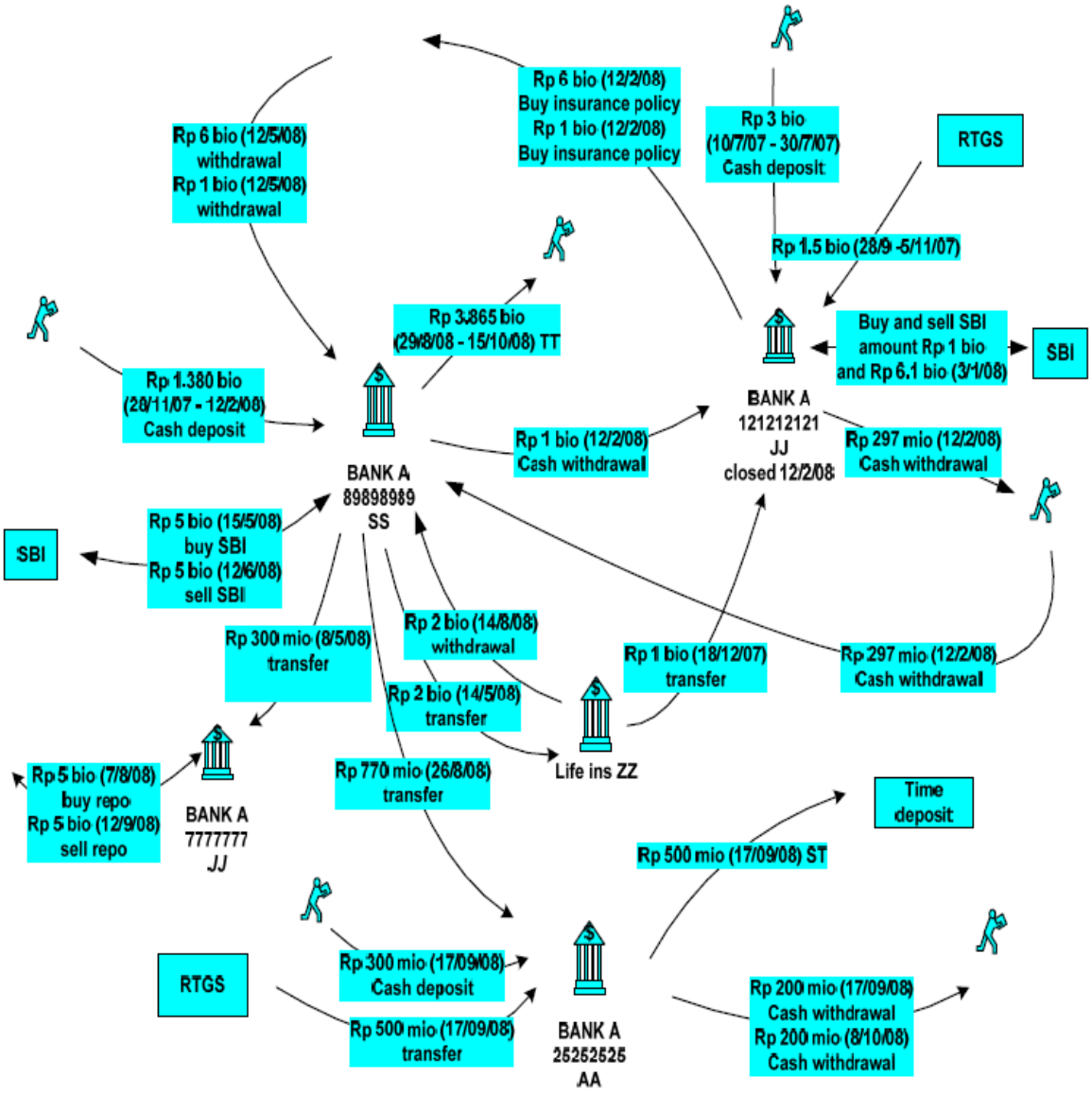
309. The case has been referred to the local tax authority in June 2011 for further profiling.

INDONESIA

310. Termination of a PEP's policy insurance premium was paid to third party who is known to be the PEP's business partner. The source of the funds to pay the life insurance premium was from the PEP's bank account. The PEP's bank transactions revealed money deposited from many parties including the PEP's business partner.

311. The money in the PEP's account was used to buy investment instrument and placing in time deposit.

Flow of Fund:



THAILAND

312. Mr A was a drug trafficker who set up a methamphetamine-producing factory near the Thai-Myanmar border. His factory had the capacity to produce 10,000 methamphetamine tablets a day. He normally hired hill-tribe people to transport the tablets to his customers, mostly in Bangkok, by using a pick-up truck. One day his hired man was caught at the checkpoint near Phetchaboon province while transporting more than 100,000 methamphetamine tablets, worth more than 10,000,000 Baht (approximately US$250,000). Because his hired man was caught red-handed, he admitted to the police that he was hired by Mr A to transport these methamphetamine tablets to Mr A's customers in Bangkok.

313. The police then ran a background check on Mr A and found that he did not have a credible profession, but owned a luxurious house and many cars and deposited a lot of money in various local banks. The police also found that Mr A transferred money many times to Ms B, his mistress. After the police had probable cause to believe that Mr A committed a drug trafficking offence and a ML offence, and that Ms B committed a criminal offence of ML, the police then asked for the approval of a judge to issue a warrant for the arrest of Mr A and Ms B.

314. At the subsequent trial, both Mr A and Ms B were found guilty. Mr A was sentenced to life imprisonment for committing a drug trafficking and a ML offence while Ms B received two years' imprisonment for committing an offence of ML.

4.12 Use of Professional Services (Lawyers, Accountants)

AUSTRALIA

315. An employee of an Australian sole principal law firm received an email from a web-based account referring to a previous telephone conversation confirming that the law firm would act on the person's behalf. The person asked the employee to accept a deposit of $260,000 for the purchase of machinery in London. The person requested details of the law firm's trust account, provided the surname of two customers of a UK bank and confirmed that costs could be deducted from the deposit amount.

316. The employee provided details of the firm's trust account and confirmed that the firm would act for the person. When the $260,000 was successfully transferred to the firm's trust account, the person requested the money to be transferred as soon as possible to a bank account in London after costs and transfer fees were deducted. The person provided sorting code, account number and swift code of an account of a bank in London. The employee executed a subsequent transfer of AUD258,799 to the designated account.[12]

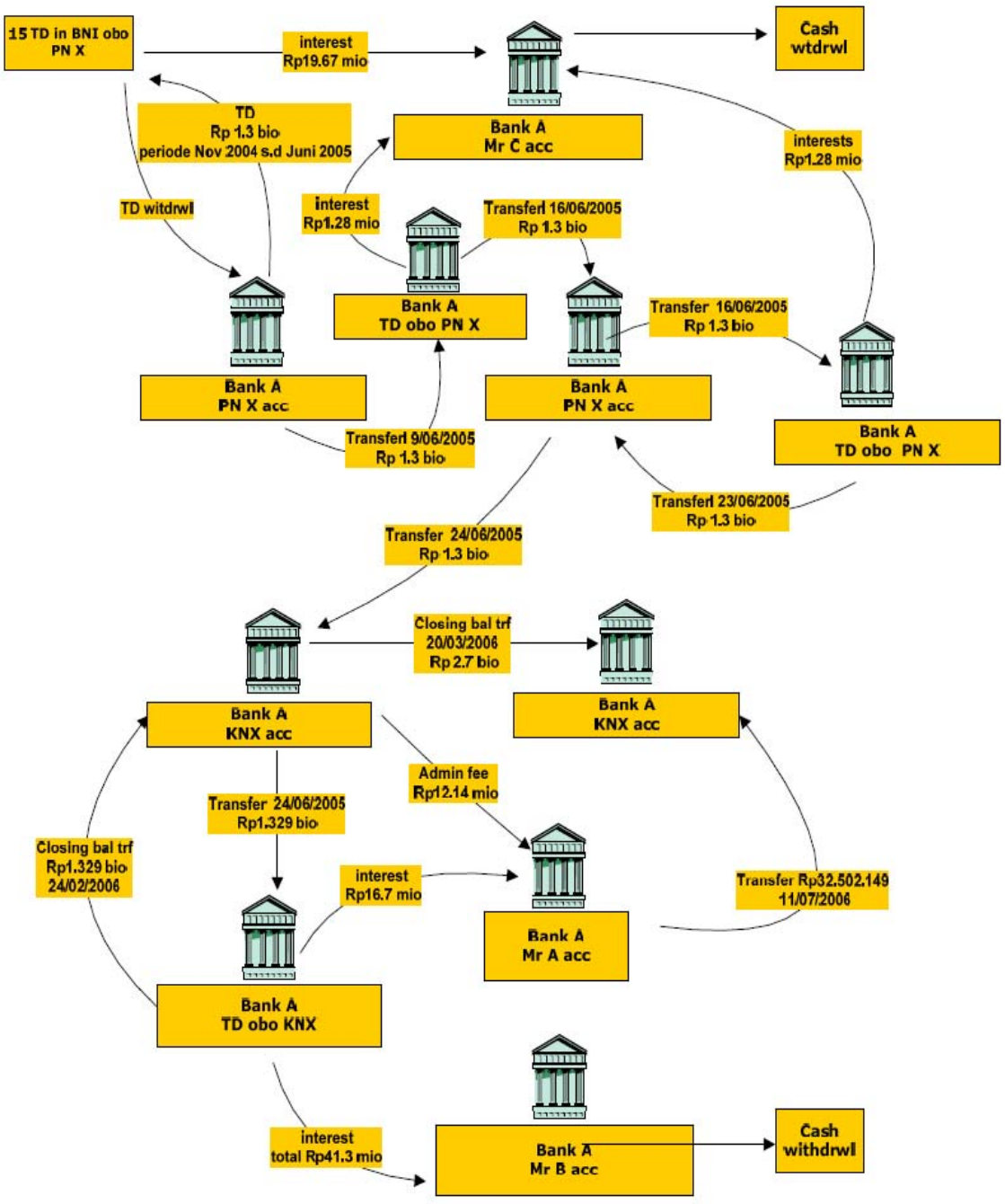
12

http://www.lawlink.nsw.gov.au/lawlink/olsc/ll_olsc.nsf/vwFiles/Anti%20Money%20Landering%20_Money%20Laundering%20&%20Trust_March%202007.doc/$file/Anti%20Money%20Landering%20_Money%20Laundering%20&%20Trust_March%202007.doc

INDONESIA

317. Mr A is The Judge in District Court X (PNX) and Mr B is The Prosecutor of District Prosecution Office X (KNX). Money movement from PNX account to KNX account amounted Rp 1.3 billion for opening time deposit (TD) obo District Prosecution Office . The interest of TD was for the benefit of Mr A (The Judge) and Mr B (The Prosecutor).

Flow of funds:



JAPAN

318. Recently revealed fact indicates that a major optical equipment maker could be involved in an illegal settlement of accounts. According to media coverage, the company, in order to conceal losses on its securities investments, used several investments funds to transfer the losses overseas.

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

AUSTRALIA

319. A law enforcement agency conducted an investigation into a criminal syndicate suspected of various offences, including account and internet-banking fraud, ML and using false identity documentation.

320. Banks alerted law enforcement after it was discovered that members of the syndicate had fraudulently transferred funds from the accounts of legitimate customers into accounts they had opened using false identity documents.

321. The criminal investigation revealed that the syndicate had used internet banking sites to access legitimate customer accounts, using fraudulently obtained customer information. Once they had access to a customer's account, the suspects transferred AUD50,000 out of the account to another account they had previously opened using a false name. Using this method, the syndicate fraudulently obtained approximately AUD500,000. The syndicate also attempted additional transfers worth AUD350,000, but these were identified and stopped prior to payment.

322. On the same day as making a fraudulent AUD50,000 transfer into their account, two members of the syndicate attended various bank branches and automatic teller machines (ATMs) in Sydney and systematically withdrew the funds from their account. Of these funds, AUD28,000 was given to a third syndicate member.

323. AUSTRAC information identified that over a four-year period individuals linked to the syndicate sent international funds transfers worth more than AUD250,000 to various countries, with the primary destinations being countries in central and eastern Europe.

324. Three members of the syndicate were arrested and charged with serious ML offences, involving conspiring to deal in proceeds of crime valued at AUD50,000 or more. The suspects were convicted and sentenced to more than six months imprisonment for their role in the ML activities.

CHINESE TAIPEI

325. Mr Shai was an intern in Bank T and in charge of payments as a front desk teller. He was assigned to handle deposits and payment business for customers. One day, a customer, Mr Shou came to the bank to renew the preferential deposit and this task was assigned to Mr Shai. Mr Shai therefore learnt Mr Shou had about 210,000 NT dollars (approx. US$7,000) in his bank account. Thus, Mr Shou, with the intention to appropriate the money, secretly printed Mr Shai's seal on a blank withdraw slip. Then, he successfully stole 200,000 NT dollars (approx. US$6,693) from the bank account.

326. Mr Shai was also assigned to be a member of the bank's Financial Electronic Data Interchange (EDI) Promotion Task Force and was authorized to handle customer account

information, manage related computer systems, and review customer's transaction records and online transactions. When Bon Lian Inc. and Shan Yuang Inc. respectively applied for registration for EDI certification with the bank, Mr Shai was assigned to process the operation. Mr Shai, with the intention of appropriating the funds in the bank accounts, lied to his superior with the reason to install EDI service system in the two companies and successfully obtained the certification cards and passwords of EDI system. After that, he privately installed the EDI service system and completed the registration and certification of the two companies in his personal laptop computer. Then, he used the laptop computer to transfer 4 million NT dollars (approx. US$133,877) from the bank account of Bon Lian Inc. into his personal bank account in another bank through EDI online transaction service for testing. After the success, he continuously transferred funds from the bank account of those two companies into his personal bank accounts in different banks through EDI online transaction service which amounted to more than 160 million NT dollars (approx. US$5.3 million) by the same method.

327. After that, Mr Shai began to launder the illegal funds by transferring funds between his personal bank accounts in different banks, withdrawing cash, paying the credit card expenses of his wife, depositing into his foreign currency bank account, exchanging into foreign currency, and buying traveller's cheques etc.

328. The criminal activity was revealed when the victims found the details of transactions and the balance did not match with the real situation. Bank T found Mr Shai's criminal activity and urgently informed all the related banks to block Mr Shai's banking accounts which amounted to 140 million NT dollars (approx. US$4.7 million) in total and this case was reported to a law enforcement agency for further investigation. By this time Mr Shai had fled.

329. With the intention of disguising and concealing the proceeds of crime, Mr Shai gave his wife the American Express Traveller's Cheques valued at US$100,000 which face value is US$ 1,000 of each and no holder's name on them. His wife requested her aunt and her friends to take them abroad and redeem them in cash for her.

330. Finally, Mr Shai was captured and accused of breach of trust and fraud offences in the Banking Act, business embezzlement offence in the Criminal Code, ML offence in the ML Control Act.

FIJI

331. A 58 year old local, Person A (a mule) was involved in an email scam that involved a foreign national acting on behalf of a supposedly bogus Company XYZ. Person A was offered a "job" as account representative at Company XYZ. Company XYZ used a Canadian address for correspondence.

332. Under this appointment, Person A was required to remit 90% of any funds deposited/ transferred into his bank account to a Person B in Malaysia and retain the remaining 10% of the funds as his commission.

333. A total of FJ$4,000 (approx. US$2,200) was transferred using an internet banking facility from one local, Person M's local bank account into Person A's local bank account between 7 September 2011 to 13 September 2011. The transfers were apparently made without Person M's knowledge or approval.

334. The funds were subsequently withdrawn from the bank account of Person A by his son Person W and remitted to Person B in Malaysia. A total of $2,200 was remitted by Person W to the same beneficiary on 7, 12 and 14 September 2011.

335. We have been able to establish that the beneficiary of the remittances, Person B is a South African passport holder and currently holds two passports.

336. We have also established other local individuals who also remitted funds to Malaysia around the same period. The beneficiaries of these remittances hold South African, Zimbabwe and Nigerian passports.

337. The case has been referred to the Fiji Police Force Cybercrime Unit in September 2011 for further profiling.

JAPAN

338. An unemployed suspect who sold illegal DVDs such as pornography and pirated contents through the internet earned approximately 4.7 million yen (USD 58,750) in total. He used an internet banking account for the payment which he managed under another person's name. The suspect was arrested for violation of the Act on the Punishment of Organized Crimes (charged with concealment of criminal proceeds etc.)

NEW ZEALAND

339. In March 2011 the following email was sent to NZ Police and demonstrates the continuing and pervasive nature of ML scams and the utilisation of legitimate business and the internet to facilitate this criminal activity.

I was contacted via email to see if I would be interested in becoming a Mystery Shopper. I said I was as I have heard that this is legitimate. I was accepted and set up a separate bank account for this on Friday. I was advised my "assignment" was to investigate (named remittance agent) and transfer money to another mystery shopper in the USA. On Saturday I saw that $3,500 had been put into my new account. I was advised that I was to transfer this on Saturday before 1pm to a Nigerian address. I then became extremely suspicious and phoned the Police and advised the situation. They gave me the SCAMwatch website and I have lodged a complaint there. I emailed the people at "Mystery Shoppers" advising I could not carry out the assignment as I could not access $3,300 via Eftpos and it would have to wait until Monday. My fee was $200 apparently. My predicament is that I have $3,500 in my bank account which I do not want. I do not want to be involved in fraud. I would like to transfer the funds back to these people. I have emails plus the bank details where the $3,500 was transferred to me. Could you please advise urgently as I will have to let these people know Monday that the money has been transferred. Do I transfer it back to them?

The sender of the email was advised to forward the money involved back to the originator, close the account, cease any further e-mail contact with the party they had been communicating with and retain any e-mails regarding the matter in case they could be of use to NZ Police. The remittance agent was contacted by NZ Police and advised of the situation and made aware of their company's name being used in this way. They reported that this activity is relatively common and not unknown to them.

4.14 Use of Violence and Coercion

AUSTRALIA

340. A law enforcement investigation into blackmail and extortion attempts resulted in the arrest of two suspects, who were both later found guilty of multiple charges.

341. Suspect A and Suspect B extorted money and other assets from a victim over a period of three years by threatening the victim, the victim's family, and their property. The extortionists' demands against the victim were initially small, but grew over time to include cash, company shares and luxury motor vehicles.

342. The victim made cash payments to the suspects and electronically transferred funds directly into the suspects' accounts, which were held in their own names. These payments totalled approximately AUD150,000. The victim was also forced to take out loans to purchase two luxury vehicles for the suspects. In addition, the suspects attempted to obtain shares in the victim's company.

343. AUSTRAC information revealed that:

- Suspect A was identified in a number of suspect transaction reports (SUSTRs) and significant cash transaction reports (SCTRs) detailing their apparent structuring of cash transactions to avoid cash reporting requirements. Additionally, while there was no record of Suspect A being employed, they regularly made large cash deposits into an account. Known associates of Suspect A were thought to have deposited and then transferred funds on Suspect A's behalf. A number of these associates were linked to Suspect A's accounts through funds they had received or transferred. One associate also held a joint account with Suspect A.

- Suspect B conducted numerous large cash withdrawals which were detailed in SCTRs submitted to AUSTRAC. Suspect B was also linked to a suspected criminal network. It was also found that associates of Suspect B had been the subject of numerous SUSTRs due to changes in their gambling behaviour, which involved significant cash amounts.

344. The resulting law enforcement investigation into the pair's activities led authorities to restrain two luxury vehicles, two properties and numerous other items, with a total value of more than AUD1 million.

345. Suspect A was charged with 36 counts relating to blackmail and extortion, and sentenced to a minimum of six-and-a-half years in jail. Suspect B was charged with 13 counts of blackmail and extortion, and sentenced to a minimum of three-and-a-half years in jail.

CHINA

Wang & Su ML Case in Chongqing

346. On 29 December 2009 the verdict of the Wang organized crime case and Su ML case were announced by the No.1 People's Court of Chongqing. Found guilty of organizing, leading criminal organizations and 5 other crimes, Wang was sentenced to imprisonment of 20 years and a fine of RMB 2.2 million Yuan (approx. US$346,270). Found guilty of ML, Su, a former policeman of Beipei Branch of Public Security Bureau of Chongqing, was sentenced to imprisonment of 3.5 years and a fined RMB 170,000 Yuan (approx. US$26,757). Other members of the crime organisation ware sentenced to imprisonment from 1 to 16 years respectively.

347. Wang's crime organisation had controlled the butchering market and monopolized the building material supplement and waste transportation industry in Beipei District of Chongqing by force since March 2000, making illicit money of over RMB 10 million Yuan (approx.US$1.5 million). Su, a policeman of Beipei Branch of Public Security Bureau of Chongqing, had misused his post to cover Wang's crime organisation and tip Wang off about police investigations since 2003. Moreover, Su helped the organisation to launder the proceeds of crime. Clearly knowing Wang's money was the proceeds of organised crime, Su opened a bank account with the ID card of his sister-in-law Yuan L and helped Wang to transfer the illicit money in 2008. After Wang transferred the illicit money of RMB 1.3 million Yuan (approx. US$205,000) to the above mentioned bank account and RMB 400,000 Yuan (approx.US$63,000) to Su' personal account, Su invested the illicit money in the Hechuan Ya'neng Building Material Factory, and signed an inveracious investment agreement in the name of his wife Yuan XQ, disguising Wang's investment.

4.15 Association with Corruption

FIJI

348. A local politically exposed person (PEP), Person ABC recently opened a USD foreign currency bank account at a local commercial bank. On 1 March 2011, Person ABC received an inward telegraphic transfer of US$100,947.67 from Royal London Insurance Co. Limited, United Kingdom into the USD account.

349. On 2 March 2011, Person ABC purchased a bank draft for US$100,947.67 (the same amount as the inward telegraphic transfer) for 'payment of legal fees'. The bank draft was made payable to a local law firm's Trust Account.

350. On the same day, 2 March 2011, Person ABC closed the USD bank account. It appears that this bank account was specifically opened to facilitate the large inward telegraphic transfer which appeared suspicious.

351. The case has been referred to the Fiji Independent Commission Against Corruption (FICAC) in April 2011 for further profiling.

THAILAND

The "School Milk" Case

352. Nimit, a former Deputy Governor of Nong Khai Province in the Northeast of Thailand, was assigned by the Governor to chair a provincial committee to procure milk for students in the province. Nimit and a subordinate conspired to ask for kickback money from the milk contractors. A contractor reported the incident to the Anti-ML Office (AMLO). The AMLO assigned an undercover officer as a milk contractor and joined a group of contractors giving 140,000 Baht (approx. US$4,440) to Nimit and the subordinate. Later, the police and AMLO officers searched Nimit's house and found 140,000 Baht in a desk in the living room. Nimit alleged that the money was his savings which had just withdrawn from the bank.

353. The public prosecutor separately prosecuted Nimit for corruption and ML offences. The court sentenced Nimit to five years' imprisonment for corruption. For the ML charge, the public prosecutor could prove beyond a reasonable doubt that Nimit acted for the purpose of concealing the true nature and acquisition of the bribe which connected

with the predicate offence of corruption. The court sentenced Nimit to two years' imprisonment for ML.

INDONESIA

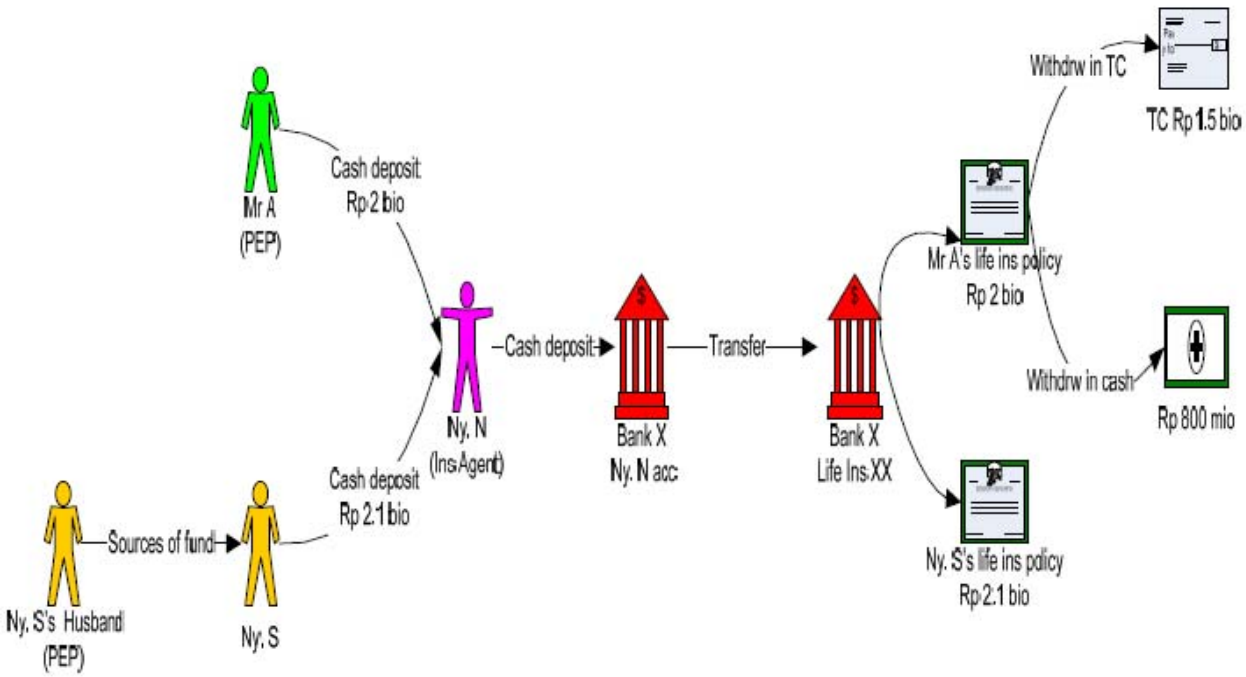
Case 1:

354. Mr A is a PEP. Mr A bought a life insurance investment related product amounting to Rp 2.1 billion. Ny. N received cash from Mr A and converted the cash into a cheque. The cheque was then used as a payment for Mr A policy through the life insurance company account.

355. Ny. S is another insured who use similar pattern of payment for her life insurance policy. Ny. S is known as a wife of another PEP at the same department as Mr A.

356. It appears that Ny.N utilized similar payment method in selling life insurance product particularly among PEPs and their families in Mr A's Department.

Flow of Funds:

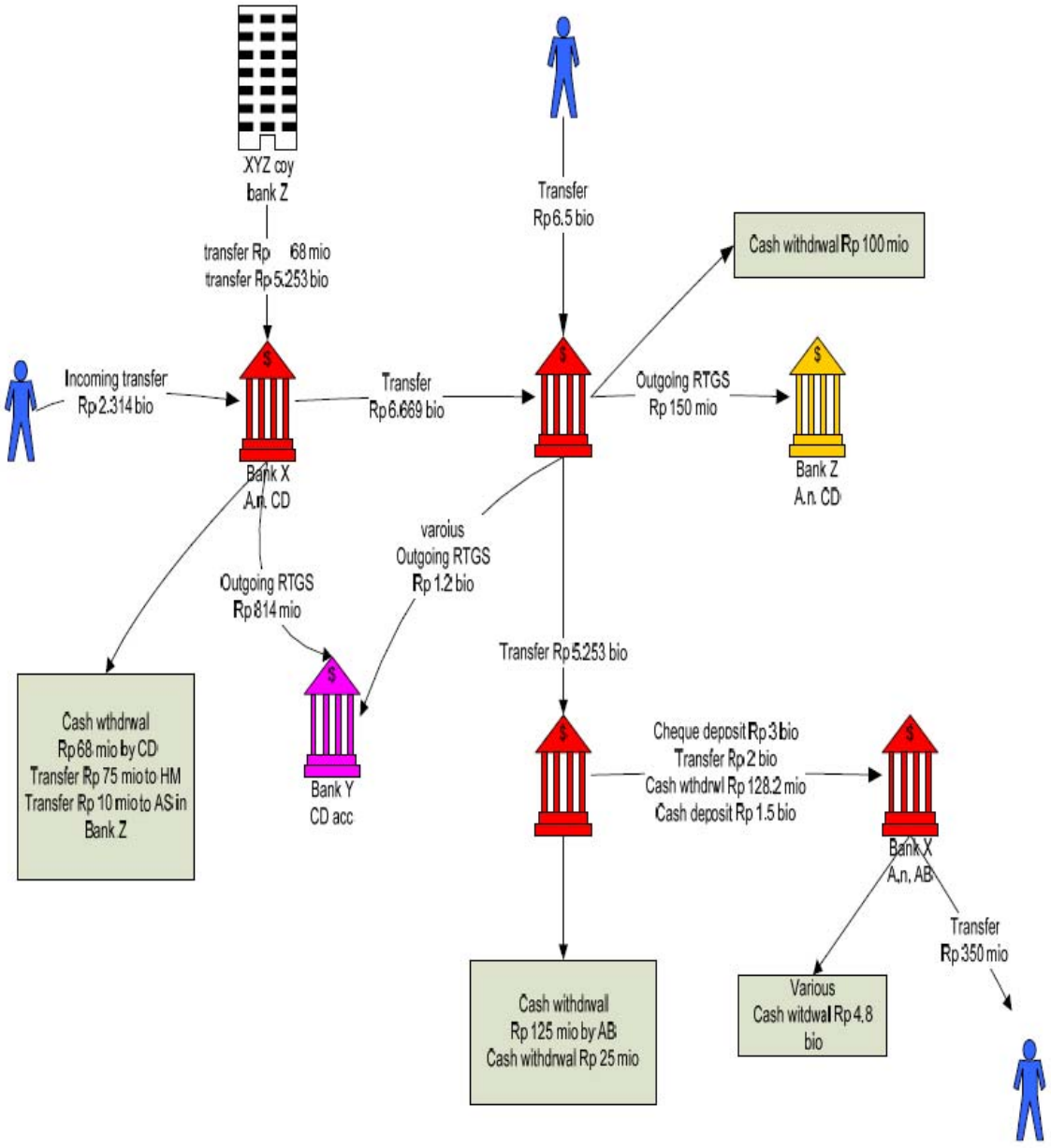


Case 2:

357. AB was a Project leader at Public Utilities Department. He established a joint account with CD (BOD of XYZ company). XYZ was a business partner of that department.

358. The Joint account received overbooking from CD's account in Bank X amounted Rp 5.2 billion - the sources of funds was from various transfers from XYZ account in Bank Z. It was predicted that the money move into joint account was resulted from corruption.

Flow of Funds:



Case 3:

359. BA was a civil servant in the Tax Department. BA allegedly accepted money in service for tax problem resolution assistance. The money was transferred to the account of his wife and children.

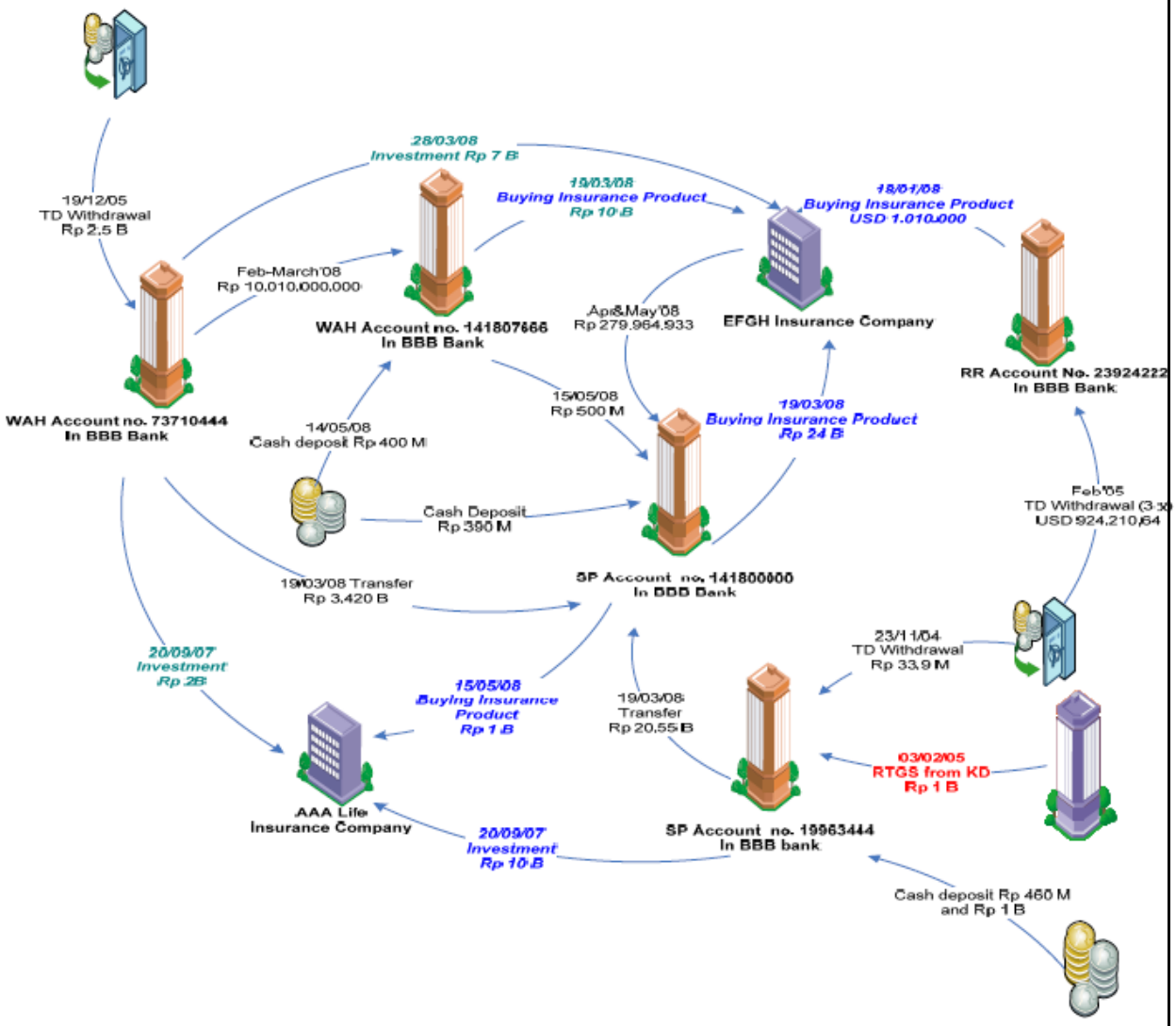
360. Money owned by BA since 2003 to 2005 amounted to Rp30 billion that was deposited in the account of his wife and children. The funds were traded in a range of banking services through YT, a manager of BBB bank.

361. The funds negotiated on behalf of the SP (wife), WAH and RR (the child).

362. The transaction was carried out in April 2010 is up to Rp 66 billion.

363. There was several transaction of cash deposit to the SP, WAH and RR account that suspected of being proceeds of crime (*structuring*). There was also an indication that KD (owner of XXX company) transferred money amounting Rp1 bio to SP Account. The money was used to bribing BA. BA convicted of ML. BA was sentenced to 12 years in prison by the High Court, in May 2011.

Flow of Funds:



CHINA

Deng ML Case in Fuzhou, Fujian Province

364. On 28 December 2009, the verdict of Deng ML case was announced in the by the Intermediate People's Court of Fuzhou, Fujian Province. Found guilty of ML, Deng was sentenced 3 years' imprisonment and fined RMB 50,000 Yuan. This was the first case applying to *The Supreme People's Court Interpretation on Several Issues in the Application of Law Concerning the Trial of ML and other Criminal Cases*, hereinafter referred to as *the Interpretation*.

365. 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, in order to avoid the investigation of law enforcement from 2006 to September 2008. In July or August 2008, for fear of being investigated for his involvement in an illegal project of land development, Chen handed the bank book to Deng for safe keeping 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 bribes.

366. On 6 August 2009, the verdict of Deng case was announced in the first instance by the People's Court of Yongtai County, Fujian Province. Found guilty of concealing and disguising criminal proceeds (Article 312 of the Criminal Law), Deng was sentenced to 6 years' imprisonment and a fine of RMB 50,000 Yuan. Deng appealed against the verdict to the Intermediate People's Court of Fuzhou. In the second instance, the Court confirmed Deng should be convicted of ML, because Deng provided a bank account to conceal and disguise the illicit money while clearing knowing it was the proceeds of Chen's briberies, and then changed the former verdict.

367. During the second instance, the lawyer defended that Deng didn't clearly know there were crime proceeds in the deposits, and this case should be heard after the trial of Chen bribery cases or at one time. The Intermediate People's Court of Fuzhou made a judgment to the defence opinions according to the Interpretation for the first time: firstly, when assisting to transfer Chen' money of RMB 4.1 million Yuan, Deng should realize these sums of money was obviously inconsistent with Chen's profession and financial conditions, which accorded with the Article 1 of the Interpretation as "clearly knowing"; Secondly, the predicate crime wasn't sentenced but verified, so it was unnecessary to stop the trial of ML case according to the Article 4 of the Interpretation.

368. It was demonstrated in this case and other similar cases that accounts of relatives had become the vital laundering channels for badger hats.

4.16 Criminal Knowledge of & Response to Law Enforcement / Regulations

AUSTRALIA

Case Study

369. AUSTRAC information alerted a law enforcement agency to the activities of a suspect who was apparently structuring larger international funds transfers into smaller amounts, seemingly to avoid reporting requirements.

370. The person came to the attention of AUSTRAC after reporting entities submitted a series of suspicious matter reports (SMRs) detailing the suspect's activities. Further investigations revealed that:

- The suspect had been making regular cash deposits into a personal bank account. The source of these cash deposits could not be established and there was no evidence of the suspect receiving salary payments into the bank account from any employer.

- On occasions, the suspect would present cash in amounts of about AUD9,900 to pay for international funds transfers to individuals who were assessed to be the suspect's relatives in China. The amounts involved in the transfers strongly suggested to reporting entity staff that the suspect was deliberately structuring the cash payments to fall just below the AUD10,000 reporting threshold for cash transactions.

371. The suspect conducted 28 international funds transfers totalling approximately AUD295,000. Most of the transfers were for the amount of AUD9,900.

372. The suspect was ultimately charged under section 142 of the AMLCTF Act 2006 with conducting transactions to avoid reporting requirements and was sentenced to four months imprisonment.

CHINESE TAIPEI

373. With the intention to disguise the proceeds derived from corruption, Mr Lee, a judge in the High Court who was charged with the crime of corruption, concealed the illegal funds of 2 million NT dollars by delivering cash of 700 thousand dollars to his unknowing younger sister depositing in her bank accounts, and then transferred to her stock trade account in another bank for investing in the stock market. Mr Lee deposited the left illegal funds into his bank account respectively with cash 460 thousand NT dollars and 800 thousand dollars, and then, he issued a cheque with the amount of 1,260 thousands NT dollars for buying a car parking space. But in 2011, Mr Lee's former bribery was uncovered by the Investigation Bureau and then he was taken into custody.

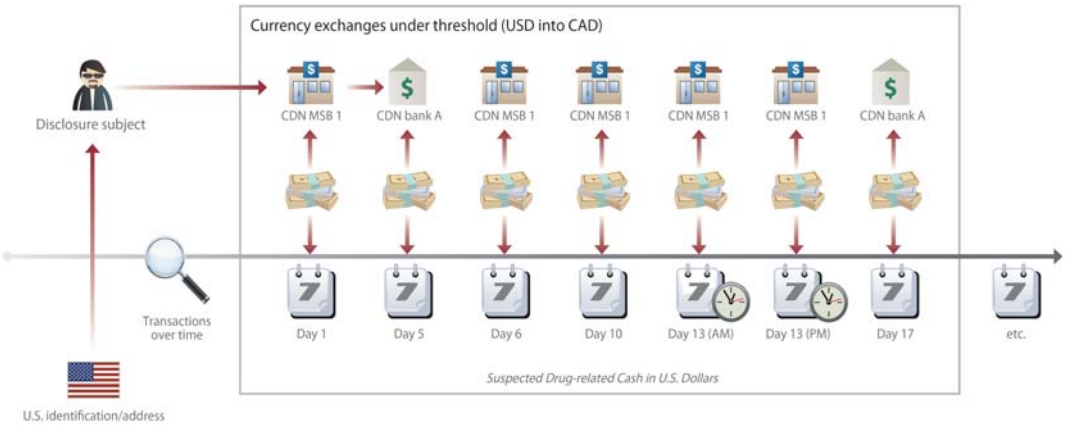
374. Mr Chang is an attorney who was authorised by Mr Lee to be the counsel in the proceedings of this case. According to the provision of Article 1 of Attorney Regulation Act, attorneys should take upon themselves the goals of promoting social justice, protecting human rights, and contributing to democratic government and the rule of law, and with the spirit of self-regulation and self-governance, attorneys should strive to faithfully execute their professional responsibilities, contribute to the preservation of social order, and work towards the improvement of the legal system. Unfortunately, attorney Chang was required by Mr Lee to incite Lee's relatives making false statements for disguising the fund was derived from bribery as mentioned above and how to deal with the investigations and interrogations conducted by prosecutors' office. He, based the consideration to assist Lee to conceal the proceeds of crime, not only consented to the collusion request but also incited Lee's relatives to make untrue statement regarding the origins of the illegal funds for covering Lee's wrongdoing. Their conspiracy was successfully revealed after the FIU of Chinese Taipei traced the proceeds of crime, and the Investigation Bureau interrogated Lee's relatives and searched the law firm of Chang.

375. As a result, Mr Lee was prosecuted with ML offence and inciting false statement offence, and Mr Chang was prosecuted with inciting false statement offence in this case.

4.17 Currency Exchanges and Cash Conversion

CANADA

376. The following case provides an example of the use of a money service business (MSB) by a U.S. resident to exchange and refine suspected drug-related proceeds.



377. STR information provided by an MSB indicated that the disclosure subject used the currency exchange MSB as part of a regular pattern of financial activity consisting of converting and refining U.S.-denominated cash through a series of structured exchanges. In this particular case, covering a two month period, the disclosure subject regularly travelled over 70 miles from the U.S. to Canada to conduct the transactions. The individual concentrated his/her currency exchanges on one particular MSB, and a bank branch in the same Canadian town. Both the MSB and the bank filed STRs on the individual.

378. STRs filed by the MSB highlighted the high frequency of visits which occurred every two or three days and sometimes twice on the same day. The reports also noted that the individual was a U.S. resident. In each case none of the disclosure subject's transactions exceeded $10,000 which would have triggered a requirement to file a large cash transaction report (LCTR) with FINTRAC.

379. Bank STRs also flagged this individual as a U.S. resident, who had travelled to their branch to undertake several thousand dollars worth of U.S to Canadian dollar exchanges in U.S. $20 bills. The bank indicated that the individual did not have an account at the bank, that no explanation could be given for either the source of funds or for why the individual would travel from the United States to undertake these currency exchanges.

380. The combined, total value of currency exchanges undertaken by this individual was over US$40,000. STRs provided by both reporting entities highlighted their suspicions of the individual's involvement in drug trafficking. This was later corroborated by law enforcement information indicating that the individual had been convicted of drug offences. The STRs filed by the MSB provided information that allowed analysis of the disclosure subject's transaction activity over time which assisted FINTRAC's determination that there were reasonable grounds to suspect ML. This case highlights how an MSB can be used to facilitate the placement and layering of proceeds by converting suspected drug cash into a different currency. It also illustrates how an MSB can simultaneously be used to "refine" suspected drug proceeds.

RED FLAGS associated with this case:

- The customer made frequent visits to conduct currency exchanges, sometimes two or three times in a given week, and sometimes in the same day.
- The client's ID indicated that the individual was a U.S. resident, but travelled a long distance to Canada to conduct transactions.
- The individual converted small denominations of U.S. cash into larger denominations of Canadian cash.
- All currency exchange transactions were below the $10,000 threshold, presumably to avoid large cash transaction report (LCTR) requirements.

4.18 Use of Credit Cards, Cheques, Promissory Notes

AUSTRALIA

Case Study

381. Funds associated with the financing of terrorism can be derived from legitimate sources, including the incomes of individuals or community donations, or through the proceeds of non-terrorism related crimes (including fraud or robbery). By using a diversity of funding sources, those planning acts of terrorism may attempt to distance themselves from the origin of the funds generated to finance those acts.

382. The following two related cases illustrate the challenge of identifying terrorism financing, given that it may model normal patterns of financial behaviour, be undertaken through low-value transactions, or not involve the financial sector at all.

Part A – Sydney

383. A joint investigation led to the arrest in November 2005 of nine Sydney suspects who authorities suspected were planning an act of terrorism in conjunction with thirteen Melbourne suspects. The group's activities included military-style training and purchasing materials they planned to use to manufacture explosives. The investigation revealed that the Sydney-based suspects relied mainly on their own incomes and efforts to fund their training activities and purchases, using their own bank accounts. Members of the group were caught shoplifting batteries, maps and electronic timers. Investigating officers also located stolen railway detonators during the execution of search warrants. The Sydney suspects regularly used false names to register mobile phones when purchasing supplies and materials for their activities. For example, members of the group established companies in false names and used these companies to avoid suspicion when ordering and purchasing chemicals. Four members of the Sydney group pleaded guilty to various terrorism offences, while the remaining five members were found guilty by a jury of conspiring to commit an act in preparation for a terrorist attack under the *Criminal Code Act 1995*.

Part B – Melbourne

384. The same joint investigation also led to the arrest of thirteen Melbourne suspects who, in conjunction with the Sydney suspects, were planning an act of terrorism. The Melbourne group also undertook military-style training and purchased materials to manufacture explosives.

385. Investigations revealed that the Melbourne-based group funded their planned activities primarily through a series of small cash donations made by the group members

to a central fund, known as the 'sandooq' (traditionally a box where all financial contributions were held). The majority of the Melbourne group were employed as electricians, tilers or panel beaters.

386. One individual was alleged to have been the treasurer and holder of the sandooq. Another group member approved group members to use funds from the sandooq. All members contributed to the sandooq, with some contributing AUD100 per month. The fund was worth approximately AUD19,000 at the time the group was arrested.

387. The suspects were also engaged in systematic credit card fraud, whereby they paid taxi drivers to provide them with the credit card numbers of unsuspecting taxi passengers. In addition, third parties provided the group with extra funds raised from a car re-birthing racket.

388. The group undertook the fundraising activities for the purpose of purchasing weapons and materials for a planned terrorist attack.

389. Nine members of the Melbourne group were found guilty of being members of a terrorist organisation. Four members were acquitted. Seven group members were also found guilty of committing acts in preparation for a terrorist attack under the Criminal Code Act 1995.

Case A

390. Law enforcement agencies jointly conducted investigations into a criminal group operating a credit card skimming scheme that targeted automatic teller machines (ATMs). The investigations resulted in the arrest of multiple suspects across several states.

391. The suspects travelled to various states throughout Australia committing offences associated with card skimming and ATM fraud. The suspects attached skimming equipment to the card readers on ATMs, which electronically recorded and stored the details of the cards as they were inserted into the ATM. The suspects also attached pinhole cameras to the ATMs, which were used to record the customers as they entered their personal identification numbers (PINs). After skimming the victims' cards, the suspects created fraudulent cards using the victims' details and accessed their accounts using the captured PINs.

392. AUSTRAC information was used to detect false identity documents used by the syndicate. This information was crucial in tracking the movement of the suspects as they travelled through various states:

- International funds transfer instruction (IFTI) reports and suspect transaction reports (SUSTRs) submitted to AUSTRAC detailed how the suspects had frequently transferred amounts of less than AUD10,000 via remittance dealers to common beneficiary customers in Romania and Bulgaria.
- AUSTRAC information also identified that the suspects had used different remittance agents to transfer money overseas on the same day.
- Authorities suspected that the remitted funds were sourced through the group's criminal card skimming activities.

393. Law enforcement officers ultimately arrested numerous suspects, including Romanian and Bulgarian nationals. A suspect arrested in Victoria pleaded guilty to six charges, including dishonestly obtaining or dealing in personal financial information, obtaining

property by deception and dealing with property suspected of being the proceeds of crime. The suspect was sentenced to six months imprisonment.

Case B

An additional and related investigation into another card skimming group ultimately resulted in the arrest of a further two suspects. The investigation was initiated when a package addressed to Suspect A was intercepted and found to contain a fake passport carrying a photo of Suspect A and several miniature cameras which could be used to record the PINs of ATM customers.

394. Suspect A was identified on closed-circuit television (CCTV) footage with Suspect B fitting cameras and skimming devices to ATMs at several locations in Sydney. Having been identified from the CCTV footage, Suspect A was arrested when he attended a local police station following a minor traffic incident. A warrant was issued for the arrest of Suspect B, who was subsequently arrested interstate – just days before his planned departure from

Additional Case

395. AUSTRAC information identified that over a three-week period Suspect A sent approximately AUD22,000 via IFTIs to Romania and the United Kingdom. In addition, AUSTRAC information identified that over a further three-month period Suspect B sent an additional AUD121,000 via IFTIs, also to Romania and the United Kingdom. This money is suspected to have been sourced through the pair's card skimming activities.

396. AUSTRAC received three SUSTRs submitted by reporting entities about the suspicious activities of Suspects A and B, including:

- the high volume of money transfers undertaken by the pair
- the structuring of transactions, apparently undertaken to avoid transaction threshold reporting requirements
- the undertaking of funds transfers to countries of interest to authorities.

397. Suspect B pleaded guilty in court to three counts of possessing implements to create fake bank cards and credit cards. He was sentenced to two years imprisonment.

CHINESE TAIPEI

398. In August of 2010, the Police broke a fraud syndicate, captured 10 suspects, and found over NTD 400,000 in cash and 570 Union Pay Cards issued by Company X in mainland China. After investigation, the Police found those 10 suspects captured were in charge of using the Union Pay Cards via ATMs to withdraw the money derived from fraud. The syndicate recruited some homeless people in mainland China to open bank accounts and apply for Union Pay Cards. Then it delivered the Union Pay Cards to the associates in Chinese Taipei by the post and falsely declared them to the Customs as regular goods. Its associates pretended to be law enforcement agents to make phone calls from southeast countries to people in mainland China and scammed them. Once those victims had remitted the money to the specific bank accounts in mainland China, the head of the syndicate would instruct the associates in Chinese Taipei to withdraw it via ATMs in convenience stores, oil stations or other remote places around Chinese Taipei. It's estimated the amount of the fraudulent money was hundreds of million. The case was referred to the Prosecutor's office for prosecution.

399. Although the upper limit of withdrawal from Union Pay Cards in Chinese Taipei is only NTD 20,000 per time and RMB 10,000 (about NTD 50,000) per day and our related

law enforcement authorities and banks/contact points have shared the information mentioned above, those cards still could work in Chinese Taipei due to the difficulties for issuing banks/Company X to verify the card holders and no legislations of blocking such kind of suspicious money and cards in mainland China.

FIJI

400. Person MB presented 14 Travellers Cheques valued at US$500 each totalling US$7,000.00 at one of the local commercial banks in September 2011. The Fiji FIU was involved in checking the authenticity of the traveller's cheques. The International Department of the local commercial bank verified the traveller's cheques with the issuer and found them to be fake. Person MB had reportedly received the travellers' cheques via mail from a scam advising him that he had won a lottery in the United Arab Emirates company draw. This case was referred by the Fiji FIU to the Fiji Police and investigations are continuing.

JAPAN

401. Counterfeit traveller's cheques have been found to be exchanged for cash in Japan. Customers who appeared at exchange counters with counterfeit cheques explained that they were offered a business from a foreign entity through email, asking them to cash some traveller's cheques without telling that they were fake. Once succeeded in encashment, the customers were supposed to be given commission fee.

MACAO, CHINA

402. A large amount of remittance had been remitted to Mr F's credit card account via a bank in country X. The card issuing bank found out that Mr F did not have any outstanding balance for settlement. A few days later, Mr F gave power of attorney to a third party to withdraw the remitted funds by draft on his behalf, claimed as repayment of loans from a friend. Within the same day, the requested draft was deposited into the account of Mr F in the same bank and all funds were then withdrawn in full as cash a couple of days afterwards. The bank found the transaction pattern of Mr F suspicious and the case was reported to the FIU and disseminated to a law enforcement agency for investigation.

THAILAND

403. At present, more and more companies in Thailand are being authorised by the authorities to provide cash card services. Some of these services are subject to registration while others are not. Money transfers can be made across cards. The AMLO has, therefore, kept a close watch on this as it can be exploited for ML/FT.

404. The AMLO has found that those committing predicate offences of ML now have more to do with cash cards. For instance, Mrs O, resident of Bangkok, who was under suspicion of drug involvement, conducted financial transactions with branches of banks located at discount stores. These frequent transactions did not involve large amounts of money. It was between 180,000-600,000 Baht each time. Later, the woman was arrested by NSB officers together with Mr M and exhibits which included 60,000 amphetamine pills, 13 grams of ice, 18 ecstasy pills, 1 gram of ketamine powder, 38 500-milligram bottles of ketamine solution, 1 motorbike, cash worth 6,000 Baht, 7 gold objects, 1 notebook computer and 2 cash cards.

4.19 Structuring and Smurfing

AUSTRALIA

405. Information provided by an international law enforcement agency initiated an Australian investigation into a ML syndicate. The investigation identified that a main suspect was providing an international ML service for Australian criminal syndicates.

406. It was alleged the suspect met with members of the criminal groups and took possession of cash, which authorities suspected was the proceeds of crimes. The suspect allegedly laundered the proceeds of crime offshore on behalf of the criminal syndicates and received a commission in return. AUSTRAC information assisted authorities to identify the ML methods used by the main suspect:

- The suspect used a number of associates to assist in the process. The main suspect would pass the cash on to his associates, who would transfer the funds overseas on his behalf. The cash was transferred in amounts of approximately AUD9,000 an activity consistent with the standard pattern of 'structuring'. The associates used their real identities when conducting the international funds transfers through banks and remittance dealers.

- On each occasion, the money was sent to one of four associates based in Turkey. The main suspect then contacted a trusted associate in Turkey and provided him with details of the funds transfers from Australia to Turkey, including the amounts sent, the sender's name, the name of the associates in Turkey who received the transfers, and a reference number for the transactions. The associate in Turkey then collected the money, combined it and deposited it into a Turkish bank account, to which the main suspect in Sydney had access.

407. Authorities identified that a total of AUD125,950 was laundered in this way over two months.

408. AUSTRAC information also assisted authorities to identify two large international funds transfer instructions (IFTIs) the main suspect had facilitated as part of his laundering activity. The suspect used a Sydney-based company to remit a total of AUD139,000 in two transactions through Australian banks to a beneficiary in Thailand. The main suspect used third parties to deposit and transfer funds in an effort to avoid being directly associated with the money transferred out of Australia.

409. The suspect was charged and convicted of ML under section 400.4 of the Criminal Code Act 1995 (which covers offences in which a person deals with money or other property worth more than AUD100,000, where there is a risk that it will become an instrument of crime5). He was sentenced to four years and three months imprisonment.

CHINESE TAIPEI

410. In 2009, Mr A organised a tele-fraud scam syndicate and served as the head of this criminal organisation. He was in charge of assigning missions to his associates, training them in fraud, and managing the proceeds of crime. They defrauded people in mainland China through relaying the scam phone call from other countries. From June, 2009 to January, 2010, they have gained illegal profit of RMB$19,575,227 from the criminal activities.

411. Knowing her husband A's criminal activities and the illegal gains, Mrs A, for the purpose of concealing and disguising the proceeds of crime, associated with Mr A to deposit multiple small amounts in their relatives' banking accounts in order to conceal the funds source for avoiding the law enforcement agency's tracing and securing the illegal money after receiving the proceeds of crime from China through underground remittance.

412. The members of this fraud syndicate were all arrested by the Police in March, 2010. However, after Mrs A was released on bail for NTD$100,000, she promptly used banking cards for withdrawing all the money mentioned above and hid it.

413. This case was prosecuted for fraud and laundering money by the Prosecutor's office in June, 2010.

FIJI

414. The Fiji FIU received a suspicious transaction report from a local commercial bank on Person MYZ who is reportedly a school teacher. Person MYZ deposited a total of $40,000.00 into his bank account in January 2011.

415. The nature of the way the deposits were made was questionable. Person MYZ used to split deposits into smaller denominations to avoid the reporting threshold of conducting a cash transaction of $10,000 or more.

416. Person MYZ accumulated these deposits gradually over a period of time and then reportedly wrote a cheque of $29,000.00 payable to a local insurance company to invest in an insurance policy. The Fiji FIU was also able to establish that Person MYZ already held two other existing policies with the same insurance company.

417. Considering the occupation and the nature of the transactions undertaken by Person MYZ, it appears that there may have been intent by Person MYZ to engage in possible structuring related activities.

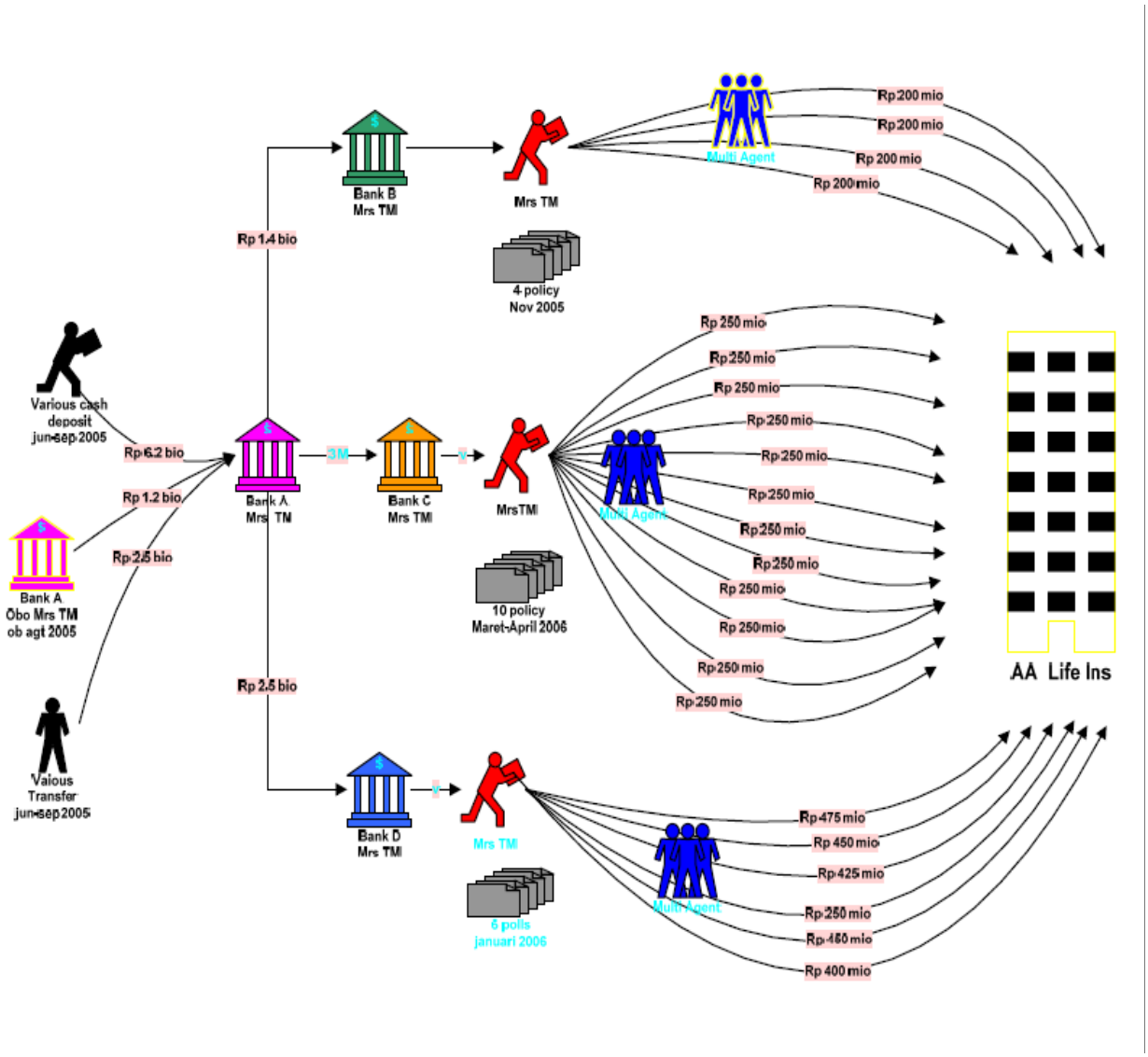
INDONESIA

418. PEP's wife (Mrs TM) bought many life insurance investment related products in cash. The payment was made below threshold of cash transaction report.

419. She used various agents in different branches of a life insurance company.

420. The source of the funds was from her 4 different bank accounts. Some of the funds were indicated to be from corruption conducted by her husband.

Flow of Funds:



THAILAND

421. The AMLO has discerned a method which can be used for ML through banks. This is by using people who earn a living by depositing and withdrawing cash from banks for others. The occupation is found most in the southern border provinces.

422. At present, the activity is closely linked to the business of currency exchange in the southern border provinces. Transactions of this type are mostly to avoid filling out the AMLO Report Form through structuring amounts subject to reporting to the AMLO into small amounts. It is notable that currency exchange agents in the southern border provinces mostly employ those depositing and withdrawing cash from banks for others to conduct transactions with banks for them while those in tourist provinces including Bangkok mostly use people who are their own employees.

Case Sample

423. The AMLO received a suspicious transaction report (STR) made by a bank that Miss S, the extramarital wife of Mr P, conducted many cash deposits and withdrawals involving 1-1.9 million Baht in each transaction and taking only banknotes of small denominations to avoid reporting to the AMLO. As a result of an investigation by the AMLO, it was found that the couple together held 70 accounts at various banks totalling a large amount of money. It was also found that Mr P had a history of drug involvement while Miss S had no such history. The AMLO, therefore, contacted the Narcotics Suppression Bureau (NSB) of the Royal Thai Police for further action.

424. Later, the NSB made an investigation and found that the couple were major drug traffickers with direct contact with the Wa, a minority group. The NSB subsequently made a bait purchase of 74 kilograms of heroin and were able to arrest the couple together with 3 other people and exhibits including 74 kilograms of heroin, Thai currency worth 15,463,520 Baht, US currency worth 114,251 dollars and bank accounts worth 12,224,993 Baht. Afterwards, AMLO officials, NSB officials and officials of the Office of Narcotic Control Board (ONCB) made a search of 13 houses of people believed to have acted for the disposal of the couple's drug proceeds and found 7,325,810 Baht worth of cash and 9 bank books worth together 39,124,923 Baht and many cars.

4.20 Wire Transfers

AUSTRALIA

Case Study

425. Investigation foiled efforts by an Asian organised crime group to import hundreds of kilograms of drugs – cocaine, ecstasy and crystal methamphetamine ('ice') – into Australia. Law enforcement officers intercepted several shipping containers from Canada and seized the drugs, worth more than AUD31 million, which had been hidden in foot spas.

426. Authorities suspected that the crime syndicate responsible for the shipments had also been responsible for multiple previous importations of illegal drugs.

427. AUSTRAC information assisted authorities to identify various suspects and entities involved in the importations:

- Financial transaction information helped identify the Canadian company believed to have supplied the foot spas used to conceal the drugs.

- AUSTRAC information also helped identify the Australian companies that were to receive the importations. The Australian companies had sent a number of international funds transfers to the Canadian company. These transfers were sent through major banks and were worth approximately AUD20,000 each.

- A Canadian national suspected of being the main organiser of the importations made a number of low-value international funds transfers from Australia to Vietnam while he was visiting Australia. Details of these international funds transfers revealed that the suspect had provided a mobile phone number when undertaking the transactions.

- This same phone number was also provided by a second suspect when sending low-value transfers to beneficiaries in Vietnam through a remittance dealer based in Australia. This second suspect was subsequently arrested for overseeing one of the drug importations.

- Other information contained in international funds transfer instruction (IFTI) reports confirmed the connection between the drug importations and the Canadian national suspected of being the main organiser behind the importations.

- AUSTRAC received a large number of significant cash transaction reports (SCTRs) from reporting entities detailing a large number of high-value cash deposits made into bank accounts belonging or connected to the suspects

Case Study

428. An investigation into a major drug smuggling operation began after law enforcement officers identified that a number of suspects under investigation had transferred more than AUD100,000 out of Australia.

429. One of the suspects was subsequently arrested while attempting to transfer AUD100,000 to Armenia through a bank. The suspect had attempted to pay for the international funds transfer with cash.

430. Following the suspect's arrest, the group's regular funds transfers to Armenia ceased for a period of time. When the group recommenced sending funds to Armenia, they employed a different method to transfer funds in an attempt to avoid detection by authorities. The method included:

- funds being transferred overseas in the last week of each month

- international funds transfers being conducted through banks and paid for with cash. However, the cash payments for these transfers were seemingly structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold

- four individuals from the group sending funds overseas at the same time. The group would travel to one suburb and transfer the funds through various branches of different banks within the suburb

- funds always being sent to the same branch of the same Armenian bank.

431. Over a four-year period the group transferred nearly AUD1.8 million to Armenia.

432. Authorities believe the transferred funds were subsequently sent to the United States, where they were used to purchase cocaine for importation into Australia.

433. The group owned a number of auto body repair shops in Sydney, and the cocaine was shipped into Australia hidden inside automobile brake drums. Authorities also believe that the group used brake drums to smuggle cash out of Australia.

434. Ultimately, two members of the group were arrested and sentenced to six years imprisonment for possession of a marketable quantity of imported cocaine.

CHINESE TAIPEI

435. Mr A was in charge of Company X which has been shut down since 2002. With the intention of deceiving for profit, he claimed that Company X had invested in international trade business in Nigeria, however, the Nigerian partner couldn't pay for goods to Company X and the Nigerian Government would shoulder the debt. Thus, Company X had a debt claim in amount of USD 20,700,000 from the Nigerian Government. Mr A lied to the public that he needed to raise money for bribing Nigerian officials and paying legal fees, travel fees, and related operational expenses, and then he could get USD 20,700,000 back. To convince the public, he showed some false obligation documents of the Nigerian central bank, deposit certificates, receipts for a loan, and letters of commitment and promised the public ten times the return for lending money to him. His criminal activities were disclosed by some victims in 2004. In 2008, Mr A was sentenced up to 7 months imprisonment by the High Court in Chinese Taipei. Nevertheless Mr A continued lying that the Nigerian Government has paid the debt and deposited in Bank Y in Dubai, and he needed operational expenses to get the money with the interest in amount of USD 30 million back to Chinese Taipei. For seeking more than 10 times profit as return, some victims carried cash by themselves to give Mr A or remitted funds to Mrs A's or third parties' banking accounts. Or Mr A instructed some victims to go to Bank Z in Chinese Taipei together, and remitted to the specific banking accounts in England via Western Union Quick Cash. In order to avoid the reporting threshold of single remittance USD 7,000, Mr A even asked those victims to use different names to structure the remittances. But once receiving the money, the local associates in England withdrew it subsequently. The amount of fraudulent money reached to NTD 95,804,480.

436. It's suspected of fraud and ML. Mr A and his associates were arrested by the Investigation Bureau in 2010. The fraudulent money deposited in Chinese Taipei has been seized by the court.

FIJI

437. Person TB arrived into Fiji from Pakistan in November 2010 and was issued with a six month short-term work permit to work for an engineering company. Person TB opened a bank account at a local commercial bank.

438. Person TB received salary deposits from the engineering company and on the same day or the day after, remitted the funds to Pakistan to a Person XYZ. The Fiji FIU established that Person TB has sent his entire salary to Pakistan. The beneficiary of the funds remitted by Person TB resides in Pakistan. The local commercial bank flagged a STR to the Fiji FIU.

439. Checks conducted by the Fiji FIU found Person TB to be allegedly a suspected terrorist reportedly detained in Pakistan in August 2009. We further established that Person XYZ is the owner of an engineering company in Lahore, Pakistan. He is also the director of a charity organization which is suspected to be diverting charitable donations and utilized the engineering company as a front to fund terrorism activities. Person XYZ was detained for 2 months in 2001 by Pakistani authorities in connection with the investigation for his involvement.

440. The case was reported by the Fiji FIU to the Fiji Police Force in March 2011 and is now being investigated for possible terrorism related offences.

INDONESIA

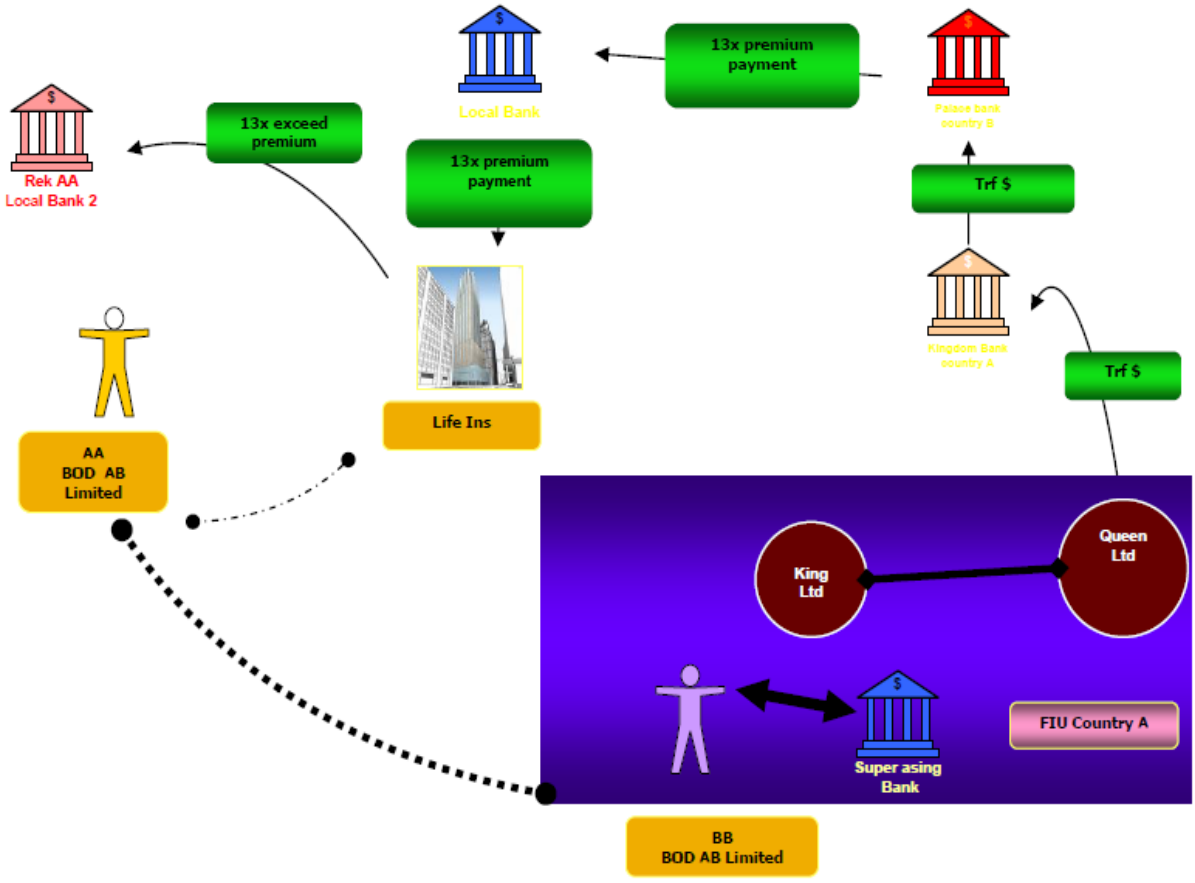
441. AA was BOD of the company ABC located in Indonesia.

442. AA receipt 13 exceeds premium payment from life insurance company.

443. The source of payment was wire transferred from company in various countries. The payment was instructed by BB in country XXX.

444. BB in country XXX was informed in conducting suspicious transaction. BB was also known as one of BOD old company ABC.

Flow of Funds:



JAPAN

445. A large scale ML conducted internationally by mainly Nigerians was concluded last year. In that case, 570 million yen (USD 7.1 million) out of 2.8 billion (USD 35 million) earned through their fraudulent activities in the U.S. was wired to Japan for laundering. In response to clarification from bank, accomplices in Japan insisted that they received payment on sold goods by submitting false documents which indicated that they had exported them, and disguised the illegally earned funds as legally earned funds.

THAILAND

446. Wire transactions have led to a larger number of suspicious transactions. At present, Thai banks offer wire services such as Internet banking, tele-banking, mobile banking, money transfers without an account and money transfers through the ATM. These services can be provided interbank, making them vulnerable to exploitation as a channel for ML.

447. A Mr S, a rancher in Tak Province, which is a high risk area for drug cultivation and trading, opened an account and obtained an ATM card with a bank in that province. Later, deposits/transfers were made into the account from other provinces, totalling 5.48 million Baht (approx. US$170,000) in just one month. During that same period, more than 250 withdrawals through the ATM were made from the account in Supanburi Province. It is surmised that Mr.S was hired to open the account by another person who wanted to prevent tracing of his own financial path.

4.21 Purchase of Valuable Assets

CHINA

Zhang & Ye ML Case in Leqing, Zhenjiang Province

448. On 25 December 2009, the verdict of Zhang and Ye illegal taking deposits from the public and ML case was announced by the People's Court of Leqing, Zhejiang Province. They were found guilty of illegal taking deposits from the public, Zhang was sentenced to imprisonment of 7 years and fined RMB 500,000 Yuan. Found guilty of ML, Ye was sentenced to imprisonment of 3 years and fined RMB 1 million Yuan. This was the first convicted ML case with the predicate crime of illegally taking deposits from the public in China.

449. Zhang had organized a "mutual assistance organisation", illegally taking deposits from the public totalling RMB over 44.9 million Yuan since October 2002. In order to disguise the illicit money, Zhang purchased several properties and automobiles. Clearly knowing Zhang's money was the proceed of financial crime, Ye provided his bank account opened in Shanghai to Zhang. From 10 April to 19 October 2007, Zhang had transferred his illicit money of RMB 19 million Yuan to Ye's account. Ye prepaid the landlord Fu the deposit of 200,000 Yuan for a villa in Shanghai in July 2007. After that, Zhang transferred the illicit money of RMB over 11 million Yuan to Ye's account for finishing the payment. Meanwhile, Zhang transferred RMB 5 million Yuan to the bank account of his friend Chen to trade stocks, and lent to others for temporary financing. In November 2007, Zhang and Ye had to cancel the purchase plan because the villa was found to be illegally built, and transferred the returned deposit, the prepayment and the penalty of RMB 8.38 million Yuan to the other bank account of Ye. When the case was investigated, Ye immediately cancelled the bank account.

Bao Concealing and Disguising Criminal Proceeds Case in Wenzhou, Zhejiang Province

450. 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. Found guilty of concealing and disguising criminal proceeds, Bao was sentenced to imprisonment of 5.5 years and fined RMB 100,000 Yuan.

451. Gao, Bao's mother, cheated to raise fund of over RMB 116 million Yuan with a figment of 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 real estates 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 gain the illicit proceeds of over RMB 9.4 million Yuan.

452. On 20 March 2009, found guilty of financial fraud of fund raising, Gao was sentenced to death penalty with confiscation of all the personal property by the Intermediate People's Court of Wenzhou in the first instance. Another son of Gao was sentenced to 8 years' imprisonment and a fine of RMB 100,000 Yuan for providing bank accounts to deposit the illicit fund. While Bao was sentenced, the Court also recovered Gao's investments in the 4 real estate under the name of Bao and confiscated his illicit proceeds of RMB 588,500 Yuan.

Wu ML Case in Guangzhou, Guangdong Province

453. On 10 November 2009, the verdict of Wu laundering case was announced in the first instance by the People's Court of Tianhe District, Guangzhou. Found guilty of ML, Wu was sentenced 3 years' imprisonment and fined RMB 5 million Yuan.

454. In September 2007, the Narcotic Control Bureau of Department of Public Security of Guangdong Province successfully solved the "6.16" drug crime case and arrested 16 suspects, including Xie and Wu, and captured illicit money of over RMB 100 million Yuan, with 5 cross-border drug criminal groups and 6 drug manufactories destroyed and another 41 drug crime cases cleared up together.

455. Xie committed drug crime and made illicit money of over 10 million Yuan from 1999 to 2003. In order to launder the proceeds of drug crime, Xie registered the Yizhong Co. Ltd in Guangzhou and entrusted Wu with task of the ML. From 2003 to 2006, Wu directly planed and invested the proceeds of drug crime in real estates, casinos and highroad projects, then purchased and sold tens of real estate by auction to gain more money. Wu' skilful technologies of ML could be divided into clear stages as follows:

	Placement stage	*Layering & integration stages*
1	Purchased two storeys of rooms in a building in Tianhe District, Guangzhou with over RMB 38.8 million Yuan and invested another 10 million Yuan to open a casino called "Flying Horse" in August 2003.	Sold the real estates and the casino at the price of RMB 64 million Yuan, gaining proceeds of 16 million Yuan, in May 2006.
2	Invested RMB 600,000 Yuan to purchase 3 apartments in Yuexiu District by auction in December 2003.	Sold the certificate of auction at the price of RMB 900,000 Yuan, gaining 300,000 Yuan.
3	Invested over RMB 20 million Yuan to purchase 9 apartments in Haizhu District and Fangcun District by auction in February 2004.	Sold to others soon and gained RMB 4 million Yuan.
4	Invested near RMB 17.8 million Yuan to purchase 21 street shops in Dongshan District by auction in March 2004.	Sold to other drug dears and gained RMB 4 million Yuan.
5	Invested RMB 7.5 million Yuan to purchase 3 apartments in Liwan District in May 2004.	Sold to others in December 2005.
6	Invested over RMB 16.5 million Yuan to purchase 44 apartments in a building in Haizhu District in December 2004.	Mortgaged several street shops for a loan to invest a highroad project in Jiangmen in January 2006.

456. This case is significant for the appearance of the professional money launderer. Previously the role of laundering proceeds was not a stand-alone function. In this case, Wu was totally attached to the crime group to deal with the laundering task, whose investments were aimed to laundering the proceeds of drug crime and gaining more money. The appearance of this kind of professional money launderer demonstrated the professionalizing trend of ML crime in China, challenging the anti-ML system.

457. Secondly, the auction of real estate became one of main channels of ML crime. It was demonstrated in this case and other similar cases that more and more criminals were inclined to invest the illicit money to real estate market and make more proceeds along with the rising house prices, which greatly damaged the development of the market, so the real estate sector should be regulated by anti-ML authority as soon as possible.

HONG KONG, CHINA

458. In 2011, Customs smashed a transnational smuggling syndicate that evaded Customs taxes in another country and laundered the proceeds of crime in Hong Kong and overseas partly through the purchase of the assets including 6 properties (real estate) with a total value over US$17 million. The mastermind and a core member were charged with ML offence(s) and their assets of over HK$460 million were restrained in Hong Kong and overseas.

PHILIPPINES

459. Immigration agents implemented a mission order to verify the immigration status of certain foreign nationals. The authorities found that JL and several foreign nationals connected with the company of JL could not give sufficient explanation of the exact status of their stay in the country. Upon deeper investigation, the authorities found JL's involvement in the manufacture of illegal drugs. The authorities discovered his clandestine shabu laboratory and a condominium unit where he was keeping his stocks of shabu and raw chemicals for manufacturing illegal drugs.

460. The authorities sought AMLC's assistance on the aspect of financial investigation, with the end in view of freezing JL's assets and subjecting the same to forfeiture. JL is the subject of several suspicious transaction reports (STRs) filed with the AMLC from which it identified that JL had several bank accounts which he opened using different aliases and falsified identification documents. The transactions in these accounts were in millions of pesos.

461. The AMLC in the course of its financial investigation established the nexus between these accounts and JL's illegal drug activity based on evidence showing that:

1. JL's bank accounts were the source of the money he used to purchase the place where he established his clandestine laboratory. He operated his clandestine laboratory inside a 3-storey building built over four (4) parcels of land surrounded with concrete fence about twelve (12) feet high designed to conceal the illegal activities inside the compound.

2. One of these accounts was also the source of the money used to purchase brand new vehicles, among which was a Jaguar X-Type car. The Jaguar was registered under one of his aliases. The same Jaguar was found to contain drug precursors to the making of shabu in connection with a lawful search conducted upon his property where he operated his clandestine shabu laboratory.

3. JL was a frequent guest and a high-roller player in the casino. Some of the most significant transactions in his bank accounts were payments into the bank account of the casino operator.

462. In sum, analysis of JL's profile revealed that he had no known business that would justify the volume of his financial transactions and acquisition of assets. He used different aliases and different identities in his bank accounts and in his other financial transactions, showing his intention to conceal his true identity. He made use of his bank accounts to transfer the proceeds of his illegal drug business, and laundered the same by placing the proceeds in time deposits, purchasing assets of high value, and playing in casinos. His multi-million fund transactions and acquisition of assets all occurred in 2001 to 2003 during the peak of JL's illegal drug operations.

463. JL is currently facing prosecution for the unlawful activity of manufacturing illegal drugs before the court and undergoing preliminary investigation for several counts of ML.

464. On petition filed by the AMLC, JL's assets as indicated below have been frozen and are now the subject of civil forfeiture proceedings:

Assets Frozen -

Funds (total):	Php	16,315,191.69
Vehicle (est. value):		2,750,000.00
Real Property (est. value):		18,340,000.00
Total Value of Frozen Assets:	Php	27,405,191.69

4.22 Use of Foreign Bank Accounts

FIJI

465. Mr HAL, a local politically exposed person charged for ML and tax evasion activities used to maintain a term deposit account at a commercial bank K in an offshore Country B. The account was opened in September 2000 with a deposit of NZ$130,000. There were nil account activity for the past ten years and accumulated interest such that the balance grew to approximately NZ$233,000.

466. In January 2011, Mr HAL instructed the commercial bank K to transfer NZ$60,000 from his term deposit account to a lawyers commercial bank account at commercial bank Z. This account is held by his lawyers located in Country B. Mr HAL advised commercial bank K that the payment was for his daughter. In May 2011, the Term Deposit account was closed. The closing balance of NZ$178,000 was forwarded by commercial bank K to Mr HAL in the form of a cheque.

THAILAND

467. A US court unsealed an indictment charging Mrs S., the executive of a Thai public enterprise, and her daughter, J.S., with one count of conspiracy to launder money, seven counts of ML, and one count of aiding and abetting.

468. From 2002-2007, Mr and Mrs G, executives of a film festival management company, who were convicted at trial of nine substantive Foreign Corrupt Practices Act violations, six counts of ML, and conspiracy, paid Mrs S. approximately US$1.8 million in exchange for more than US$ 14 million worth of contracts. The payments were made through numerous businesses and U.S. bank accounts to bank accounts in the United Kingdom, the Isle of Jersey, and Singapore held in the name of J.S. and an unnamed friend. These payments were disguised as “commission” payments in their books and records.

4.23 Use of False Identification

AUSTRALIA

Case Study

469. The discovery of a lost wallet at a fast food outlet led to a law enforcement operation that uncovered several cases of identity fraud. The wallet contained several different forms of identification, all featuring different names but bearing a photograph of the same individual.

470. Investigating officers established that the suspect maintained several false identities, while the suspect’s wife possessed a false driver’s licence.

471. It was established that the suspect had been using the names of real people to create some of his false identities, although it was never established if these people were complicit in the suspect’s fraudulent activities.

472. AUSTRAC information included seven suspicious matter reports (SMRs) linked to the suspect, although it was impossible to differentiate between transactions undertaken by a suspect while using false identification and legitimate transactions undertaken by

the actual identity holders. Six of the SMRs detailed the suspect's suspicious behaviour at gambling venues, including:

- cashing out gambling chips worth a total of AUD89,000 in structured amounts below the AUD10,000 cash transaction threshold
- a reluctance to provide identification at gambling venues.

473. The SMRs also suggested that the suspect had used some of his various aliases to conduct these gambling activities.

474. AUSTRAC information also showed that, over a one-year period, the suspect had made a number of significant cash withdrawals from a bank account, totalling AUD620,000.

475. During the same period, the suspect sent a number of international funds transfer instructions (IFTIs), primarily to India and China, totalling AUD103,000.

476. The suspect was ultimately charged with identity fraud and with using accounts made out in false names.

JAPAN

477. Gangsters affiliated with the Boryokudan disposed of stolen car navigation systems by selling them on the internet through online auctions and using IDs registered under another person's name. The winning bidders were instructed to transfer a total of approximately 440,000 yen (USD 5,500) to the bank account under another person's name, managed by the suspects. The suspects were arrested for violation of the Act on the Punishment of Organized Crimes (charged with concealment of criminal proceeds etc.).

INDONESIA

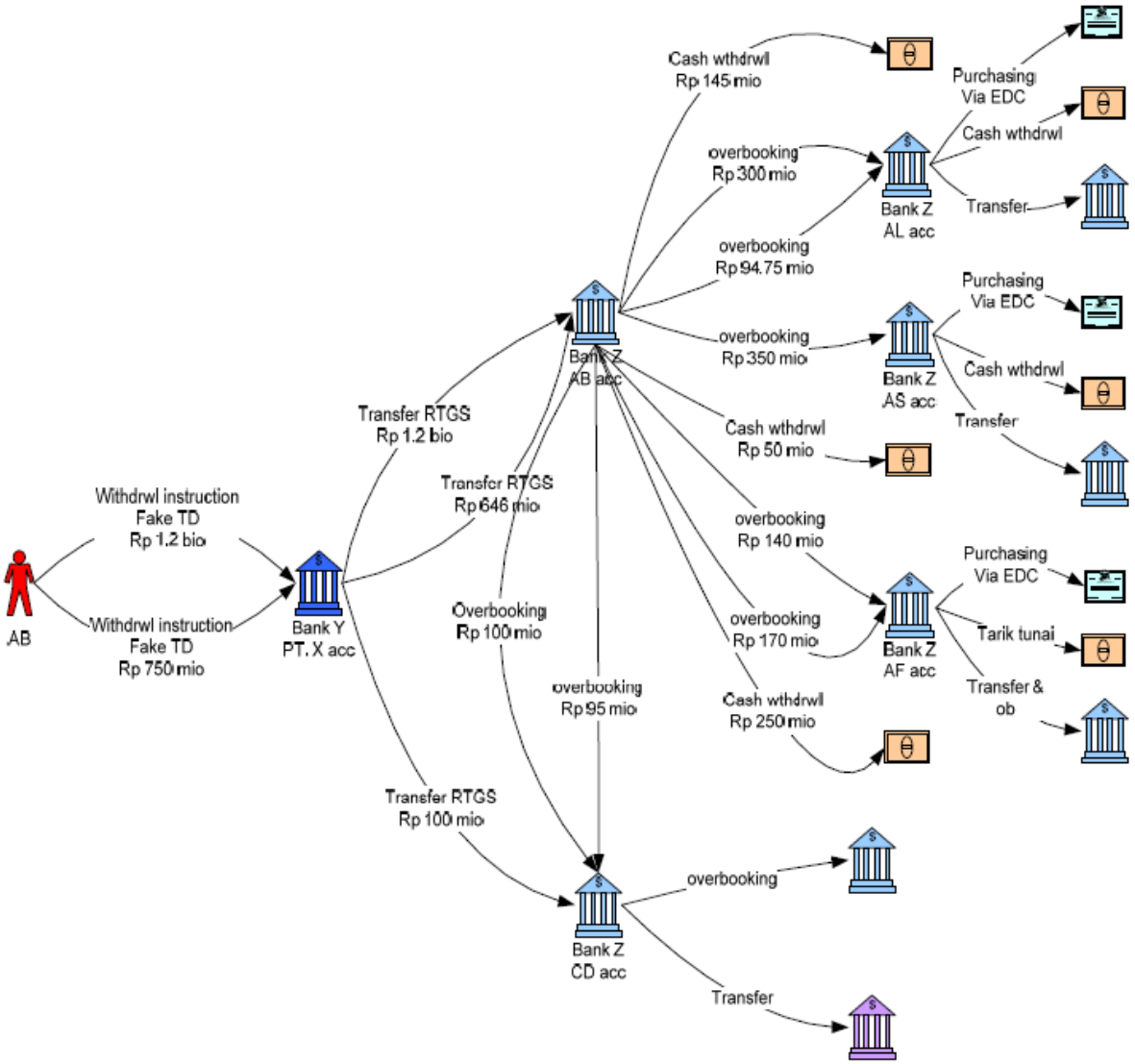
478. AB is BOD of Company X

479. Person using AB's identity to instruct Bank to terminate of TD belongs to Company X.

480. The result of the withdrawal process was transferred to AB's account in Bank Y and CD's account in Bank Z.

481. The funds in those accounts was withdrawn in cash and some were overbooked to various parties.

Flow of Funds:



4.24 Purchase of portable valuable commodities (gems, precious metals etc.)

CHINESE TAIPEI

482. Mrs A was in charge of the unregistered Company X and operated a 'Ponzi scheme' unauthorised banking business from 2003-10, including receiving deposits from the public and initially paying an inflated rate of interest. Mr A was in charge of exploiting the money received from the public. Ms B, Mrs A's sister carried out Mrs A's instruction. They attracted 7,342 depositors to provide NTD 18,148,500,000 (approx. US$606,692,930) in total until the scheme was detected and Mr and Mrs A were arrested by the Investigation Bureau.

483. The Investigation Bureau found that Mr and Mrs A used the following to launder proceeds of the Ponzi scheme: a) purchasing 85 pieces of real estate in the names of third parties, mortgaged them to the bank and got the loan; b) buying stocks in domestic and foreign stock markets in the names of third parties; c) investing in other companies in the names of third parties; d) buying USD 52,953, GBP 110,019, and HKD 4,779,554; e) buying pre-sale homes valued NTD 793,900,000 (approx. US$26539577) in the names of themselves and third parties; f) buying 170 pieces of antiques and 118 pieces of valuable wood furniture; g) remitting USD 6,740,000 to foreign banking accounts in Singapore.

484. After searching their houses and premises and checking all relevant banking accounts and safe boxes by the Investigation Bureau, the above items have been frozen and seized by the court, and Mr and Mrs A and Ms B were accused of breaching the Banking Law and ML Control Act by the Prosecutor's Office in 2011.

JAPAN

485. An alternative remitter who smuggled luxury watches out of Japan in order to transfer the value has been detected. The total value was JPY1.5billion or USD20million.

5. ACRONYMS

AC - Anti Corruption
ADB - Asian Development Bank
AGD - Attorney General's Department
AML - Anti-ML
AMLD - Anti-ML 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
CTR - Cash Transaction Report
DIAC - Department of Immigration and Citizenship
EAG – Eurasian Group on Combating ML and Financing of Terrorism
EDD - Enhanced Due Diligence
EFT - Electronic Funds Transfer
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
IFTI - International Funds Transaction Instruction
INTERPOL – International Criminal police Organisation
KPK – Indonesia's Corruption Eradication Commission
LEA - Law Enforcement Agency
MENAFATF – Middle East & North Africa Financial Action Task Force
ML - ML
MLA - Mutual Legal Assistance
MONEYVAL - The Committee of Experts on the Evaluation of Anti-ML Measures and the Financing of Terrorism
MOU – Memorandum of Understanding
MSB - Money Service Bureau
NZD - New Zealand Dollar
RMB - Chinese Renminbi
SCTR - Significant Cash Transaction Report
SEC - Security Exchange Commission
STR - Suspicious Transaction Reports
SUSTR - Suspicious Transactions Report
TCSP - Trust and Company Service Providers
TF - Terrorism Finance
UN - United Nations
USD - United States Dollar
VAT - Value Added Tax