

APG Yearly Typologies Report

2013



**Asia/Pacific Group
on Money Laundering**

Asia/Pacific Group on Money Laundering

18 July 2013

APG Yearly Typologies Report 2013

Applications for permission to reproduce all or
part of this publication should be made to:

APG Secretariat
Locked Bag A3000
Sydney South
New South Wales 1232
AUSTRALIA

Tel: +61 2 9277 0600

E Mail: mail@apgml.org

Web: www.apgml.org

© July 2013/All rights reserved

CONTENTS

INTRODUCTION.....	4
1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2012 - 2013	5
2. OVERVIEW OF TYPOLOGY PROJECTS BY FATF AND FATF-STYLE REGIONAL BODIES.....	9
3. TRENDS IN MONEY LAUNDERING & TERRORISM FINANCING	17
4. CASE STUDIES OF ML AND TF	41
5. USEFUL LINKS	115
6. ACRONYMS	117

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 customer due diligence and suspicious transaction 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 2012-2013

4. The APG Typologies Working Group continued its work in 2012-13 under the leadership of India and Fiji as Co-chairs. In July 2012 the APG Typologies Working Group met to determine the work program for the year, including the in the Asia/Pacific region and the conduct of an APG Typologies Meeting in late 2012 hosted by Vietnam in Hanoi.
5. 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.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2012 - 2013

1.1 2012 APG Typologies Workshop and Capacity Building Seminars

7. Each year the APG brings together AML/CFT practitioners from investigation and prosecution agencies, financial intelligence units, regulators, customs authorities and other relevant organisations to consider priority ML and TF risks and vulnerabilities. In recent years APG has taken the opportunity to combine the Typologies Workshop with Capacity Building Seminars to share practitioners' experience on priority topics.
8. The agenda of APG Typologies and Capacity Building Workshops are designed to achieve a number of objectives:
 - Bring together the APG community of practitioners to share experience and foster networks of cooperation.
 - Support research being undertaken by the APG Typologies Working Group
 - Facilitate APG members to contribute to FATF-led typologies studies;
 - Share best practice and strategies for practical application of AML/CFT measures related to previous typologies studies and other implementation issues.
9. Vietnam hosted the APG Typologies Workshop in Ha Noi from 19 - 23 November 2012 attended by more than 170 delegates from 34 APG members and nine organisations. The workshop was jointly chaired by Mr Razim Buksh, Director of Fiji's FIU and Mr Nguyen Huu Nghia, Chief Director of Banking Supervisory Agency, State Bank of Vietnam. The agenda included a range of topics designed to support on-going FATF projects, as well as APG and APEC work.
10. Typologies discussion topics included:
 - *ML/TF vulnerabilities from gold and gem dealers, real estate agents, lawyers and accountants* (APG contributing to the APEC DNFBP study)
 - *Hawala/Underground Banking* – ML/TF vulnerabilities (in support of the global FATF study)
 - *Laundering the Proceeds of Corruption* – case studies and possible countermeasures.
 - *Counterfeit Currency* (in support of the global FATF study)
11. The Capacity Building workshop involved three technical seminars, including a meeting with representatives of the private sector. The technical seminars were generously supported by the Commonwealth Secretariat.
12. The technical seminars covered:
 - *Trade-based money laundering* (building on the APG's July 2012 study) and laundering the proceeds of tax offences.

- *‘Following the Money’* – addressing the policy gap in proceeds of crime and prosecuting money laundering – supporting a culture and practice of prosecuting ML and recovering assets.
 - *Building strategic partnerships between government and the private sector.*
13. While previous APG Typologies workshops have included limited private sector representatives, the seminar with the private sector 2012 Typologies Workshop was the first time private sector representatives from across the region had been invited with a tailored agenda over a number of days.
 14. The sessions aimed to expand partnerships between the public and private sectors on AML/CFT typologies, including opportunities to involve the private sector in national risk assessments, building the profile of AML/CFT risk management, enhancing industry cooperation on AML and drawing on industry experience in the selection and conduct of studies of ML and TF typologies.
 15. APG and industry representatives indicated a strong preference for further engagement on regional typologies issues. Delegates expressed support to consult on the establishment of a regional APG / Private Sector Typologies Contact Group to support enhanced information sharing and options for joint government / private sector typologies studies. The Contact Group could also support further joint public / private sector typologies-related events.
 16. Keynote presentations were given by VISA, Deloitte Touche Tohmatsu, and Bank of Tokyo-Mitsubishi.
 17. The outcomes from the APG Typologies and Capacity Building workshops in Vietnam will play a positive and practical role in improving regional cooperation and countermeasures for AML/CFT across the region.

1.2 2013 Revised FATF Standards and Pacific Typologies Workshop

18. In March 2013 AUSTRAC and the APG hosted a Workshop on the Revised FATF Standards and Pacific Typologies. The workshop was attended by more than 60 delegates from 12 Pacific APG member jurisdictions, as well as from Australia, Indonesia, New Zealand, the United States and the United Kingdom. The Pacific Island Forum Secretariat (PIFS), the Pacific Island Law Officers network (PILON), Kiribati and Tuvalu also attended. The workshop was hosted by AUSTRAC and sponsorship assistance was also provided by the United States and PIFS.
19. The following topics were discussed:
 - *Money Laundering Risks Associated with Offshore Financial Centres (OFCs)*, including the financial products available in Pacific Island jurisdictions, the major markets for those products and cases where such products have been misused. A project on this topic will be carried out over 2013 – 2015, co-led by the Cook Islands and Samoa.
 - *Frauds and Money Laundering in the Pacific*, highlighting the techniques, methods and types of fraud, and the threats from money laundering associated

with domestic and transnational frauds across the Pacific. New Zealand and Fiji have been co-leading a project that will be concluded during 2014.

- *Recovering the Proceeds of Corruption in the Pacific*, considering the methods and issues associated with corruption activities in the Pacific region, as well as practical measures related to the recovery of the proceeds. A project is being co-led by Papua New Guinea and Tonga and will be carried out over 2013-2014.
 - *Trans-Pacific Drug Trafficking Routes*, introducing the nature of the routes in the Pacific, the points of contact, the size of the markets and the financial vulnerabilities and risks with respect to money laundering. A new APG typologies project on the topic will be carried out over 2013-2015, co-led by Tonga and another Pacific APG member jurisdiction.
 - *Revised FATF Standards* – this was the third workshop on this topic since July 2012. The workshop briefed members on the key changes to the FATF recommendations and assessment methodology and provided delegates with an opportunity to apply the new standards to an aspect of their own AML/CFT regime.
20. A survey of the participants found that the workshop increased their knowledge of all the topics covered. The success of the Pacific Typologies Workshop gave rise to a call for future sub-regional typologies events to enhance understanding and build operational capacity. In addition to the topics covered at this workshop, participants indicated that they would like to see some of the following topics included in possible future typologies events: tax evasion; the natural resources sector; casinos; cybercrime; and human trafficking.

1.3 Status of current projects and possible new projects

21. *Gold – Money Laundering and Terrorist Financing Risks and Vulnerabilities* – a Concept Note and Project Plan was submitted to, and endorsed by, the APG Typologies Working Group in July 2013. The APG project co-leads are India and Australia.
22. The project will examine the characteristics of gold production, movement, trade and markets with a focus on the illicit risks. The aim of the project is to identify the techniques, trends and methods of ML and TF associated with gold; the risks and vulnerabilities, problems and possible solutions for investigations of ML / TF and predicate offences associated with gold; and identify ‘red flag’ indicators that could assist various stakeholders, including DNFBPs, financial institutions and others to capture relevant data and, as appropriate, identify reporting suspicious activity associated with the precious metals market. This topic will be one of the breakout sessions at the 2013 APG/EAG Joint Typologies Workshop.
23. The APG is contributing to several FATF typologies projects, including one on ‘*The Risk of Terrorist Abuse in the NPO Sector*’ and a new one on ‘*Financial Flows linked to illicit production and trafficking of Afghan drugs and associated ML/TF activities*’. These projects will also be featured in the 2013 Typologies Workshop.

Private Sector Outreach on Typologies

24. APG is pursuing further typologies-focused dialogue between government and private sector representatives. This builds on the contact during the 2012 Typologies Workshop, which focused on opportunities for sharing experience of assessing ML/TF risk. APG is also discussing a mechanism for ongoing contact and cooperation with the private sector on typologies research and capacity building. This may include an APG Typologies Working Group private sector contact group focusing on AML/CFT compliance specialists in financial institutions.
25. During the 2012 Typologies Workshop sessions with the private sector a number of issues were discussed which will help to set the scene for ongoing cooperation between APG and the private sector on typologies. Issues include the risk information elements compliance teams take into account when preparing AML/CFT risk assessments, including enterprise risk, product risk, country or market risk and customer risk. A challenge is to ensure that compliance teams have access to credible typologies as one of the inputs to analysis of parameters of risk.
26. The 2012 workshop included discussion of the importance of shared approaches between government and the private sector to help to build awareness of and the professional profile of AML/CFT Risk Management within financial institutions. Participants considered the important roles for industry associations in making AML/CFT a priority. Other issues include publicity and awareness as a broader element of corporate responsibility and ‘selling the message’ of shared purpose between governments and the market.
27. At a practical level, the 2012 workshop considered opportunities to support compliance teams in their efforts to ensure that all stakeholders within enterprises understand the benefits of a strong compliance function through quantifying costs of reputation risk, sanctions, post-event remediation, etc. Law enforcement and prosecutors highlighted opportunities to expressly recognise positive inputs from compliance teams in court during ML prosecutions.

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

28. A range of typology studies have been published in 2012 and 2013 by the FATF and several other FSRBs, including:

2.1 FATF Typology Projects

*Illicit Tobacco Trade*¹

29. The FATF Study into the illicit tobacco trade found that illicit tobacco represents a significant percentage of the global cigarette market, estimated to amount to tens of billions of dollars. Given its cash intensive and profitable nature, the illicit tobacco trade is also a vector for money laundering, as it presents low levels of risk for the offenders in terms of detection, seizure and prosecution. Some cases were identified which included proceeds of illicit tobacco trade were used in terrorist financing.
30. The FATF report into *Illicit Tobacco Trade (ITT)* highlighted the need to enhance the international cooperation and recognise the illicit trade in tobacco as a significant global money laundering and terror financing threat.
31. Key areas of concern covered in the report include:
- The percentage of lost government revenues due to evaded taxes and customs duties.
 - Identifying the nature and extent of the risks posed by illicit tobacco trade in comparison to enforcement actions taken to curb the phenomenon.
 - The final destination and purpose of aggregated illicit funds.
 - The methodologies used to launder these illicit funds and the potential to uncover new mechanisms specific to ITT, and
 - A need to better understand the totality of ITT criminal finances, including opportunities for disruptive activity targeting perceived or identified financial pinch points (such as during the laundering of street cash following sales of illicit tobacco products).
32. The purpose of the report is to:
- Define the illicit trade in tobacco, including the supply chain associated with the different types of smuggling.
 - Determine and assess the extent of the money laundering and terror financing (ML/TF) vulnerabilities associated with the illicit trade in tobacco and illustrate this via case studies provided by key contributors.

¹ <http://www.fatf-gafi.org/topics/methodsandtrends/documents/illicittobaccotrade.html>

- Identify possible indicators to assist financial and non-financial institutions in uncovering, reporting and countering smuggling activities, the misuse of trade practices and money laundering or terrorist finance techniques.

Money Laundering and Terrorist Financing Related to Counterfeiting of Currency²

33. The FATF study examined the illicit financial flows related to counterfeiting of currency. Counterfeit currency threatens the integrity of the financial system through criminal groups producing counterfeit currency as a profit-making activity in order to sell or resell it for illegal gain; terrorist groups using counterfeit currency for financing their activities; and states and/or terrorist groups using counterfeit currency as a means of economic warfare against other countries.
34. The report mainly focuses on the first two of these elements, acknowledging that it is the involvement of the international organised crime groups which make the ML issue especially relevant. On the other hand, use of counterfeit money to finance terrorism appears to have distinct regional characteristics.
35. The report aims to:
 - Identify the linkages between counterfeiting of currency and organised crime, terrorist financing and other crimes.
 - Identify and describe ML and TF methods associated with counterfeit currency and contrast the methods of placement of counterfeit currency with those of other criminal proceeds.
 - Identify AML/CFT measures that are useful in detection of counterfeiting of currency and associated to ML and/or TF.
 - Identify red flag Indicators for detection of suspicious transactions relating to counterfeit currency.
 - Identify gaps in the legal framework and/or mismatch in the operational interaction of LEAs, customs and FIUs preventing successful investigation and prosecution of ML/TF arising from counterfeit currency.
36. The report discusses various policy initiatives to tackle the issue by international organisations and governments, as well as operational practice of LEAs, both domestically and on the international level. A number of red flag indicators were identified to help raise awareness among both public and private sector stakeholders.

Red Flag indicators

37. Red Flag indicators are generally common to most of the predicate crimes. The Red Flag Indicators for detection of suspicious transactions relating, *inter-alia*, to Counterfeit Currency have been identified as follows, of which point number v and viii relate specifically to counterfeit currency:
 - i. Activity inconsistent with customer profile.
 - ii. Multiple deposits below a certain threshold.

² Report to be published shortly. http://www.fatf-gafi.org/documents/documents/plenary-outcomes-june-2013.html#COUNTERFEIT_CURRENCY

- iii. Same day transactions conducted at different bank branches.
- iv. Deposit from different counters under the designated threshold.
- v. Cash deposits made to one account at the same place by multiple individuals.
- vi. Splitting large currency deposits among several accounts.
- vii. Customer makes frequent deposits or withdrawals of large amounts of currencies for no apparent business reason or for a business that generally does not generate large amounts of cash.
- viii. Small value cash deposits in multiple locations followed by immediate cash withdrawals in locations where counterfeit currency groups are active.
- ix. Subjects wanted by the authority for currency counterfeiting offences.
- x. Cash deposits with small denomination banknotes, to perform wire transfers.
- xi. The banknotes brought by customers being small denominated and dirty, existence of stains demonstrating that it has been carried concealed in various elements and giving off a smell,
- xii. Packaged carelessly and precipitately, lacking or exceeding substantially the declaration of the customer when counted, coming across with counterfeit banknotes in a bankroll.
- xiii. The involvement of high denomination banknotes, this is by virtue of the fact that high denomination bank notes carry larger intrinsic value.

ML/TF Vulnerabilities of Legal Professionals³

- 38. Since the inclusion of legal professionals in the scope of the FATF Recommendations in 2003, there has been extensive debate within the profession as to whether there is evidence that legal professionals have been involved in ML/TF.
- 39. The FATF study confirms that there are indeed cases in which legal professionals have been involved in ML and asserts that criminals seek out the involvement of legal professionals in their ML schemes, at times because a legal professional is required to complete certain transactions, and at other times to access specialised legal and notarial skills and services which could assist the laundering of the proceeds of crime and the funding of terrorism.
- 40. Among other vulnerabilities, the report discusses the use of legal professionals to provide a veneer of legitimacy and/or respectability to the client's activity, as well as the perception that legal professional privilege/professional secrecy would delay, obstruct or prevent law enforcement action being taken against the client.
- 41. Key aspects of the report include the large number of case studies (over 100 were taken into account) that support the findings, as well as a separate section on red flag indicators drawn from those cases and educational material provided by self-

³ <http://www.fatf-gafi.org/media/fatf/documents/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf>

regulatory bodies and competent authorities. The majority of case studies in the report relate to ML activity, although the report identifies that similar methodologies are capable of being used for TF activity.

42. The report also discusses the issue of professional secrecy and privilege, and the implications this issue has on lawyers being subject to the AML/CFT regime. It also addresses whether the application of the FATF Recommendations is consistent with fundamental human rights and the ethical obligations of legal professionals.

2.2 EAG - The Eurasian Group

EAG Member States' FIUs Cooperation for the Purpose of Preventing Terrorist Activities of Organizations Acting in the Eurasian Region and not Listed in the International List (UN) Of Terrorist Organizations, 2012⁴

43. The study looked at the main ways of information co-operation between FIUs in relation to possible financing of terrorist and extremist activities by persons associated with organisations on the national lists of prohibited terrorist and extremist organisations. The EAG is developing a strategy for the establishment of a uniform Regional List of Terrorist and Extremist Organisations (Regional EAG List) for use by the EAG member states.

Misuse of Non-Profit Organizations for Money Laundering, 2012⁵

44. This typology project was proposed and steered by the Financial Monitoring Committee of the Ministry of Finance of the Republic of Kazakhstan.
45. The aim of the study was to enhance the role of FIUs in combating offences associated with NPOs and it recommends that FIUs:
- Arrange work in this area with the application of the ML/FT risk-based approach.
 - Integrate information from the national NPO register on those NPO's activities that pose the highest ML/FT risk, into the information systems of FIUs.
 - Arrange financial monitoring of NPOs that pose high ML risk for identifying suspicious transactions.
 - Synchronize the NPOs database with the list of persons associated with extremist and terrorist activities in order to identify the NPOs in which such persons have interest.
 - Implement the computer-aided (automated) procedure of identifying organizations in the NPO sector whose operations have the suspicious activity indicators.

⁴ http://eurasiangroup.org/files/Typologii%20EAG/WGTYP_2012_9_eng.pdf

⁵ http://eurasiangroup.org/files/Typologii%20EAG/WGTYP_2012_7_eng.pdf

Money Laundering and Terrorist Financing with Use of Physical Cash and Bearer Instruments, 2012⁶

46. This study, led by the Republic of Belarus, concluded that the reasons contributing to the risk of money laundering involving the use of cash and bearer instruments include:
- Poor quality of internal control measures in banks and non-bank financial institutions.
 - Insufficient level of reporting by banks and non-bank financial institutions of unscrupulous customers identified in the course of internal controls (as a consequence of the above reason).
 - Gaps in the relevant legislation that make the use of cash and monetary instruments for criminal purposes possible.
47. The report recommends that particular attention should be paid to the establishment of permanent partnership relations with the private sector as an effective tool for identifying risks in different areas.
48. As a separate measure, it is recommended to consider possible changes to applicable laws governing the circulation of currency and monetary instruments, which will make it possible to:
- lower to a safe level the threshold for cash withdraws by individual entrepreneurs and legal entities;
 - introduce an obligation for legal entities and individual entrepreneurs to pay income tax when carrying out cash-out transactions above the threshold;
 - introduce mandatory identification of persons discharging bearer monetary instruments and set limits on discharge of bearer monetary instruments; and
 - limit settlements between legal entities, as well as between legal entities and individuals, involving the use of monetary instruments.

2.3 ESAAMLG – the Eastern and Southern Africa AML Group

Typologies Report on Money Laundering Related to Illicit Dealings in and Smuggling of Motor Vehicles in the ESAAMLG Region, 2012⁷

49. This study was aimed at identifying vulnerabilities of money laundering and terrorist financing associated with illicit dealings in and motor vehicle smuggling through case studies from the region in order to identify the trends and methods used to launder the proceeds generated from the illicit dealing in and smuggling of motor vehicles.
50. Based on the case studies, it is clear that bonded warehouses and Financial Institutions are being misused to facilitate money laundering activities with the real estate being the most vulnerable area where the proceeds are used. The study has also shown that insurance companies are widely affected by fraudulent claims made by motor vehicle owners who illegally export their vehicles and later report them stolen.

⁶ http://eurasiangroup.org/WGTYP_2012_10_eng.pdf

⁷ <http://www.esaamlg.org/userfiles/Illicit%20Dealings%20in%20and%20Smuggling%20of%20Motor%20Vehicles%20Report.pdf>

51. One of the key findings of this study, as with the predecessor ESAAMLG typologies reports, is that law enforcement officers do not investigate cases beyond the predicate offence to establish the money laundering aspect, neither is there proper direction/guidance to law enforcement by prosecution and the courts in that regard.
52. It was further established that there is no proper maintenance of statistics of criminal cases. This adversely affects the extent of assessing the magnitude of ML related to illicit dealings in and smuggling of motor vehicles in the region.
53. General Indicators:
- Same people transporting vehicles across the borders.
 - Tempered registration/chassis number and information plate.
 - Different registration numbers for the same vehicle.
 - Unreported accident incidences.
 - Duplication of registration numbers.
 - Motor vehicle insurance claims from the same dealers.
 - Change of motor vehicle colours.
 - False Foreign registration plates.
 - Change of ignition keys.
 - Irreconcilable records on import and export of motor vehicles entering and leaving a warehouse.
 - Misclassification of motor vehicles on documentation.
 - Falsified customs clearing documents.
 - Conflict of interest in official duties by officers.
 - Huge foreign purchases.
 - Use of cash to facilitate transactions (air tickets and hotel bookings).
 - Vehicles being sold at low prices.
 - Proxy registration.
 - Abuse of exemption facility for returning residents.
 - Use of front companies.
 - Same people crossing borders with different luxury vehicles.
 - Foreign nationals conducting business unrelated to work permits.
 - Same officers assisting particular customers.

2.4 GAFISUD - The Financial Action Taskforce of South America

54. In May 2012 GAFISUD and the Egmont Group held a joint Typologies meeting in Ecuador. The cases presented and relevant red flag indicators can be found at: http://www.gafisud.info/pdf/Joint_typologies_GAFISUD_EG_meeting_2012_concept_paper--.pdf
55. Amongst the cases described there are number which include remittance, including use of hawala; trade based money laundering, including factoring businesses; and ML associated with illegal trading in gold.

2.5 GIABA – The Inter-Governmental Action Group Against Money Laundering in West Africa

56. In May 2012 GIABA published a *Typologies Report on Tax Crimes and Money Laundering in West Africa*⁸.
57. A number of indicators and red flags were identified based on the various case studies presented.
58. Indicators:
- Non-remittance of tax proceeds by authorized tax collectors.
 - Preference and usage of non-bank value transfer systems.
 - Ostentatious and conspicuous lifestyles and sudden unexplained wealth.
 - Maintenance of multiple financial and accounting records.
 - Systematic reduction in tax revenue.
 - Preference for cash transactions.
 - Huge amounts involved in activities that have no link with declared activity, neither by income nor by the importance of the sector.
 - Under statement of account by corporate entities.
 - Structuring of employee salaries/entitlements to allocate substantial amount payable to non-taxable incomes/sub-heads.
 - Former tax officials working as tax consultants for corporate high net worth companies.
 - Consistent exceptionally good reports for corporate entities by tax administrators.
 - So-called re-investment of large amount from profits before tax where zero tax provision on such investment exist.
 - Unusual transactions without any economic justification.
 - Revenue/income manipulations.
 - Tax waivers for products or services that are monopolised by a few companies.
 - Frequent interactions between company officials and particular tax officials (so called fixers).
 - Importing goods into low tax country and then moving them to high tax country (profit based on tax rate).
59. Red flags:
- False declaration of merchandise and significant discrepancies between the values of the commodity reported on the invoice and the commodity's fair market value.
 - Award of bonuses that seem to exceed industry expectations.
 - Use of acronyms to open bank accounts for diversion of official cheques.
 - Transactions aimed at reducing tax liabilities, including transfer pricing.
 - Use of two set of tax collection registration numbers
 - Absence of value added tax registration number on receipts while the VAT has been claimed.
 - Non-declaration on receipts of tax amount claimed.

⁸http://www.giaba.org/media/f/433_GIABA%20TYPOLOGIES%20REPORT%20ON%20TAX%20CRIMES%20AND%20MONEY%20LAUNDERING%20IN%20WEST%20AFRICA.pdf

- Use of different types of receipt to sell the same goods or offer the same service.

2.6 The Egmont Group

The Role of Financial Intelligence Units in Fighting Corruption and Recovering Stolen Assets⁹

60. The paper aims to:
 - Increase awareness of corruption, AC and asset recovery among FIUs.
 - Present case scenarios, good practices and parameters for FIUs to the fight against corruption.
 - Describe the position and role of the FIU in the asset recovery process.
61. The study concentrates on the role and responsibilities of an FIU and how the FIU can contribute to fighting corruption within a national and international AML/CFT and AC structure.

⁹ <http://www.egmontgroup.org/library/download/229>

3. TRENDS IN MONEY LAUNDERING & TERRORISM FINANCING

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

AUSTRALIA

62. AUSTRAC publishes annual Typologies and Case Studies Reports to assist reporting entities meet their AML/CTF obligations. Each report contains numerous case studies, typologies and indicators.
63. The July 2012 AUSTRAC Typologies and Case Studies Report¹⁰ examines financial typologies used to commit serious transnational crime comprising use of cheques and cash couriers. The report also examines potential vulnerabilities comprising of digital currencies and virtual worlds, voucher system products and offshore online money remitters.
64. The report includes 21 case studies that were initiated or supported by reports submitted to AUSTRAC by account and deposit-taking, gambling and remittance service businesses. The case studies feature an array of offences, including large-scale tax evasion, advance fee fraud and investment scams, identity theft and drug trafficking.
65. All six Typologies and Case Studies Reports (2007 – 2012) are available on the AUSTRAC website - <http://www.austrac.gov.au/typologies.html>
66. AUSTRAC also produced the following five research and typologies papers to reporting entities and partner agencies.
 - Research Paper: Digital Currencies and Virtual Worlds
 - Typology Paper: Third Party Cash Couriers
 - Typology Paper: Misuse of Cheques
 - Research Paper: Voucher Systems Products
 - Research Paper: Offshore Online Money Remitters
67. Abbreviated versions of these reports are included in the Typologies and *case studies report 2012*.

CANADA

68. The *Money Laundering and Terrorist Activity Financing Watch: January-March 2012*¹¹ presents a quarterly review of news articles summarising relevant group-based, activity-based and country-based money laundering and terrorist activity financing issues, and alerts readers to new financial mechanisms or technologies that could possibly be exploited for money laundering or terrorist activity financing purposes in Canada.

¹⁰ http://www.austrac.gov.au/files/typ_rprt12_full.pdf

¹¹ <http://www.fintrac.gc.ca/publications/watch-regard/2012-07-eng.pdf>

69. In April 2013 FINTRAC published *Money Laundering Trends and Typologies in the Canadian Securities Sector*¹². Through this report FINTRAC seeks to address questions about money laundering that are relevant to the Canadian securities sector and have been observed in their analysis of financial transactions involving the sector.
70. The report comprises three main sections: The first section provides an overview of the Canadian securities sector, statistics on its reporting to FINTRAC and trends in suspicious transaction reports submitted to FINTRAC by securities dealers over the past several years.
71. The second section discusses some of the most common money laundering methods and techniques observed in relation to the sector, and presents case examples and money laundering “red flags” based on a review of FINTRAC cases disclosed between 2007 and 2011. The third and final section of the report describes additional and emerging money laundering risks for Canadian securities dealers.

NEW ZEALAND

72. The FIU produced an *AML/CFT National Risk Assessment (NRA)* in 2010. A revised version of the NRA is under development and is expected by the end of 2013. This is an open source document and can be viewed at: <http://www.justice.govt.nz/policy/criminal-justice/aml-cft/publications-and-consultation/20110308-NRA-2010-Primary-Document-FINAL.pdf>
73. The FIU produces an AML/CFT Quarterly Typology Report four times a year. This is an open source document available to all interested parties on a subscription basis¹³.
74. The three Sector Supervisors in New Zealand (the Reserve Bank of New Zealand, the Department of Internal Affairs, and the Financial Markets Authority) have all produced AML/CFT Sector Risk Assessments and a number of guideline documents pertinent to their respective reporting entities. These are all open source documents¹⁴.

FIJI

75. The Fiji FIU has conducted basic and informal research on ML/TF methods and trends. The Fiji FIU continues to provide this information through the following:
 - The 2011 Annual Report, which includes case studies from Suspicious Transaction Reports and two major case studies on successfully prosecuted money laundering cases in Fiji. The report also includes emerging, continuing and declining money laundering trends. Fiji FIU 2011 Annual Report is available on Fiji FIU’s website - www.fijifiu.gov.fj

¹² <http://www.fintrac-canafe.gc.ca/publications/typologies/2013-04-eng.pdf>

¹³ Quarterly Typology Reports for 2013 are available at <http://www.police.govt.nz/service/financial/fiu>

¹⁴ Reserve Bank of New Zealand: http://www.rbnz.govt.nz/regulation_and_supervision/anti-money_laundering/guidance_and_publications/4345201.pdf; Department of Internal Affairs: [http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/\\$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf](http://www.dia.govt.nz/Pubforms.nsf/URL/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf/$file/AMLCFT-SectorRiskAssessment-FINAL-1April2011.pdf); Financial Markets Authority: <http://www.fma.govt.nz/media/186534/aml-cft-sector-risk-assessment.pdf>

- In September 2012, the FIU organized a compliance officers AML forum for the banking sector and the securities sector wherein recent case studies and trends were shared with participants.

HONG KONG, CHINA

76. On-going studies are being conducted on the money laundering risks in the real estate market, remittance agents in relation to casino, and new payment methods.

MALAYSIA

77. Malaysia is currently undertaking a National ML/TF Risk Assessment (NRA) to assess ML/TF risk at the national level. This NRA will enable the authorities, to better understand the scale, sources, trend and methods of money laundering and identify the vulnerabilities in the AML/CFT system and controls.
78. The outcome of this NRA will act as guidance to the FIU, law enforcement agencies, regulators and relevant authorities to direct and prioritise intervention and resources to the identified risks. Essentially, this is to support structured and focused implementation of strategies to build a strong, robust and effective AML/CFT regime and application of the risk-based approach in implementing certain AML/CFT measures in line with the international standards.
79. Financial Stability Research Project: Hawala system and its potential impact on the economy and financial system.
80. Bank Negara Malaysia is conducting research on the hawala system and its impact on the economy and financial system. The purpose of this research is to have a good understanding of hawala practices to support policy efforts in increasing the prospects for channelling the hawala through the formal systems, as well as to safeguard the financial system against financial crimes.
81. Areas of research include:
 - a) principles behind the hawala system and its modus operandi;
 - b) contributory factors to the proliferation of the hawala practice; and
 - c) the broader implications of the hawala practice on the Malaysian economy and the financial system; and potential regulatory challenges in addressing this issue.

SOUTH KOREA

82. The Korean FIU (KoFIU) publishes two official documents annually. One is its annual report and the other is the Money Laundering Trends Review. Both publications cover the overall issues related to money laundering and terrorist financing. They will be published during the first half of 2013.

USA

83. In July 2012 FinCEN published *Real Estate Title and Escrow Companies: A BSA Filing Study* Assessing Suspicious Activity Reports and Suspicious Form 8300 Filings Related to Real Estate Title and Escrow Businesses 2003–2011¹⁵.

¹⁵ http://www.fincen.gov/news_room/rp/files/Title_and_Escrow_508.pdf

84. The study presents a range of typologies where title and escrow companies appear to have been abused by money launderers, as well as a number of cases where the companies, or criminals fraudulently representing themselves as legitimate companies, were suspected of being involved in facilitating illegal activity.
85. This comprehensive review provides greater context to understand the individual instances previously identified by FinCEN in its studies of mortgage fraud and money laundering in the real estate industries, as well as in supporting criminal investigations and prosecutions that involved title and/or escrow companies.
86. Issue 22 of *The SAR Activity Review - Trends, Tips and Issues*¹⁶ was published in October 2012. Included in this publication is an industry perspective on the AML risks presented by business funded prepaid cards.
87. In May 2013 Issue 23 of *The SAR Activity Review - Trends, Tips and Issues*¹⁷ was published. Of particular interest is a chapter on Suspected Money Laundering in the Accountancy Profession – An Assessment of Depository Institution SARs to Identify Vulnerabilities and Reporting Trends.
88. Issue 18 of *The SAR Activity Review – By the Numbers*¹⁸ for 2012 was also published in May 2013. By the Numbers is published once a year and incorporates numerical data covering a decade of Suspicious Activity Report (SAR) filings through the most recent twelve-month period, for each of the filing industries for which a form has been developed. *By the Numbers* serves as a companion piece to *The SAR Activity Review – Trends, Tips & Issues*, which provides information about the preparation, use, and utility of SARs.

3.2 Association of Types of ML or TF with Predicate Activities

AUSTRALIA

Serious and organised investment fraud

89. AUSTRAC is part of a high-level government taskforce established in response to a rise in serious and organised investment fraud in Australia.
90. Established by the Australian Crime Commission Board, Task Force Galilee cooperates with state and federal government agencies to combat the growing threat of cold-call investment fraud being perpetrated by organised crime groups offshore.
91. As a member of Task Force Galilee, AUSTRAC's financial intelligence plays an important role in the detection and investigation of these frauds. This sophisticated form of fraud, sometimes referred to as boiler-room fraud, seeks out Australians in or approaching retirement age with savings to invest.

¹⁶ http://www.fincen.gov/news_room/rp/files/sar_tti_22.pdf

¹⁷ http://www.fincen.gov/news_room/rp/files/sar_tti_23.pdf

¹⁸ http://www.fincen.gov/news_room/rp/files/btn18/sar_by_numb_18.pdf

92. Typically, the fraudsters contact victims over the phone and use an array of persuasive techniques to build trust before enticing the victims to transfer funds into bogus investments.
93. In recent years, authorities have identified more than 2,600 victims, with at least \$113 million in savings lost to date, although these estimates are conservative.

BRUNEI DARUSSALAM

94. Based on crime statistics, predicate offences which can be associated with money laundering are smuggling (including smuggling of fuel and cigarettes), drug trafficking and theft.

FIJI

Money Laundering

95. The methods of money laundering in Fiji through financial institutions are general and are associated with various predicate offences. For example, large cash deposits into a personal account have been linked to fraud, forgery, corruption and tax evasion.

Terrorist Financing

96. Fiji does not have any successfully prosecuted cases of terrorist financing. There have, however, been investigations on foreign businessman (in particular Pakistani nationals) that are remitting business funds to individuals in Pakistan that are reportedly linked to terrorist organizations.

HONG KONG, CHINA

97. Many ML activities are associated with different kinds of deception e.g. email fraud, boiler-room fraud, and telephone deception.
98. In some cases of this nature the account holders appeared to be innocent, as they had no idea about the deposits and were willing to refund the payment to the victims. Such claims were well supported by the transaction history of the bank accounts.
99. The above findings suggested that some money launderers might use their genuine business partners/counter-parties' bank accounts to receive crime proceeds. In some other cases, money service operators would be misused in the layering processes of the money laundering activities.

INDIA

100. Hawala has generally been found associated with TBML, smuggling, TF and channelling funds abroad.

INDONESIA

Corruption

Purchase of insurance policy premiums, followed by an early withdrawal (early termination)

101. State Parliament Treasurer was reported to transfer money to an insurance company for payment of the life insurance premiums for 17 city councillors at the end of the year and then again in January at the beginning of year. At the end of January all insurance premiums were transferred into a personal account of each member of the Council and on the same day the funds were withdrawn in cash through ATMs.

Depositing cash

102. There are many cases involving an indication of bribery involving members of Parliament who made deposits and cash withdrawals on a reported account and then transferred the funds to the accounts of other parties who were identified as officers of political parties.

103. Most of the funds were then transferred again to a family account to open private deposits. The cash transactions generally did not have the underlying transaction information, so that the relationship and the purpose of the transaction were not clear.

Placement in and Purchase of Investment in Life Insurance Policies and Mutual Funds

104. A 'Person' works as a civil servant and has 21 life insurance policies that are spread across multiple insurance companies, with insurance reported for himself and his wife and children. A Person also conducts some investment in the securities of companies in the form of several units of the mutual funds.

105. Patterns of transactions carried out for the placement of funds in some sectors of investment is one indicator of money laundering.

Narcotics Trafficking Crime

106. Illegal transaction of remittances from abroad into Indonesia using money remittance or hawala transactions that generally utilize remittances from Indonesian Workers (TKI) in countries with migrant workers.

107. Delivery and confirmation was done through an electronic communication from the agent to the hawala agent overseas in Indonesia and was followed by the physical transfer of funds. So the funds that come to the migrant workers' family are probably derived from narcotics trafficking, while funds belonging to migrant workers abroad are directly used by the narcotics business network abroad.

Terrorism Financing Crime

108. Some people were convicted of using funds obtained by hacking an internet site for financing terrorism, after previously carrying out money laundering by sending money to some other parties and purchasing valuable items.

JAPAN

109. Fraud is the most common predicate offence. Loan-sharking, theft, child pornography and prostitution are also evident.

NEW ZEALAND

110. In relation to ML, drug offences continue to present as the most common predicate offence for ML.
111. Of note is the increase of interest by Inland Revenue (tax revenue) in pursuing ML convictions in relation to tax evasion. Whilst small in number at present, this will become an area of increased attention and resourcing in the future.
112. New Zealand has never had a TF related prosecution.

SAMOA

113. Confiscations during Police raids have demonstrated that the use of illegal drugs, mainly marijuana, continues to be of great concern. There have also been a few cases which involved hard drugs such as cocaine and methamphetamine.
114. In this connection, the SFIU's assistance is always sought to obtain relevant financial information on the individuals that have been charged, from banks and other financial institutions, for evidence during prosecution procedures in Court. In the meantime, financial institutions are instructed to undertake enhanced due diligence and ongoing monitoring of the bank accounts of those arrested.

SOUTH KOREA

115. The main pattern of money laundering in Korea is mostly observed in the private sectors such as finance, banking, trade and construction.
116. Cash transaction is the most common method of money laundering and money laundering has tended to become more sophisticated over the years with internationalization and development of communication technology.
117. Embezzlement, tax evasion and smuggling are the most common predicate offences associated with money laundering. Terrorist financing cases have not been reported in Korea.

TONGA

118. Drugs and fraud are the predominant predicate offences.

3.3 Emerging Trends; Declining Trends; Continuing Trends

AUSTRALIA

Established typologies and potential vulnerabilities

119. The *Typologies and case studies report 2012* provides details about established typologies. The report examines two typologies used to enable and commit transactional crimes and tax evasion which are currently of particular interest to law enforcement, namely:

- the use of cheques to evade tax; and
- the use of third-party cash couriers to undertake money laundering.

120. The report also examines a number of channels vulnerable to money laundering and terrorism financing, including:

- digital currencies and virtual worlds;
- voucher payment systems; and
- offshore online money remitters.

121. Although limited evidence exists to date of criminal misuse of these channels in Australia, overseas cases illustrate some of the ways in which they can be exploited.

BRUNEI DARUSSALAM

122. Continuing trends indicated by STRs received include the structuring of funds, involving high volumes of small transactions and numerous accounts.

CANADA

123. Based on a review of cases disclosed by Canada's FIU (FINTRAC), the methods or techniques used to launder money in Canada have remained relatively consistent over the past four years.

124. The following, presented in no order of importance, are the main methods or techniques used to carry out money laundering in Canada:

Use of International EFTs

125. In Canada, EFTs are used after the money generated from criminal activities is placed in the financial system, or when terrorist financiers send or receive funds related to terrorism.

126. Individuals often use EFTs to complicate the money trail or to conceal the funding of terrorism. They may send or receive EFTs in Canada or in foreign countries, offshore locations, and tax haven countries with weaker anti-money laundering laws. Domestic EFTs are also used to move illicit proceeds between various bank accounts in Canada.

127. Individuals involved in the drug trade normally introduce their illicit funds into the financial system through various methods, including large cash deposits into business accounts, which are often followed by purchases of EFTs. In many

fraud cases, illicit funds are already in the financial system and are moved to foreign bank accounts, either in a bank secrecy country or offshore location.

128. Based on an analysis conducted by Canada's FIU from 2007 to 2011, fraud-related cases involved four times the number of EFTs than drug-related cases, which suggests that the use of EFTs is a common method employed in fraud schemes.
129. According to the same analysis, many of the jurisdictions where international EFTs in case disclosures were most commonly sent or received had the following characteristics:
- Many sending or receiving jurisdictions had previously or currently been declared deficient in their AML/AFT regimes by the FATF.
 - Many were known as offshore financial centres and had strong bank secrecy laws.
 - Some were known for their drug supply and smuggling routes.
 - Others were popular financial or transshipment hubs in Europe, Asia, and the Middle East. Countries with strong trade and financial ties with Canada, notably the USA and the UK, were also prevalent.

Use of Money Service Bureaus and Currency Exchange Businesses

130. MSBs and currency exchange businesses continue to play a role in money laundering activities in relation to all predicate offences. Of note, drug traffickers are particularly frequent users of these institutions, in order to conduct US and Canadian dollar cash conversions to assist in illicit cross-border activities.
131. Cash purchases of EFTs are also a common technique used by individuals laundering illicit funds through MSBs and currency exchange businesses.

Use of Casinos

132. Individuals use casinos to launder money in Canada and they employ various techniques to do so, including converting smaller denominations of currency to larger ones (known as 'refining'), exchanging currencies and purchasing casino chips. One commonly used technique is for money launderers to purchase casino chips with cash, conduct minimal play, and then redeem the chips for either cash or cheque.

Use of Businesses

133. Businesses that handle a high volume of cash transactions are attractive to launderers of drug proceeds and often include convenience stores, gas stations, bars, restaurants and food-related wholesalers and retailers. These businesses allow for the commingling of illegitimate and legitimate cash funds. In cases of investment fraud, front companies are registered in foreign jurisdictions and the proceeds of fraud are sent to the foreign accounts of these companies.
134. Based on an analysis conducted by Canada's FIU from 2007 to 2011, 68% of drug-related cases consistently involved at least one business. Examples of

businesses and sectors observed in drug-related cases were MSBs, construction, shipping or freight, import or export, travel, real estate, electronics, pharmaceuticals, convenience or grocery stores, food and entertainment, automobiles, hydroponics/indoor gardening, trucking and gas stations.

135. According to the analysis, fraud cases involved corporate entities more often than in other types of cases, particularly when the fraud involved purported securities. For example, it has been observed that businesses can act as conduits to receive investments from victims that can then be easily transferred to accounts held in offshore banking centres. Other types of fraud, such as debit/credit card fraud, can utilize the services of collusive merchants to perpetrate the fraud.
136. From 2007 to 2011, 84% of fraud-related cases involved at least one business. Examples of businesses and sectors observed in fraud-related cases are holding companies, financial services companies, investment or securities companies, real estate development, consulting firms, energy sector, precious metals, life insurance, technology (e.g. aviation, computers, etc.), medical supplies, food and entertainment and the auto industry.

Bulk Cash Smuggling

137. This is a prominent method used by criminal organizations to move the proceeds of crime from Canada to foreign destinations, particularly the US, Mexico, and Colombia. Canadian authorities have recently seen a large increase in seizures and investigations resulting from bulk cash smuggling.
138. It should also be noted that there has been an increase in trade-based and real estate-related money laundering schemes in recent years in Canada.

Emerging trend

139. The new payment methods that have been adopted in recent years (e.g., prepaid cards, internet payment methods) and the innovations that are being further developed and adopted in this space (e.g., mobile banking) are a particular focus.
140. Evidence suggests, however, that money laundering carried out using new payment methods, such as prepaid cards and internet payments systems, is still small in Canada. For example, Canada's FIU reports that, during the last three years, only 2-5 per cent of cases disclosed to law enforcement and other agencies involved these payment methods.
141. It is suspected that one or more terrorist groups in Canada are using an international trade-based money laundering scheme to send funds overseas in support of terrorist groups.

FIJI

Emerging trend

Laundering proceeds from corruption

142. The number of corruption related cases reported to Fiji FIU has increased over the years. Fiji FIU has received STRs involving high level government officials as a result of financial institutions monitoring accounts of customers.

Declining trend

Use of false identification

143. Fiji FIU has noted a decrease in the number of cases involving fake identification cards such as passports, birth certificates.

Continuing trend

Use of nominees, trusts, family members or third parties

144. Between January and August 2012, the Fiji FIU received a total of 15 STRs involving unauthorised transfers from internet banking accounts. These accounts were suspected to be accessed through phishing. Third parties were contacted through online job advertisements to remit money received through these unauthorised transfers to overseas beneficiaries.

HONG KONG, CHINA

145. A rising trend was noted for email scam activities in which the culprit(s) compromised email accounts of goods supplier/buyers. They then disguised themselves as suppliers to send fraudulent emails to request buyers to deposit payments into a designated bank account opened in Hong Kong. On failing to receive goods, the victimized buyers then contacted the genuine suppliers and discovered the scams.

INDIA

146. With financial transactions coming under enhanced monitoring, hawala is being looked as a safe mode of transfer of money by criminal syndicates. Thus hawala is emerging as a big challenge.

INDONESIA

147. Based on data on Suspicious Transactions received by Indonesian FIU for the year 2012, as well as research and analysis of the STRs that have been submitted by the FIU to law enforcement officers during the same period, it is known that the predicate offenses can be divided into several different categories according to the trends.

Increasing trend

148. AML cases involving narcotics offenses and taxation, respectively, increased by 53.5 per cent and 16.6 per cent, compared with 2011.

Continuing trend

149. Corruption remains the first-ranked offence, based on the analysis by the FIU. The analysis indicated 57.6 per cent of STRs are corruption-related and this is expected to remain high.

150. The *modus operandi* of corruption is financial transactions using cash deposits made by PEPs or State Officials and involving families and other third parties. An additional continuing trend discovered by FIU is cuckoo smurfing. Criminals use money remitters for laundering the proceeds of crime from psychotropic substances.

Declining trend

151. There is some indication of some criminal acts that showed a downward trend during the period 2011 to 2012. One of the crimes is the criminal act of bribery and embezzlement.

MACAO, CHINA

152. Throughout the period from January to June 2012, a total of 982 STRs had been received by the Macao FIU, with 691 STRs coming from the gaming sector and 289 STRs from the financial sector (including banking, insurance and financial intermediaries) respectively, while other sectors such as real estate submitted two STRs during this same period.

153. The commonest money laundering methods detected from the STRs received are as follows:

- Unable to provide ID / important personal information.
- Possible match with International Watch-list or other black list.
- Chips conversion without gambling activities.
- Currency exchanges / cash conversion.
- Suspicious wire transfers.
- Significant cash deposit with non-verifiable source of funds.
- Use of cheques / promissory notes / account transfer etc. to transfer funds.
- Irregular large cash withdrawals.
- Suspected illegal financial business.
- Gambling activities (casinos, horse racing, internet gambling etc.).

154. From January to June 2012, 115 STRs were disseminated to the Public Prosecutions Office and were consolidated into nine cases filed for investigation. The cases under investigation were mainly related to fraud, corruption and the use of false documents.

Emerging trend

155. Based on the statistics of cases under investigation, there is an emerging trend in the use of new payment methods as means of moving funds across borders and this increases the ML/TF threat of using such systems for illegal purposes. Some of the suspicious cases found are related to overseas PEPs or members of organised crime. The new payment methods commonly used include internet banking, credit/debit cards, ATM, etc.

MALAYSIA

Emerging trends based on STRs

Reports on internet/wire transfer scams are increasing, involving cross border transfer of funds:

- a) Foreigners or individuals associated to foreigners opening accounts in different/multiple banks.
- b) Multiple inward remittances received from various entities in different countries.
- c) Funds received were withdrawn in cash and via ATM at various locations immediately upon receipts leaving low balances.
- d) Transactions made were not consistent with individual's profile.

Continuing trends based on STRs

Large and rapid movement of funds (transit accounts)

- a) Large values of cheques and cash deposited into bank account followed by immediate cash withdrawals.
- b) Funds transferred in and out of an account on the same day, or within a relatively short period of time.
- c) Camouflaging movement of funds to third parties with cash withdrawals.

Unjustified banking transactions

- a) Deposits are not justified, considering the nature of business or profession.
- b) Deposits were inconsistent with the volume generated by the business.
- c) No economic rationale and / or bona fide purposes.
- d) Deposits were structured below the reporting requirement to avoid detection.
- e) Deposits at various branches and times for no logical reasons.
- f) Substantial inter-account transfer between related accounts.
- g) Multiple cash deposits into an account followed by a large transfer to other third parties account/countries.

NEPAL

156. The following are the identified, or suspected, trends and types of ML in Nepal:

- False identification
- Misuse of ATM card for the purpose of receiving Indian currency
- False source of income
- Under or over invoicing
- Real estate including a lesser amount mentioned in the land deed than the market price

- Tax/revenue evasion
- Trade based ML
- Extortion
- Illegal telephone service Voice over Internet Protocol (VoIP)
- Fund siphoning
- Currency exchange and smuggling
- Use of hundi
- Structuring, use of complex structure of companies
- Use of family members/relatives or friends, corruption

Emerging trends

- Currency exchange from Nepal to India without licence
- TBML
- Banking frauds
- Corruption
- Extortion
- Real estate
- Tax evasion

Declining trends

- Revenue
- Extortion
- Indian currency exchange.

NEW ZEALAND

157. The existing banking and financial environment remains the main conduit for ML, in line with jurisdictions all over the world.
158. The use of shell companies has been a particular issue for New Zealand over the last 1-2 years and remains an area of concern. However, efforts are underway to strengthen legislation and tighten processes and procedures around the formation of shell companies to ensure criminal abuse of New Zealand companies is greatly reduced.

SAMOA

159. With the increasing use and introduction of IT products and services such as, phone and mobile banking, scam activities continue to pose a high risk and vulnerability to the general public and bank customers who are being misled to believing of getting large money value rewards for no clear or apparent reasons or proof that they actually engaged in genuine transactions.

SOUTH KOREA

160. Unlike many other countries where drugs, terrorism, organized crime and human trafficking pose serious threats to the AML/CFT system, South Korea finds

economic crimes such as tax evasion and embezzlement more challenging issues. Utilizing tax havens and paper companies to evade tax and illegally move assets overseas has become a social issue lately in South Korea. The money laundering threat is not such a great in general in South Korea, however, there is a potential threat arising from economic crimes.

SRI LANKA

Emerging and Continuing Trends

- Remitting money out of Sri Lanka purported to be payment for imports, where no actual imports had taken place
- Use of accounts to collect funds from human smuggling and trafficking.
- Use of accounts to collect proceeds of the drug trade
- Frauds relating to internet and e-banking
- Use of accounts for third party deposits where depositors were requested to deposit money into an account as job application registration fees, investment schemes or lottery contributions. Such deposits were then immediately withdrawn through ATMs

Declining Trends

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

THAILAND

161. Current trends involve the use of electronic money, such debit cards or e-payment transactions, arising from the wide use of the internet for mobile electronic payment instruments.

TONGA

162. Tonga reported drugs and fraud as continuing trends.

USA

New Trends

163. The use of money mules – intermediaries who provide legitimate identifying information to open bank accounts and who then send and receive funds but have no role in the underlying predicate crime – is widespread.

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

164. Australia has recently adopted stronger enforcement measures in recognition of the threat posed by some alternative remittance services. Under section 229 of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act), the Chief Executive Officer of the Australian Transaction Reports and Analysis Centre (AUSTRAC) may make written Anti-Money Laundering and Counter-Terrorism financing rules. The rules are binding legislative instruments. The recently registered rule 44 permits the AUSTRAC Chief Executive Officer to de-register high-risk money remitters.
165. The Australian regulatory framework in relation to money laundering has multiple hierarchical legislative layers. The first layer is specific anti-money laundering legislation, with secondary layers of taxation, banking, superannuation and corporation laws. The Australian anti-money laundering regulatory regime has been developed in conjunction with international regulatory schemes implemented under international instruments for combating transnational crime and organised criminal groups.
166. To strengthen existing arrangements, amendments were recently made to the *Proceeds of Crime Act 2002 (Cwlth)* to target criminal business structures, including the financial and material assets of criminal entities — recognising that such measures are crucial to disrupting organised crime. The amendments introduce a range of measures (principally ‘unexplained wealth’ provisions) to extend and enhance the Commonwealth asset confiscation regime. These measures are intended to increase the capacity of the Commonwealth to successfully respond to organised crime by targeting wealth derived from criminal activity.
167. Organised crime will consistently seek to exploit areas that receive less regulatory attention. Collectively, domestic groups and individuals who launder the proceeds of crime demonstrate a significant capability to change and adapt in response to increasing regulatory controls. While they vary in sophistication, they are able to purchase specialist advice, exploit corporate structures and conceal this activity within a myriad of legitimate financial transactions.
168. The strong regulatory controls for mainstream financial institutions may displace criminal attention towards products and services considered to attract less regulatory focus. Accordingly, less regulated parts of the Australian financial sector, and offshore jurisdictions with high levels of organised crime and limited national anti-money laundering controls, are areas of ongoing vulnerability for Australia.

BRUNEI DARUSSALAM

169. A recent legislative development is the enactment of the Criminal Asset Recovery Order, 2012 (“CARO”) on 16 June 2012. A comprehensive piece of legislation

which replaces and repeals overlapping provisions contained in the Anti-Money Laundering Act Chapter 209, the Drug-Trafficking (Recovery of Proceeds) Act Chapter 178 and the Criminal Conduct (Recovery of Proceeds) Order. Procedural complexities contained in the previous laws are now removed and provisions are clarified to increase transparency and enable relevant authorities in Brunei Darussalam to successfully take action against those who intend to make illicit use of the financial system.

170. Key provisions in CARO include the definition of “serious offence” which now means any offence for which the penalty is death, imprisonment for a term of not less than six months or a fine of not less than B\$1,000 (section 2); the criminalisation of money laundering (section 3); the obligations of financial institutions and designated-non-financial businesses and professions (DNFBPs) to perform customer due diligence requirements (sections 4 – 14); the power of the FIU to act as the central agency for the receipt, analysis and dissemination of STRs (section 15); and the reporting of physical currency and bearer negotiable instruments (CBNI) which exceed B\$15,000 (sections 35 – 47).
171. CARO also enables relevant law enforcement agencies to recover assets through: restraining orders (sections 49 – 59); confiscation and benefit recovery orders (sections 60 – 82); non-conviction based forfeiture order & forfeiture of property without prosecution (sections 83 – 84); and unexplained wealth declarations (sections 85 – 90).
172. In terms of mutual legal assistance, Part V (Foreign Orders) of CARO now contains provisions, amongst others, for the registration of foreign restraining confiscation and benefit recovery orders, allowing foreign countries to request assistance in the location of proceeds of crime in Brunei, and allowing for the entering into of Asset Sharing Agreements.
173. The first CARO case was brought to court in September 2012 when a foreigner was charged for bringing in close to half a million dollars into Brunei Darussalam without filing a declaration. The court’s decision is still pending.
174. Using its powers under section 137 (Directions to prevent money laundering) of CARO, FIU issued a direction to banks to report the issuance of B\$10,000 notes to FIU on a monthly basis as a mechanism for the monitoring of high denomination notes.
175. Another legislative development was the issuance of the Anti-Terrorism (Terrorist Financing) Regulations, 2012, which received royal assent on 8 December 2012. The Regulations requires every person in Brunei to freeze without delay funds or other assets of terrorists, those who finance terrorism and terrorist organisations in accordance with relevant United Nations resolutions. It also allows the Minister responsible for internal security matters to designate persons for the purpose of freezing the designated person’s assets, either at the Minister’s own motion, or at the request of a foreign jurisdiction.

FIJI

176. A sub-committee of the National AML Council, the AML Legal Working Group, was developing guidelines on the disposal of proceeds of crime after asset

forfeiture. The guidelines have been approved by government and are being implemented.

INDIA

177. The Indian Law which deals with Money Laundering (The Prevention of Money Laundering 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.
178. Other major changes included delegation of powers of search, seizure and survey; increase the number of Investigating Officers under the Prevention of Money Laundering Act; modifications of certain legal provisions to bring clarity and to make them unambiguous.
179. All these legislative changes have resulted in a sharp increase in the number of cases booked, value of assets attached (frozen), number of arrests made and number of prosecution filed, since 2009.
180. The regulators too have issued directions to the stakeholders of the respective sector to report transactions which are suspected from AML/TF perspective. This too has also started yielding results.
181. Further necessary amendments are being processed in line with FATF recommendations.

MACAO, CHINA

182. The project for revising the AML/CFT Law and Regulation is now at the stage of consultation. Comments will be collected from all the reporting entities and relevant business associations. The private sector consultation period will finish by the end of 2012 and will be followed by a review of the final drafts within the first half of 2013, before passage through the legislation process. After the draft is finalized, the next step will be to revise the guidelines of the different supervisory agencies to cope with the proposed revisions in the law and administrative regulations.
183. Regarding the implementation of necessary sanction measures under UNSCR 1267 and 1373, the Law Reform and International Law Bureau (DSRJDI) is under the process of drafting appropriate legislation to establish a freezing mechanism and effectively enforce freezing orders from United Nations Security Council Resolutions.

MALAYSIA

Legislative and Regulatory Framework Developments

184. The Money Services Business Act (MSBA) was enforced on 1 December 2011 to further strengthen the safeguard of money services business industry (comprising remittance, money changing and wholesale currencies business) against abuses of illegal purpose.

185. Twenty six offences from various pieces of legislation have been included in year 2012 as predicate offences under the Second Schedule of the Anti-Money Laundering and Anti-Terrorism Financing Act (AMLATFA). These bring the total of predicate offences to 286 from 42 Legislations.

Law Enforcement Developments

186. The Royal Malaysian Customs Department (RMCD) has introduced the Customs Declaration Online System (CADS) in 2011 for generating statistics on the declaration of cash and bearer negotiable instrument at the border.

Policy / Coordination Developments

187. The National Coordination Committee to Counter Money Laundering (NCC) is enhancing its roles as a decision making and coordinating body for the national AML/CFT regime by structuring the meeting into two levels of meeting:

- a) High Level NCC Meeting that will focus on the formulation of policy and strategic direction for Malaysia's AML/CFT regime; and
- b) NCC Working Group Meeting that will focus on the operational issues pertaining to the implementation and effectiveness of initiatives approved by the NCC.

188. The enhancement is aimed at providing more effective mechanisms to expedite policy approval processes and to monitor implementation of AML/CFT measures.

NEW ZEALAND

AML/CFT Countermeasures - Financial Crime Group

189. The Financial Crime Group (FCG) was established on 1 December 2009 and is made up of four Asset Recovery Units (ARU) located in Auckland, Hamilton, Wellington and Christchurch, a core administrative/analytical team at police national headquarters and the FIU.

190. The purpose of the FIU is to provide financial intelligence and investigative support to its stakeholders, including Police, and to assist the NZ Government to fulfil its obligations to the FATF and the UN. The FIU collects, collates and analyses information provided by external parties (foremost banks and other financial institutions) and develops financial and intelligence profiles to initiate and assist investigations.

191. One of the core FIU functions is to receive, collate, analyse and disseminate information contained in Suspicious Transaction Reports (STRs) which financial institutions are required to report by law. Approximately 5,000 are received annually.

192. Key points:

- Decision-makers must have a clear understanding of the criminal environment so they can allocate resources to address the identified issues. It is the role of intelligence to provide this clear understanding.

- The targeting of offenders and crime problems through the use of financial intelligence is a significant step toward realising intelligence led policing.
- The financial targeting model has resulted in the identification of a number high profile targets and assisted in the execution of numerous successful arrests, prosecutions and asset seizures.
- In relation to asset seizure this represents a real success story for the FCG and NZ Police. Both the restrained and forfeited figures represent substantial sums that are no longer available to fund future crime. Such actions also damage the prestige gained from criminal offending, reducing the status of such 'role models' in the criminal community and highlighting that crime will not be allowed to pay.
- The FIU and the ARUs contribute significantly to the New Zealand All of Government Response to Organised Crime (AGROC) financial targeting model; making it more likely that offenders are identified and caught and their proceeds of crime seized more effectively.

Asset Seizure

193. The Criminal Proceeds (Recovery) Act 2009 (CPRA) came into effect on 01 December 2009 replacing the Proceeds of Crime Act 1991. The earlier legislation depended on a criminal conviction before asset recovery could take place but, with the advent of the CPRA, asset recovery actions can now be taken in New Zealand under a civil regime. This means that a criminal conviction is no longer required and the assets and profits of crime can be forfeited using the civil standard of proof i.e. on balance of probabilities.
194. ARU cases are investigated using complex forensic accountancy and financial analysis processes, which are undertaken as part of a whole-of-government approach that includes other agencies such as Customs, the Serious Fraud Office, and the Inland Revenue. The ARUs also collaborate with overseas law enforcement agencies and provide advice on matters relating to proceeds of crime policy and legislation.
195. The goal of the CPRA is to deter and disrupt crime by removing the financial base of offending and by making crime less profitable and attractive and is administered by the four ARUs. Despite the fact that criminal convictions are no longer required, the ARUs take action in both the criminal and civil arenas.
- 'Criminal' actions are taken against assets that are found to be the 'instruments of crime' e.g. a residential property used to manufacture methamphetamines.
 - 'Civil' actions are taken against assets that are acquired or derived from criminal offending e.g. a car bought with the proceeds of drug dealing.
196. Cases are becoming increasingly complex and frequently part of nationwide operations. 83% of the 398 ARU cases are linked to drug offending, with 39% of these specifically linked to methamphetamines.
197. Significant results have been achieved in the three years of the CPRA's operation.
- ARUs¹⁹ have investigated 482 cases.²⁰

¹⁹ These cases are referred from both Police Districts and from agencies external to Police, such as the Organised and Financial Crime Agency of New Zealand (OFCANZ), Interpol, Inland Revenue, and the Ministry of Social

- 50% increase in case loads in the past 12 months.
- 1278 assets worth an estimated \$208 million have been investigated so far.
- Cash and bank accounts worth \$36.4 million, cars/vans/4-wheel drives worth an estimated \$10.9 million (involving 262 vehicles), and 192 residential properties worth an estimated \$77.4 million are the dominant asset types.
- NZ Police currently hold Restraining Orders over assets worth an estimated \$106 million pending further enquiries and court action.
- By the end of September 2012 an estimated \$18.5 million worth of assets had been made subject to Forfeiture Orders.²¹

Proactive Financial Offender Targeting process (PFOTP)

198. The FIU and National Intelligence Centre (NIC) have collectively designed and implemented a targeting model to prioritise, assess and target individuals suspected of generating and laundering proceeds of crime. This is called the Proactive Financial Offender Targeting Process (PFOTP) and essentially combines information contained in STRs with intelligence held in NZ Police and other databases in order to estimate the level of criminality associated with the transaction(s).
199. The current process in its simplest form can be considered to consist of three strands; a Prioritisation Strand, Assessment Strand and a Targeting Strand.
200. Once targets have been identified initial profiles are completed. These are assessed by NIC and FIU management to decide on suitable targets for full and in-depth
201. This measure is achieved by using a matrix that evaluates the information known by NZ Police about the persons involved in the transaction against the nature of transaction itself and the grounds for suspicion as perceived by the financial institution. A weighting score out of 100 is then determined. The higher the score, the higher the priority is given to the STR for analysis. Every STR received by the FIU is evaluated in this way.
202. Analysis in anticipation of further investigation - a process of de-confliction²² is also undertaken as part of the tasking and coordination process.
203. This process demonstrates the importance of both intelligence units adopting a synchronised and de-conflicted approach to identifying criminal targets through financial and other intelligence. The process helps identify clear delineation of responsibilities to encourage the efficient use of intelligence and avoid duplication of work.
204. The importance of financial intelligence in identifying criminal targets is such that two (at times three) FIU analysts are permanently embedded within the NIC targeting group. This structure works well as information can be shared

Development. This is because the Commissioner of Police has the mandate to commence actions on behalf of all government law enforcement agencies.

²⁰ All dates correct as at 30th September 2012.

²¹ Deductions are necessarily made from this total, such as payments made to mortgagees and legal Aid and the costs of managing assets while on restraint.

²² Information is shared between agencies and investigative units to ensure that they are not targeting the same persons of interest and to avoid 'blue-on-blue' situations.

efficiently between both units bringing a cohesive approach their intelligence products.

Case Studies

Taskforce DARED - value of STRs

205. Taskforce DARED commenced in October 2011 to actively generate investigative leads from STRs submitted to the FIU. A number of cases have been investigated resulting in internal and external agency referrals for further investigation. One such case was Mr X who after initial investigation by Taskforce DARED was forwarded to Auckland District to complete the arrest process. He was recently arrested and charged with a number of drug related offences, money laundering and firearms offending. A number of assets and money have been restrained. Of note was that Mr X was largely unknown and was only identified from the STR reports, demonstrating the value of financial targeting.

Operation ARK - asset seizure success

206. Operation ARK involved the arrest of 19 people following a year-long investigation into the manufacture and supply of ecstasy across New Zealand. The syndicate, which was being co-ordinated by a number of individuals in the Auckland region, is thought to have been responsible for the bulk of the ecstasy supply in New Zealand and the arrest of its members represented a significant success for Police in reducing the amount of ecstasy on the streets.

207. On the back of Operation ARK, the ARUs obtained restraining orders over 161 assets thought to be worth an estimated NZ\$21 million²³. Enquiries on on-going in this case with additional assets being discovered and added to the list of those restrained. Forfeiture proceedings will take place in due course.

NEPAL

- Financial Institutions are implementing AML/CFT measures, so customers are facing due diligence and becoming more conscious in not getting involved in illegal activities, which is at the same time triggering STRs.
- Supervisors are implementing AML/CFT supervisory tools in directing and inspecting RIs so as to ensure that proper and effective mechanism in place.
- FIU is improving its analytical capacity. Many directives and 12 supervisory manuals have been developed and implemented.
- Department of ML Investigation and other LEAs are working in a coordinative manner to investigate and prosecute offences. Joint investigation has stated.
- Government. DMLI, Regulators, FIU and RIs themselves are conducting sensitizing programs to their stakeholders by interactions, trainings and publications as well through various types of media.

²³ These assets include 20 residential properties, 25 cars, 103 cash sums/bank accounts, 5 motorcycles, and 3 boats.

SOUTH KOREA

208. The South Korean government amended article 17 of the Financial Transaction Report Act in March 2012, in order to set up a new provision to impose sanctions against financial institutions and employees of the financial institutions that violate the customer due diligence obligation.

209. The Act came into force on March 22, 2013. The Act heightens the awareness of financial institutions and their employees of the reporting duties by clearly stipulating obligations and sanctions related to customer due diligence. The amended Act contributes in lowering money laundering risk in South Korea.

THE PHILIPPINES

210. The two major developments in the Philippine AML/CFT Regime are as follows:

Amendments to Republic Act No. 9160 (Anti-Money Laundering Act of 2001, AMLA)

211. Section 11 of AMLA, as amended (amended by Republic Act No.10167 which was enacted on 18 June 2012), now allows *ex parte* bank inquiry. The application for bank inquiry is now filed with the Court of Appeals, which must act on the application within 24 hours from the filing thereof. This is a welcome development in the investigation of money laundering.

Enactment of Republic Act No. 10168 (“An Act Defining the Crime of Financing of Terrorism, Providing Penalties Therefore and for Other Purposes”)

212. The two important key features of the Republic Act No. 10168 are as follows:

- a) Authority of the Anti-Money Laundering Council (AMLC) to inquire into or examine deposits and investments with any banking institution or non-bank financial institution and their subsidiaries and affiliates without court order in relation to any property or funds that are in any way related to financing of terrorism or acts of terrorism or to any property or funds of any person or persons in relation to whom there is probable cause to believe that such person or persons are committing or attempting or conspiring to commit, or participating in or facilitating the financing of terrorism or acts of terrorism.
- b) Authority of the AMLC to issue freeze order against property or funds related to financing of terrorism or acts²⁴ of terrorism. The AMLC, either upon its own initiative or at the request of the Anti-Terrorism Council is authorized to issue an *ex parte* order to freeze without delay:
 - i) property or funds that are in any way related to financing of terrorism or acts of terrorism; or
 - ii) property or funds of any person, group of persons, terrorist organization, or association, in relation to whom there is probable cause to believe that they are committing or attempting or

²⁴ Based on Art.8 STF Convention (Identification, detection and freezing of terrorist-related funds for purposes of possible forfeiture), UNSCR 1267 (for UN designated person/s), and UNSCR 1373 (domestically designated person/s). Freeze *without delay* is based on UNSCR 1267 and 1373.

conspiring to commit, or participating in or facilitating the commission of financing of terrorism or acts of terrorism.

SRI LANKA

213. The Parliament approved amendment Acts on Prevention of Money Laundering Act No. 5 of 2006 (PMLA) and Convention on the Suppression of Terrorist Financing Act No. 25 of 2005 (CSTFA) on 21st September 2011. Two amended Acts, Prevention of Money Laundering (Amendment) Act No. 40 of 2011 and Convention on the Suppression of Terrorist Financing (Amendment) Act No. 41 of 2011 were effective from 6th October 2011.
214. The main objective of these amended Acts is to incorporate the recommendations made by the APG in 2006 Mutual Evaluation/identified by the ICRG Process.
215. Convention on the Suppression of Terrorist Financing Act (CSTFA) No. 25 of 2005 was amended to expand the applicability of terrorist financing law to include:
- citizens of Sri Lanka and non-citizens while present in Sri Lanka;
 - expanding the definition of “Funds” to includes assets of every kind be it tangible or intangible, movable or immovable” which are kept in Sri Lanka or outside Sri Lanka;
 - expanding the terrorist financing offence to include acts committed by terrorist group single terrorist; and
 - expanding the powers given for Police to freeze/suspend terrorist funds and properties relating to the terrorist financing or activities before indictment.
216. Prevention of Money Laundering Act (PMLA) No. 5 of 2006 was amended to include:
- expanding the applicability of law to cover persons who commit money laundering offence while in Sri Lanka;
 - recovery of corresponding value of the properties related to a money laundering offence in the absence of properties derived/realized through money laundering,
 - reduction of 7 year threshold to 5 years covering more offences punishable under money laundering offence and
 - inclusion of foreign predicate offence as unlawful activity.
217. Sri Lanka promulgated regulations to implement UNSCR 1373 & 1267 on 15th May 2012 and 31st May 2012 respectively.

4. CASE STUDIES OF ML AND TF

4.1 Association with corruption (corruption facilitating ML or TF)

CHINESE TAIPEI

218. Mr A was the owner of Company W. Mr B was the nominal owner of Company X which was controlled by Mr A. Mr C, a friend of Mr A's, was the owner of Company Y. Mr D was the division chief of the information management division of state owned Hospital Z. Mr E was a computer engineer under the direction of Mr D.
219. Mr D and Mr E were responsible for the procurement of Hospital Z's medical computerized system and maintenance contract from 2007 to 2010. Mr D demanded Mr A, who intended to win the bidding, to pay bribes for giving favour in the procurements, and abetted Mr E to set up some unnecessary qualification requirements to drive out other potential competitors.
220. Mr A used Company A as a tender, and borrowed the names of Mr B's Company X and Mr C's Company Y to participate in the bidding. In this way, Company A usually won the bids. After winning the bids each time, Mr A would pay Mr D by cash or remit the bribe to the designated bank accounts of Mr F (one of Mr A's friends) or Company G and then withdrew cash or issued bearer cheques to Mr D.
221. During the abovementioned period, Mr D accepted bribes worth more than NTD 6 million (about USD200,000) in total. This anti-corruption case was successfully investigated by the Taipei Field Division of the Investigation Bureau and the abovementioned suspects were charged with violation of Government Procurement Act, bribery, corruption and money laundering by the prosecutor of the Shi-Lin District Prosecutors Office in September 2011.

INDIA

222. Twenty seven (27) investigations associated with corruption and involving INR 4032 million (USD80.6 million) worth of assets are under investigation.
223. A case under investigation involved corruption facilitating terrorist funding. The terrorists were controlling the authority in a statutory body for area development and were siphoning off funds given for development, for creating personal assets as well as for terror-related operations. Some of these funds were diverted to two other jurisdictions and have since been frozen.

PAPUA NEW GUINEA

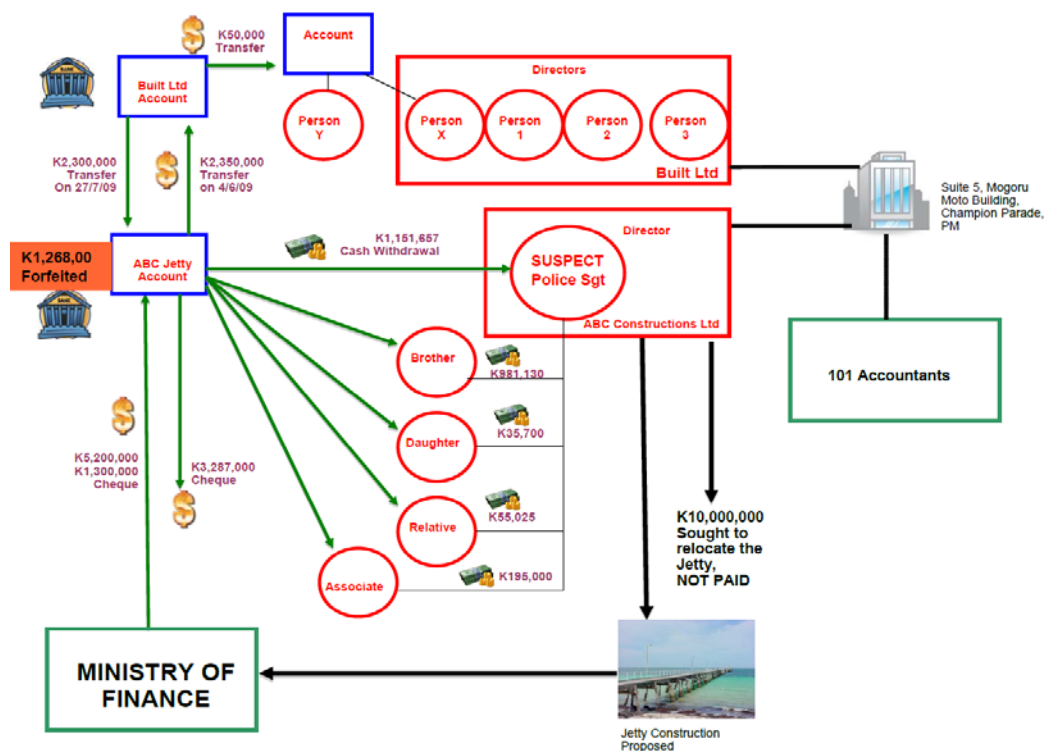
224. The suspect was employed by the Department of Police as a Chief Sergeant. The suspect was the sole Director and shareholder of a company, ABC Constructions Ltd ("ABC"). ABC was incorporated in Papua New Guinea on 30 September

2004. ABC's registered office was listed as Suite 5, Mogoru Moto building, Champion Parade, Port Moresby. However, this office was occupied by a business named 101 Accountants. ABC did not lodge any documents with the Investment Promotion Authority and the company was deregistered on 31 March 2005.

225. On 13 March 2009 a contract was awarded to ABC to build a jetty for a province. Proper tender processes were by-passed in awarding the contract to ABC.
226. On 28 April 2009 the suspect opened a bank account under the name of "ABC Jetty Account". The suspect was the sole signatory to that account. On 28 April 2009 a cheque in the sum of K5,200,000 (USD2,418,604) was deposited into the ABC Jetty account. On 10 December 2009 a further cheque in the sum of K1,300,000 (USD604,650) was deposited into the ABC Jetty Account. In each case, the cheque was drawn by Department of Finance from the Transport Sector Ports & Jetty Subsidy.
227. On 3 October 2008 another company named Built Ltd ("Built") was incorporated in Papua New Guinea. X and three others were Directors of Built. The address listed as the registered office of Built was the same address listed as the registered office of ABC which was occupied by 101 Accountants. Y was the Principal of 101 Accountants. X and Y were married.
228. On 4 June 2009 the sum of K2,350,000 (USD1,093,023) was transferred from the ABC Jetty Account to the bank account of Built. On 27 July 2009 the sum of K2,300,000 (USD1,069,767) was transferred from the account of Built to the ABC Jetty Account. The balance of K50,000 (USD23,255) was transferred to another account. The transaction was described "in favour of X and Y".
229. Funds totalling K5,232,000 (USD2,433,488) were subsequently depleted from the ABC Jetty Account through cash and cheque withdrawals. A sum of approximately K3,287,000 (USD1,528,837) was withdrawn through bank cheques (unknown recipients). The suspect made cash withdrawals totalling K1,151,657 (USD535,654). The suspect's brother, a former politician, withdrew a total of K981,130 (USD456,339). The suspect's daughter withdrew a total of K35,700 (USD16,604) and another relative withdrew a total of K55,025 (USD25,593). An associate also withdrew a total of K195, 000 in cash. No work was done at the project site.
230. ABC Construction had requested a further K10 million (USD4,651,162) to relocate the jetty when the matter was brought to the attention of authorities. No criminal charges were laid.
231. On 8 February 2010 a non-conviction based restraining order was obtained in relation to the remaining balance of the ABC Jetty Account (K1,268,778.41) and the balance of the suspect's personal bank account (K32,881.70).
232. The restraining order was made on the basis of a reasonable suspicion that the suspect had committed the following offences:
- Conspiracy to defraud.
 - Obtain goods by false pretences.
 - Misappropriation.

- Money Laundering.

233. On 16 July 2010 the proceedings were settled on the basis that K1,268,778.41 (USD590,129) be forfeited to the State and K32,881.70 (USD15,293) be returned to the suspect. A copy of the court order giving effect to the forfeiture was served on the bank. The bank was given instructions to transfer the forfeited funds to the Consolidated Revenue Fund but did not immediately effect the transfer.
234. On 6 August 2012 the suspect and her brother, a former Member of Parliament, attended the bank and presented a forged order purporting to set aside the forfeiture order.
235. On 20 September 2012 the bank permitted a deal with the forfeited property by allowing the suspect to withdraw the funds. On 21 January 2013 the bank repaid the forfeited amount to the State from its own funds.



SAMOA

Police vs. Mr A and B (Government Officials)

236. Mr A and B were formerly employed in the Ministry of Finance and were charged with numerous counts of Official Corruption pursuant to section 35 of the Crimes Ordinance 1961.
237. Mr A was a Senior Accounting Officer in the Accounts Payable/Expenditure Section while Mr B was an Assets Officer who often assisted the Accounts Payable/Expenditure section with customer queries and follow-ups for cheque payment claims. For a two year period, the two would collude in issuing false or

fictitious invoices and involve a third party for receiving the payments in which later they would receive monies or bribes in return of their efforts.

4.2 Laundering proceeds from corruption

FIJI

238. The Fiji FIU received a request from Fiji's anti-corruption authority for a financial background check on a senior public servant working for the Ministry of Transport who was under their investigation. Checks conducted on her bank account revealed suspicious transactions including:

- large cash deposits (apart from salary) made into two of her bank accounts - over a period of 3 years totalling FJ\$178,000 (USD96,608);
- an inward remittance of FJ\$12,600 (USD6,838) from a foreigner known to the Fiji FIU. This foreign individual had been previously reported to the Fiji FIU in an STR. The day after this remittance was received into the senior officer's bank account, a cash withdrawal of the same amount was made; and
- a cheque of FJ\$24,450 (USD13,270) was deposited into her bank account by a motor vehicle dealer - these funds were used to purchase a new motor vehicle for the senior public servant.

239. Investigations continue.

HONG KONG, CHINA

240. In early 2012, three foreign passport holders were wanted by foreign countries for fraud and money laundering. Investigations revealed that the subjects remitted large amount of funds overseas, which were suspected to be proceeds of corruption-related offences, overseas via their newly opened bank accounts in Hong Kong. Arrest warrants were issued against the three subjects and around HK\$7.7 million (USD992,390) and EUR\$26.5 million (USD35,403,231) worth of assets were frozen.

INDONESIA

241. Former chief of the Traffic Corps National Police Headquarters, Insp. Gen. Djoko Susilo, was named as a suspect in the driving simulator corruption/graft case. Djoko, a two-star police general, stands accused of involvement in massive corruption in relation to a Rp 200 billion (\$20.6 million) project to procure driving simulators for use in testing driving license applicants in 2011. This project caused Rp 144.9 billion (US\$14 million) of state losses.

242. The Corruption Eradication Commission (KPK) continues to pursue a number of assets associated with the driving simulator project. Djoko has 35 property assets such as land, apartments, and luxury homes. Most allegedly come from the proceeds of corruption money from the driving simulator project. Total assets reached Rp 200 billion. In addition, some Djoko assets are outside Indonesia (including apartments in Melbourne, Australia, and Singapore). In addition to

property, Djoko invested the money in businesses, for example, investing in three public refuelling stations in Jakarta.

243. So far, the Anti-Corruption Commission has charged Djoko under the AML law and seized 11 of Djoko's properties. Some of them are listed as belonging to Dipta Anindita, Djoko's third wife. The Anti-Corruption Commission has also found evidence of the flow of funds from the account to Mahdiana Djoko (his second wife) and a number of relatives. The Anti-Corruption Commission has also prevented Djoko's wives from going abroad.

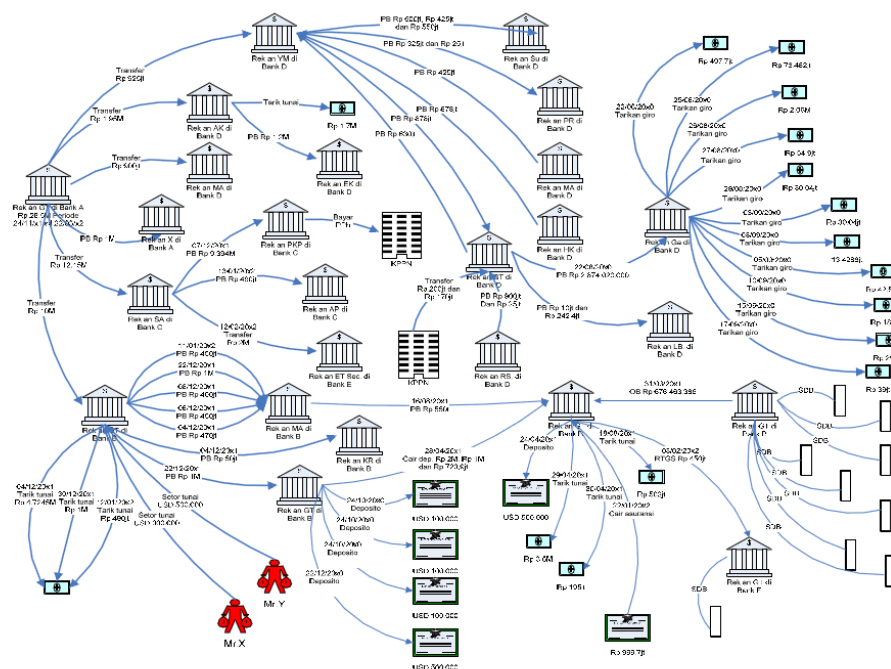
Gayus Halomuan Tambunan case

244. Gayus originally caught investigators' eyes in March 2009. By age 30 he had managed to accumulate bank balances totalling more than \$3 million, equivalent to more than 250 years' worth of his 8 million rupiah monthly salary.

245. Prosecutors brought charges against Gayus and froze his bank accounts in October 2009 but unfroze them a month later. His trial began in January with prosecutors asking for a penalty of a year in jail.

246. Despite having Rp 28 billion (\$3.1 million) in two bank accounts, Gayus managed to get the police to unfreeze his money and was acquitted by the Tangerang District Court on March 12 on the relatively minor charge of embezzlement, on the grounds of “insufficient evidence.”

Laundering proceeds in Gayus case:



4.3 Underground banking/alternative remittance services/hawala

AUSTRALIA

247. The Australian Crime Commission (ACC), together with its partners, have identified ongoing vulnerability of exploitation by organised crime in the alternative remittance sector and have produced jointly with AUSTRAC a strategic assessment that analysed the extent of criminal exploitation by, and of, alternative remittance service providers. This represents a challenge to law enforcement nationally.

Op Masalas

248. Through this ACC-led joint investigation with Victoria Police, the services of a remittance business based in Melbourne and Vietnam were targeted for money laundering activities. The operator of this business is alleged to have been responsible for laundering illicit profits on behalf of high-level drug trafficking groups.

249. The investigation resulted in the seizure of cash and drugs during July, August and September 2011 including some \$2.5 million (USD 2,379,960) in cash, just over one kilogram of cocaine, over 26.3 kilograms of heroin and 9.4 kilograms of methyl amphetamine. Eleven people were arrested for a variety of offences including trafficking drugs, money laundering and possessing the proceeds of crime.

CANADA

Khat Trafficking to Fund Terrorism

250. The drug, khat (short for *Catha Edulis*), is not a prohibited substance in many countries, including England and the Netherlands. In Canada, however, khat is a prohibited substance under the Controlled Drugs and Substances Act, as it contains the chemicals known as cathine and cathinone.

251. The majority of khat users in Canada are of Somali, Yemeni, Ethiopian, and Kenyan descent. It has been determined that the UK is a primary transshipment point of khat, which is widely produced in the Horn of Africa for European and North American markets. Due to the perishable nature of the drug, khat is usually smuggled into Canada by air within days of being harvested. The Canada Border Services Agency (CBSA) seizes more khat by weight than any other prohibited substance. Over the past five years, 57 tonnes of khat have been seized at ports of entry to Canada.

252. In 2010, CBSA officers seized a total of 12.7 tonnes, with an estimated street value of \$6.4 million (USD6,278,375). This is an increase from 2009, when 10.4 tonnes were seized. Significant khat seizures have been made through Air Cargo, Air Passenger and Courier mode. The shipments are falsely labelled, often utilizing counterfeited legitimate shipping labels and or paid through fraudulent corporate accounts.

253. European countries are the principal transit points for khat destined for Canada—particularly the UK and the Netherlands. This is due to khat being legal in both countries. In 2010, over 85 per cent of the total quantity of khat seized (10.8 tonnes) transited the UK, nearly double the amount seized in the previous year.
254. It is believed that some of the proceeds from the sale of khat are being used to fund the Somali Islamist group known as al-Shabaab, a listed terrorist entity in Canada. It is believed that the proceeds of the sale of khat in Canada are sent via hawalas, registered MSBs, or financial institutions to Europe and/or Dubai, and then to Somalia. In one such case, a major khat importer made 29 cash transactions in various currencies through a registered MSB to England, totalling \$45,000. These transactions, which occurred over a 2.5 month period, were all under Canada's reporting threshold of \$10,000.

CHINESE TAIPEI

Case 1

255. From January 2008 to October 2010, Mr Lee and Mr Liao operated cross-strait underground banking between Mainland China and Chinese Taipei which violated the Banking Act.
256. Mr Lee directed Mr Liao to inform the clients to deposit funds into the accounts of Mr A, B & C in Bank X, the accounts of Mr D, E & F in Bank Y and the accounts of Mr H & I in Bank Z which were controlled by Mr Liao. Then Mr Liao would inform Mr Lee to deposit the equivalent RMB to the bank accounts in Mainland China designated by the clients. Mr Lee and Mr Liao checked the information of clients and the remitting details by fax every day. Mr Lee paid Mr Liao NTD35,000 (about USD1,666) per month while Mr Liao paid bona fide Ms Ye as reward for operating the abovementioned bank accounts by case.
257. During the period, Mr Lee and Mr Liao operated cross-strait underground banking totalling up to NTD 5,110,867,700 (about USD 170,362,256).
258. This case was investigated by the Taipei Field Division of the Investigation Bureau and the abovementioned suspects were charged with violation of the Banking Law by the prosecutor of the Shi-Lin District Prosecutors Office in June 2011.

Case 2

259. Mr Tsai and Mr Chen were respectively a representative and a staff member of Lung X International Trading Company. Chen and Tsai were aware that only banks may conduct transactions related to domestic and international currencies.
260. Since 2005, they illegally used the accounts of 16 individuals, including Mr Hung, to operate underground currency exchange business and collected NTD2,000 (about USD67) processing fee for every RMB100,000 (about USD16 thousand).
261. The total transactions in and out of these accounts amounted to over NTD7,898 million (about USD 236 million).

262. The Investigation Bureau referred the case to Taipei District Prosecutor's Office for further investigation on 26 August 2011.

INDIA

263. A group of people with foreign currency was intercepted by enforcement agencies. These people led the agency to another Person "B" who was to be given that currency. Person B further led them to Person "M". During a search certain documents were recovered and it was found that Person M was dealing in unauthorised exchange of currency through a network of people who were acting as his branches. The transactions were only in the currency of a particular jurisdiction. The people of the other jurisdiction came to this jurisdiction. They exchanged currency through Person M and his network which they use to buy goods and take to their homeland through different channels.
264. Similarly some traders from this jurisdiction went to buy goods from the other jurisdiction for which they took the currency of the other jurisdiction from person M. A branch-wide account was also maintained.

SAMOA

265. Mr A received a winning notification. After paying many fees through a money transfer operator, he received a partial payment cheque of USD20,000. He went to cash the cheque at the bank but later found out it was a fake cheque.
266. Ms K ran beach fale accommodation. A fraudster made an online booking and sent over traveller's cheques for more than the actual price. He asked to have the cheques cashed and have the balance sent back to him through a money transfer operator. The traveller's cheques were later discovered to be fakes.
267. There were several other cases referred where scammers sent emails pretending to be a person in a difficult situation. Instructions indicated that they needed help and monetary assistance either for a lost passport or hotel accommodation, etc.

4.4 Use of offshore banks and international business companies, offshore trusts

MONGOLIA

268. In December 2011 the General Intelligence Agency (GIA) of Mongolia detained citizens of Belarus "O" and "S" who were residing in Mongolia and who opened over 50 accounts in one of the Mongolian commercial banks.
269. In order to open such numerous accounts "O" and "S" established seven representative offices of UK and Russian companies and 8 legal entities in Mongolia. The Mongolian bank opened accounts based on the furnished documents, including an investment agreement for geological exploration. Under this investment agreement during the two year period from 2009 to 2011 4.3

billion roubles (USD 160 million) was received from a private Russian commercial bank “S”.

270. The Mongolian bank informed “O” and “S” on every occasion about the rouble transactions from Russia. Then all the received roubles were converted into dollars and euros and placed into the accounts of the above-mentioned companies to obfuscate its origin. After numerous, confusing, domestic transactions all the money finally converged in the account of a UK registered company “F”. Company “F”, operating as a foreign trading company’s representative office in Ulaanbaatar, transferred dollars and euros as a payment for loans and textile equipment to Cyprus, Latvia, Lithuania, Turkey, British Virgin Islands and 15 other countries.
271. Eventually, investigators revealed that the money was never used under the investment agreement for geological exploration; everything was transferred to foreign countries. The private Russian commercial bank was announced as a bankrupt in December 2010, the UK registered company “F” was a shell company which was liquidated in 2009, all documents provided by citizens of Belarus were false and almost all recipients of the money in Cyprus, Latvia, and British Virgin Islands were Russian citizens.

4.5 Use of professional services (lawyers & notaries)

FIJI

272. An STR was made on a finance company in Fiji that allegedly approved and opened a loan account of \$450,000 (USD244,168) for Company X, without the directors of Company X, Person A and B being present at the time of the account opening. The loan was for the purchase of two properties by Company X.
273. It was established that the loan documents were signed by Person B when the account was opened, however it was confirmed that Person B was not in the country when the loan account was opened. Therefore, Person B’s signature may have been forged.
274. The loan documents were witnessed by two separate lawyers. Interviews conducted with the lawyers revealed that a third party (vendor) had brought pre-signed loan documents to the lawyers to witness the documents. Thus, the directors of Company X, Person A and Person B, were not physically present before the lawyers when the documents were executed.
275. The case is currently being investigated by the Fiji Police Force for suspected fraud and violations of the Financial Transactions Reporting Act.

JAPAN

276. In the course of investigation by Japan Police of loan-sharking cases, it was found that a large amount of criminal proceeds had been transferred to the bank accounts of various companies which were identified as shell companies. It was also revealed that a certified administrative procedures specialist was involved in

the creation of the companies which had Boryokudan gangsters on their board of directors.

277. Upon receiving requests from customers, mainly through the Internet, which was on a non-face-to-face basis, the specialist prepared the articles of the company and other application documents without conducting appropriate customer identification. The number of transactions involving the specialist from 2008 to 2011 was at least over 1,000 cases.
278. While Japan Police arrested several suspects for violation of the Act on Punishment of Organized Crimes, as they concealed about 370 million yen (about USD 47 million) from March 2011 to Feb 2012, they failed to arrest the certified administrative procedures specialist for the charge as an accomplice because he insisted that he had never been aware of the plot of the customers.
279. However, the investigation succeeded in taking the case to prosecution for violation of the Act of certified administrative procedures specialists in March 2012, by looking at the fact that he had not maintained records adequately. In addition to the criminal charge, an administrative order was delivered by the prefectural governor who supervised the certified administrative procedures specialist, based on the Act on Prevention of Transfer of Criminal Proceeds in July 2012 for failing to take adequate measures for customer identification and record keeping.

SRI LANKA

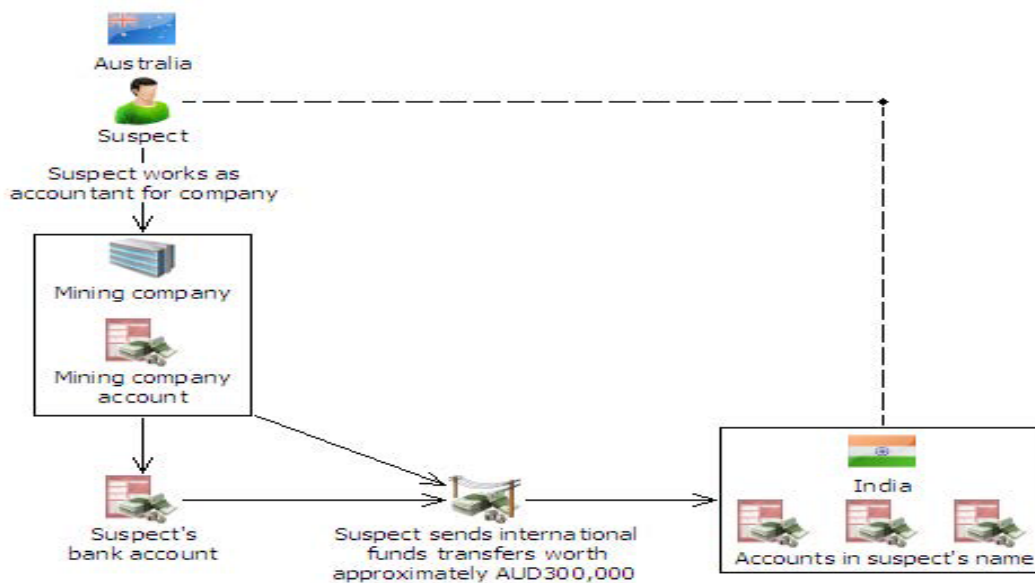
280. Three companies in a company group, “A”, “B” and “C”, were engaged in the provision of legal consultancy services, secretariat services and real estate buying and selling respectively. A reporting agency, a bank, reported that in addition, these companies were supporting residents outside Sri Lanka to purchase real estate properties in Sri Lanka without meeting local requirements and related laws.
281. Company A introduced foreign citizens to open investment accounts in the bank concerned. Further, A was registering companies (shell) in various names and company B would act as the secretariat for all these companies. The registered addresses of these companies was the same as that of company B. Company C would purchase real estate in Sri Lanka, using the money deposited by foreign citizens, in the name of these shell companies. Subsequently the ownership of these shell companies would be transferred to foreign citizens with the ownership of the real estate purchased.
282. As per the prevailing law in Sri Lanka, any non-resident who purchases real estate in Sri Lanka is subject to a property tax and various limitations. The above methodology applied by these companies helped to evade tax laws in Sri Lanka.
283. The case has been referred to relevant law enforcement authorities for necessary action.

4.6 Use of professional services (accountants)

AUSTRALIA

Mining company accountant siphoned \$1 million into offshore accounts

284. An Australian-based mining company initiated an internal investigation after it was suspected an employee had stolen more than AUD1.1 million over a three-year period. The company identified the suspect through internal audit processes and the matter was referred to law enforcement authorities for further investigation.
285. The law enforcement investigation revealed that the suspect, an accountant employed by the company, had abused his position of trust by systematically making a series of unauthorised international transfers over a three-year period. The transfers were made from a company account to a number of offshore accounts held in the suspect's name and a number of his family members' names.
286. An STR submitted by a bank suggested that an outgoing funds transfer of AUD27,500 from the suspect's personal account appeared to be sourced from company funds. The suspect was the beneficiary of the outgoing transfer and bank staff noticed that four days prior to the transfer, the exact amount of AUD27,500 was transferred into the suspect's account from a company account.
287. AUSTRAC analysis found a number of transaction reports linked to the suspect. These supported the allegation of theft and identified the significant extent of the financial activity undertaken by the suspect.
288. AUSTRAC information revealed that the suspect was the beneficiary of 17 outgoing IFTIs to India in amounts of between AUD2,400 and AUD33,400. Funds were sent from either the suspect's personal Australian-based bank account or from the company's account. In total, approximately AUD300,000 was transferred, all believed to be the proceeds of the theft.
289. Law enforcement officers contacted the suspect while he was overseas. The suspect surrendered to authorities on his return to Australia. The suspect was charged with 10 counts of stealing and sentenced to seven years imprisonment. After serving four years the suspect was deported from Australia.



290. The jurisdictions involved were Australia and India. Indicators in the case included:

- Customer receiving multiple large-value domestic transfers into their personal account from a company account, followed by an outgoing international funds transfer equivalent in value to the domestic transfer.
- International funds transfers from an individual's account to several offshore accounts held in the same name.
- International funds transfers inconsistent with transaction history.

4.7 Real estate, including roles of real estate agents

AUSTRALIA

Case 1

Secret cash payment used to avoid stamp duty and launder money

291. A vendor and purchaser colluded to transfer a property at an agreed price but then record the formal transaction price as significantly lower than the agreed price. The purchaser paid the difference between the two prices to the vendor in cash, which was not recorded on any of the formal conveyancing documents.

292. The vendor deposited the cash into his bank account on a date close to the date on which the contracts for the sale of the property were exchanged, indicating to law enforcement officers that the cash actually formed part of the total sale price.

293. Understating the official sale price of the property was an act of fraud allowing the offenders to avoid paying the required amount of stamp duty on the property. It is also suspected that the cash involved in the transaction was the proceeds of other criminal activities and that the transaction was an attempt to launder the illicit cash through the real estate sector.

294. Law enforcement action was taken against the offenders and the property in question was seized under the *Proceeds of Crime Act 2002*.

Case 2

High-value assets purchased to conceal illicit profits

295. Approximately 60 bank deposits of amounts less than AUD10,000 were deposited into an individual's account within a four-month period, totalling AUD550,000. Money was also deposited at a credit union.

296. Following this series of structured deposits into the accounts, the individual in question purchased three real estate properties with bank cheques, and a high-value motor vehicle with AUD66,900 cash. It is not known how the significant amount of cash required to pay for the car was delivered to the motor vehicle dealer, but it was withdrawn from a bank account and paid to the dealer in two instalments.

297. A law enforcement investigation commenced and the suspect was eventually charged with supplying prohibited drugs and money laundering offences, and approximately AUD1.5 million worth of assets have been restrained.

CHINESE TAIPEI

Case 1

298. The AMLD received an STR from bank X in July 2011 which described the suspicion as follows: "Ms Chen purchased gift certificates for NTD10,569,000 (USD353,708) at Branch A of the bank on July 13, 2011 and then cashed it and deposited it in Ms Chen's bank account at Branch B on the same day."

299. The AMLD analysed, filtered, and conducted preliminary investigation into the STR and found Ms Chen was possibly involved in an economic crime. Then, the information was referred for further investigation.

300. The case scenario is summarized as follows: Company C engaged in the sale of IT products. Ms Chen was the marketing manager of the Inkjet Imaging Systems Division of Company C who was mainly responsible for product marketing and promotional incentives for consumers and distributors.

301. Company C outsourced Company F to be responsible for external incentives matters. Ms Chen was the contact person for this matter. For the purpose of getting benefit illegally, in March 2009 and July 2011 Ms Chen ordered Company F to purchase gift certificates with the balance of the planned budget that had not been spent in promotional incentives. Ms Chen lied about having the gift certificates forwarded to other distributors on Company F's behalf. However, Ms Chen immediately cashed those gift certificates in Branch B of Bank X upon acquisition of the certificates bought at Branch A of Bank X. Ms Chen deposited the money in her account in Bank X and then transferred the funds to her and her spouse's bank accounts in other banks.

302. The AMLD found that the amount involved reached NTD174,393,000 (USD5,836,399) in the form of real estate, funds and stocks which were used for laundering the proceeds of crime.
303. The case was prosecuted by the Prosecutors Office in February 2012. Ms Chen was accused of embezzlement in accordance with Paragraph 2, Article 336 of the Criminal Code. During the investigation, the proceeds of crime were frozen, including Ms Chen's bank accounts in Bank D and E amounting to NTD32,706,910 (USD1,094,109) in total and two pieces of real estate under the names of Ms Chen and her spouse for a total of 297.7 Pings.

Case 2

304. The AMLD received STRs separately from Bank A and B on January 22, March 18, October 20, and November 2, 2010 which described the suspicion of Mr Chang frequently depositing cash into his bank account which was structured on purpose to avoid the reporting threshold for currency transactions that had been in place since January 2010. This exposed a suspicion of money laundering triggering the STR.
305. Company H had frequently made deposits below the declaration threshold into the bank account of Company S in Bank B and then made withdrawals for an equivalent amount from a different branch. It was suspected of committing a money laundering crime. Customer F's personal checking account had a lot of recent and large amount deposits and withdrawals. Two cheques from this account, issued respectively in the sums of NTD12,320,000 (USD412,294) and NTD19,500,000 (USD652,267) were presented and cashed in other banks on October 25 and October 26 2010. These large amount transactions were incommensurate with the purposes of the account stated at the time of applying for account opening, which were for personal daily expenses, insurance fees and education expenses.
306. The AMLD analysed, filtered, and conducted preliminary investigation to the STR and found that Mr Chang had accepted deposits from the public and transferred the funds into Mr Wang's bank accounts through online banking services. Then the syndicates withdrew the money or transferred it to the bank accounts of others in multiple small amounts. The AMLD suspected Mr Chang and the syndicates were involved in an underground banking business that violates the Article 29-1 of the Banking Act. This case was referred to Hsinchu City Field Office of the Investigation Bureau for further investigation.
307. The case scenario is summarized as follows: Mr Qin was the president of the international business Group D. He offered high interest to attract depositors and provided incentives, including bonuses, tours, and luxury cars, for the staff who had excellent performance in collecting deposits. There were 199 branches for engaging in the illegal activities to absorb deposits and distribute interest and 21,561 depositors savings were involved, totalling NTD4,759,697,571 (USD159,315,696) in Group D. Mr Qin had spent part of the money in purchase of 411 pieces of real estate valued at NTD1,200,000,000 (USD40,160,137) under the names of Mr Qin, Mr Chang, and Mr Lin.

308. During the investigation, the Prosecutors Office ordered for the involved money to be frozen, including Mr Qin's 122 banking accounts amounting to NTD16,060,128 (USD537,467) and the above 411 pieces of real estate, valued at NTD1.2billion (USD40,155,119). This case was referred to the Prosecutors Office for prosecution.

INDONESIA

Dhana Widyatmika Case

309. Junior taxman Dhana Widyatmika (DW) was indicted on multiple felony charges, including accepting bribes and money laundering. DW allegedly used bribes to buy properties, cars and jewellery and is claimed to have kept money on behalf of other graft suspects in numerous bank accounts and used it to make business investments, especially in real estate and car dealing.

310. The Indonesian FIU has solid evidence to prove that Dhana has been collecting fortunes that are suspected to have come from illicit sources arising from of his position as junior taxman. In the indictment, prosecutors said that in 2011, Dhana had made Rp129.2 million (USD13,041) in annual income as a tax officer.

MALAYSIA

Ponzi Scheme Perpetrated by Professional (Lawyer)

311. *Methods used:*

- Use of nominees or third parties etc.
- Use of professional services (lawyers)
- Real estate

312. Mr A was a lawyer turned businessman where he established a property investment company which offered services to investors to buy properties at a lower price and an option to re-sell at higher price. The difference between the purchase price and selling price would be distributed to the investors as investment return. In addition, all the investors were required to pay a substantial amount in member fees to the company annually.

313. Mr A appointed two legal firms to complete the legal documentation on the sales and purchase transactions on the properties for the investors.

314. Initially, the investment scheme was carried out in accordance with the law. However, as the number of members grew, Mr A and his team could not obtain sufficient optional-properties to meet the demand of the increasing investors. He started to hire proxies by recycling the properties among the existing investors, proxies and the new investors. The same units of properties were sold and resold to investors via proxies and new investors at a different price. The profit would then be ploughed back to the investors to gain trust and confidence for further investment, which resulted in the value of investments multiplying tremendously.

315. Investors were initially not suspicious of the investment scheme by the investment company because the monies needed to purchase the invested

optional properties were deposited into a trust account opened by the two legal firms. They trusted that the lawyers would carry out due diligence work on the optional properties they had purchased.

316. However, the monies that the investors banked-in were then partially paid as return to the other investors, but the majority of it was siphoned out by Mr A. Approximately 100 million of ringgit (USD31,721,967) was transferred out to a foreign country before Mr A and his family absconded from the country.

317. The investigation revealed that the investment scheme had lured a total of 500 investors, who suffered losses of 250 million ringgit (equivalent to USD76 million), while the 200 properties registered under proxies' name were valued at not more than 70 million ringgit (equivalent to USD21 million). The case is currently being investigated for cheating and money laundering offences.

TONGA

318. The case involves an on-going investigation and inquiries into possible advance fee fraud conducted by foreign nationals colluding with Tongans, where local properties are being advertised on a website seeking potential investors.

319. One of the suspects in this case is a foreign national who has an outstanding arrest warrant for fraud and money laundering cases. There are international complaints from investors who invested in these properties but they were actually not for lease.

4.8 Trade in gold, gems and precious metals

AUSTRALIA

Hong Kong, nationals avoided thousands in Goods and Services Tax (GST) in jewellery import fraud

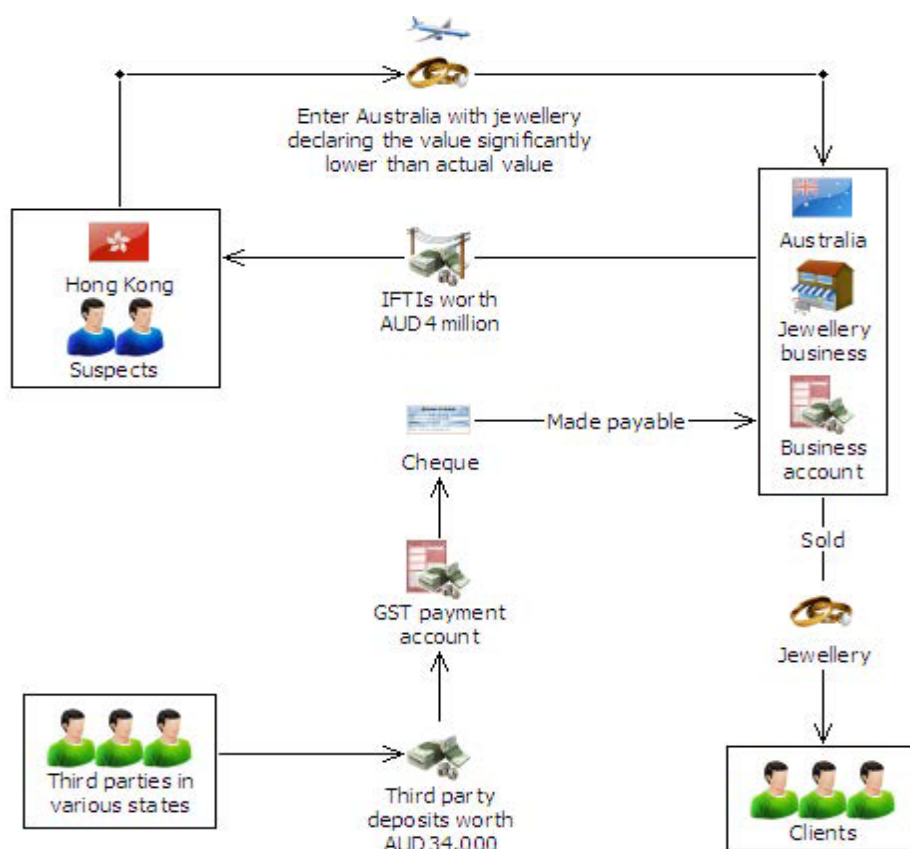
320. A suspicious matter report (SMR) informed a joint-agency investigation into a criminal syndicate which was undertaking significant tax evasion. The two suspects, one the director of an Australian jewellery business and the other an employee, were using the business to avoid paying the GST on imported jewellery.

321. The suspects were Hong Kong nationals. They would periodically enter Australia with jewellery, declaring the value of the goods significantly below their actual value. The suspects would sell the jewellery to clients based in Sydney, Melbourne, Adelaide and Brisbane and send the profits back to Hong Kong.

322. The suspects had created a GST payment account with their financial institution. A GST payment account would usually be used to set aside funds to pay GST liabilities to the Australian government. AUSTRAC received an SMR from a reporting entity indicating that, over a six-month period, the GST payment account had received primarily cash deposits worth approximately AUD34,000. These deposits had been made by unknown third parties in New South Wales and

Victoria. It was believed the cash deposits were from the proceeds of the jewellery sales.

323. The cash deposits were in amounts less than the AUD10,000 cash transaction reporting threshold and were therefore not reportable under the AML/CTF Act's transaction reporting requirements. The proceeds of these deposits were then withdrawn via cheques made payable to the business account operated by the jewellery business.
324. Authorities identified large discrepancies between the declared value of the imported jewellery and the funds remitted to Hong Kong by the jewellery business. This was a strong indicator that the suspects were under-declaring the value of the imported jewellery and, thereby, evading paying the correct amount of tax. The proceeds of jewellery sales were remitted to Hong Kong and reported to AUSTRAC through international funds transfer instructions (IFTIs).
325. Over a five-year period, the suspects' jewellery business declared more than AUD120,000 worth of imported jewellery upon entry into Australia. AUSTRAC information identified that various individuals working for the jewellery business had sent IFTIs worth more than AUD4 million to Hong Kong in the same period – funds that authorities established were the proceeds of the jewellery sales.
326. When authorities became aware of the scheme, the suspects' passports and jewellery were seized upon their travel into Australia.
327. Both suspects were served with taxation notices of assessment and departure prohibition orders. However, the two suspects fled Australia in contravention of the departure prohibition orders, using false documentation.
328. The jewellery seized by authorities was sold at auctions, raising almost AUD700,000. This amount was used to offset the loss of revenue for the Australian government.



329. Offences included Tax evasion and fraud. Jurisdictions involved included Australia and Hong Kong, China. Indicators in the case included:

- Account activity inconsistent with business profile.
- Cheques from a GST payment account made payable to companies or individuals, rather than to the Australian Taxation Office (ATO).
- Third-party cash deposits into a GST payment account in various states.
- Using the functions of a GST payment account as a normal business account.

FIJI

330. An export consignment containing 26 undeclared gold bars weighing 2.3 kilograms was detained by Fiji Customs officials on 25 June 2012 in Suva, Fiji.

331. The investigations conducted revealed the error in tariff classification of the gold bars where it should have been classified as semi-manufactured gold attracting export duty. Thus the value of the consignment declared in the Export entry documents was F\$178,875.00 (USD97,057) and the export duty was under paid by F\$5,326.22 (USD2,889).

MONGOLIA

332. In 2012 GIA of Mongolia detained a Mongolian driver “B” who attempted to smuggle 3kg of gold into China. “B” disclosed a widespread Chinese gold smuggling network, which started in 2011. The investigation found that Chinese

citizens “D”, “Yu”, “Li” and “Bao” established a construction and foreign trade “shell” Company “X” in Mongolia in 2011 and in addition to that engaged in illegal gold mining. Investigations revealed that illegal gold mining associated with smuggling was their main income, not construction or foreign trade.

333. Inquiries from bank and non-bank financial institutions showed that “D”, “Yu” received from China almost every day over USD150.000 in cash (approximately 3kg worth of gold).
334. During a three month period, 57 kg of gold was smuggled and over USD 4 million was laundered by “D”, “Yu”, Li” and “Bao”.

THAILAND

Thai baht currency exchanged for foreign currencies used to buy gold

335. The case involved the proceeds of drug trafficking in Thai baht being exchanged for foreign currency with money changers who also conducted a currency distribution business.
336. Steps in the laundering process included:
1. The money derived from drug trafficking was exchanged for foreign currency before being smuggled out of Thailand. (Foreign currency can be taken out of Thailand, but must be declared at customs.)
 2. The foreign currency originating from the drug trade deals was later used to buy gold.
 3. When the gold was sold, the proceeds from the sale were treated as business income ‘in good faith’.

4.9 Trade based money laundering and transfer pricing

CHINESE TAIPEI

337. Mr Chang was the nominal owner of Company A which was controlled by Mr Chen. Mr Lin was the owner of Company B and he designated a mainlander, Ms Qu, as the nominal owner of Company B, registered in Marshall Islands and designated an American, Mr Joseph, as the nominal owner of Company C registered in B.V.I.
338. In March 2008, Mr Chen and Mr Chang considered that the solar energy industry was going to have a booming future. Thus they decided to cooperate with Mr Lin and invest NTD500 million (about USD17 million) into Company B in the name of Company A to run a production line of solar energy equipment.
339. They then planned to manipulate the stock price of Company B and undertake an insider trading scheme. Considering that Company A only had funds of no more than NTD100 million (about USD3.3 million), they created the illusion of investing an amount of NTD500 million by transferring NTD100 million from Company A’s account in Bank M to the Company B’s account in Bank X, then to

Company C's account in Bank Y in the Marshall Islands, then to Bank D's account in Bank Z in B.V.I. and then back to the account of Company A.

340. They remitted funds this way five times from July to September 2012, which made it appear that Company A invested NTD500 million in Company B. After the last time the funds of NTD100 million were transferred to the account of Company B, Mr Chen withdrew them by cash and deposited this into several of his nominal accounts to manipulate the stock price of the company.
341. The stock prices of company B were successfully manipulated from NTD6 to NTD 19 per stock, booming more than three times. Meanwhile, Mr Lin and his wife, Mrs Liu, a teacher at an elementary school, used their personal account in Bank X and those of Teacher Ding and Teacher Chen, who were Mrs Liu's colleagues, to buy the stocks of Company B with NTD10 million (about USD333 thousand) to undertake insider trading and they gained more than NTD20 million (about USD666 thousand).
342. In December 2008, the Taipei Field Division of the Investigation Bureau received a letter of accusation and began an investigation. AMLD also received an STR from Bank X indicating that the bank account of Company B was usually operated by the employees of Company A including withdrawals and deposits in cash. AMLD disseminated the information to the Taipei Field Division of the Investigation Bureau.
343. In February 2011, the abovementioned suspects were all charged with embezzlement of the company's assets and manipulating the stock prices. Mr Chen and Mr Chang were prosecuted by the Taipei District Prosecutors Office and sentenced to 12 years and Mr Lin was prosecuted and sentenced to 10 years, all were fined NTD100 million (about USD3.3 million).
344. In April 2012, Mr Lin and his wife, Mrs Liu were charged with insider trading and the prosecutor also appealed to confiscate the proceeds of crime amounting to NTD20 million (about USD666 thousand).

FIJI

345. Person B, a 25 year old businessman was the director of Company X, which was involved in importing kava into Fiji from another Pacific Island country.
346. It was established that deposits totalling approximately FJ\$2.7m (USD1,465,013) were made into the personal bank account of Person B within a period of two years. Withdrawals totalling approximately FJ\$2.6m were also made within the same period.
347. Further analysis showed that Person B was importing kava from Country A. Person B was reportedly buying the kava at a price which appeared to be unrealistic and seemed to decline for the subsequent imports. Thus imports were being undervalued so that less tax was payable.
348. The Fiji FIU also established that another related Company Z shared the same address as Company X and both appear to have remitted substantial amounts to Country A.

349. The matter has been referred to the local tax authority for further profiling and investigations.

INDIA

Case 1

350. Searches were conducted on the premises of X Group of Companies and resulted in the seizure of incriminating documents as well as huge amounts of cash, indicating the supply of diamonds in dubious trades which were only on paper, with bills/invoices being issued for only nominal commission without supplying diamonds.

351. The foreign inward remittances, in the guise of advances for exports, were received from persons other than buyers. These were for the purpose of channelling the funds parked abroad in the guise of export proceeds. The suspected hawala transactions were carried out and the funds received from abroad were diverted to activities other than those relating to exports and included large scale investment in real estate. The company is involved in money-laundering (including cross-border) and accounts in foreign jurisdictions have been traced and frozen.

Case 2

352. Company A mis-declared goods and thus under invoiced imports. The differential between the high value of goods and lower value of goods was remitted abroad through hawala. The search of the company's premises led to recovery of documents which showed the extent of undervaluation. Further follow-up revealed the hawala operator network through which compensatory payments had been made abroad.

MALAYSIA

Evasion of Customs Duties Involving Beer and Liquor Trade

Methods used:

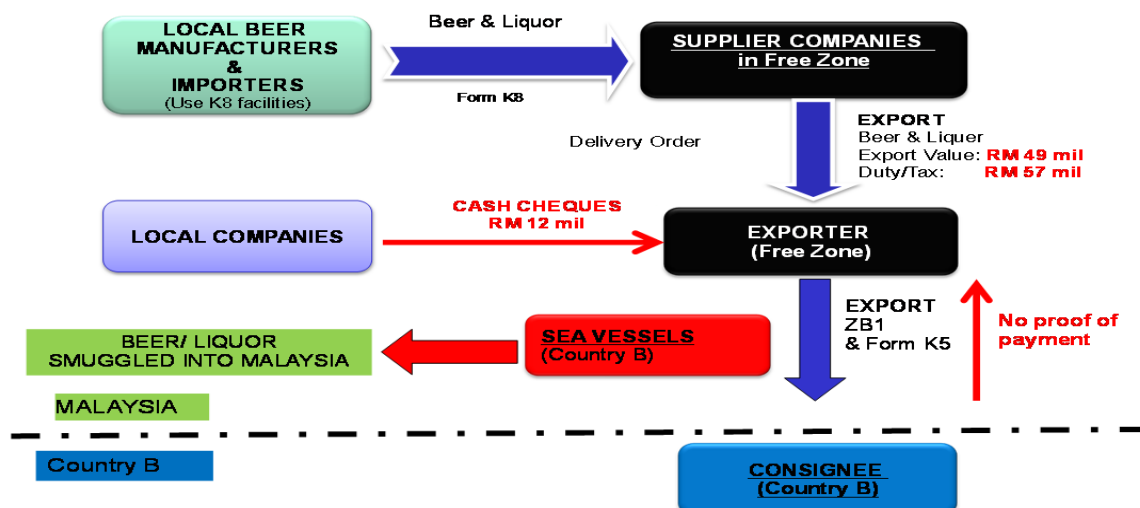
- Use of false export documentations.
- Trade based money laundering and transfer pricing.
- Use of credit cards/cheques.
- Use of shell companies/corporations.

353. A group of manufacturers, traders and exporters, importers and shipping vessels were involved in a case to evade import duties and taxes on imports of consignments of beer and liquor that were exported from Malaysia and subsequently smuggled back into the country.

354. Duty free beer and liquor were moved from the licensed warehouses belonging to the Beer Manufactures/Importers located in Malaysia to the warehouses of the Supplier Companies in the Free Trade Zone (FTZ) under a customs removal permit form which does not require any customs duties to be paid. The Supplier Companies then resold and moved the duty-unpaid beer and liquor to the

Exporter located in the free zone using delivery orders. These goods were then exported out of the FTZ through two foreign Country B sea vessels under the FTZ legislation.

355. Customs documentations and FTZ declaration records revealed in total a large export trade of beer and liquor valued in excess of USD16 million and customs duties in excess of USD20 million through the port in Malaysia to the port of Country B, where the consignments were purportedly discharged. This raised a red flag to the Customs since the trading involved an unusually large quantity of beer and liquor imported by Country B, which has very stringent and restricted importation for such products.
356. Financial investigations revealed that no payments were received from Country B for all the exports made from Malaysia. The payments made into the account of the Exporter were from local cash cheques issued by locally registered companies and most of the companies were later found to be untraceable. In 2011, Customs seized 13 accounts belonging to the Exporters valued at approximately USD650,000 for a serious offence of evading of customs duties.
357. A check on Customs and FTZ Authority records verified that the goods were uploaded into the Country B registered sea vessels, thus proving export. However, trade and export declaration documents did not disclose any Bills of Lading for the shipment or any references to bills of lading and insurance in the export declarations.
358. A surveillance operation on one of the sea vessel led to the detention of the sea vessel while unloading a consignment of beer/liquor, using feeder crafts, at a place in Malaysia that was not a legal landing place or a place of import after leaving the Malaysian port en route to Country B. The vessel's captain and 11 crew members were subsequently charged in the Malaysian Courts leading to the forfeiture of the sea vessel.
359. In 2012, verification with Customs records in Country B confirmed that there was no evidence of imports into Country B from Malaysia, thus proving the lack of legitimate trade. The intermediary who dealt with the two consignees in Country B was found to be a nominee of the Malaysian exporter. The sea vessel was also registered in the name of the nominee. The case is currently being investigated for customs tax evasion and money laundering offences.



SRI LANKA

360. Mr A, Mrs A and Mr B (brother of Mrs A) were directors of a company “K” registered under the Board of Investment (BOI) of Sri Lanka. Since its registration they enjoyed various benefits such as tax holidays. Further, Mr and Mrs A formed another company in country “U” and transactions were carried out using these two companies.
361. Investigations by Sri Lanka Customs revealed that the company in country U was exporting goods with high value to Sri Lanka (the importer in Sri Lanka is company “K”). However, in the Customs Declaration these goods were declared as low value items denying a considerable amount of Customs Duties to the Government. Investigations further revealed that the two companies had collectively smuggled 22 shipments on previous occasions before being detected by the Customs Officials.

4.10 Association with human trafficking and people smuggling

FIJI

362. Immigration officials intercepted three girls at Nadi International Airport in October 2012. They told the Immigration authorities that they were going to work at a local massage parlour; however, they did not have work permits.
363. Investigations and interviews with the three girls revealed that two foreigners residing in Fiji and a Fiji national had facilitated the trafficking of the three girls.
364. The first accused is a Thai National. He was charged with three counts of Trafficking in Persons: Contrary to Section 112 (5) of the Crimes Decree, 2009. He has been charged as being a facilitator of human trafficking. The second accused is a citizen of the United Kingdom. He has been charged with three counts of Trafficking in Persons: Contrary to Section 112 (5) of the Crimes Decree, 2009. He has also been charged as being a facilitator of human trafficking.

365. The third accused is a Fiji national. He has been charged with three counts of Domestic Trafficking in Persons: Contrary to Section 115 (3) of the Crimes Decree, 2009. He has also been charged as a facilitator of human trafficking.
366. Another Fiji citizen who is a former Asian national has been charged with Rape: Contrary to Section 207 (1) and (2)(a) of the Crimes Decree, 2009. He has been charged as a principal in the second degree. That is, someone else committed the rape but he (by virtue of a joint enterprise) is also culpable. He has also been charged with three counts of Sexual Servitude: Contrary to Section 106 (1) of the Crimes Decree, 2009.
367. The victims are all Thai Nationals. There are three victims and these charges relate to each accused person's individual degrees of participation in respect of their interactions with the three victims over the course of 5 – 9 September 2012. All accused persons are currently remanded in custody.

SAMOA

368. Several cases of suspected human smuggling, involving suspected offenders originating from foreign countries, have been under surveillance by the Police and Transnational Crime Unit (TCU).
369. In all of these cases, large amounts of cash were declared at the airport to support the passenger's travel (\$50,000 Samoan Tala [USD21,490] upwards). All claimed to be travelling to Samoa as a tourist. Authorities found that the first thing these people did after arriving was to try and apply for visas into New Zealand/Australia. When denied, they would apply for visas into American Samoa. They showed no signs of exploring Samoa.
370. Risk assessment and analysis indicates that Samoa is exposed to being used as a transit point for these activities. All have departed the country and some have claimed asylum in other countries in the Pacific. Unfortunately, due to lack of proper laws and regulations, authorities could only monitor their movements.
371. The revised Crimes Bill 2012 which should be passed by Parliament soon provides a proper legal framework for authorities to effectively prosecute and govern such criminal activity in the future.

SRI LANKA

372. Customer "R" opened a Current and Savings Account at a local commercial bank on 11th May 2012. On 11th and 14th May he deposited LKR 13 million (USD 101,088) into his account in cash. During the same period a newspaper article published revealed that Mr R had been arrested by law enforcement authorities on the suspicion that he had organized people for illegal migration.
373. Based on the suspicion of human smuggling the bank filed an STR with the FIU. Immediate steps were taken by the FIU to suspend banking transactions on the account maintained by Mr R.

374. Law enforcement authorities were able to arrest people who were waiting for illegal migration and evidence given by them revealed that they had given large sums of money to Mr R as his fees.

THAILAND

The case of human trafficking offence committed by a karaoke restaurant used as a front to cover a prostitution business

375. A karaoke business was established as a front business that lured a number of women for prostitution. Thai police officers raided the place and rescued the victims.

376. The offender was later charged with a criminal offence and the case was referred to the Anti-Money Laundering Office (AMLO) to pursue civil forfeiture. Finally, the offender's property, which included cars, land and an apartment building were seized, with a total value of nearly 20 million baht (approximately USD 6,666,000).

4.11 Use of nominees, trusts, family members or third parties

AUSTRALIA

377. AUSTRAC information assisted a law enforcement investigation that led to the arrest of a suspect who had laundered a significant amount of cash raised through drug trafficking. The investigation found the suspect had used a variety of methods to launder the money:

- The suspect arranged for a family member to deposit the illicit cash into a number of different bank accounts held by that family member.
- The accounts were held at a number of different institutions to avoid arousing the suspicion of any one financial institution.
- To further avoid scrutiny, the cash deposits were structured to fall below the AUD10,000 transaction reporting threshold.
- The suspect then purchased a legitimate business and established an associated corporation.
- The proceeds of crime were periodically withdrawn by cheque from the family member's accounts and deposited into the company account operated by the suspect.
- The cheque deposits were subsequently explained by the suspect as being a loan from the family member to pay the purchase price of the business.

378. More than AUD420,000 was laundered using these techniques.

379. The investigation also uncovered more than AUD650,000 in cash that the offender had hidden in a shed. Law enforcement officers ultimately charged the suspect with money laundering.

FIJI

380. The Cybercrime Unit of the Fiji Police Force received two reports last year whereby a total of \$12,500 (USD6,782) was illegally transferred from a business bank account to another unrelated account in the same bank. The money was withdrawn by the account holder and handed over to a third party (suspect) who, after taking his share remitted the balance of the funds to Nigeria.
381. The suspect sent about \$8,000 (USD4,340) from a foreign exchange dealer on different occasions over a period of five days. The suspect used the identification (ID) of various third parties and managed to remit the funds to Nigeria. The remittances were reportedly facilitated by the money remittance agency who allowed the suspect to remit the funds using different names and identification (in the absence of the ID owners) to different beneficiary customers in Nigeria.
382. The case is under investigation by the Fiji Police Force.

INDONESIA

Bahasyim Asyi'efie Case

383. In Indonesia's latest high-profile corruption verdict involving a tax collector, former Jakarta tax office director Bahasyim Assifie was convicted of corruption and money laundering related to bank accounts worth more than USD7 million in the names of his wife and children. He was sentenced to 10 years in prison.
384. Part of the Indonesian FIU's Analyst Result, which was disseminated to the investigator, claimed that the Rp66 billion (USD7.3 million) in his accounts did not come from honest sources.
385. Bahasyim's claims that he invested the money abroad and ran a jewellery business were not supported by convincing evidence, the judge said. His business partners in the Philippines and China had presented statements that they jointly ran several businesses with Bahasyim, but those statements were one-sided and prepared only after the case was prosecuted.
386. It is believed that the defendant collected Rp60 billion plus USD681,000 between 2002 and 2009 through illegal means by misusing his position and authority as a civil servant. The judge said Bahasyim, in his official report to the Corruption Eradication Commission (KPK), claimed that his fortune was valued at only Rp10 billion.
387. Investigations found that Bahasyim, 58, kept his money in bank accounts in the names of his wife, Sri Purwanti, and his daughters, Winda Arum Hapsari and Riandini Resanti. Winda, who had Rp17 billion in one of her accounts, was still a student when the accounts were opened.
388. As a civil servant, the defendant normally received only Rp20 million to Rp30 million per month, the judge noted. In addition to the prison time, the panel also ordered the money in the family accounts to be seized by the state.

389. Indonesian Financial Transaction Reports and Analysis Centre (INTRAC) found over 300 transactions involving the family accounts worth a total of around Rp932 billion (USD 93,624,117).
390. Bahasyim regularly circulated the money among the various family accounts in transactions so numerous that they raised suspicion at INTRAC.
391. Bahasyim also bought a house worth about Rp8 billion (USD803,640) in Jakarta's upscale Menteng district in 2005 and registered it under his son's name. The defendant said the money was meant as business loan to a company belonging to his son, Kurniawan Arifka. Bahasyim also failed to present evidence of a business agreement or other deal to support the claim that the money was meant as an investment, said the panel.
392. Bahasyim became director of tax examinations and investigations in the Jakarta tax office in October 2002, with the power to interrogate taxpayers, seize documents, launch searches and recommend legal action. He held several positions in the Jakarta Tax Office between 2002 and 2007, and was moved to the National Development Planning Agency (Bappenas) in 2008.

MACAO, CHINA

393. Mr X made transfers from Bank A to Bank B, amounting to over \$6 million shortly after opening an account in Bank B. After such transfers, Mr X then used a third party as a nominee to buy/sell shares in overseas capital markets.
394. Mr X got a significant gain by selling all the shares shortly after the share price sharply rose up. The same transaction pattern repeatedly happened in the following weeks. Mr X finally cashed out all the gains which were almost double from his investment capital.
395. After the FIU's investigation, it was found that there were a lot of STRs related to these overseas listed companies. These companies had been abused for a long time as a puppet in the hands of speculators who had ties to the chairmen of these companies. The chairmen were being accused of market manipulation and insider trading.

MALAYSIA

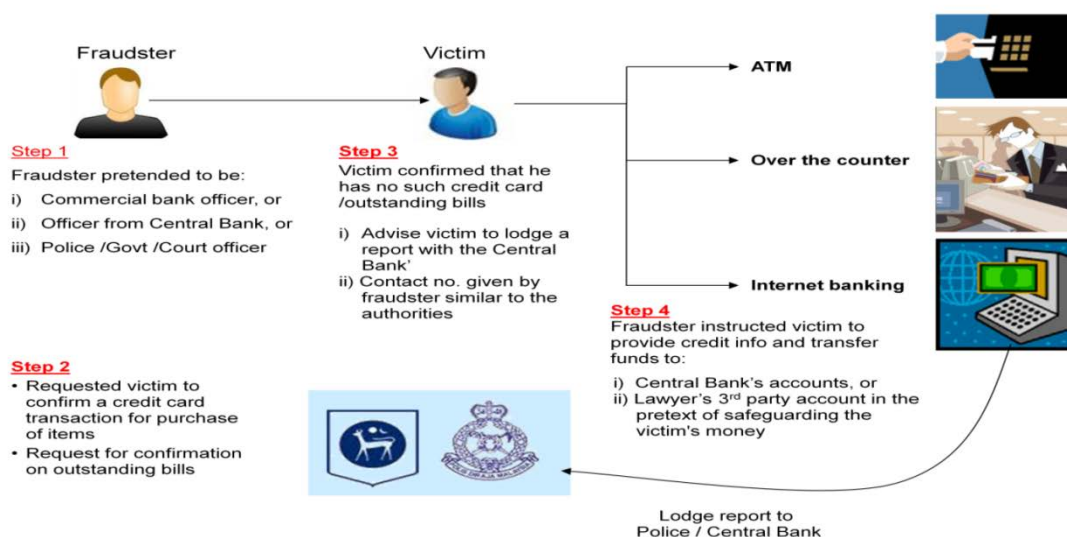
Scam Using Third Party's Accounts

Methods used:

- Use of nominees, trusts, family members or third parties etc.
- Use of internet/tele-communication technology.

396. A syndicate scammed victims into transferring their monies into third parties' accounts by making phone calls to the victims. The fraudster would claim to be an officer from the central bank or police headquarters or a commercial bank who was investigating the victim's bank account for suspected irregular activities. For example, alleging that the victim's credit card has been abused for purchasing merchandise locally/abroad.

397. Victims were instructed not to hang up the phone while the fraudster transferred the call to supposedly the relevant investigation department officers. The technology used by scammers is called spoofing via Voice over Internet Protocol (VoIP) which enables the telephone number of the relevant authorities or banks to be displayed on the phone.
398. As the victims were convinced that they were speaking to officers in the relevant authorities/banks, victim were then told to transfer money to a 3rd party account in the pretext of safeguarding the victim's money or to make payment to a special account pending investigations to avoid being charged in court.
399. Investigations revealed that the syndicate advertised in the local newspapers to target and recruit individuals comprising mainly youths/students/lower income job holders to create a pool of 3rd party savings accounts.
400. The third party accounts were opened with a minimum deposit amount and were then used to receive the funds deposited by the victims shortly after the opening of the account. This was then followed by immediate withdrawals in cash within one (1) hour. Third party account holders were reported to receive between RM250 (USD76) to RM1,000 (USD306) plus commission for every account opened and when monies were successfully transferred by victims. The case is currently being investigated for cheating and money laundering offences.



SINGAPORE

401. Tan Wei Chong was a relationship manager with the Overseas Chinese Banking Corporation. Between October 2009 and August 2010, in the course of his work, he misappropriated customers' funds totalling USD4.72 million and EUR 88,122. The Commercial Affairs Department (CAD) investigation revealed that Tan Wei Chong withdrew monies from the accounts of four customers in 23 transactions.
402. He submitted forged documents to his bank colleagues to deceive the bank into believing that the account holders were applying to transfer funds from their accounts. He used the same ruse to make eight cash withdrawals from the accounts. In these fraudulent transactions, he either used forms signed in blank by the account holders or simply forged their signatures on the documents.

403. To avoid detection, Tan routed the monies taken from the customers' accounts through bank accounts of his family members and he eventually withdrew the money in cash. All that money was spent on his gambling habit. Tan Wei Chong was betting excessively with internet casinos and soccer gaming sites.
404. On 1 June 2011, Tan Wei Chong was charged in court for 31 counts of cheating and 15 counts of money laundering. On 29 June 2011, he was sentenced to seven years' imprisonment after pleading guilty to 11 cheating charges and four money laundering charges.

THE PHILIPPINES

405. FB is a former high-ranking officer of NN Bank's Wealth Management Group which catered to high value clients with bank deposits of less than Php4 million (USD92,724). FB allegedly lured clients into investing with him by promising higher interest rates for time deposits than what NN Bank offered and high referral fees over the standard rates.
406. On 25 February 2011, NN Bank requested the FIU for an investigation and subsequent filing of a criminal complaint for money laundering against FB. According to NN Bank, FB, by virtue of his position of trust and confidence as Relationship Manager in NN Bank in its X Branch, embezzled at least USD14 million from his clients' accounts. FB simulated bank transactions in order to withdraw clients' funds without their knowledge and authorization. Thereafter, the funds were appropriated by FB and transferred to beneficiaries who had no connections at all to these clients.
407. FB's fraudulent schemes were committed using the following means: (1) unauthorized funds transfer; (2) fictitious time deposit transactions; and (3) fictitious investment products allegedly purchased from FF Financial Services.
408. Under the first scheme to defraud the depositors, FB caused the unauthorized fund transfers by withdrawing his clients' funds, or transferring such funds directly to his account or to the accounts of his beneficiaries or third parties. These withdrawals and fund transfers were made without the clients' consent or authorization, evidenced by the case withdrawal receipts with forged signatures and unauthorized applications for fund transfers.
409. Under the second scheme, FB was able to obtain deposits from his clients by enticing them to invest in fictitious time deposit transactions. The database of NN Bank shows that none of the purported time deposit confirmation forms were entered into the bank's system for processing; hence, these time deposits were fictitious and non-existent.
410. Under the third scheme, FB was able to entice customers to part with their funds by offering them fictitious investment products, such as fixed income investments, unit investment trust funds and registered mutual funds, allegedly offered by FF Financial Services. It was found that the documents, representing the investment products issued by FB to his customers, were falsified and non-existent based on the records of FF Financial Services.

411. Through these schemes, FB was able to defraud his depositors in eighty-two (82) transactions, with a total amount of Php97 million and USD832,000.
412. FB implemented the “hold mail” on all notices and statements and changed the registered mailing addresses without the client’s knowledge or consent by replacing the same with the home address of a staff member, or his father’s office, in order to prevent the client from receiving notices or statements which would reflect the fraudulent transactions.
413. FB tampered with some funds in order to utilize these unlawfully taken monies from the clients’ accounts to run his National Basketball Association (NBA) cards trading business. Using these embezzled funds, he imported NBA cards from Country U through an entity named W Distribution and sold them through the internet to clients from Country U and Country R.
414. FB used other persons and entities as beneficiaries of the stolen funds in order to run his NBA trading cards business and his money laundering activities. Funds that were obtained from clients’ accounts were issued in the form of a manager’s cheque, or were transferred to, or were the subject of fund transfers to, the accounts of:
1. His two partners, namely: EA of EA’s Toy Car Shop, and Mr TA of TAE Collectibles.
 2. Mr SW, DG and W Distribution.
 3. SVG Development Inc. and SVG Corporate Holdings.
 4. PK, GE and RU.
 5. Mrs BCC, thru the latter’s foreign exchange dealership; and OL and Ringside Inc.
415. These persons and entities were consistently made the beneficiaries of the fraudulent transactions. W Distribution received as much as USD2.894 million.
416. Based on the FIU’s investigation, it was confirmed that the dollar account of EA’s Toy Shop with Account No. 444 in NN Bank was held jointly by EA and FB who both opened the said account. There were fund transfers from this account to the account of SW and W Distribution.
417. It was also found out that various movements/transfers of funds between the accounts of FB, SVG Development Inc., GE; PK and RU. FB, GE and PK and RU were among the shareholders of SVG Development Inc. and SVG Corporate Holdings.
418. In 2009 and 2010, FB acquired three vehicles: Mercedes Benz C200 and E300 and Mazda CX-7.
419. BCC was also the beneficiary of at least twenty-three (23) fraudulent transactions made by FB. An analysis of the database search showed that for every debit transaction/movement against the account of FB, a corresponding credit was also made on the account of BCC and/or Cano Mart.
420. Investigation reports also showed that FB processed at least forty-one (41) fraudulent transactions where OL and Ringside Inc. were the beneficiaries. In these transactions, FB, without authorization from his clients, purchased Manager’s cheques from the accounts of two clients and deposited these cheques

in the names of OL, Ringside Inc. and its directors JL and HS. The total amount of the fraudulent transactions is Php33.070 million (USD 766,574).

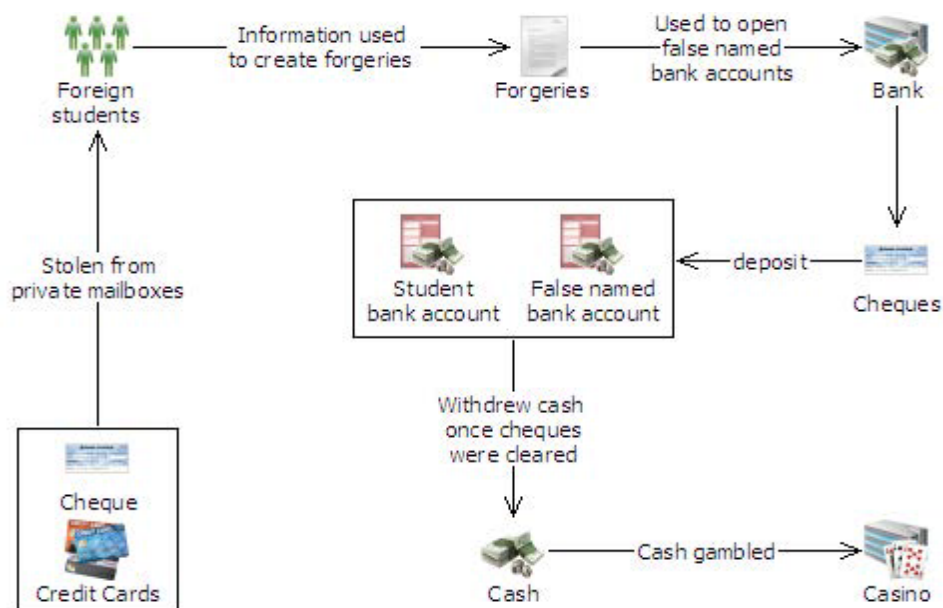
- 421. Investigation by the FIU disclosed that FB held various accounts with FF Bank located in Country K.
- 422. A petition for civil forfeiture has already been filed by the FIU against the funds that were generated by the frauds committed by FB and his cohorts.

4.12 Gambling activities (casinos, horse racing, internet gambling etc.)

AUSTRALIA

Asian crime syndicate recruited foreign students to steal and launder money

- 423. An Asian crime syndicate, which included an expert forgery artist, recruited foreign students to open bank accounts, steal mail and launder stolen cash. The students were among a number of third parties, also referred to as ‘runners’, enlisted to commit crimes for the syndicate.
- 424. The scam began with the theft of cheques and credit cards from private mailboxes. The stolen documents were altered to create forgeries of sufficient quality to deceive bank tellers. The foreign students would deposit the cheques into their own bank accounts or accounts set up using false names.
- 425. When a cheque cleared, the money was withdrawn and gambled at casinos to mix or co-mingle it with legitimate cash – a common money laundering methodology.
- 426. An investigation uncovered more than 350 falsely named bank accounts that had more than AUD8 million laundered through them. Suspicious matter reports (SMRs) submitted by banks indicated that one member of the syndicate had made regular deposits below the AUD10,000 threshold for reporting cash transactions to AUSTRAC.
- 427. One suspect was arrested and charged with eight counts of dealing with the proceeds of theft. The individual had allegedly stolen a cheque for more than AUD500,000 from a deceased estate. The individual attempted to launder the proceeds of the fraudulently obtained cheque through a casino.
- 428. A second suspect was arrested and charged with six offences, including making a false document to obtain a financial advantage. A third suspect was also arrested and charged with identity fraud and money laundering offences.



429. Indicators in this case included:

- Customer making large cheque deposits despite having no known source of income.
- Customer undertaking transactions that appear inconsistent with their profile and transaction history.
- Large-value cheque deposits into newly opened, or student, bank accounts followed by immediate cash withdrawals once cleared.
- Structuring of cash deposits to avoid reporting requirements.
- Use of false identification to open bank accounts and conduct transactions.

HONG KONG, CHINA

430. In 2010, a bookmaking syndicate placed a substantial amount of bets on horse races with the Hong Kong Jockey Club (HKJC) so as to off-set the risk of illegal bets received outside Hong Kong.

431. The concerned HKJC betting accounts and bank accounts had handled over HK\$743 million (USD95,762,950) since 2012. In June 2012, the investigation turned over with 16 persons arrested and HK\$22 million in the involved HKJC betting accounts and HK\$5.7 million in the relevant bank accounts withheld.

4.13 Abuse, misuse, direct operation of non-profit organisations

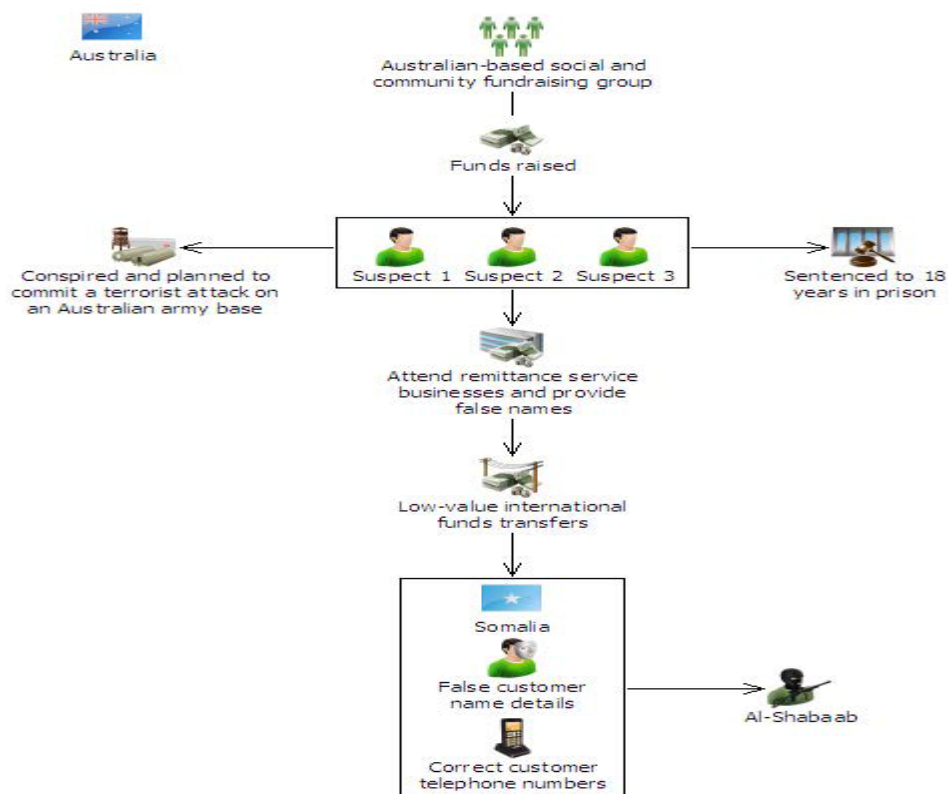
AUSTRALIA

Australian terror suspects sent funds to Somalia to support terrorist group

432. A joint-agency investigation led to the arrest of five suspects on charges of conspiring to commit a terrorist attack on an Australian army base. Investigations revealed the group had sent funds destined for use by the Somalia-based terrorist

group, al-Shabaab. The group had also facilitated travel for Australian-based supporters to attend overseas military training camps. Funds remitted offshore by the suspects did not go directly to al-Shabaab but to entities linked to al-Shabaab's activities in Somalia.

433. Investigating officers, assisted by AUSTRAC information, discovered that the suspects had sent thousands of dollars in low-value IFTIs to Somalia. Authorities suspected these IFTIs were to support the aims of al-Shabaab and associated military training activities overseas.
434. The suspects sent the funds via remittance service businesses, often using false names for the overseas beneficiary customer to obscure the money trail. However, the telephone numbers recorded in the IFTIs for the overseas customers were correct.
435. Investigating officers concluded that the suspects used the customers' correct phone numbers to ensure the funds arrived safely and were handed to the correct customer in Somalia. In this case, the information reported in the IFTIs was valuable intelligence for the investigation officers to use to corroborate other information or consider leads in the investigation.
436. In general, the group members paid for the remittances to Somalia using their own funds. The group also remitted funds that had been raised by Australian-based social and community fundraising groups – a common terrorism-financing method internationally. There was no evidence to suggest that members of the social and community groups involved were aware that the funds being raised were to be remitted to East Africa in support of al-Shabaab.
437. Three suspects were found guilty of conspiring to plan an Australian-based terrorist attack and were sentenced to 18 years jail to serve 13 years and six months. Two of the suspects were found not guilty.



438. This case involved offences of conspiring to plan a terrorist attack and involved the use of remittance services. Indicators included:

- Low-value international funds transfer to a high-risk jurisdiction.
- Use of false identification when sending funds offshore.

CHINESE TAIPEI

439. In December 2009, the AMLD received an STR indicating some staff of Hsing X Senior High School regularly withdrew funds from the account of the school by cash or cheques and deposited the funds into some personal accounts. After analysing, AMLD disseminated the information to the Investigation Bureau.

440. The investigators found that Mr Gu served as the Chairman of Hsing X Senior High School and the Board Member of Hsing X Institute of Technology. The school's income and expenditure should have been recorded according to the school accounting system.

441. In order to pay off personal debts, Mr Gu abused the duty of controlling the board in both schools and used the school's finances to open another account in name of the schools without it being subject to the school's accounting supervisory system. Mr Gu used the school's certificates of deposit to borrow a large amount of money and deposited the loans into the above mentioned account.

442. When the competent agency conducted audits, Mr Gu paid off the loans and used the certificate of deposit for loan cycling up to 1,548 times to a total of NTD15.6

billion (over USD520 million) and concealed the proceeds of crime through the bank accounts of staff members.

443. The case was referred to the Banciao District Prosecutor's Office on August 15, 2011. And the abovementioned suspect was prosecuted and sentenced to seven years in prison in January 2012.

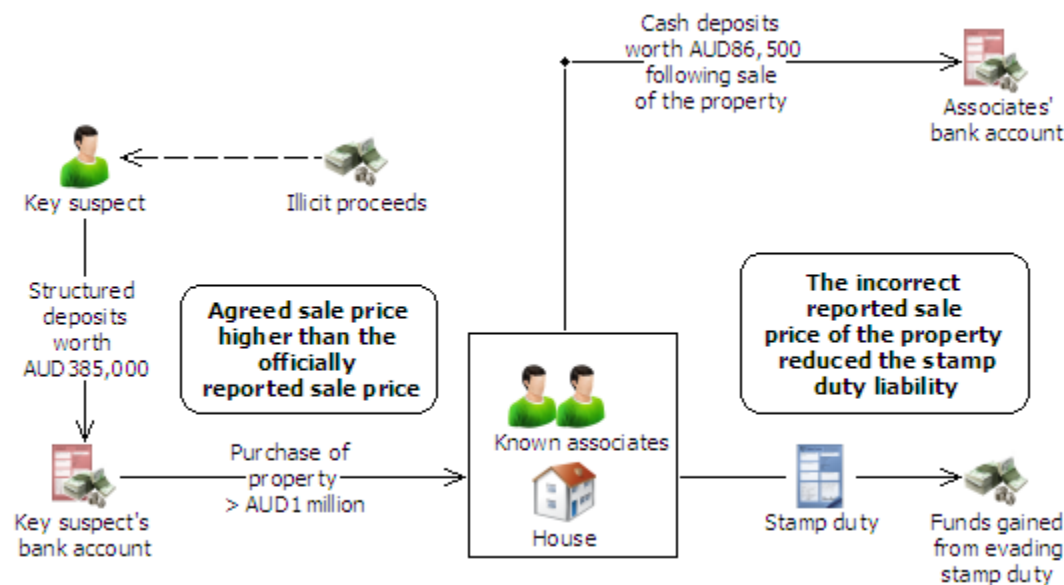
4.14 Purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.)

AUSTRALIA

Missing stamp duty led authorities to uncover large-scale cocaine importations

444. A joint-agency investigation into cocaine distribution was initiated by law enforcement agencies, with AUSTRAC information proving to be of vital importance. The investigation uncovered a large-scale drug importing syndicate operating within Australia.
445. Law enforcement agencies were made aware that a key suspect had recently purchased a home for more than AUD1 million from two known associates. Further enquiries revealed that the purchase was partially financed through a series of structured cash deposits totalling approximately AUD385,000.
446. Law enforcement agencies investigating the suspicious purchase searched AUSTRAC's financial transaction data. They found nine cash deposits totalling more than AUD86,000 were made by the vendor of the property following the sale. These deposits suggested the vendor received additional cash funds after the sale of the property. This indicated the actual sale price was higher than the officially reported sale price and this would have reduced the stamp duty liability. This activity is an indicator of money laundering and a methodology for stamp duty evasion.
447. Further investigations into a number of suspects revealed that over an 18-month period, one suspect made 114 structured cash deposits totalling more than AUD600,000. During this time, a second suspect had deposited approximately AUD360,000 in 50 structured deposits. This activity appeared to be a further attempt to launder the proceeds of crime.
448. At that stage, law enforcement agencies believed that a number of suspects were conspiring to import drugs into Australia. AUSTRAC alerted the law enforcement agencies to one suspect and his family who had sent multiple international funds transfers to Lebanon, with a total value of approximately AUD100,000. Law enforcement agencies, using AUSTRAC information, investigated the circumstances around the money sent to Lebanon. As a result, a series of search warrants were executed at a number of locations.
449. As a result of this joint-agency operation, 13 people were arrested and charged with offences relating to possession of drugs, firearms offences and money laundering. In addition, AUD13.5 million in cash, two kilograms of cocaine, 17 firearms, a number of prestige cars and a house were seized.

450. Seven of the 13 persons arrested were sentenced to jail for periods ranging from five to 30 years. Four persons, who assisted the key syndicate members in laundering the proceeds of crime, received good behaviour bonds.



451. This case involved both use of banking channels and real estate transactions. Indicators from the case were:

- Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history.
- International funds transfers to a high-risk jurisdiction.
- Structured deposits into a bank account, used to purchase high-value assets (real estate).
- Structuring of cash deposits over an extended period to avoid reporting requirements.

FIJI

452. The Fiji Police Force uncovered a drugs case with a street value of FJ\$4 million (USD 2,170,391). The drugs (marijuana) were cultivated by villagers on an island located north of Fiji. The proceeds from the sale of the drugs were used to purchase:

- Household items such as flat screen television sets, DVD players, beds, sofa sets, tables and chairs, gas stoves.
- Fibreglass boats and outboard engines.
- Building materials such as timber, roofing irons, concrete blocks, and solar panels.

HONG KONG, CHINA

453. Members of an international crime syndicate established shell companies and opened bank accounts in Hong Kong to dissipate crime proceeds through buying gold bars, diamonds and real estate in Hong Kong.

454. Investigations resulted in a total of eight foreign nationals arrested and HK\$85 million (USD10,955,268) worth of crime proceeds seized. Four of those arrested were charged with money laundering, with proceedings for restraining and confiscating HK\$150 million crime proceeds in progress.

INDONESIA

Malinda Dee Case

455. INTRAC, Indonesian FIU, established a dedicated team to develop intelligence and worked intensively with The National Police (Criminal Investigation Division Investigator).
456. INTRAC informed the Police of every new finding on an hourly basis by studying the money-laundering indications in 36 suspicious transaction reports from two insurance firms and nine banks. INTRAC also conducted a special audit of Citibank, recommending the bank to strengthen its “know your employee” policy and improve its know your customer principles, particularly for private banking.
457. The investigation identified that Malinda embezzled money and laundered around Rp40 billion (USD4.4 million) from wealthy clients at Citibank Indonesia between 2007 and February 2011.
458. She had carried out 117 illegal transactions, 64 of which were in local currency and 53 of which were in US dollars. She allegedly stole the money by falsifying transfer documents and transferring funds to a variety of recipients, including her sister Visca, Malinda’s common-law husband Andhika Gumilang, Visca’s husband Ismail bin Janim and three of Malinda’s companies. Malinda used four identity cards to conduct the frauds, whereas Andhika was found to be in possession of seven fake identification cards which were used to open bank accounts for Malinda’s money.
459. Andhika Gumilang, Ismail and Visca were sentenced for several years in prison for money laundering for their part in helping to hide illicit funds embezzled from Malinda’s wealthy Citibank customers.
460. Likewise, the South Jakarta District court sentenced Malinda Dee to eight years in jail after she was found guilty of the embezzlement of well above USD4.4 million from customers’ accounts between 2007 and February 2011 and laundering the stolen funds through other bank accounts in an attempt to cover her tracks.
461. The court also seized two Ferrari, a Porsche, a Hummer and a Mercedes Benz which were bought by Malinda using stolen money.
462. Bank Indonesia also imposed sanctions on Citibank, following the Malinda embezzlement case. The bank was prohibited from signing up new customers for its premium wealth services for one year.

MACAO, CHINA

463. Ms Q was a premier customer of a bank in country A. Her bank account suddenly received a large remittance and then she transferred it into her credit card account for purchase of jewellery.
464. Previous transaction records showed that she had the usual pattern of making payment in advance to her credit card account, and there were also other frequent transactions incurred in various famous-branded boutiques and jewellery stores every month.
465. According to the information gathered by the FIU, it was observed that Ms Q was using her credit card account to transfer funds from overseas by way of purchasing jewellery with her credit card.

4.15 Investment in capital markets, use of brokers

AUSTRALIA

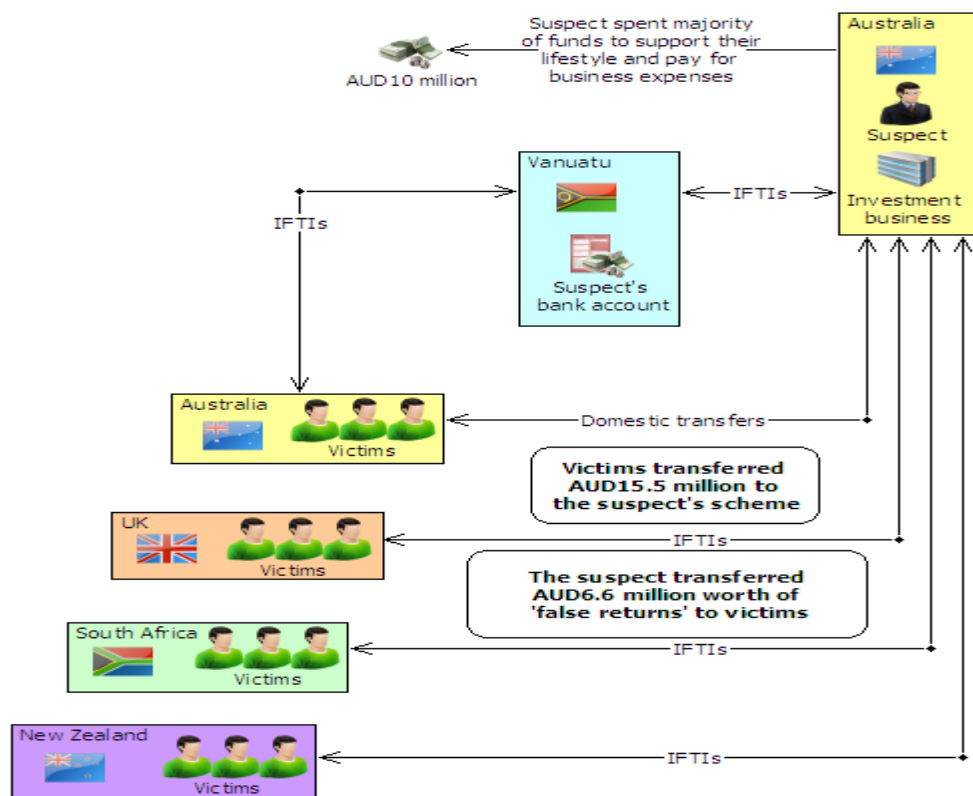
466. Some investment fraud also involves substantial planning and organisation and uses sophisticated methods and techniques. Professional facilitators such as lawyers, accountants and money remitters play a key role in providing access and opportunity for criminals. As regulations are tightened, this specialised involvement is likely to increase.
467. Agencies that are stakeholders in relation to this type of offence include the Australian Securities and Investments Commission, the Australian Prudential regulation Authority, the Australian Taxation Office, the Australian Federal Police, Treasury and Finance departments and other agencies responsible for regulating the finance sector and industries affected by the activity. The effective operation of the business and financial sectors is integral to a prosperous economy and the intrusion of organised crime groups is cancerous and difficult to remove once it has taken root.

Conned investors lost millions in investment Ponzi scheme

468. A law enforcement agency conducted an investigation into a suspect who operated a Ponzi scheme in which approximately 220 victims lost more than AUD15.5 million they believed had been invested legitimately.
469. Over a nine-year period the suspect maintained a facade of heading a successful investment business. As the director of a group of companies, the suspect claimed to operate a legitimate managed investment scheme, including self-managed superannuation funds (SMSFs). The suspect claimed to trade in global derivatives and equity markets, promising extraordinarily high returns to potential investors.
470. The scheme grew by word of mouth with friends, relatives and acquaintances of the suspect and victims investing in the scheme. Victims of the scheme were from Australia, South Africa and the United Kingdom. While some victims

initially received money from their investment, the majority lost their investments, including family inheritances, retirement funds and savings.

471. AUSTRAC information contributed to the investigation by identifying bank accounts, international funds transfer instructions (IFTIs) and transactions made by victims. AUSTRAC information identified bank accounts in Vanuatu linked to the suspect. Some victims reported signing contracts and transferring money to a company based in Vanuatu. AUSTRAC information indicated that money transferred to Vanuatu was later transferred to Australia, predominantly for the benefit of the suspect.
472. All IFTIs linked to the scheme were made through banks and some incoming IFTIs represented transfers from overseas victims. AUSTRAC information showed that over a four-year period:
 - Incoming IFTIs totalled more than AUD1.4 million, with the majority of the funds transferred from Vanuatu and New Zealand. IFTIs were also received from the United Kingdom.
 - Outgoing IFTIs totalled more than AUD610,000, of which more than AUD500,000 was transferred to Vanuatu.
473. Analysis of the transaction data showed most of the funds the suspect received from victims were applied for purposes other than investment. Of the AUD15.5 million received from victims, AUD6.6 million was returned to investors as either 'false returns' or as payments when investors left the scheme. More than AUD2.8 million was invested in high-risk derivative trading which returned only AUD900,000.
474. More than AUD10 million was spent to support the suspect's lifestyle and pay for business expenses. Significant business expenses were outlaid to maintain the illusion of a successful managed investment scheme, including rent for a well-appointed office in a popular location.
475. Subsequent analysis of financial data showed monthly transfers between AUD30,000 and AUD50,000 from the accounts of the group of investment companies to the suspect's credit card account. The suspect also raised more than AUD36,000 in donations for two charities, which the suspect used for personal and investment purposes.
476. The suspect was charged with seven offences relating to fraud and forgery, and was sentenced to 13 years imprisonment.



477. Jurisdictions involved in this fraud-related money laundering included Australia, New Zealand, South Africa, United Kingdom and Vanuatu. Indicators included:

- High-value international funds transfers to/from Australia for no apparent logical reason.
- High-volume account activity involving significant amounts of funds.
- International funds transfers to a high-risk jurisdiction.
- Multiple customers conducting international funds transfers to the same overseas beneficiary.
- Use of overseas bank accounts.

FIJI

478. FIU received a request for financial information from the Fiji anti-corruption authority. The request involved a prominent medical practitioner, Mr X. The FIU's checks revealed that Mr X and his family maintained investment accounts at a local investment broker. The breakdown of the investment accounts were as follows:

- Mr X - valued at \$37,075 (USD20,116)
- Wife of Mr X - valued at \$31,600 (USD17,146)
- Son of Mr X - valued at \$43,300 (USD23,494)

479. The total value of the investment accounts maintained by Mr X and his family was \$112,000 (USD60,770).

MACAO, CHINA

480. A foreigner, Mr Y, came to Macao SAR, China and setup an offshore investment company and opened a bank account under the company's name.
481. Mr Y also setup a website to demonstrate the investment company's background and achievements for potential investors, stating that the company had a strong investment team that could help to invest in stocks with a high return in short period of time. Mr Y started reaching out to clients worldwide by phone and email to persuade them to invest funds in stocks.
482. As a result, a number of clients around the world remitted funds amounting to over USD8 million to the investment company's bank account. After receipt of the funds, the balance was transferred out and the account was cancelled. As per the incident reported, and after investigation, two of the victims reported in person to claim and the suspect was identified. The case is still in the process of further litigation.

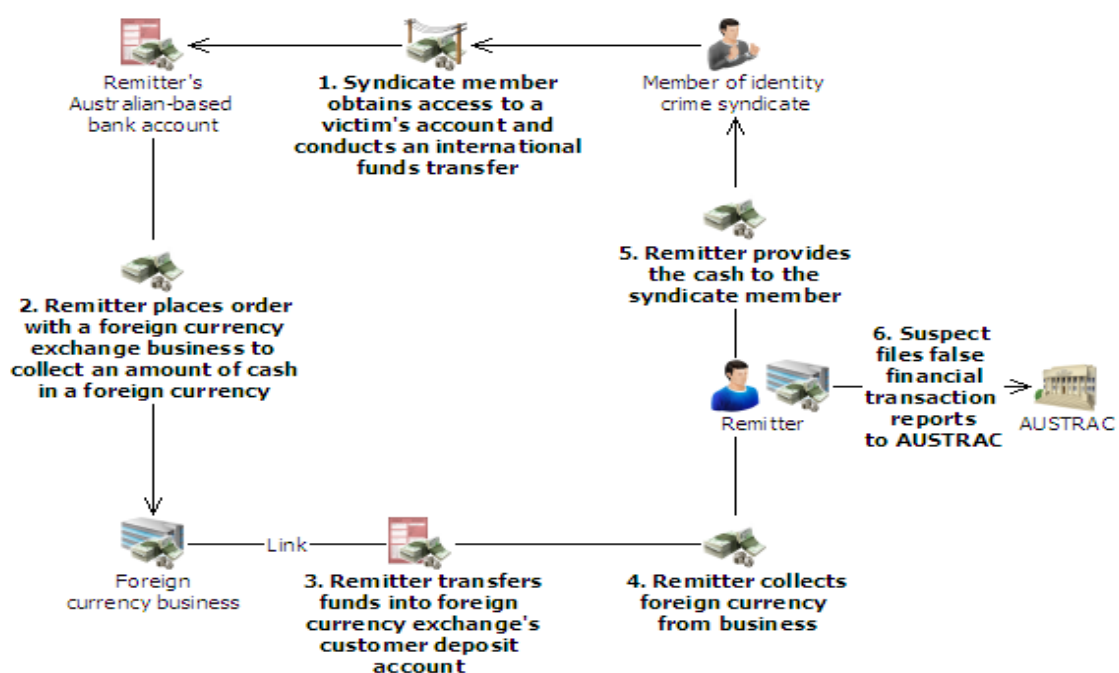
4.16 Mingling (business investment)

AUSTRALIA

Money laundering remitter jailed after sending false reports to AUSTRAC

483. Law enforcement conducted an investigation into a remittance service provider suspected of falsifying customer information on transaction reports and submitting false information to AUSTRAC to facilitate money laundering.
484. AUSTRAC information was critical to the law enforcement investigation to help identify that the remitter and his remittance business had assisted a criminal syndicate with laundering the proceeds of identity fraud.
485. The identity fraud involved money fraudulently withdrawn from the bank accounts of innocent third parties. A key element in the laundering of criminal proceeds involved the remitter disguising the funds and concealing the identity of members of the criminal syndicate.
486. The typical activity undertaken to launder the illicit funds involved:
1. A member of the identity crime syndicate would obtain access to a victim's account and arrange for funds from the account to be sent as an international funds transfer instruction (IFTI) into an Australian account operated by the remitter.
 2. The remitter would place an order with a foreign currency exchange business to collect an amount of cash in foreign currency equivalent to the value of the stolen funds.
 3. Using the stolen money, the remitter would transfer funds into the foreign currency exchange's customer deposit account.
 4. The remitter would visit the foreign currency exchange to collect the foreign currency.
 5. With the original stolen funds now laundered into foreign currency, the remitter would provide the foreign currency, less a commission, to a member of the criminal syndicate.

6. As a last step in concealing the money trail, the remitter would file a significant cash transaction report (SCTR) with AUSTRAC detailing the payment to the syndicate member, but using false identification details to conceal the recipient's true identity from authorities.
487. Analysis of financial transaction activity by law enforcement, supported by AUSTRAC analysts, revealed the remitter had reported approximately AUD3.5 million in SCTRs over a two-year period.
488. Further law enforcement investigation found that the majority of recipients recorded in these transaction reports could not be identified or did not exist. Over this same period, 15 foreign exchange transactions were reported to AUSTRAC totalling over AUD1.1 million. The value per transaction ranged between AUD10,000 and AUD 200,000.
489. AUSTRAC also received suspect transaction reports (SUSTRs) relating to the remitter's financial transactions with other reporting entities. Information within the SUSTRs, combined with further analysis of personal financial transactions undertaken by the remitter, revealed a range of suspicious activity, including:
- the remitter's reluctance to explain the source of funds to bank staff;
 - the depositing of large amounts of cash into an account followed by an international funds transfer on the same day;
 - the use of third parties to make international funds transfers on the remitter's behalf.
490. The law enforcement investigation collected evidence confirming the remitter was involved in money laundering on behalf of third parties. The remitter was charged and convicted on multiple counts of dealing with the proceeds of crime worth more than AUD100,000 contrary to section 400.4 of the *Criminal Code Act 1995*. The remitter was ultimately sentenced to five years and six months imprisonment, with a minimum of three years and seven months. The remitter was also charged and convicted of money laundering offences.



491. Indicators in this case included:

- International funds transfers sent directly to individuals rather than an overseas business contact.
- Multiple entities often linked via address or phone number, sending international funds transfers to the same overseas beneficiaries.
- Significant increase in cash deposits received by the remitter.
- Sudden increase in transactional activity inconsistent with the remitter's established business profile or transaction history.
- Unauthorised account transfers.
- Use of false identification.

4.17 Use of shell companies/corporations

AUSTRALIA

Shell companies and cash payments used in million dollar tax fraud

492. AUSTRAC information assisted law enforcement to identify a criminal syndicate which was facilitating large-scale tax evasion for a number of clothing manufacturers.

493. Investigations revealed that over a three-year period, more than AUD52 million was deposited into and withdrawn from accounts operated by the syndicate. Many of these transactions were reported to AUSTRAC by reporting entities via the submission of significant cash transaction reports (SCTRs). During this period the annual financial activity of the syndicate increased dramatically from approximately AUD750,000 in the first year to more than AUD17.5 million in the last year.

494. The syndicate would receive cheques from the manufacturing businesses and deposit them into accounts linked to 'shell companies'. Once the cheques had cleared, the syndicate would withdraw the cash in multiple amounts and secretly return the cash to the businesses.

495. Two suspect transaction reports (SUSTRs) submitted by reporting entities triggered AUSTRAC's automated monitoring system. The information in the SUSTRs, along with AUSTRAC's additional analysis of related financial activity, identified 10 clothing manufacturing businesses in one geographic location which had been conducting large cash withdrawals over an extended period of time.

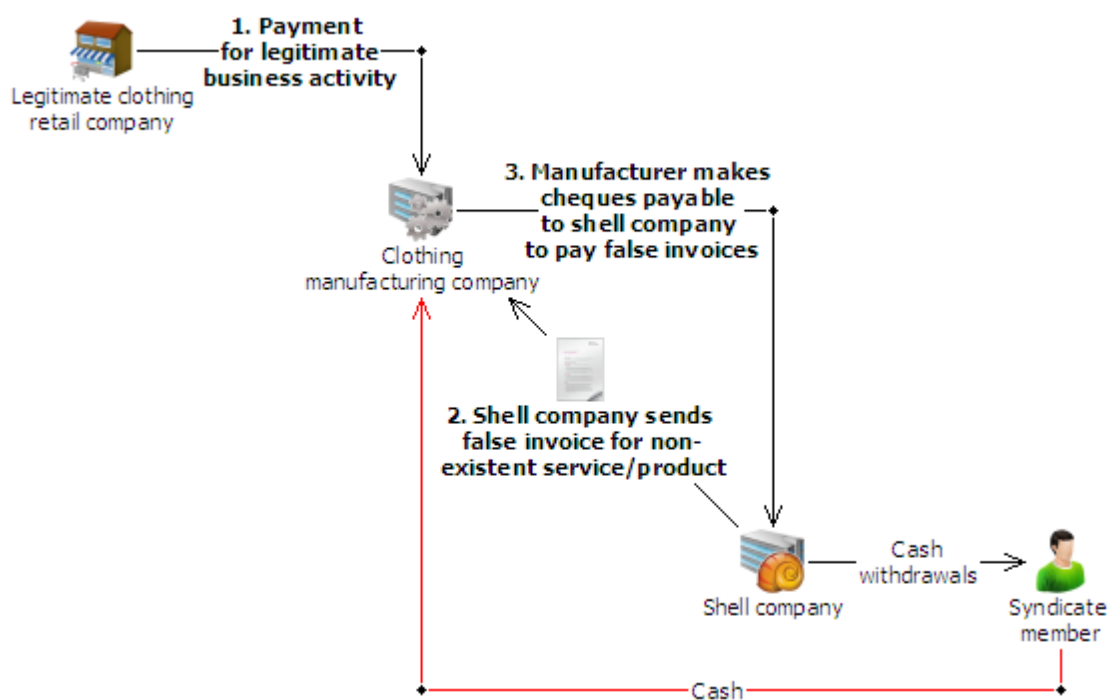
496. The SUSTRs also identified unusual financial activity involving members of the syndicate who were frequently depositing cheques into company accounts, followed by cash withdrawals equivalent in value to the cheque deposits, on the same day. This information prompted AUSTRAC to produce a financial intelligence assessment report for law enforcement agencies about these businesses.

497. The fraud allowed the manufacturing companies to evade income tax and other taxation obligations and move their profits into the cash economy. Authorities

believe that, because employees working for the manufacturing companies were paid in cash, they were also able to claim welfare benefits while working.

498. The method used by the syndicate to facilitate tax evasion is as follows:

1. A number of legitimate clothing retail companies paid a clothing manufacturing company for the production of garments. These payments were for legitimate business activity and the retail companies were not complicit in the scheme.
2. The promoters of the scheme made approaches to the garment makers and offered to help them to reduce the amount of tax they were paying, less payment of a commission to the promoters of between 5 per cent and 10 per cent.
3. A series of shell companies were set up using details of members of the group of companies who had been approached by the promoters and paid a small amount of money for their personal details. These details were then used to register the companies, obtain workers compensation insurance and open bank accounts in order to create a facade of legitimacy.
4. With the assistance of the promoters, the shell companies created false invoices and issued them to the clothing manufacturers for the provision of fictitious goods and services. These false invoices enabled the manufacturer to claim tax deductions for subcontracting expenses that were never incurred.
5. The manufacturers made cheques payable to the shell companies to pay the false invoices.
6. Members of the syndicate deposited the cheques into the accounts of the shell companies.
7. Once the cheques had cleared, the syndicate members withdrew the funds from the accounts via multiple cash withdrawals using debit cards issued to the accounts of the shell companies. These withdrawals were undertaken across various bank branches.
8. The syndicate returned the cash to the manufacturer, minus a commission.
9. The manufacturers used the cash to fund their lifestyles and pay cash wages to their employees, thereby avoiding income tax obligations.



499. Further investigations revealed that a bank assistant manager had maintained a close relationship with the syndicate. The assistant manager used her influence over other bank staff to ensure AML/CTF reporting procedures were ignored. Members of the syndicate had also offered gifts to bank tellers to build rapport and encourage them to skip some stages of their AML/CTF program, thereby helping the syndicate avoid detection by AUSTRAC.

500. Typically, a complicit staff member would allow a syndicate member to withdraw funds from multiple shell company accounts at the same time, even though they did not have the right to do so. The promoters actively sought the services of these bank staff, even knowing which staff would be working on particular days of the week.

501. The good working relationship law enforcement had with members of the bank's AML/CTF team proved to be vital in the ultimate success of the law enforcement investigation.

502. AUSTRAC also received a number of suspicious matter reports (SMRs) from reporting entities which helped reveal the methodology used by the syndicate.

503. Within the SMRs, reporting entities identified the following 'grounds for suspicion':

- Several cheques written by the manufacturing companies were deposited (often several times in one day) by the syndicate members into multiple accounts operated by the shell companies. The syndicate members repeatedly requested quick clearances for the cheques.
- Funds were withdrawn from accounts as cash as soon as the proceeds of cheque deposits cleared, often on the same day, across multiple branches.
- The manufacturing businesses were associated with more than AUD16 million in cash withdrawals over a twelve-month period.

504. When law enforcement officers moved to stop the syndicate, they restrained more than AUD1 million in cash, as well as a number of properties. Two members of the syndicate who facilitated the scheme were charged with dealing in proceeds of crime worth AUD1,000,000 or more, contrary to Section 400.3(1) of the Criminal Code Act 1995.

505. Indicators involved in this case included

- Customer offers incentives to representatives of a financial institution to assist bypassing AML/CTF procedures.
- Repeated requests for quick cheque clearances by customer.
- Same day cheque deposits, followed by cash withdrawals of an equivalent value to the cheque deposits, across multiple branches.
- Significant value and volume of cash withdrawals.
- Significant value and volume of cheque deposits into bank accounts.

CHINESE TAIPEI

506. Mr Tseng, Mr Chen and Mr Hsueh engaged in transporting textiles from Mainland China to Chinese Taipei as their business for commission. From 2005 to March 2011, for the purpose of helping their clients, including Chuan X Textile Company, to inflate the sales figures for the deduction of sales tax, they used their companies, or nominal companies such as Jin X Ming Company, to issue fake uniform invoices with a total amount of NTD2,559,900,485 (over USD85 million) as certificates for proceeds. They also charged 5% to 6.5% as reward.

507. In addition, in order to balance the import and sales for Chuan X and other companies, they set up nominal companies such as Jin X Ming, and Guan X, etc. to issue fake uniform invoices with a total amount of NTD2,518,125,121 (USD84,281,457).

508. The case was forwarded to Shihlin District Prosecutor's Office on 18 November 2011 by the Investigation Bureau.

HONG KONG, CHINA

509. In October 2010, a foreign passport holder, with the assistance of a secretarial company, set up a shell company and opened a bank account in Hong Kong.

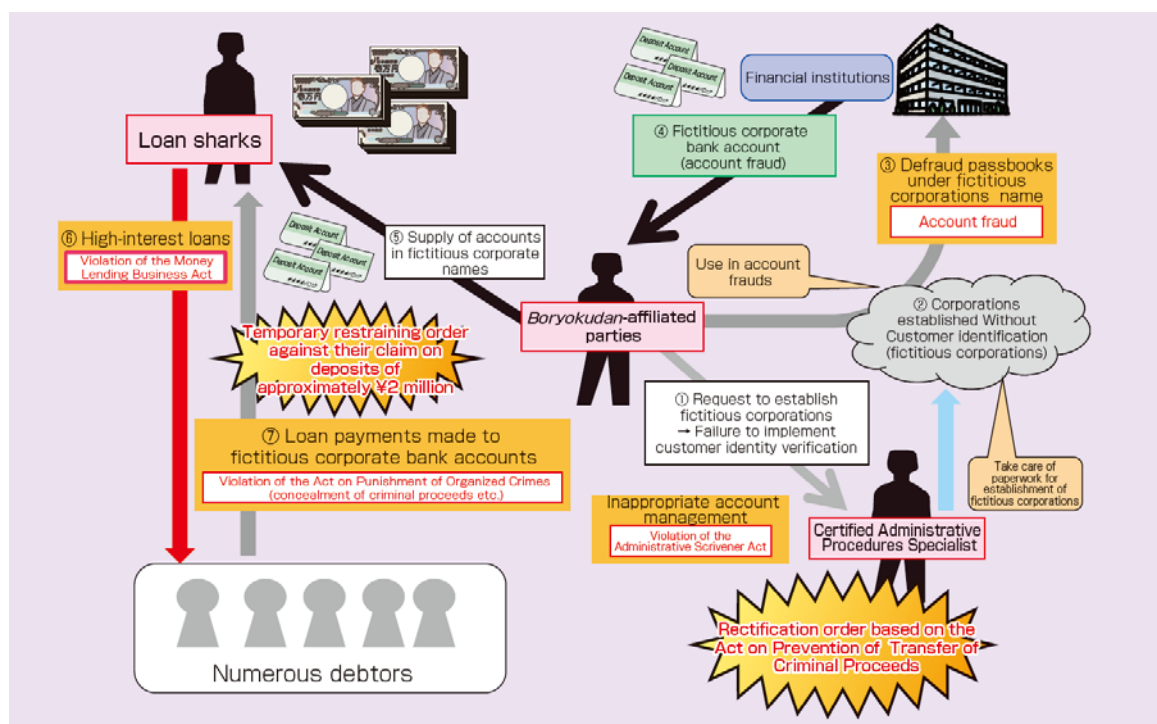
510. Five overseas victims from different jurisdictions were deceived into transferring money amounting to HK\$3.17 million (USD408,566) to the bank account of this shell company. The suspect left Hong Kong before the case was reported, but Police took swift action to withhold the remaining balance in the bank account.

JAPAN

Concealment of criminal proceeds etc. in large-scale violations of the Moneylending Control Act

511. Men unregistered in the moneylending business lent illegal high-interest loans to the managers of small and medium sized firms in financial difficulty.

512. A number of debtors made loan payments in the amount of approximately ¥370 million (USD3,902,754) to bogus accounts made in the names of shell companies. The man was arrested for violations of the Act on Punishment of Organized Crimes (concealment of criminal proceeds etc.). A temporary restraining order was also issued on the sum of approximately ¥2 million (USD21,093) remaining in the accounts noted above.
513. The accounts mentioned above are part of several hundred accounts established in the names of shell companies by the members of the Rokudaime Yamaguchi-gumi, the Kudokai and other Boryokudan for the purpose of loan payments. The relevant Boryokudan members were arrested for account fraud for having defrauded the banks of those accounts.
514. Furthermore, a certified administrative procedures specialist who was involved in setting up the corporations that Boryokudan members misused for opening bank accounts, was issued a Rectification Order from the Governor of Hiroshima after receiving an Opinion Statement from the National Police Safety Commission (NPSC) / the National Police Agency for his failure to identify customers under the Act on Prevention of Transfer of Criminal Proceeds.
515. The certified administrative procedures specialist was also arrested for the lack of preparation of account ledgers in violation of the Administrative Scrivener Act²⁵.



²⁵ Japan Financial Intelligence Center (JAFIC), *Annual Report 2012*, 52-53, http://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/data/jafic_2012e.pdf

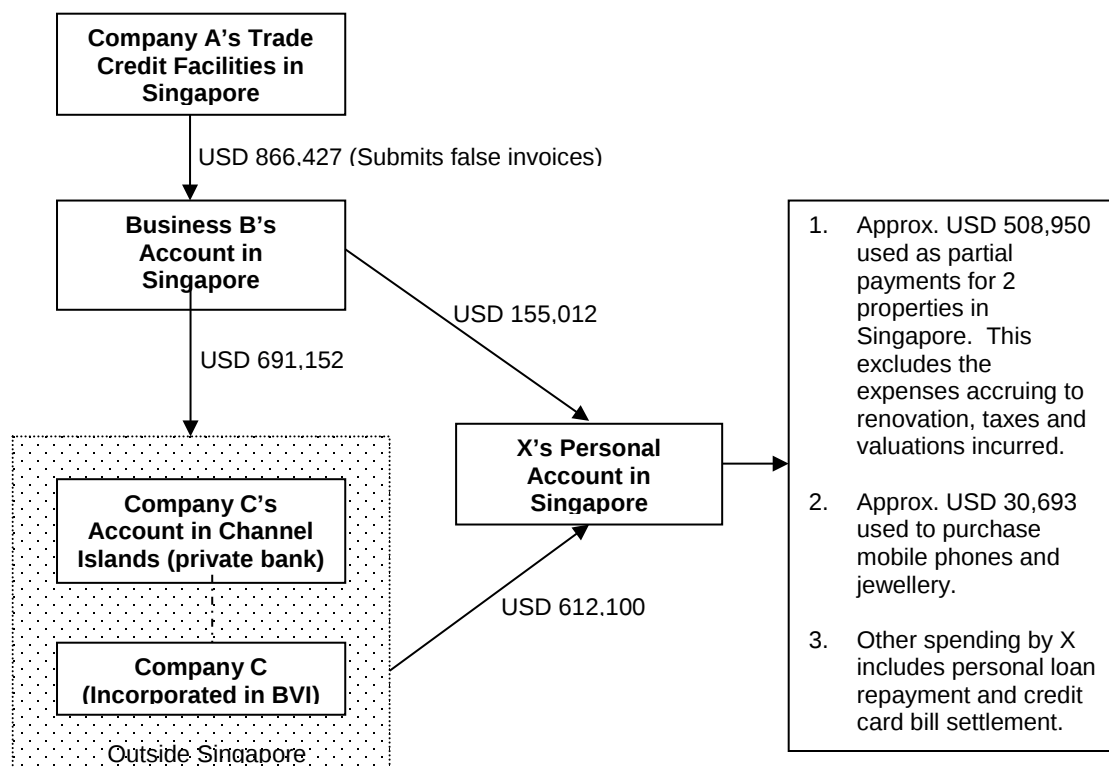
MACAO, CHINA

516. Mr X from country C registered an investment company and opened several multiple currency bank accounts in country M. Shortly after the accounts were opened, large amount of funds were transferred into the bank accounts through different channels, including cash, cheques, account transfers and remittances.
517. Upon receiving the funds, Mr X immediately remitted them to different individuals and companies. Mr X claimed that the source of funds was investment funds from customers to invest in foreign property and the outflow was their dividends, most of the counterparts came from country C.
518. Along the process, Mr X also set up several related companies in different parts of the world, and his partners and he held several property investment companies in country M with the same address. It was suspected that these related companies were shell companies.
519. The transaction pattern was deemed unusual as the outflow of funds was made to other counterparts instead of the investors themselves, which did not correspond to the reason given of dividend distribution. In addition, the bank in country M also revealed that the Mr X's partners opened several bank accounts with the same transaction pattern as Mr X.
520. With this case, the FIUs of these countries exchanged information for analysis and further investigation. It was revealed that most of the companies held by Mr X and his partners were shell companies, which might be involved in boiler-room operations or fraud cases overseas, and the bank accounts in country M were being used to transfer funds to overseas accounts.

SINGAPORE

521. X, a director of Company A, submitted fictitious invoices to a bank to induce the said bank to disburse six sums totalling about USD870,000 to X's sole-proprietorship (Business B). These sums were purportedly to pay a foreign company for purchases, financed by Company A's trade credit facilities with the bank.
522. After receiving the monies from the bank, Business B transferred about USD 155,000 to X's personal account in Singapore. Another USD700,000 was transferred to a Channel Islands private bank account maintained by a shell company (Company C) registered in the British Virgin Islands. X and his wife were the directors of Company C. About USD615,000 was subsequently transferred from Company C's Channel Islands bank account to X's personal account in Singapore.
523. Most of the criminal proceeds consolidated in X's personal account were subsequently used to purchase two properties in Singapore. Some of the proceeds were also used to purchase mobile phones and jewellery.

524. The following simplified fund flow diagram summarizes the fund movements:



525. X was eventually prosecuted on four ML charges, of which two were related to removal of criminal proceeds out of Singapore, one related to conversion of criminal proceeds into property and one related to transferring of criminal proceeds. The Court sentenced X to 15 months imprisonment for money laundering. The sentence was to run concurrently with X's predicate offence sentence of 54 months imprisonment.

4.18 Laundering of proceeds from tax offences

AUSTRALIA

Company evaded millions in cigarette tax through duty free fraud

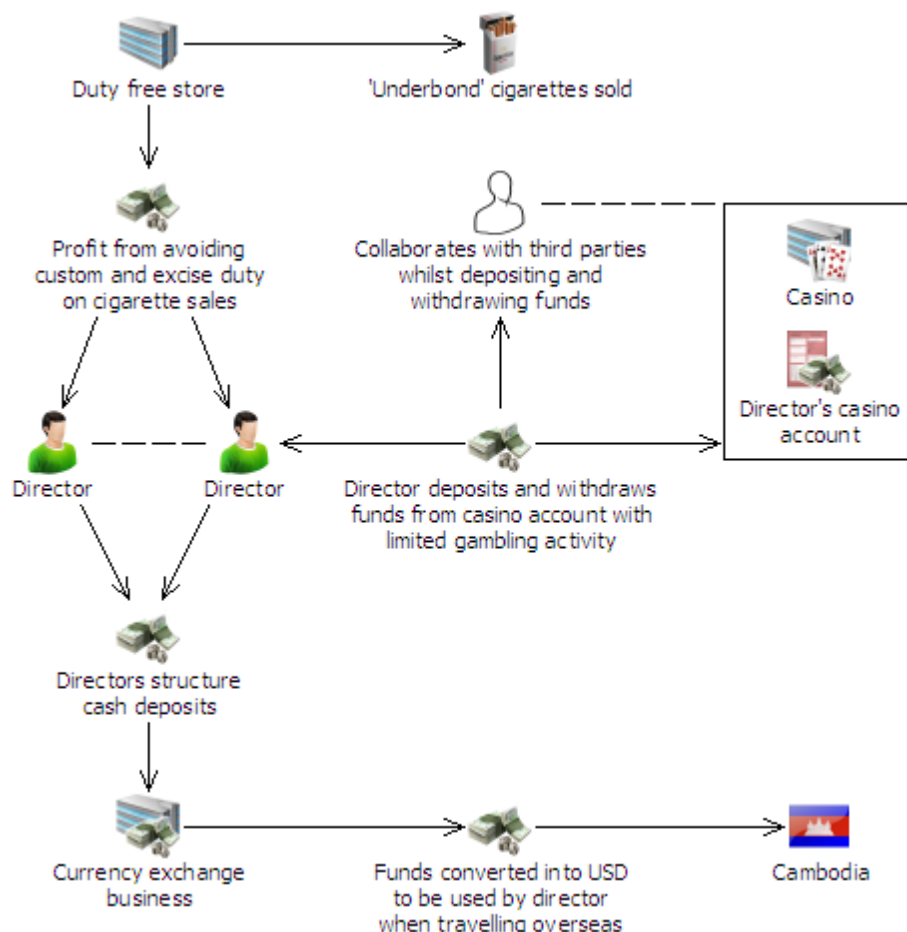
526. AUSTRAC information assisted authorities with an investigation into a company suspected of a multi-million dollar duty free fraud. The investigation resulted in the company and its two directors being convicted of fraud-related charges.

527. The investigation revealed that over a three-year period, a complex arrangement was set up where the directors of the company, which traded as a duty free store, sold large quantities of 'under bond' cigarettes (cigarettes on which excise duty had not been paid). The directors sold the cigarettes and profited by avoiding paying the required customs and excise duty. In total, authorities believe that the suspects evaded more than AUD2.5 million tax.

528. In accordance with AML/CTF reporting requirements, reporting entities submitted a range of financial transaction reports indicating suspicious activity

by the company and its directors, involving currency exchange business and casinos. Authorities believe the suspects undertook a range of activities to launder and hide the substantial proceeds of the cigarette sales:

529. One of the directors travelled regularly to Cambodia and would visit currency exchange businesses in Australia to convert funds to US dollars before each trip. When converting currency amounts worth more than AUD10,000, the two directors regularly refused to complete significant cash transaction reports (SCTRs), instead opting to structure the cash into smaller amounts to avoid the SCTR reporting requirement.
530. This structuring activity led to a total of 44 suspect transaction reports (SUSTRs) being submitted about the two directors, with the majority coming from a currency exchange business. It was also reported that the suspects had asked reporting entities whether or not their transactions would be recorded and reported to the Australian Taxation Office (ATO), a further indication that they were involved in illegal activity and were concerned about attracting the attention of authorities.
531. AUSTRAC also received SUSTRs from a casino highlighting one suspect's continued use of a casino account to deposit and withdraw funds, despite undertaking limited gambling activity. The reports indicated the suspect was a regular patron at the casino. While the suspect's gambling activity remained limited, the amounts gambled had increased substantially over an eight-year period. It was also reported that the suspect had collaborated with a number of third parties while depositing and withdrawing funds at the casino.
532. In all, AUSTRAC information showed that the two directors and associates made cash deposits worth more than AUD20 million into their business banking account.
533. The company and its directors were convicted and ordered to repay the AUD2.5 million in tax they had evaded. In addition they were ordered to pay penalties of more than AUD600,000, as well as the Commonwealth's legal costs of AUD140,000. The convictions finalised a long-running and complex investigation.



CHINESE TAIPEI

534. Mr Chou was the actual responsible person of Tung X International Co. and Mr Chen was the Vice General Manager of the said company. Mr Chou instructed Mr Chen to forge transaction documents between Tung X International Co. and Computacenter UK Ltd., Chuan X, two well-known transnational corporations, since October 2003.
535. They used waste materials as high end products to export and defraud NTD 500 million (about USD 17 million) in tax refunds. After the shipment arrived in Hong Kong, China they used the foreign nominal company that they established, Golden Season Limited, to export it back to Yung X International Co. and financed over NTD 2 billion (about USD 68 million) from Standard Chartered Bank.
536. Since 2006, they also used over 10 nominal companies such as Na X Company and Yu X Technology provided by Mr Cheng to issue uniform invoices without actual transactions and concealed the abovementioned tax refunds. They then financed approximately NTD800 million (about USD 27 million) from banks.
537. This case was referred to Banciao District Prosecutor's Office on 8 March 2011 by the Investigation Bureau.

FIJI

538. The Fiji FIU received a request for information from the local tax authority in 2009 regarding information on offshore remittance transactions conducted by Person B and Company X.
539. The Fiji FIU was able to establish that Person B and his wife, Person C were the directors of Company X. Company X has business accounts maintained at three commercial banks in Fiji. It was established that Person B and Person C are the signatories to the business bank accounts held at two of the commercial banks. Person XY, the son of Person B and Person C, was the signatory to a business cheque account and property loan account held at the third commercial bank.
540. It was established that Person XY and his sister Person YW had a few term deposit accounts that held significant account balances. The age and occupation of Person XY and Person YW does not appear to match with the deposits made into their personal bank accounts.
541. It was suspected that business proceeds from Company X have been transferred to the bank accounts of Person B, Person C, Person XY and Person YW to possibly evade tax. The case has been referred to the local tax authority for possible tax evasion.

HONG KONG, CHINA

542. Between March 2009 and November 2010, a foreign passport holder opened a bank account in Hong Kong for receiving sale proceeds amounting to US\$1.4M for tax evasion purpose.
543. The offender was subsequently convicted of tax evasion offence in the overseas jurisdiction where he ran his business in October 2012.

4.19 Use of the internet (encryption, access to IDs, international banking, etc.)

AUSTRALIA

Suspicious cash transactions helped undo Nigerian fraud suspect

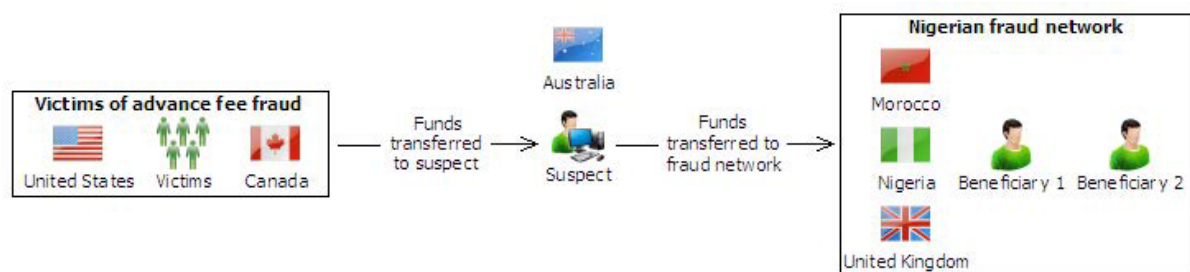
544. AUSTRAC alerted law enforcement authorities to frauds facilitated by a suspect in Australia who was part of a large-scale Nigerian fraud network. The suspect allegedly scammed more than AUD500,000 from overseas victims via the internet.
545. The suspect came to AUSTRAC's attention after a suspect transaction report (Sustr) was submitted by a reporting entity. The report, which had triggered AUSTRAC's automated monitoring system, revealed that the suspect had conducted unusually high-volume and high-frequency international funds transfer instructions (IFTIs) to Nigeria.

546. The funds transfers were paid for in cash and appeared to be structured to avoid the threshold transaction reporting requirements. Authorities established that the suspect used variations of her name when conducting transactions.
547. AUSTRAC staff analysed financial transaction reports submitted by reporting entities and identified the following:
- Over a 10-month period the suspect undertook 35 outgoing IFTIs totalling approximately AUD160,000. The funds were consistently sent to two recipients in Nigeria.
 - International funds transfers were conducted through a remittance service provider and paid for with cash. The cash payments were seemingly structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold.
 - Over a 10-month period the suspect was the recipient of nine incoming IFTIs from the United States totalling approximately AUD140,000, suspected to be the proceeds of the fraud.
 - The suspect conducted numerous large cash withdrawals and deposits which were detailed in significant cash transaction reports (SCTRs) submitted to AUSTRAC. Over a two-month period the suspect withdrew cash totalling more than AUD86,000 and deposited cash totalling more than AUD52,000.
 - Over an 11-month period, reporting entities submitted seven SUSTRs to AUSTRAC about the suspicious activities of the suspect. The SUSTRs identified unusually large cash transactions to fund IFTIs to Nigeria and the apparent structuring of transfers to avoid the cash threshold reporting requirements.
548. AUSTRAC identified that the funds sent to Nigeria appeared to be sourced from a number of cash withdrawals made from the suspect's account and from funds sent from an individual in the United States directly to the suspect. A portion of the funds remained in the suspect's bank account and were believed to represent a commission.
549. The resulting law enforcement investigation revealed the suspect operated the fraud from home and used various names to communicate with victims over the internet. The suspect secured payments from victims by asking for financial help.
550. AUSTRAC searches were conducted on additional name variations the suspect used to perpetrate the scam. AUSTRAC information showed the suspect was the subject of an additional eight SUSTRs. Reporting entity staff observed that:
- within one month of opening a bank account, the suspect received approximately AUD150,000 and withdraw all the funds;
 - the suspect's income and occupation were inconsistent with the high value of transactions she was undertaking;
 - the suspect became evasive and upset when asked routine questions about a transaction requiring the submission of a SCTR; and
 - the suspect changed the method of withdrawing funds seemingly to avoid threshold reporting requirements, by withdrawing the daily limit of AUD3,000 on a daily basis at various bank branches, then withdrawing another AUD1,000 from automatic teller machines (ATMs).

551. Further searches were conducted on name variations used by the suspect and identified that the suspect:

- received an additional AUD318,000 in incoming IFTIs from the United States and Canada;
- sent an additional AUD207,000 to beneficiaries in Nigeria, the United States, United Kingdom and Morocco;
- was the subject of an additional eight SCTR for deposits totalling approximately AUD124,000 and 11 SCTR for cash withdrawals totalling approximately AUD172,000; and
- may have provided false identification to conduct outgoing IFTIs to Nigeria.

552. Law enforcement officers executed a search warrant on the suspect's premises and seized cash totalling approximately AUD29,000. The suspect was arrested and charged with six counts of fraud and one count of possessing tainted property. The suspect was convicted and sentenced to six years imprisonment.



553. Indicators in this case:

- Cash withdrawals conducted at various bank branches and ATMs on the same day.
- Customer undertaking transactions which appear to be inconsistent with their profile and/or transaction history.
- High-value cash deposits to pay for international funds transfers.
- High-value international funds transfers to/from Australia for no apparent logical reason.
- Multiple high-value international funds transfers to a high-risk jurisdiction.
- Structured cash payments just below the cash reporting threshold used to pay for international funds transfers.
- Use of false identification to conduct transactions.

CHINESE TAIPEI

554. During August and September 2010, Mr Chen and Mr Wang repeatedly used 43 forged American Express, Visa and Master credit cards to purchase gift cards at many restaurants and hotels. There were a total of 184 expenditures with the amount of NTD1,647,368 (about USD55,000).

555. They then sold the gift cards on the internet making a profit of over NTD620,000 (about USD20,000). The case was referred to the Prosecutor's Office on June 24, 2011 by the Investigation Bureau.

Fiji

Case 1

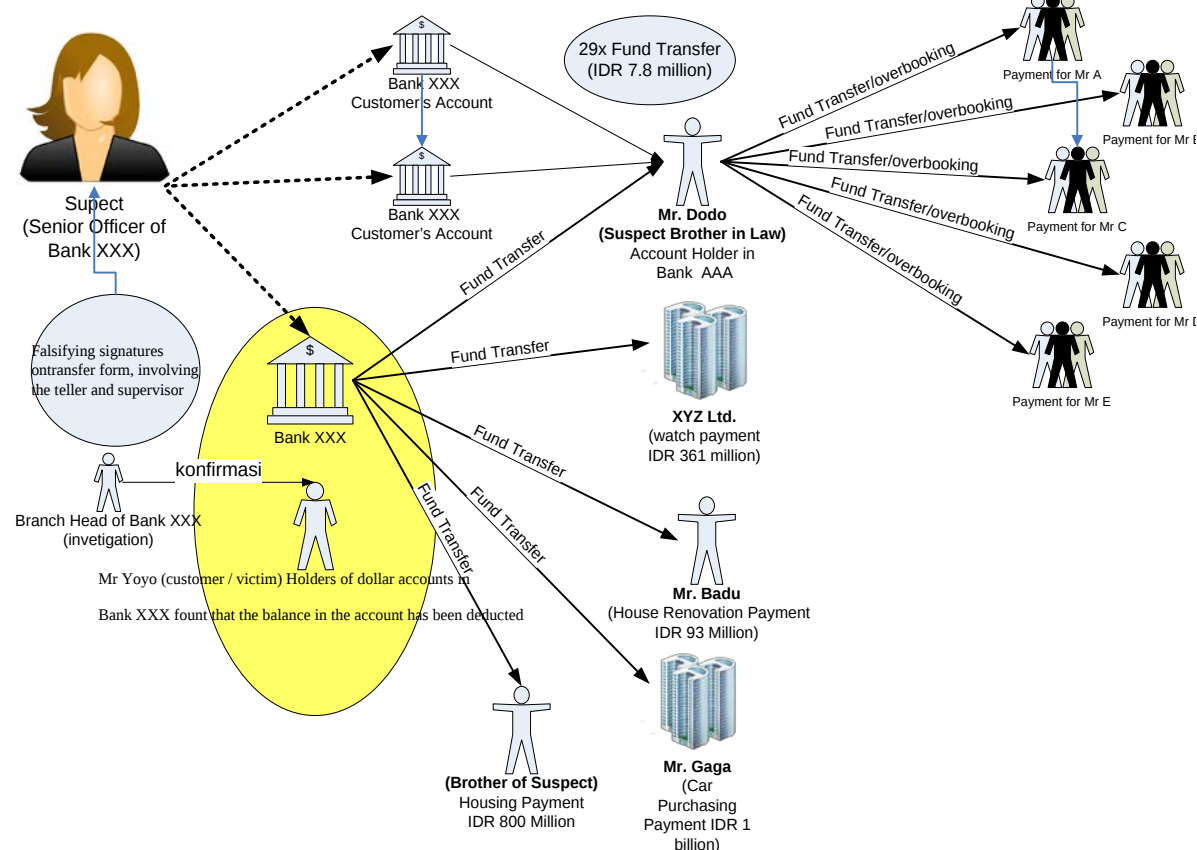
556. This case involved a Sales Consultant, Mr X. He was contacted by Mr Y based in the United States of America via email to join his company as a local representative.
557. As a local representative in Fiji, Mr X was to receive 10% of all remittances made to Mr Y together with a monthly salary of \$US7,000.
558. Mr X maintained two separate accounts at a local bank. Between 8 March and 11 March 2012, unauthorized transfers totalling FJ\$4,680 were made from five different bank accounts into Mr X's bank account which is maintained at the same commercial bank.
559. On 9 March 2012 the local Bank placed a STOP on Mr X's bank account. However Mr X used a new password to access his account through internet banking and transferred \$1,000 to his other bank account within the same bank. The bank also placed a STOP on his other account.
560. Mr X was able to withdraw and remit a total of FJ\$2,200 to a Ms Z in USA through a local foreign exchange dealer. He remitted the funds with the assistance of his workmates (\$500 per person in a day) to avoid the approval under Fiji's Exchange Control Act.

Case 2

561. Person A was an unemployed businessman from Vanuatu and a resident in Fiji. Person B contacted him by email and phone and suggested a "business/investment arrangement". Person A acceded to this and gave his bank account to Person B. Person B was to remit US\$15,000,000 to Person A to invest for him. However the funds were locked in the Bank of America and could only be unfrozen and remitted to the Person A on the payment of taxes to the bank. The money to pay these taxes would be credited to Person A's account by Person B and they were then to be sent on to a lady in Washington State, U.S.A. who work for the Bank of America to settle the outstanding taxes.
562. Person A received two funds transfers into his account which he sent on to the lady as instructed. Most of the remittances were made through a foreign exchange dealer. Person A's account was credited with funds by telegraphic transfer from the Cook Islands.
563. The funds credited/transferred to Person A's account were made through authorised access into some local customers bank account who fell victim to a phishing scam.
564. Person A was convicted and sentenced on 12 April 2012. He was charged for two counts of Money Laundering and sentenced to seven years imprisonment.

INDONESIA

565. A senior bank employee (Mrs A) was assisted by several other staff working together to commit acts of embezzlement. The action was carried out using a fake specimen signature of the customer on the funds transfer form.
566. The available funds in the customer's (the victim) accounts were withdrawn without the knowledge of the customer, but using the documents as if it was valid. The funds were then channelled into a brother-in-law's account, who then sent it to a third party account to meet the needs of Mrs A.
567. In addition, there were also funds from the customer (victim) that were directly sent to other third parties for the purpose of payment to the benefit of Mrs A.



JAPAN

Case 1

568. A Chinese man, who was a computer programmer, sold counterfeit branded sunglasses, wallets, and other products by using internet auctions
569. He had the purchasers deposit their payments, totalling approximately 1.6 million yen (USD16,875), into a bank account opened under a fictitious name by using a forged identification document. He was arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds etc.).

Case 2

570. A man who was selling stimulant drugs illegally by using internet bulletin boards and other means was arrested for violation of the Stimulants Control Law (joint

possession for profit). The arrest was initiated by information provided by the Internet Hotline Centre operated by National Police Agency.

571. In addition, the subsequent investigation discovered that these men used an internet bank account in someone else's name, under their control, as an exclusive account for trafficking of stimulant drugs, into which a total of approximately 1 million yen (USD10,548) had been deposited by their customers.
572. The suspects were then arrested for violation of the Anti-Drug Special Provisions Law (concealment of drug-related criminal proceeds etc.).

THAILAND

573. AMLO received a call from a foreigner who spoke in English, with an Arabic accent. He introduced himself as Mr W from the Middle East. He requested AMLO to immediately release his cheque which he had sent through the Worldwide Express Courier Company.
574. He claimed that this cheque was from Yahoo for a winning lottery and AMLO had no right to hold it. After talking with an AMLO officer he realized that he had fallen for a scam, someone who pretended to be a Yahoo Coordinator in a lottery program had taken his money.
575. Mr W lost USD650 by transferring the money via Western Union before he contacted AMLO. AMLO's name had been used to make the whole scheme look real.
- Mr W lost USD650.
 - Anti-Money Laundering Office's name had been used and abused.
 - The spread of email and very easy access to email-harvesting software made the cost lower of sending scam letters through the internet extremely cheap.
 - There are many victims around the world who have fallen for this scam and lost a lot of money.
 - Secretary-General of AMLO has made an order to undertake an additional inquiry and gather information for making a complaint.
576. Receipts for the money showed that the money was transferred by Mr W to Mr S by Western Union and the telephone number of Mr S. AMLO did an investigation to identify: whether Mr S really existed and if he is the same person who was involved in this case; who is the owner of the telephone number that the scammer gave for a contact number?
577. After a two month investigation AMLO got a lot more evidence related to Mr S, and the telephone number that the scammer used was included. AMLO sent the case to the Police Criminal Suppression Division for further legal action. One week later the police arrested Mr S. The court considered to put him in jail for two years.

TONGA

578. An investigation was made into unauthorised withdrawals using internet banking where TOP\$1500 (USD840) was transferred to a second account.

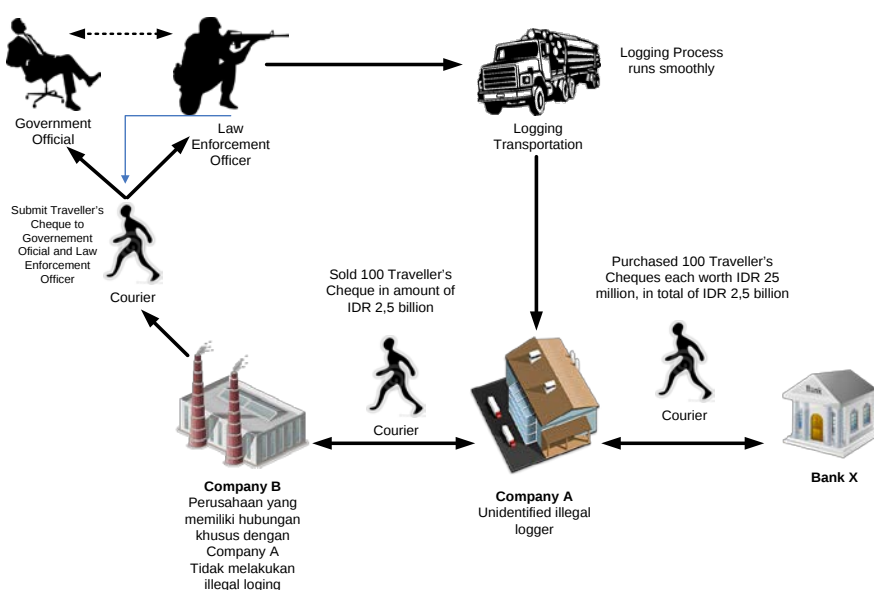
579. Perpetrators from Nigeria contacted the second account holder to remit TOP\$1000 (USD560) to Nigeria whilst the account holder kept the balance.

4.20 Association with illegal logging

INDONESIA

580. There was a flow of funds to forestry ministry officials and law enforcement officers brought in by couriers using Travellers Cheques instruments to facilitate the delivery of wood logs into a wood processing company.

581. Travellers Cheques were purchased by a timber management company to facilitate the company's operations in performing activities in the field of wood processing.



4.21 Currency exchanges/cash conversion

INDONESIA

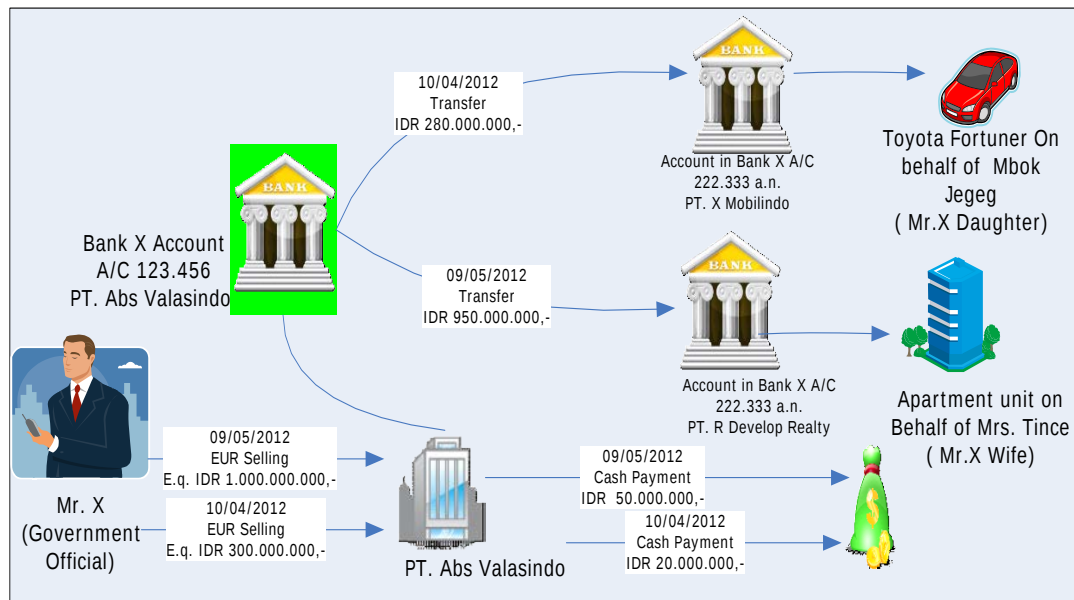
582. The Indonesian FIU received Suspicious Transactions from a currency exchange dealer regarding Foreign Exchange on Forex USD exchange carried out by a Politically Exposed Person (Mr X) who conducted two transactions during April to May 2012 with a total value equivalent to Rp. 1.3 billion (USD30 million).

583. Details of the transaction are as follows:

- At the time of the currency exchange, currency exchange cash proceeds are requested by Mr X to be directly transferred to the account of Property Company (PT R Develop Realty) amounting to Rp. 950 million and PT. X Mobilindo of Rp. 280 million.
- Having been traced at Bank X, it is known that the remittance transaction to the account of PT. X Mobilindo is a payment transaction on the purchase of an automobile for Son of Mr X, while the other remittance to the account of PT.

R. Develop Realty is a payment transaction on the purchase of apartment for Wife of Mr X.

- There is a tendency for disguising financial transactions in the purchase of valuable possessions using currency exchange transactions.



4.22 Currency smuggling (including issues of concealment and security)

CANADA

Cash Couriers

584. It is believed that a terrorist fundraising network with links into Europe is operating in Canada, primarily in Vancouver, Toronto, and Montreal.

585. The network raises funds in Canada and then converts the funds into Euros in Canada, based on the view that the conversion will attract less scrutiny in Canada than in Europe. Once the funds are in Euros, cash couriers use air travel to transport the currency to Europe. It appears that this approach is utilized in order to avoid placing the funds into the financial system, which is viewed as embodying a greater risk of detection.

FIJI

Case 1

586. Two nationals from Chinese Taipei (Mr X and Mr Y) failed to declare cash totalling US\$55,000 when they arrived into Fiji. The profiles and amount of currency concealed in the luggage of the two individuals are as follows:

- Mr X, 47 years old, businessman - US\$35,000 was concealed in his luggage;
- Mr Y, 37 years old, businessman - US\$20,000 was concealed in his luggage.

587. According to interviews with the two individuals, they did not fully understand English. The two individuals were discharged without conviction on the condition that they paid \$1,000 each to Court.

Case 2

588. A Chinese national, a banking analyst of 27 years old, arrived into Fiji and failed to declare USD17,000. The money was stored in an envelope in his bag and according the interview, he forgot that the currency was to be declared.

589. A fine of \$300 was imposed on the accused and a default of 300 days imprisonment.

TONGA

590. An investigation is now pending trial where an incoming passenger from China failed to declare cash over USD10,000.

4.23 Use of credit cards, cheques, promissory notes, etc.

FIJI

591. The FIU received a suspicious transaction report involving a bank officer, Person A. Person B (Person A's husband) maintained a credit card facility in the bank where Person A was employed.

592. Person A accessed Person B's credit card account without authority, and increased the credit limit of the account on two occasions. Person A was then withdrawing funds from Person B's credit card account. The case is under investigation by the Fiji Police Force.

HONG KONG, CHINA

593. A group of members from neighbouring jurisdictions, led by a ringleader, came to Hong Kong, China and opened bank accounts at various branches of the same bank. They claimed to be professionals with high incomes and requested the issuance of credit cards.

594. They then used the credit cards to purchase luxury items or buy overdrafts until the limits were exhausted. They also withdrew all the bank deposits, and lost contact thereafter.

SRI LANKA

595. Local commercial bank "B" filed an STR on the suspicion that the personal account of the president of a charitable organization was being credited with large sums of money.

596. Investigations into the alleged transactions revealed that donations were made to the charitable organization using credit cards through the internet payment gateway provided by bank "B". Once the funds were credited to the account of

the charitable organization the funds were being transferred to various individual accounts including the account of its president and Treasurer.

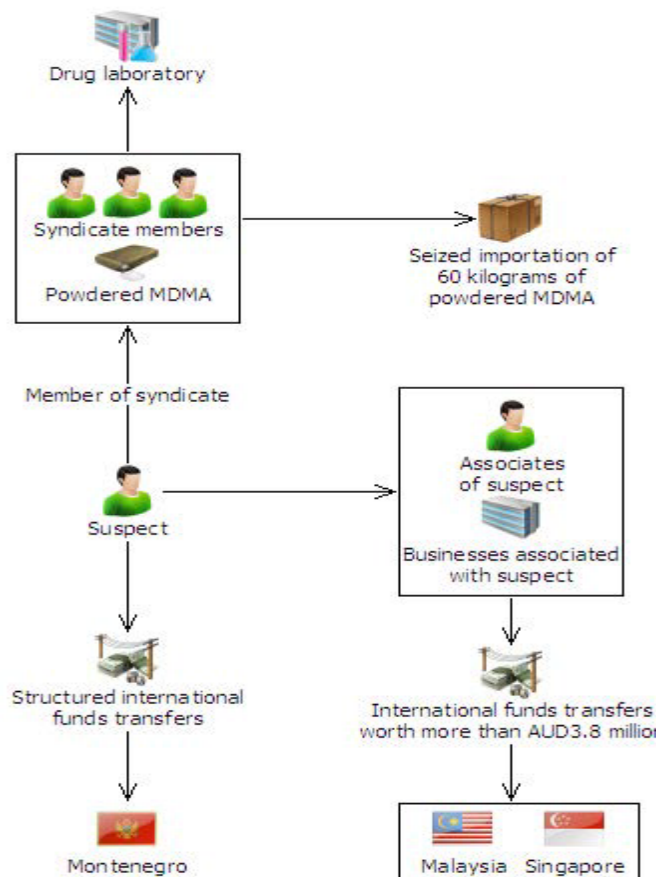
597. It was further revealed that the payment through credit cards had been made without the knowledge of the card holder, hence payments made through the internet payment gateway had been charged back, incurring a loss of LKR 263 million (USD2 million) to the bank.

4.24 Structuring (smurfing)

AUSTRALIA

Australian and international law enforcement combined to dismantle ecstasy syndicate

598. Successful cooperation among state, federal and international law enforcement resulted in the dismantling of a major drug syndicate responsible for importing methylenedioxymethamphetamine (MDMA) – the powdered equivalent of ecstasy – into Australia. The international syndicate, coordinated by a suspect based in Montenegro, imported MDMA into Australia to manufacture ecstasy tablets.
599. Four Australian suspects were arrested for their role in the operation, which led to the largest MDMA seizure recorded by a state police force in Australia.
600. Following an investigation into a previous importation of 60 kilograms of powdered MDMA, a covert operation was set up by law enforcement to identify and disrupt the illicit activities of the perpetrators. Syndicate members were closely monitored and investigators uncovered an illegal drug lab with an estimated capacity of producing drugs worth AUD24 million. When authorities moved to arrest the syndicate members they seized a large quantity of powdered MDMA, with the potential to produce more than 350,000 ecstasy tablets.
601. AUSTRAC information revealed more information about the syndicate's activities:
- One of the suspects had undertaken two 'structured' international funds transfers to Montenegro. Both transfers were sent via remittance services within a five-day period.
 - Individuals and businesses associated with the above suspect undertook outgoing international funds transfers (IFTIs) worth more than AUD3.8 million, predominately to Singapore and Malaysia.
602. The main suspect in the syndicate was charged with importing a commercial quantity of MDMA and conspiracy to traffic a commercial quantity of MDMA and was sentenced to 25 years on each charge, to be served concurrently.
603. The other three suspects were sentenced to between 14 and 17 years imprisonment for conspiracy to traffic a commercial quantity of MDMA.



CHINESE TAIPEI

604. Mr Hsu was the Chairman of the listed Ching X Fu Company. Mr Chuang, Mr Wang and Mr Lin were respectively the Chairman, CEO and President of the listed San X Biotech Company.
605. Between June 1, 2007 and September 30, 2008, Mr Hsu used 19 nominal accounts from the company. Mr Chuang and Mr Wang used 15 nominal accounts. Mr Lin then solicited 22 individuals including Mr Chiu to conduct investments for stock manipulation by using the prospects of Ching X Fu Company as lure. The price of the company stock was hiked up from \$8.99 on 4 June 2007 to \$26.9 on 11 March 2008.
606. Total illegal proceeds reached NTD209,250 thousand (about USD700 million). The Investigation Bureau referred the case to Taichung District Prosecutor's Office for further investigation on 24 June 2011.

HONG KONG, CHINA

607. In June 2011, the mastermind and members of a fraud syndicate of another jurisdiction were convicted outside Hong Kong for pyramid selling fraud involving over HK\$1.2 billion (USD154 million). Investigations revealed that the syndicate maintained various bank accounts in Hong Kong, China for receiving crime proceeds totalling HK\$690 million (USD89 million). The mastermind's

wife was later arrested in Hong Kong when attempting to withdraw HK\$202 million (USD26 million) by cashier order. The arrested person was charged with two counts of ML offence with HK\$238 million worth (USD30 million) of assets restrained.

4.25 Wire transfers

BANGLADESH

Terrorist Financing Through Wire Transfer

608. First Indication

- Sources of information: Media report & STR from a commercial bank.
- FIU collected primary information from banks.
- FIU conducted inspection at the related banks.
- Based upon that information, the FIU analysed the case.
- FIU analysis revealed funding through wire transfers.
- Funds originated from a foreign country B through a country A-born national residing and holding joint citizenship status of that country B, named Mr X.

609. Activities in Country B

- Funds were collected by Mr X from that foreign country through voluntary donations disguised as social and charitable work.
- In addition to fund collection activities, Mr X had a respectable professional career in the foreign country which helped him camouflage his true intentions.
- Funds were wired To:
 - ❖ One Country A based institution, a religious home and orphanage owned by Mr X and another person Mr Y.
 - ❖ One Individual (Mr Y, a permanent resident of Country A and an ally of Mr X).
- Mr X and Mr Y were among the directors of the aforesaid institution.

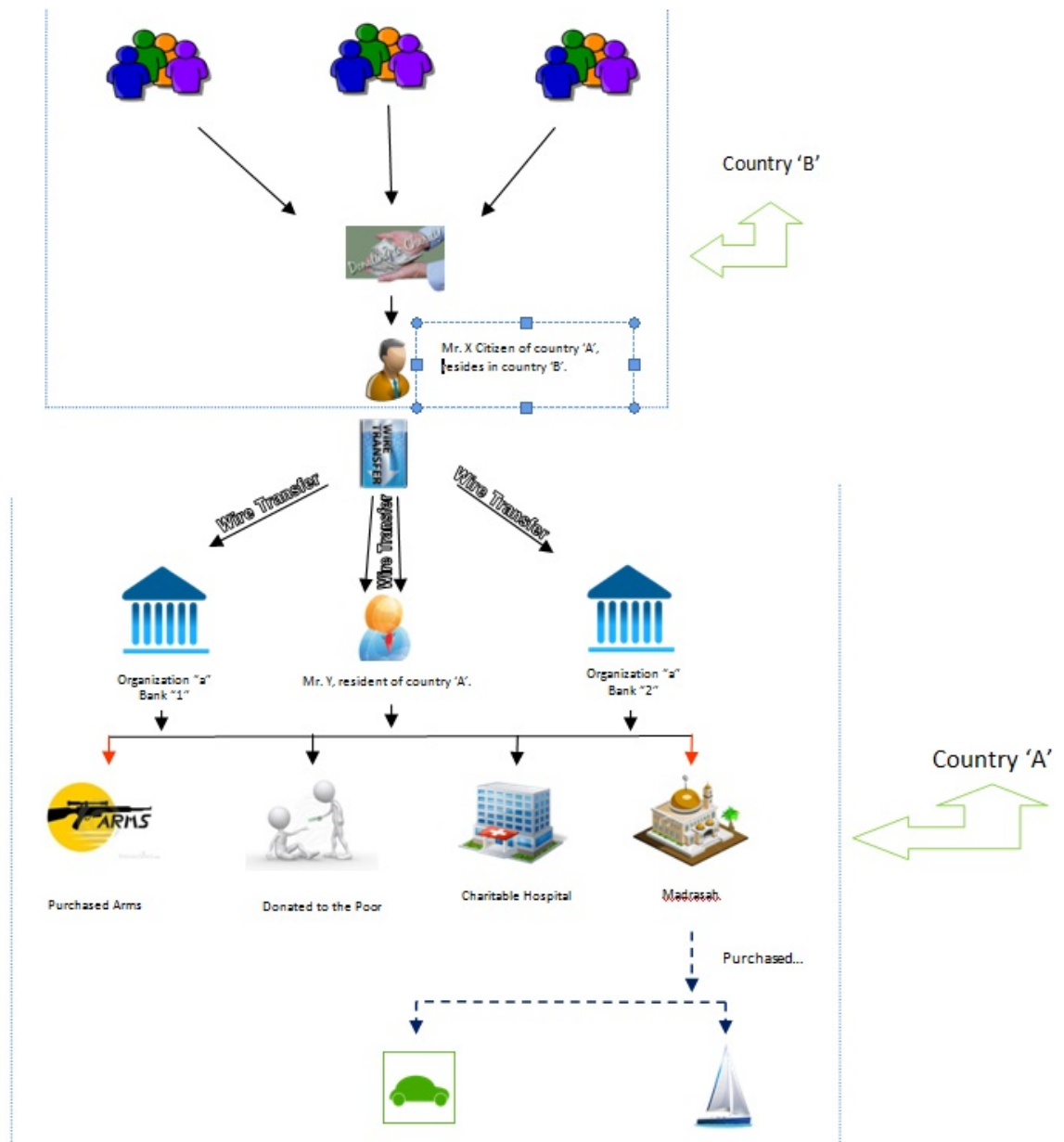
610. Activities in Country A

- A part of the wired funds was utilized to construct mosque and a charitable hospital.
- Part of the wired funds were donated to poor people.
- All these charity functions were conducted to create a positive social image.
- The remaining part of the funds was used to establish a religious school (madrasa) at a very remote area of the southern part of Country A.
- The madrasa was similar to a fort with trenches all around it.
- The madrasa fund was used to buy heavy vehicles and expensive boats.
- Some of the funds were transferred to an arms dealer.
- Incorporating above information, the FIU prepared a report and sent it to LEA.

611. Final Outcome

- Police raided the madrasa based on intelligence reports.
- Police recovered abundant arms and ammunition.

- The case is now under trial.



CHINESE TAIPEI

612. Mr Han was the Chairman of Yang X Travel Agency. Mr Li was the manager of the agency's tourism department.
613. In July 2009, the travel agency organized international group tours and collected a total of NTD5,736,884 (about USD200,000) from customers to cover the tour costs. The money was not used to pay tour expenses; instead it was appropriated for other purposes. As a result, the tours could not go ahead as scheduled.
614. To prevent the capital from being confiscated after the agency's cheque bounced, Mr Han instructed Mr Li to wire over USD100,000 to Mr Li's personal account in the Cheng Dong Branch of First Bank, but purportedly for the Da X Travel

Agency in Singapore to conceal it. Then, Mr Li used part of the money to pay off money owed to the tour groups and took the remaining NTD2,132,676 (about USD71,000) into his personal possession as salary and pension owed to him by the company. The case was referred to Taipei District Prosecutor's Office on May 20, 2011 by the Investigation Bureau.

FIJI

615. Person A and Person B (husband and wife) were the managing directors of Company X. Person B maintained five offshore accounts in Country Z. Person A and Person B had both been remitting funds to Country Z & Country W.
616. Company X maintained a local business bank account at Bank XYZ. It was established that on a few occasions, mutilated notes were deposited into this business bank account.
617. The Fiji FIU also established that the daughter of Person A and Person B resided in Country Z and the sister of Person B resided in Country W. These third parties appear to have been beneficiaries of the business proceeds of Company X that were remitted to Countries Z and W.

HONG KONG, CHINA

618. A syndicate in jurisdiction A established two offshore trading companies and opened two bank accounts in Hong Kong. Between 2005 and 2008, numerous victims all over the world were deceived into remitting money (totalling about USD30million) into these two bank accounts.
619. Acting on information provided by overseas LEAs, Police arrested two persons-in-charge of the companies, who were found engaging some remittance agents to remit the 'sales proceeds' via Hong Kong back to Jurisdiction A. The arrested persons were charged for ML offence(s) in Hong Kong.

THE PHILIPPINES

620. Country K requested assistance from Country R. Country K is conducting an investigation on the following individuals for violations of its criminal laws by conspiring with each other and others to submit false and/or forged documents and/or statements to defraud AA Bank and BB Group, and of money laundering in the amount of £700 million (USD1 billion):
1. AK a.k.a. SK
 2. AL a.k.a. ML
 3. MHB
621. The crimes were allegedly perpetrated between 2003 and 2007, when AA Bank advanced around £700 million (USD1 billion) to one of its customers through a number of companies on the understanding that the loans were guaranteed by Gold Properties, an "A"-rated well-known property company in Country H.
622. AA Bank was to fund AK's purchase of commercial properties in Country K, through a number of companies created for the purpose, known as the Special Purpose Vehicles (SPVs). The SPVs, as landlords, would thereafter lease the

properties to other SPVs which, in turn, would lease those to tenants in occupation.

- 623. AK, MW, and MHB, misrepresented to AA Bank that Gold Properties was the parent company of the tenant SPVs, and that in return for the guarantees from Gold Properties, a reverse premium of cash back would be paid by AA Bank to the tenant SPV. AA Bank relied on the misrepresentations. Hence, the release of £700 million to AK, MW, and MHB.
- 624. Gold Properties denied any involvement with AK, MW, and MHB, informing AA Bank that the documents the latter relied upon were forgeries.
- 625. Country K believes that MW concealed the proceeds of the fraud by passing them to RR (MW's wife) through her bank accounts in Country R. RR received cash deposits in Country K bank account during the period of the fraud even if she has not declared any income from employment in Country K since 2005.
- 626. Country K found that AK is in fact SK who has previous conviction in 1995 for fraud with ML. He changed his name from SK to AK in 1998. MW, on the other hand, is in fact ML. ML has previous convictions in 1993 for obtaining and selling false passports and in 1995 for fraud with SK.
- 627. Country K identified two bank accounts in the name of RR in Country R where the proceeds of the above mentioned unlawful activities were transferred namely, Account No. 111 in SS Bank and Account No. 888 in CC Bank.
- 628. Country R, after further investigations, discovered that RR holds three other bank accounts (two in NN Bank and one in SS Bank). It was found out that these bank accounts have various large transactions. Investigations conducted by Country R revealed that GG, sister of RR, received remittances from RR.
- 629. The bank accounts of GG also have numerous large transactions.
- 630. Country R's investigation also showed that Spouses MW and RR owned one condominium unit and two (2) parking slots. It appears that they acquired the above-mentioned properties through a loan from SS Bank. However, no loan or real estate mortgage is annotated in the titles.
- 631. The funds found in the bank accounts and the aforesaid real properties are now the subject of a freeze order.

SRI LANKA

- 632. Mr "A" a resident non-national of Sri Lanka has been a director of small medical centre since the year 2000. He has opened several foreign currency accounts with an International Bank operating in Sri Lanka. The bank filed a suspicious transactions report stating that there were an unusually large number of inward and outward remittances to/from his account.
- 633. Inquiries into the account revealed that he had received inward remittances to the value of USD3 million from a company in country "T" and has remitted the same amount of money to various parties in several other countries. The single transaction value of outward remittances was within the range of USD 2,000 to

USD50,000 whereas for inward remittances, it was within USD2,000 to USD500,000. The explanations given were that inward remittances were from his business partners and outward remittances were for investments in stocks and purchase of properties.

634. The investigators were unable to identify valid reasons for such fund transfers and the case was referred to the Exchange Control Department of the Central Bank of Sri Lanka to investigate any violations of the Exchange Control regulations. Further, the matter was referred for the FIUs of the respective countries from where the funds were remitted in and out.

4.26 Use of foreign bank accounts

AUSTRALIA

Superannuation accounts targeted in a multi-million dollar identity theft

635. AUSTRAC information was used extensively by a law enforcement agency to investigate a multi-million dollar identity theft and fraud syndicate that targeted superannuation accounts.
636. Members of the syndicate stole cheques, superannuation statements and personal bank statements from the mailboxes of unsuspecting victims and used this information to produce high-quality counterfeit identity documents. These documents were then used to conduct frauds.
637. Syndicate members also approached some victims directly, offering them early access to their superannuation funds and requesting details of their funds to facilitate access to their superannuation benefits.
638. The criminal syndicate carried out four variations of the fraud, using the following methods to obtain superannuation funds from unsuspecting victims:
1. The syndicate member steals a victim's identification papers and opens a self-managed superannuation fund (SMSF) in the victim's name. The syndicate member then sets up a linked, but fraudulently obtained, bank account using the details of the new SMSF. Assuming the victim's identity, the syndicate member contacts the victim's superannuation provider and requests that they 'roll over' the funds from the legitimate superannuation fund into the new, fraudulent SMSF. The syndicate member then withdraws the funds from the new SMSF account and sends them to the syndicate member's offshore account using remittance service providers.
 2. The syndicate member offers a victim the chance to access their superannuation funds early. Scammers usually target victims who are struggling with debt, unemployed and from non-English speaking backgrounds. The victim, enticed by the offer, provides their financial and identification details to the syndicate member to facilitate the early release of the funds. The syndicate member withdraws the funds and takes approximately 20 per cent as their fee. The balance is paid to the victim in cash.

3. As a variation of the above method, the syndicate member offers early access to superannuation funds to lure a victim to provide their financial and identification details. In this instance, the syndicate member uses this information to steal all the victim's superannuation funds. The victim receives nothing.
4. The syndicate member offers to roll over a victim's superannuation into a legitimate fund that they claim will offer a better return. The victim provides the syndicate member with their financial and identification details. The syndicate member rolls over the victim's funds into the syndicate member's fraudulent SMSF and then withdraws the funds from the bank account.

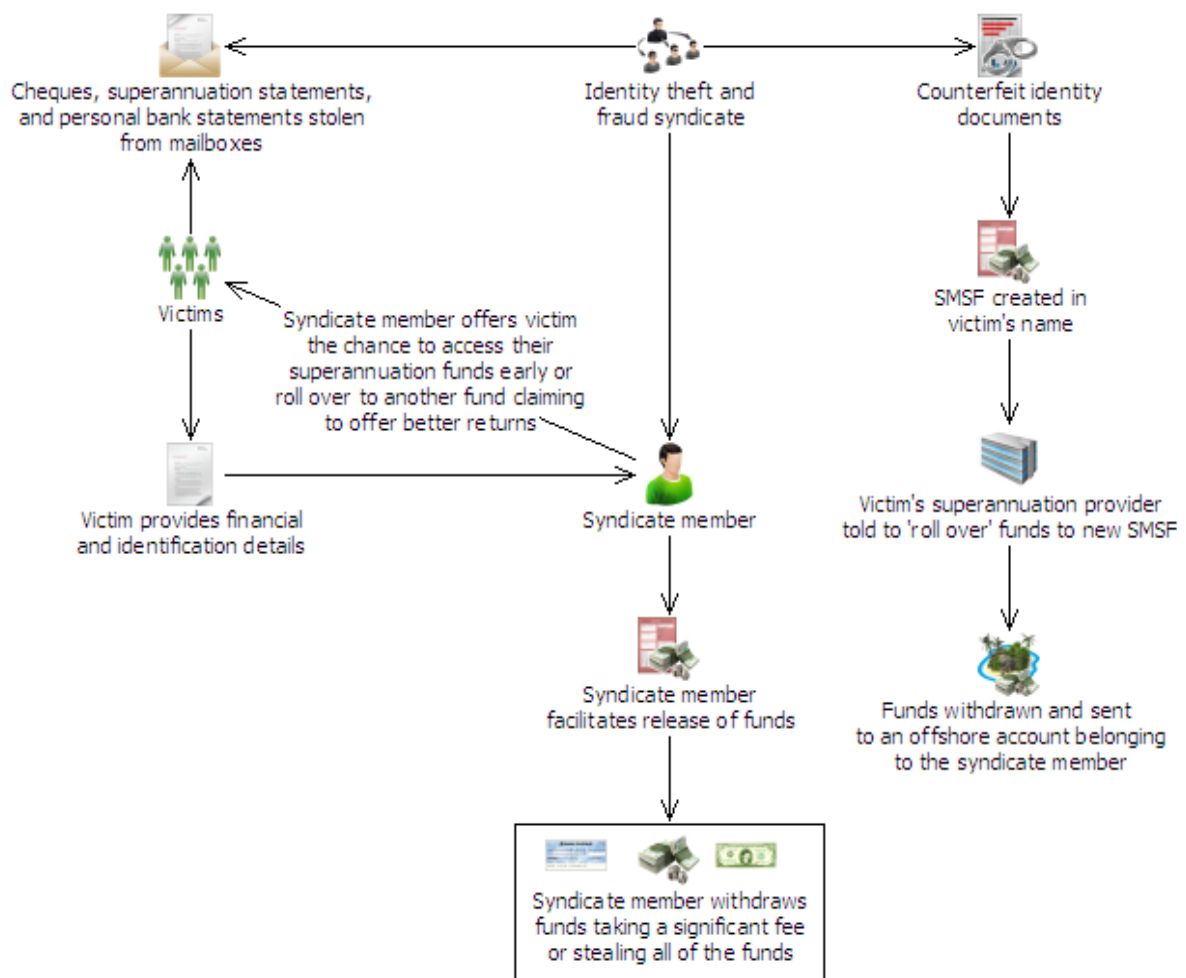
639. AUSTRAC received suspicious matter reports (SMRs) and suspect transaction reports (SUSTRs) detailing information about individuals suspected of perpetrating the fraud. Information in these reports, combined with further AUSTRAC analysis, identified a large criminal syndicate which was:

- Receiving regular cheque deposits into newly opened accounts and paying an additional fee to ensure the cheques cleared quickly. Once the cheques were deposited, the funds were withdrawn from the accounts, either via cash (in amounts of AUD1,000–AUD20,000) or via cheques (valued at between AUD6,500 and AUD45,000) made payable to third parties. The cash withdrawals of AUD10,000 or more were reported to AUSTRAC as significant cash transactions.
- Submitting fraudulent applications to roll over funds from victims' superannuation funds managed by retail or industry fund managers, into accounts held by the syndicate members.

640. One particular SMR alerted a law enforcement agency to the suspicious activities of a syndicate member. The SMR identified the syndicate member as the signatory to two business cheque accounts which had been newly opened to operate two SMSFs. Over a three-month period these accounts received more than AUD500,000 worth of funds which had been rolled over from several superannuation funds. Once the funds were deposited into the new cheque accounts, they were immediately withdrawn by the syndicate member. Information about the international transfers was submitted by reporting entities to AUSTRAC via international funds transfer instructions (IFTIs).

641. A total of 25 syndicate members were charged with more than 2,500 offences involving the laundering of over AUD8 million in fraudulently obtained funds.

642. The head of the syndicate, who controlled three bank accounts which turned over AUD1.6 million, was charged and found guilty of 57 counts of identity fraud and money laundering relating to transactions valued at more than AUD550,000.



643. Indicators in this case included:

- Customer submits a fraudulent application to roll over funds from a superannuation account into a newly opened account.
- Customer undertaking large deposits and cash withdrawals inconsistent with their established customer profile.
- Significant cash and cheque deposits/withdrawals from newly opened accounts.
- Significant value and volume of cash deposits into newly opened bank accounts.
- Significant value of funds rolled over into a recently opened SMSF account, followed by immediate cash withdrawals.
- Use of false identification.

FIJI

644. A local business director remitted business funds into his multiple personal bank accounts in Country K. Business funds totalling FJ\$378,783 (USD205,526) was remitted to multiple bank accounts maintained at different commercial banks in different localities of Country K over a period of 3 years.

645. Common suspicious indicators included:

- Director remitting multiple large remittances ranging from \$5,000 to \$15,000.
- Total of \$378,783 outward remittances over a period of 3 years.

- Funds were remitted into multiple bank accounts in Country K.
- Bank accounts were maintained in different branches of the commercial banks in Country K.
- The director was using money remittance services to remit large cash transactions.

646. The suspicious transaction patterns of the individual raised a high flag on all the transactions of the business director. A proactive STR (PSTR) was raised internally by Fiji FIU (using an intelligence software: the Alert and Monitoring System & Data Mining System - AMS/DMS) for further background checks on the business director.

647. During the analysis it was established that the director held permanent residency status in Country K and made frequent payments to his Visa debit card through a foreign exchange company.

648. He breached the Central Bank's Exchange Control requirements by not providing proper tax clearance documents for the payments made to his Visa debit card. Furthermore it was established several of his business accounts were closed on the same day. After further analysis the FIU established a possible tax evasion offence and the case was referred to the local tax authority for further investigations.



JAPAN

Fraud by an Investment Advisory Company

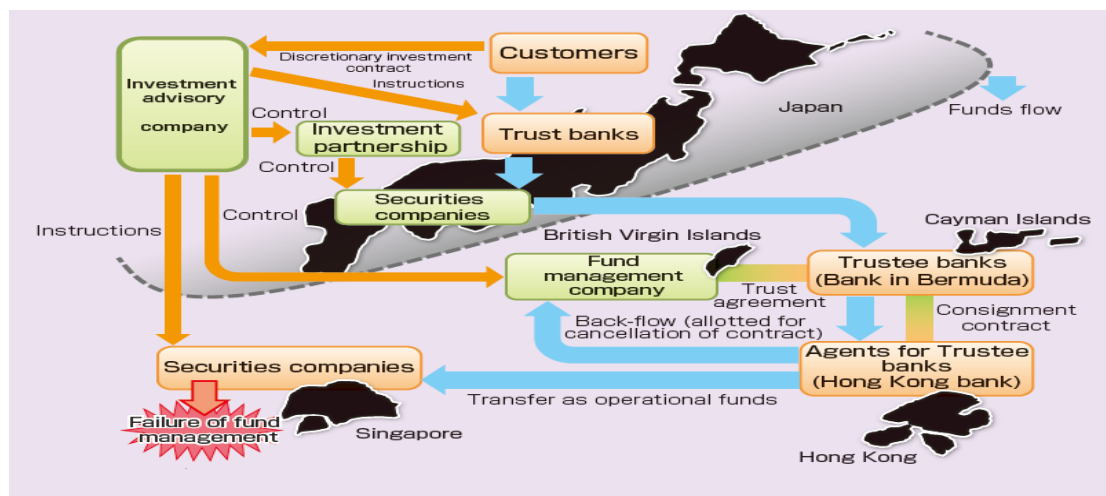
649. The president and other executives of an investment advisory company managing funds, under discretionary investment contracts with several corporate retirement funds, hid various losses incurred in the operation.

650. These executives were arrested on fraud charges, specifically for defrauding new customers into believing that their business operations were sound and generating funds.

651. The company established trust bank contracts between fund management companies under their umbrella organization and overseas banks.

652. This created a structure where the funds were difficult for Japanese authorities to trace as the funds generated through this scheme were sent overseas and, in addition, moved to highly secret bank accounts overseas.

653. This scheme hid the firm's management issues completely²⁶.



SINGAPORE

654. T incorporated two companies in the British Virgin Islands and set up bank accounts for the two companies with banks in Singapore and another Asian Country. All the accounts set up in Singapore could be operated via the internet. These accounts in Singapore were used to receive criminal proceeds from scam victims overseas.

655. The perpetrators of the scam sent out emails in the name of an organization in Europe. The perpetrators informed the clients of the organization that they still owed the organization monies for the services rendered, and requested the clients to send the monies to one of the said accounts in Singapore.

656. Monies received in the Singapore accounts were remitted out to bank accounts overseas within days of receipt. Within four months, more that USD 2 million passed through the accounts.

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

658. T was eventually prosecuted for two ML charges relating to the facilitation of the transfers of criminal proceeds. There was no evidence that he was involved in the predicate offence. The court convicted and sentenced T to 8 months imprisonment for money laundering.

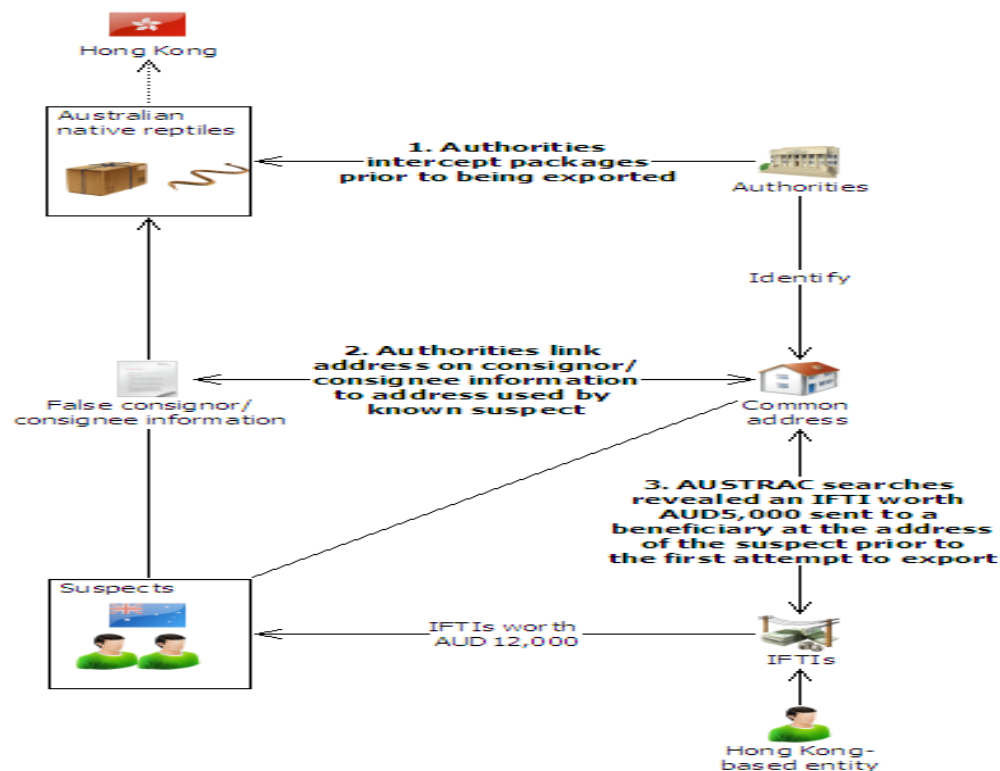
²⁶ Japan Financial Intelligence Center (JAFIC), *Annual Report 2012*, 62, http://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/data/jafic_2012e.pdf

4.27 Use of false identification

AUSTRALIA

Suspects attempted to smuggle native reptiles hidden in stuffed toys

659. AUSTRAC information contributed to the arrest of two Hong Kong nationals based in Australia suspected of being involved in the illegal exportation of Australian native reptiles.
660. Authorities intercepted a parcel destined for Hong Kong which contained native Australian reptiles concealed in stuffed toys. The suspects used false consignor and consignee information in an attempt to evade detection by Customs authorities. AUSTRAC information revealed a link between the address listed on the parcel and an address associated with a person previously suspected of involvement in wildlife smuggling.
661. Searches of the AUSTRAC database revealed an incoming international funds transfer instruction (IFTI) report for AUD5,000 (which included the same address as the one on the intercepted parcel) that was sent to a person based in Australia. The funds were sent from Hong Kong to Australia a week before the attempted export.
662. Over a 12-week period a total of six packages in four consignments were intercepted by authorities. Further searches of AUSTRAC information identified that the Australian-based suspect was the beneficiary of incoming international fund transfers totalling more than AUD12,000 from the same Hong Kong-based entity. The incoming international funds transfers were made shortly before each attempt to export wildlife.
663. Authorities executed a search warrant on a residential property in Australia and seized various Australian native reptiles, soft toys, packaging and postage material. The Australian-based suspect and an associate were arrested for attempting to export Australian native reptiles. Both were convicted for offences under environmental protection law.



Offence	Reptile smuggling
Customer	Individual
Industry	Banking (Authorised Deposit-Taking Institutions)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Hong Kong
Designated service	Account and deposit-taking services
Indicators	Multiple low-value international funds transfers

HONG KONG, CHINA

664. Three overseas victims were deceived to remit a sum of USD90,000 into an account in Hong Kong designated by fraudsters. Police enquiries revealed that the passport provided by the account holder for opening the account had been reported lost by a genuine owner in another jurisdiction.

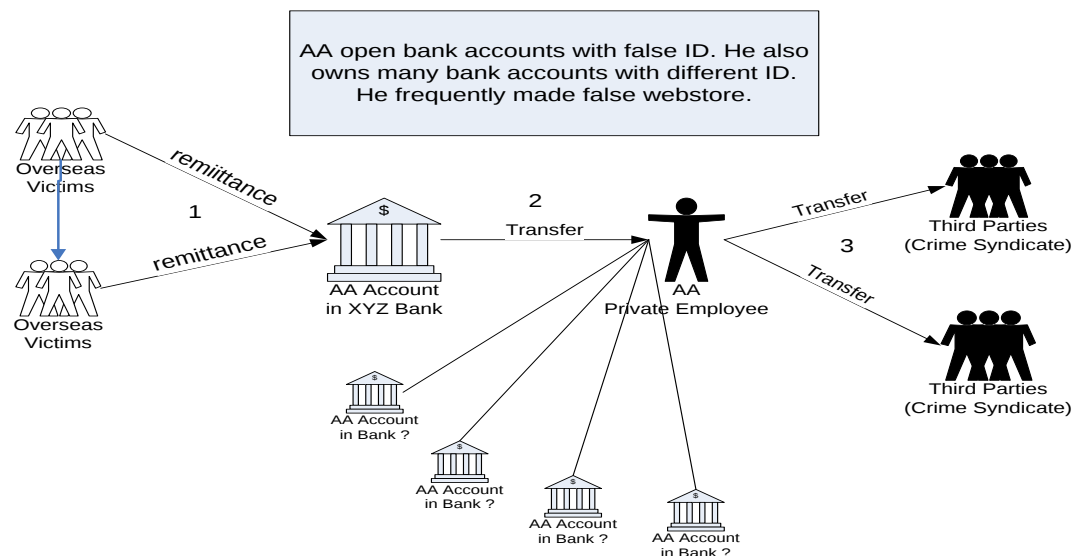
665. Police managed to freeze the account, with HK\$700,000 (USD90,000) of crime proceeds restrained and subsequently confiscated.

INDONESIA

Internet Fraud Case Using False Identity

- There was a large amount of funds from few people outside Indonesia to an AA account at XYZ bank.
- AA was known as a private employee.
- Funds were entered then withdrawn on the same day and transferred to a number of other third-party account (syndicate) over a short time and leaving a minimal balance.

- There were complaints from victims who sent money to an account at Bank XYZ and requested the funds be returned. However XYZ bank could not return the money because the funds had already been transferred.
- There was a report from Interpol that the victim transferred the funds in response to advertising on the internet and was persuaded to send funds to the account of the seller company's AA.
- After checking the address at the company, it revealed fictitious sellers.
- AA often opened up a new web site address if it succeeded in deceiving victims, as well as opening new accounts in different banks with fictitious documents.



SINGAPORE

666. Liew Chee Meng Anderson was an executive with the Ministry of Home Affairs. Between January 2007 and January 2011, he submitted forged 'email approvals' for the purchase of shopping vouchers to the Ministry's finance officers, leading them to believe that the purchases were for the Ministry's activities and events.
667. Liew used the vouchers for personal purchases of branded goods. He misappropriated a total of \$617,087 (USD489,000) in this manner. The police investigation resulted in the recovery of \$470,000 (USD373,000) in cash and other assets.
668. On 5 January 2012, Liew was convicted and sentenced to eight years and eight months' imprisonment for cheating, forgery, criminal breach of trust as a servant and money laundering.

5. USEFUL LINKS

Anti-Corruption Research Network

669. The Anti-Corruption Research Network (ACRN) is an online platform and the global meeting point for a research community that spans a wide range of disciplines and institutions. ACRN is a podium to present innovative findings and approaches in corruption / anti-corruption research, a sounding board to bounce off ideas and questions, a marketplace to announce jobs, events, courses and funding. The periodic spotlight section also looks at specific corruption issues and highlights key research insights and contributions on the selected topic.

<http://corruptionresearchnetwork.org/>

Basel Institute of Governance

670. The Basel Institute on Governance is an independent not-for-profit competence centre specialised in corruption prevention and public governance, corporate governance and compliance, anti-money laundering, criminal law enforcement and the recovery of stolen assets.

<http://www.baselgovernance.org/>

Center for Global Counterterrorism Cooperation (CGCC)

671. The CGCC is a non-profit, nonpartisan policy institute dedicated to strengthening international counterterrorism cooperation. It works to build stronger partnerships to prevent terrorism among many actors and across many levels:

- the United Nations, regional organizations, and states
- communities, police, and governments
- researchers, practitioners, and policymakers
- survivors of terrorism around the world

672. The CGCC builds these partnerships through collaborative research and policy analysis and by providing practical advice. CGCC develops innovative counterterrorism programming and training and assists key stakeholders to develop sustainable solutions to preventing terrorism. CGCC is working to improve intergovernmental cooperation at the global, regional, and sub-regional levels; support community-led efforts to counter violent extremism; ensure respect for human rights and the rule of law; and empower civil society and victims of terrorism to speak out. As transnational threats evolve, CGCC is also working to foster a new generation of holistic, rule of law-based responses to organized crime and other forms of transnational violence.

<http://www.globalct.org>

The Egmont Group

673. For FIU information and links to FIUs with websites.

<http://www.egmontgroup.org/>

Global Financial Integrity

674. Global Financial Integrity (GFI) promotes national and multilateral policies, safeguards, and agreements aimed at curtailing the cross-border flow of illegal money. In putting forward solutions, facilitating strategic partnerships, and conducting research, GFI is making efforts to curtail illicit financial flows and enhance global development and security.

<http://www.gfintegrity.org/>

FATF/ FATF-Style Regional Bodies

CFATF - Caribbean Financial Action Task Force (FSRB)

EAG - Eurasian Group (FSRB)

ESAAMLG - Eastern and South African Anti Money Laundering Group (FSRB)

FATF - Financial Action Task Force

GAFISUD - Grupo de Acción Financiera de Sudamérica (FSRB)

GIABA - Groupe Inter-Gouvernemental d'Action Contre le Blanchiment de l'Argent en Afrique (FSRB)

MENAFATF - Middle East and North Africa Financial Action Task Force (FSRB)

MONEYVAL - Council of Europe, Committee of Experts on the Evaluation of AML Measures and FT

Regional Organisations

ADB/OECD Anti-Corruption Initiative for Asia-Pacific

OCO - Oceania Customs Organisation (Secretariat)

International Organisations

Commonwealth Secretariat

IMF - International Monetary Fund

UNODC - United Nations Office on Drugs and Crime

UNODC-GPML - Global Programme on Money Laundering

WCO - World Customs Organization (English)

World Bank - AML/CFT

6. ACRONYMS

AC - Anti-Corruption
ADB - Asian Development Bank
AGD - Attorney General's Department
AML - Anti-Money Laundering
AMLD - Anti-Money Laundering Department
ATM - Automatic Teller Machine
AUSTRAC - Australian Transaction Reports and Analysis Centre
BNI - Bearer Negotiable Instrument
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
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
ICRG – International Cooperation Review Group
IFTI - International Funds Transaction Instruction
INTERPOL - International Criminal Police Organisation
KPK - Indonesia's Corruption Eradication Commission
LEA - Law Enforcement Agency
ML - Money Laundering
MLA - Mutual Legal Assistance
MOU - Memorandum of Understanding
MSB - Money Service Bureau
NPO – Non-Profit Organisations
OFC - Offshore Financial Centre
PEP - Politically Exposed Person
SAR – Suspicious Activity Report
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
UNSCR – United Nations Security Council Resolution
VAT - Value Added Tax