APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2015

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

Approved and adopted, 16 July 2015

APG Yearly Typologies Report 2015

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

CONTENTS

INTRODUCTION

Background

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

2. The Yearly Typologies Report is an important output that is provided under the APG's Strategic Plan and the APG Typologies Working Group Terms of Reference. It 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 2014-2015

4. The APG Typologies Working Group continued its work in 2014-15 under the leadership of Mongolia and Fiji as Co-chairs. In July 2014 the APG Typologies Working Group met to determine the work program for the year, including the conduct of a joint FATF and APG Typologies Workshop in November 2014 hosted by Thailand in Bangkok.

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 2014 - 2015

1.1 2014 Joint FATF/APG Experts' Meeting on Typologies

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/Technical Seminars to share practitioners' experience on priority topics.

8. The agendas of APG typologies 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 Financial Action Task Force (FATF) and FSRB-led typologies studies; and
- Share best practices and strategies for practical application of AML/CFT measures related to previous typologies studies and other implementation issues.

9. The 2014 FATF/APG Joint Experts' Meeting on Typologies and APG Technical Seminars were held in Bangkok, Thailand, from 24-28 November 2014, hosted by the Government of Thailand and the Anti-Money Laundering Office, Thailand.

10. The Joint Experts' Meeting (JEM) took place 24-26 November and involved approximately 250 delegates from 54 jurisdictions and eight international organisations. The JEM was co-chaired by APG Typologies Working Group (TYWG) Co-Chairs Razim Buksh (Fiji) and Bazarragchaa Tumurbat (Mongolia) and FATF RTMG Co-Chairs Martin Tabi (Canada) and Leonard de Jager (the Netherlands).

11. This year the JEM plenary session included a keynote address on beneficial ownership, a case study presentation from the APG region, an update on key typologies projects of regional and international interest and a panel discussion on the results of national risk assessments. In addition to the plenary discussions there were three parallel typologies workshops:

- Transparency of beneficial ownership
- Third party money laundering
- Trade-based money laundering

12. Prior to the JEM, on Sunday 23 November, a joint APG/Egmont Group seminar was held for the 18 FIUs in the APG region that are members of the APG, but not yet members of the Egmont Group. The seminar covered essential membership and FIU operational information, which elicited very positive feedback from all who participated.

13. Following the JEM, on 27-28 November, the APG held two technical seminars. These seminars were conducted as part of the APG's capacity building programme and involved APG

member and observer organisations, as well as approximately 25 representatives from the private sector who had been invited through the APG primary contact points. The two seminars discussed:

- Making Asset Recovery Work
- AML/CFT and New Technology: Understanding Cyber and Technology Enabled Crime

14. The technical seminars aimed to expand partnerships between the public and private sectors on AML/CFT typologies. It was also an opportunity to enhance industry cooperation on AML and draw on industry experience in the selection and conduct of studies of ML and TF typologies.

15. The outcomes from the workshops and seminars in Thailand will play a positive and practical role in improving regional cooperation and countermeasures for AML/CFT across the APG region.

1.2 Status of current projects and possible new projects

16. The APG/FATF joint project on *Gold – Money Laundering and Terrorist Financing Risks and Vulnerabilities* is being co-led by India and Australia and has been carried out over the 2013-2015 period. The final report will be presented to the FATF in June 2015 and APG plenary in July 2015 for endorsement, after which it will be published on the APG and FATF websites. The project team included representatives from: Argentina, Australia, Bahrain, Bangladesh, Belgium, China, Denmark, Ecuador, Germany, Ghana, Haiti, Hong Kong, India, Iraq, Malaysia, Nepal, Pakistan, Peru, Qatar, Russia, St Kitts-Nevis, Switzerland, Thailand, UAE, USA, Zimbabwe, APG, CFATF, EAG, Egmont Group, ESAAMLG, FATF, GAFILAT, GABAC, GIABA and MENAFATF.

17. The project examined the characteristics of gold production, movement, trade and markets with a focus on the illicit risks. The aim of the project was 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 designated non-financial business and professions (DNFBPs), financial institutions and others to capture relevant data and, as appropriate, identify reporting suspicious activity associated with the precious metals market. The APG is also progressing four Pacific-focused typologies projects due to be completed over the 2013-2016 period: *ML and Frauds in the Pacific,* being co-led by Fiji and Vanuatu; *Recovering the Proceeds of Corruption in the Pacific*, being co-led by Papua New Guinea and Tonga, in conjunction with the Pacific Islands Law Officers' Network (PILON); *ML/TF risks Associated with Offshore Centres in the Pacific*, being co-led by the Cook Islands and Samoa; and *ML/TF Risks Associated with Trans-Pacific Drug Trafficking Routes*, co-led by Tonga and Vanuatu.

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

18. A range of typology studies have been published in 2014 and 2015 by the FATF and several other FSRBs, including:

2.1 FATF Typology Projects

Financing of the Terrorist Organisation Islamic State in Iraq and the Levant[1]

19. The FATF's report on the financing of the Financing of the Terrorist Organisation Islamic State in Iraq and the Levant (ISIL) analyses how this terrorist organisation generates and uses its funding. This knowledge is crucial in order to determine how FATF and the international community can choke off ISIL funding.

20. Information collected from a wide range of sources and countries such as Saudi Arabia, Turkey and the United States, demonstrate that ISIL's primary source of income comes from the territory it occupies. The appropriation of the cash held at state-owned banks gave ISIL access to an estimated half a billion USD in late 2014. The exploitation of oil fields also generates significant funds for ISIL, particularly when it first took control of them. This report identifies other sources of funding that ISIL relies on to finance its terrorist activities and the regular investments into its infrastructure and governance requirements.

21. Globally, there has been a strong and clear response on the need to disrupt ISIL's financial flows and deprive it of its assets. Many countries have established stronger legal, regulatory and operational frameworks to detect and prosecute terrorist financing activity, in line with the FATF Recommendations. But more needs to be done. This report highlights a number of new and existing measures to disrupt ISIL financing, for example:

- Request countries to proactively identify individuals and entities for inclusion in the UN Al Qaida Sanctions Committee list.
- Share practical information and intelligence at an international level, both spontaneously and on request, to effectively disrupt international financial flows.
- Suppress ISIL's proceeds from the sale of oil and oil products, through a better identification of oil produced in ISIL-held territory.
- Detect ISIL fundraising efforts through modern communication networks (social media).

22. Further in-depth research is needed to determine the most effective countermeasures to disrupt ISIL funding.

[1] http://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

2.2 ESAAMLG – The Eastern and Southern Africa AML Group

Typologies Report on Money Laundering and Terrorist Financing Through the Money Remittance and Currency Exchange Sector in the ESAAMLG Region[2]

23. The report aims to provide an overview of the regulatory framework, the supervision and sanctioning regimes, as well as identifying money laundering and terrorist financing methods and techniques involving money or value transfer and currency exchange service providers.

24. The identified risks of ML/TF through the remittance and currency exchange sector detailed in the report are mainly related to clients, owners or agents. The case studies cited and described in the report also point to links between money laundering in the money or value transfer sector and other criminal activities (e.g., fraud, tax evasions, trafficking in human beings, smuggling, drug trafficking).

25. The report's findings indicate that the majority of ESAAMLG member countries have not identified the money or value transfer and currency exchange sectors as targets for those advancing terrorism financing activities. This finding is despite other open sources regarding this sector as high risk as far as terrorism financing activities is concerned. This is attributed to the lack of, or poor, controls that mitigate its inherent terrorist financing risk exposures. Through the analysis of case studies and other materials, the project team was also able to compile numerous examples of indicators of potential money laundering activities related to transactions, customer profile and behaviour, as well as specific indicators for currency exchanges and money or value transfer service providers that may help the industry to identify and describe suspicious behaviours and protect themselves against money launderers and other criminals.

26. Although its findings, based on responses from ESAAMLG member countries, do not support this, other sources indicate that particular risks involved with the sector are related not only to the misuse of the sector services for laundering money but also to the owning of such businesses by criminal groups and corrupt employees co-operating with criminals.

27. The report equally points to regulatory and supervisory control weaknesses which clearly encourages laundering through the money or value transfer and currency exchange sectors. From the findings, it is clear that there is a low detection of money laundering in comparison to the size of the industry as a whole. Unlike other sectors like the banking sector, it is also clear that many countries in the ESAAMLG region do not have adequate mechanisms to help increase the detection rate of money laundering and terrorist financing activities in bureaux de changes and other money remitters. With an understanding of risk exposures in the sector, the report also provides recommendations (points for consideration) at an international cooperation level and at a national level for involved stakeholders such as LEAs, FIUs etc.

2.3 The Egmont Group

Best Egmont Case Award (BECA) book of Egmont Financial Analysis Cases

28. The Egmont Group's Training Working Group t published the first *Best Egmont Case Award (BECA) book of Egmont Financial Analysis Cases*. The book is the product of the first three years of the BECA competition and showcases the excellent work done by FIUs in identifying and prosecuting money laundering offences.

29. The book contains material that can be used in the widest context and its audience will be anybody who is interested in understanding how financial analysis is a vital component of a money laundering investigation. The twenty-two cases have been broken down by investigation type and

[2] http://www.esaamlg.org/userfiles/Typologies_Report_mvts.pdf

include examples of bribery, corruption, drug trafficking, fraud, human trafficking, organised crime and terrorist financing.

30. The book can be accessed here: http://www.egmontgroup.org/library/cases

2.4 Others

Financial Transactions and Reports Analysis Centre of Canada (FinTRAC)

Mass Marketing Fraud: Money Laundering Methods and Techniques – January 2015[3]

31. Mass marketing fraud is a crime which is growing in scope and one that incurs substantial losses to victims worldwide. This typologies and trends report aims to identify techniques and methods that are used to launder the proceeds of mass marketing fraud, based on an analysis of voluntary information records and financial transaction reports included in FINTRAC disclosures to Canadian police services and foreign financial intelligence units.

32. Several categories of mass marketing fraud exist, each with particular characteristics designed to defraud victims. Almost all of the cases analysed for this report involved businesses and the automotive sector is one of the main sectors suspected of being used to launder the proceeds of mass marketing fraud.

33. Structuring and the use of nominees are two money laundering methods which have been observed by FINTRAC. While financial institutions appear to be used for suspected money laundering associated to certain mass marketing fraud schemes, many schemes appear to leverage money service businesses not only to receive funds from victims, but to launder the illicit proceeds as well.

34. Red flags indicating the use of businesses to launder the proceeds of mass marketing fraud (based on the analysis of financial transaction reports and voluntary information records) include:

- Receipt of funds from or depositing of funds (electronic funds transfers or cheques) by individuals who do not appear to be related to the business activities of the company holding the account;
- Repeated transfers of funds from a personal account to a business account;
- Repeated deposits of cash into the account of a company that is active in a sector where cash transactions are unusual;
- Receipt of electronic funds transfers into a business account followed by one or more electronic funds transfers to the country from which the wire payments initially originated.

35. Red flags indicating the use of businesses to launder the proceeds of mass marketing fraud (based on the analysis of financial transaction reports and voluntary information records) include:

- Repeated and atypical deposits of cheques issued by a money service business into a bank account;
- Repeated and atypical deposits of cash into a bank account;

[3] http://www.fintrac-canafe.gc.ca/publications/typologies/2015-02-eng.asp
http://www.fintrac-canafe.gc.ca/publications/typologies/2015-02-eng.pdf

- Atypical or "uneconomical" electronic funds transfers (e.g., United States to Canada followed immediately by Canada to the United States) made for no reason.

36. Red flags for the use of structuring and nominees in the laundering of proceeds of mass marketing fraud (based on the analysis of financial transaction reports and voluntary information records) include:

- Individuals alternating between several money service businesses in order to make electronic funds transfers to the one person;
- Individuals making several small electronic funds transfers through a money service business or bank on behalf of the one person or a group of persons over a short time period;
- Individuals' receiving several small electronic funds transfers from the one person or a group of persons over a short time period.

3. TRENDS IN MONEY LAUNDERING & TERRORISM FINANCING

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

AUSTRALIA

AUSTRAC Typologies and Case Studies Report

37. To help both industry and government partners detect threats, AUSTRAC produces research on current and emerging money laundering and terrorism financing vulnerabilities.

38. The annual AUSTRAC typologies and case studies reports highlight the diversity and gravity of the threats which money laundering and other serious offences pose to Australian businesses and the community.

39. In compiling these reports, AUSTRAC draws on the combined knowledge of its financial intelligence analysts and partner agencies, to provide real-life examples of how commercial systems can be misused by criminals.

40. All eight typologies and case studies reports (2007 – 2014) are available on the AUSTRAC website, www.austrac.gov.au/typologies.html

National risk assessment on terrorism financing

41. AUSTRAC has prepared a national risk assessment on terrorism financing (NRA TF), which is smaller in scope than the 2011 national threat assessment on money laundering. The classified version of the report was released in April 2014. The public version of the NRA TF, *Terrorism financing in Australia 2014*, which aims to assist industry to identify and mitigate terrorism financing risks was released in September 2014. The report is available on the AUSTRAC website, http://www.austrac.gov.au/publications/corporate-publications-and-reports/terrorism-financing-australia-2014

FIJI

42. The Fiji FIU has conducted only basic and informal research on ML/TF methods and trends. The Fiji FIU continues to provide this information through the following:

- The Fiji FIU Annual Report, which in 2013 included case studies from Suspicious Transaction Reports and one major case study on a successfully prosecuted ML case in Fiji. The report also included emerging, continuing and declining money laundering trends. A copy of this report is available on Fiji FIU's website; www.fijifiu.gov.fj
- AML Compliance Officers Forum – ML typologies, trends and indicators are shared during this forum with AML compliance officers of financial institutions.

INDONESIA

43. Indonesia regularly conducts research or studies on ML/TF methods and trends. If there is a current issue or special issue regarding ML/TF methods and trends, non-routine research is conducted. The research, however, is only published internally, and only for limited distribution externally.

44. In the past, research or studies of ML/TF methods pertaining to certain predicate crimes, the transaction methods used, and the reported party profile has been conducted.

45. Recent research or studies on ML/TF methods and trends conducted includes the typology of ML cases that have been decided in the court. The research indicated that the dominant predicate crimes reported are corruption and narcotics. The dominant transaction patterns are transfer via ATM, cash deposit, cash withdrawal, and redemption of insurance policy.

SINGAPORE

National Risk Assessment

46. On 10 January 2014, Singapore published its first National Risk Assessment (NRA) report on money laundering and terrorism financing (ML/TF). The NRA report was the culmination of a government-wide exercise that lasted two years and covered 14 financial sub-sectors1 and eight non-financial sectors[1] in Singapore. Most sectors were found to have a robust regime in place to combat ML/TF, but there were a number of sectors where controls could be strengthened. These include remittance agents, money-changers, internet-based stored value facility holders, corporate service providers and pawnbrokers. Relevant government agencies will be strengthening the legislative and supervisory framework through the year to address the risks in these sectors more effectively.

3.2 Association of Types of ML or TF with Predicate Activities

BRUNEI DARUSSALAM

47. Between 2013 and 2014, the most prevalent predicate offences associated with ML investigations that have been conducted are non-declaration of cross border transport of cash, unexplained wealth and corruption.

CHINESE TAIPEI

48. In recent years, the CIB has investigated a number of transnational frauds and found that criminals obtained large amounts of illicit money from these crimes. Close analysis of the means of money laundering showed that they made extensive use of hawala and alternative remittance systems.

FIJI

Money Laundering

49. The methods of money laundering through financial institutions in Fiji are generally associated with various predicate offences. For example, significant cash deposits detected in personal bank accounts have been linked to possible fraud, corruption and tax evasion.

Terrorist Financing

50. Fiji does not have any incidents or reports of terrorist financing cases, therefore there have been no prosecutions of terrorist financing. There have, however, been investigations of foreign businessmen (in particular foreign nationals from a South Asian country) remitting business funds from Fiji to individuals in the South Asian country that are reportedly linked to terrorist organisations.

INDIA

51. The cases investigated by National Investigation Agency (NIA) show various trends of ML/TF. For example:

(i) Involvement of public servants and contractors in the misappropriation of Government funds and their criminal misconduct, which facilitated the funding of a terror organisation. Workers of NC Hills, Autonomous Council, set up by government were involved in misappropriation of government fund, and facilitating funding of terrorism.

(ii) Use of banking and non-banking channels and trusts for the funding of terror activities.

(iii) Extortion by extremists to fund terror activities.

(iv) Use of offshore banks, international business companies and offshore trusts in facilitating terror funding. An offshore disaster relief fund based in a South Asian country, and reported to have its headquarters in that country, was allegedly used by a terrorist organization to fund terrorist organisations and their families in India.

(v) Utilisation of proceeds of terrorism to purchase/acquire land, flats and vehicles (movable/immovable properties) for terrorist organisations.

(vi) Using some portions of counterfeit currency in funding of terrorism.

(vii) Smuggling and trafficking counterfeit currency along with drugs and weapons through foreign nationals.

(viii) Use of formal and non-formal banking channels, trade based routes, cash couriers by trusts acting as a front organisation for terrorist groups. A South Asian trust and other domestic legal entities were allegedly found to be involved in financing terrorist activities through formal and non-formal banking channels, trade based routes, and cash couriers.

INDONESIA

52. According to the most recent STR statistics, the predicate activities mostly associated with ML are fraud, corruption, and gambling. However, corruption is the predicate activity mostly associated with ML according to the more detailed analysis.

JAPAN

53. Instances of concealment of criminal proceeds consisted largely of cases in which offenders attempted to transfer funds to bank accounts under the name of other persons.

54. For example: A person from a civil engineering business solicited his acquaintance to buy deposit passbooks. The acquaintance and others bought at 60,000JPY several deposit passbooks which the man used to defraud financial institutions. The offenders were arrested on charges of purchasing stolen goods with compensation and for violating the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

MACAO, CHINA

55. Throughout the period from January to June 2014, a total of 877 STRs were received by Gabinete de Informação Financeira (Financial Intelligence Office, Macao SAR), with 663 STRs from the gaming sector, 213 STRs from the financial sector (including banking, insurance and financial intermediaries) and 1 STR from another sector. Common money laundering methods detected from STRs received are as follows:

- Chips conversion without / with minimal gambling activities;
- Suspicious wire transfers;
- Use of cheques / promissory notes / account transfer etc. to transfer funds;
- Unable to provide ID / important personal information;
- Suspected PEP related transaction;
- Irregular large cash withdrawals;
- Significant cash deposit with non-verifiable source of funds;
- Possible match with international watch-list or other black list;
- Use of Counterfeit Notes;
- Account holder issues / receives casino cheques.

56. From January to June 2014, 76 STRs were disseminated to the Public Prosecutions Office. These cases were mainly related to fraud and remittance. The Judiciary Police processed 55 cases which were mainly related to fraud, trade finance, use of debit card and cross border cash smuggling.

MALAYSIA

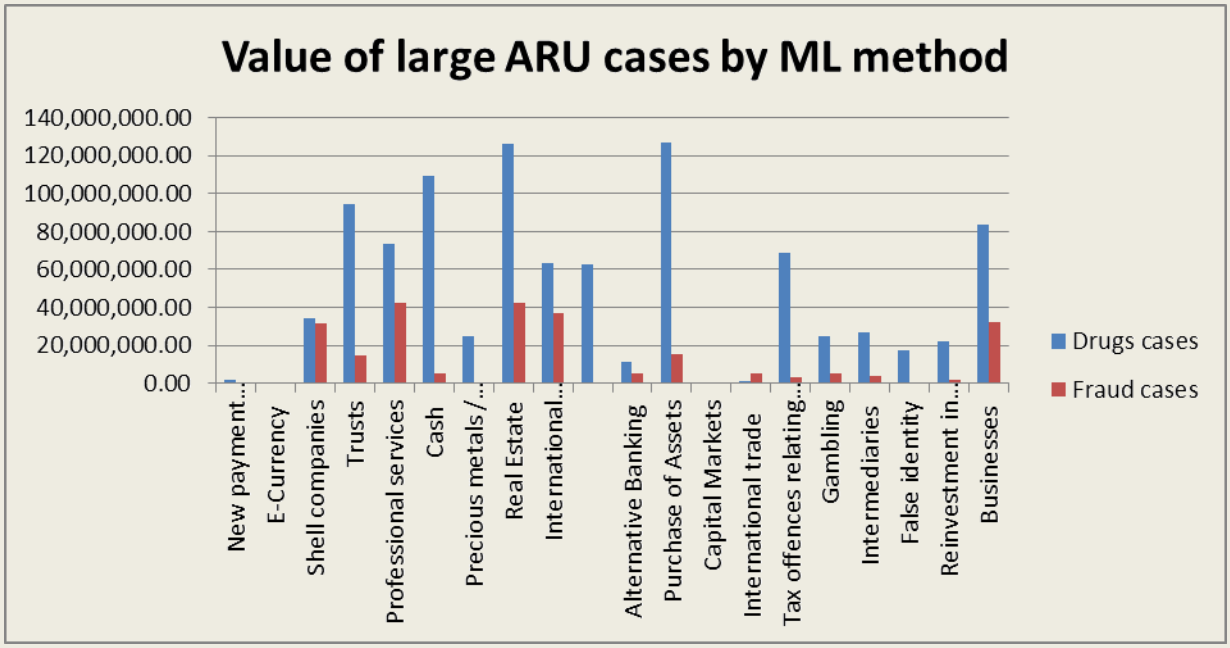
57. Most of the ML cases are related to drugs, smuggling, corruption, fraud/scam, customs duties and tax evasion. This is also in line with high risk threats identified under Malaysia's National Risk Assessment (NRA) which was completed in June 2014.

MONGOLIA

58. According to the police, particular predicate offences known to be associated with ML and TF include:

- Embezzlement of state funds through public tender, and purchase of goods through state funds
- Fraud cases including credit card fraud and identity theft
- Smuggling of gold
- Smuggling of contraband goods

NEW ZEALAND



REPUBLIC OF KOREA

59. The most prevalent pattern of money laundering in the Republic of Korea is observed in the private sectors such as finance, banking, trade and construction. Cash transactions are still the most widely used method of money laundering. Embezzlement, tax evasion and smuggling are the predicate offences associated with money laundering. TF cases are not yet reported in the Republic of Korea.

THAILAND

60. Proceeds derived from drug trafficking, sex exploitation and human trafficking are laundered by opening front businesses or buying real estate, mostly through nominees.

3.3 Emerging Trends; Declining Trends; Continuing Trends

BRUNEI DARUSSALAM

61. Based on case studies provided by various law enforcement agencies on investigations conducted into predicate offences, the FIU is of the view that there is an emerging trend of predicate offences associated with unlicensed financial activity within the formal sector.

62. In addition to the above, the FIU is of the view that there is a continuing trend being reported in Suspicious Transactions Reports of mingling of personal and company funds in accounts held by persons.

FIJI

63. Emerging Trends:

- Email Spoofing - The target has been local business entities that purchase goods and services from overseas. There had been unauthorised access of emails between the local business entity and their supplier overseas. The local business entity will eventually be advised through the unauthorised access that due to some unknown reasons the supplier's bank account overseas had changed and that they need to immediately send the money to new bank account.

- It has been established that the new bank accounts do not belong to the supplier but to those who had gained unauthorised access to the emails and redirected the payment.

64. Declining Trends:

- Use of false identification - The FIU has noted a decrease in the number of cases involving fake identification cards such as passports and birth certificates. This is due to some recent measures undertaken by the relevant authorities in Fiji.

- Use of a minor's bank account to deposit funds.

65. Continuing Trends:

- Currency smuggling is a continuing trend for Fiji. A number of cases were identified where travellers have failed to declare cash of $10,000 and above when arriving into or departing Fiji.

- There were 16 cases of persons brought before the court for failing to declare currency in 2013. In 2014, there were 7 cases of failure to declare at the border by travellers. Some of the cases reported relate to cross-border between Fiji and other Pacific Island countries.

INDONESIA

66. The banking industry is still being used by ML perpetrators to launder their proceeds of crime. However, it is a declining trend. As indicated in recent research, transfer via ATM, cash deposit and cash withdrawals are still used as transaction patterns. However, the increasing strictness of the regulation regarding banks created a new trend for ML, such as using mainly cash transactions (for example, using cash for asset purchase), and the use of non-banking financial industry, especially money changers and money remittance businesses.

67. Recently, the predicate crime of fraud and taxation is increasingly associated with ML, even though corruption is still the predicate crime mostly associated with ML.

JAPAN

68. Fraud and theft are common predicate offences.

69. For example: a company employee and his wife stole around 16 million JPY in cash from a commuter ticket sales office counter of a railway station, and concealed around 9.7 million JPY out of the 16 million JPY by burying the money underground in a forest[4]. They were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

70. A member of a Korean theft group stole a luxurious watch (worth 10 million JPY at the current price) from a house and concealed it in the ceiling of the bathroom where he was staying[4]. He was charged with violating the Act on Punishment of Organized Crime (concealment of criminal proceeds).

71. As a continuing trend, drug trafficking is also common.

72. For example: an associate of Boryokudan (Yakuza/organised crime group) illicitly retailing methamphetamine sent it to his customer by home delivery. He had his customer transfer the purchase price to a bank account opened under the name of third party, and around 3.1 million JPY was transferred to the account. He was arrested for violating the Anti-Drug Special Provisions Law (concealment of drug-related criminal proceeds).

MACAO, CHINA

73. Based on statistics of cases under investigation, there is an emerging trend in the use of new payment methods as a 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 a few individuals using hundreds of different valid credit/debit cards to withdraw cash from ATMs.

74. New payment methods like credit/debit card transactions can now be carried out in a more convenient way and in numerous channels, funds can be withdrawn or converted much quicker and transnationally than through more traditional channels. This can complicate the monitoring process and make it difficult to trace or confiscate criminal proceeds.

MALAYSIA

75. Based on STRs submitted to the FIU as at August 2014, the top 3 suspected offences are tax-related, fraud and smuggling.

76. The continuing trends identified from the STRs analysis include the following:

- Increasing trend in reports on internet/wire transfer scams involving cross border transfer of funds
    - Foreigners or individuals associated to foreigners opening accounts in different/multiple banks;
    - Multiple inward remittances received from various entities in different countries;
    - Funds received were withdrawn in cash and via ATM at various locations immediately upon receipts, leaving low balances in the accounts;
    - Mismatch between transactions and accountholder profiles.
- Large and rapid movement of funds (transit accounts)

[4] This case example has been included because this kind of offence is dealt with as a concealment of criminal proceeds applied in the context of the national legislation which stipulates money laundering in Japan.

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

- Unjustified banking transactions
    - Deposits are not justified considering the nature of the business or profession;
    - Deposits were inconsistent with the volume generated by the business;
    - Deposits at various branches and times for no logical reason;
    - Substantial inter-account transfer between related accounts;
    - Multiple cash deposits into an account followed by a large transfer to other third parties account/countries.

MONGOLIA

77. Emerging trends:

- Sale of drugs and psychotropic substances, especially ice (crystal methamphetamine hydrochloride)
- Credit card fraud

78. Declining trends:

- Currently, declining trends are not identified by the Mongolian Police. However, due to increased inspections and reporting requirements from the Financial Information Unit, offenders may choose methods other than banking and financial institutions to launder proceeds of crime and illicit activities

79. Continuing trends:

- Association of ML with corruption, embezzlement, bribery of state funds
- Real estate purchase of valuable assets in foreign countries, especially luxury houses, apartments, vehicles in Korea, Hong Kong, Japan, USA.
- ML through establishing legal entity and building service sector real estate in Mongolia (e.g. involving a Korean organized crime group)
- Cash couriers/currency smuggling (concealment) to exchange currencies in Mongolia as government control of currency exchange bureaus is not enforced to the full-extent
- Trade-related ML through invoice manipulation, trade mispricing in purchase of goods from abroad, either through legal persons or state institutions responsible for purchase of public goods
- Use of gatekeepers/professional services: accountants, bankers, companies, company service providers
- Wire transfer
- Use of shell companies
- Use of offshore banks/companies
- Use of credit cards
- Use of family members, third parties

- Identity fraud and use of false identification
- Use of foreign bank accounts

REPUBLIC OF KOREA

80. Economic crimes such as tax evasion and embezzlement continue to be the most challenging issues. Utilizing tax havens and paper companies to evade tax and illegally moving assets overseas continue to pose problems.

- Declining trends are not currently identified by the Korean law enforcement agencies. Continuing trends include
- tax evasion and utilizing tax havens and paper companies,
- association of ML with corruption, embezzlement and bribery of state funds,
- foreigners or individuals associated to foreigners opening accounts in different/multiple banks and
- funds received were withdrawn in cash and via ATM at various locations immediately upon receipt, leaving low balances in the accounts.

SINGAPORE

Money Mules

81. In 2012, a new trend emerged whereby money mules recruited from social networking websites with promises of love and friendship were used to launder money.

82. In many of these cases, the victims claimed that their email accounts were compromised. The individuals who compromised the email accounts would then use the email accounts to send fraudulent instructions to the victims' banks to transfer funds to bank accounts in Singapore. The victims would only realise that the fraudulent transfers were made a few days later, and would then attempt to get their banks to recall the funds.

83. The bank accounts in Singapore are held by "money mules", who were earlier recruited by the criminal syndicate via online social networking websites to receive and thereafter withdraw or transfer funds. These money mules may have wittingly or unwittingly assisted the criminal syndicate to launder the proceeds of crime.

84. Our findings suggest that there is a high possibility that the syndicate is well organised:

- The same perpetrator had made contact with different mules;
- Different mules have received funds from the same victim account;
- The same mule has received funds from different victims;
- Different mules have made transfers to the same beneficiary; and
- The same mule has made transfers to different beneficiaries.

85. The data also suggests that it is likely that a transnational criminal syndicate is behind these crimes, as:

- The victim accounts were based in a foreign country,
- The perpetrators appear to be based in a foreign country,
- The fraudulent funds were subsequently transferred to bank accounts in Singapore, and

- Most of the fraudulent funds have been transferred out of Singapore to other jurisdictions.

86. It is interesting to note that the crime is orchestrated in a way such that the funds flow across several jurisdictions, and this heightens the challenges faced by law enforcement authorities from each jurisdiction in their investigation processes.

87. The FIU and law enforcement unit has worked closely with STR-filers and foreign counterparts to address this issue. We have shared our preliminary findings with the Association of Banks in Singapore compliance task forces to disseminate the indicators to members. We have also disseminated information via the FIU and law enforcement networks to encourage foreign victims to identify themselves and provide evidence. We are currently working on a joint project with a foreign country project to address this trend collectively.

THAILAND

88. Emerging trend: use of a nominee to hold assets or accounts, especially by corrupt politicians.

89. Declining trend: smurfing has declined because money launderers now know that authorities are monitoring this type of transaction.

90. Continuing trend: buying precious metals or gems and real estate.

91. In general, the same methods are still being used. However, there is a tendency for criminals to make their techniques more complex such as combining methods e.g. using of non-related nominee to open an account to receive the proceed and use the fund to buy precious metal or stones and carried overseas, and thus make it more difficult for authorities to detect.

3.4. Effects of AML/CFT Counter-Measures

AUSTRALIA

92. Australia's customer due diligence (CDD) regime has undergone substantive reform through the implementation of amendments to the Anti-Money Laundering and Counter-Terrorism Financing Act Rules Instrument 2007 (No. 1) (the AML/CTF Rules). The CDD amendments require regulated businesses to take steps to ensure they know the identity of the beneficial owner and strengthen CDD requirements in high risk situations, for example when dealing with politically exposed persons.

93. There have also been legislative developments relating to AML/CTF Countermeasures. As the existing AML/CTF countermeasures regulations applied to Iran were due to sunset on 1 April 2014, the regulations were remade along with some minor technical amendments to enhance readability and an additional exemption from the transaction prohibition for Australian diplomats in Iran.

94. Under the enhanced remitter registration regime, Australia has been working to identify remittance providers who are suspected of being involved in criminal activity, as well as those who may have an inability or unwillingness to comply with obligations under the AML/CTF Act. The Eligo National Task Force (Eligo), led by the Australian Crime Commission, has assisted AUSTRAC in determining whether remitters are compliant with relevant obligations under the AML/CTF Act. This has also assisted AUSTRAC in enhancing methods for identifying and assessing high-risk remitters.

FIJI

95. Since the introduction of the "unexplained wealth" provisions in Fiji's Proceeds of Crime (Amendment) Decree 2012, Fiji FIU has seen an increase in the number of Suspicious Transaction Reports on possible unexplained wealth cases from members of the public.

MONGOLIA

96. Mongolia has improved its ML and CFT legislation since enactment of an independent law on combating money laundering and financing of terrorism in 8 July 2006. After identifying some of the shortcomings, in May 2013, the Parliament approved a revised version of the AML/CFT law. It introduced new concepts including politically exposed persons, ultimate owner, and shell banks. Also, it cross-referenced the list of PEPs and their family members in the Conflict of Interest Law. These developments have improved 'Know Your Customer' obligation of the financial institutions. In July 2013, Mongolia was removed from the list of relatively high risk jurisdictions with strategic AML/CFT deficiencies for making evident achievements in the AML/CFT framework in the country.

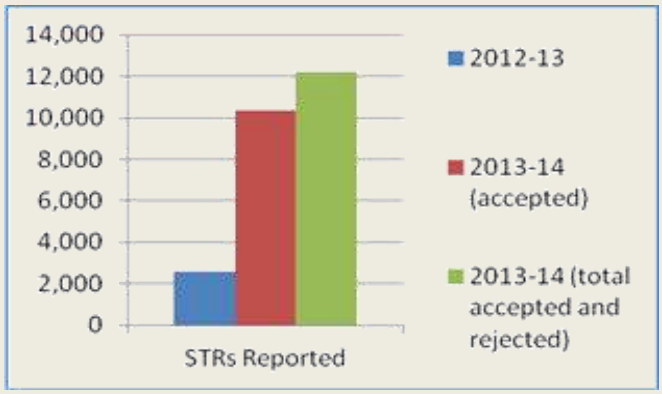
97. Mongolia amended the Criminal Code in January 2014, expanding the predicate offences of money laundering to all crimes. Resulting from this development, criminal cases related to money laundering are opened by the Police and law enforcement appears to be willing to promote the application of the statute. However, the prosecution and conviction of those cases remains a challenge as this is still a new type of crime, and law enforcements lack general capacity in prosecuting this type of crime.

NEW ZEALAND

98. Suspicious Transaction Report (STR) reporting to the Financial Intelligence Unit has increased considerably since the commencement of the AML/CFT Act reporting regime on 30 June 2013.

99. The number of STRs has increased significantly from around 2,600 in 2012-13 to 10,353 STRs accepted in 2013-14 (during 2013, 1846 STRs were also rejected by the FIU). See Figure 1 below.

Figure 1: Number of STRs received 2012 to 2014



100. The number of transactions in STRs has also significantly increased, indicating a higher quality of STRs since the commencement of the new reporting regime.

101. In 2012-13, 10,448 transactions worth NZD 516 million (about 4 transactions per STR) were reported to the FIU compared to 2013-14 when 86,937 transactions (over 8 transactions per STR) worth NZD 3.5 billion were reported in accepted STRs. See Figure 2 below.

Figure 2: Number of transactions in STRs

4. CASE STUDIES OF ML AND TF

4.1 Association with corruption (corruption facilitating ML or TF)

INDIA

102. There are two cases involving siphoning of development funds allocated to an autonomous council in connivance with the CEO, public servants and contractors, and sending the money for the purchase of arms and ammunition for waging war against the state. On the basis of investigations made and evidence collected, the charge sheet was filed against 15 accused in the National Investigation Agency (NIA) special court. Since there was involvement of public servants in misappropriation of government funds and their criminal misconduct, forgery etc., the matter was referred to the Central Government for investigation by the Central Bureau of Investigation after obtaining consent from the concerned State. The Central Bureau of Investigation has registered six cases under Prevention of Corruption Act. Presently, trial proceedings in the main case are going on in the NIA special court.

INDONESIA

103. A head of a narcotics penitentiary, Mr. X, entered into a criminal conspiracy with the prisoners charged in a narcotics case. The prisoner bribed him so that they could control a drugs business in the prison. According to INTRAC's analysis of the STRs, there were some suspicious funds flowing to the accounts of the head of the penitentiary and some accounts of his family (son and grandson) that were used as a storage account. The flow of funds came from transfers via mobile banking from the prisoner's account. The source of the funds was from the sale of narcotics when the prisoner was held in the penitentiary. In 2012, the case was uncovered and Mr. X was indicted to 13 years imprisonment and a fine of USD100,000.

THAILAND

104. A joint panel of the Office of the Attorney-General (OAG) and National Anti-Corruption Commission (NACC) has agreed to indict a former executive of a state agency in a bribery case. The executive and her daughter were accused of taking bribes from a foreign firm and many other related businesses to her and her daughter's accounts overseas including cash courier to Thailand, awarding it a 60-million-baht contract. The firm allegedly paid the executive about USD 1.8 million (53.7 million baht). The executive has allegedly violated the law governing offences committed by state organisations or officials and also breached the act governing tendering to a state agency. The bribing couple is imprisoned in the US while the corrupt Thai official is being tried in Thailand.

4.2 Laundering proceeds from corruption

FIJI

105. Fiji FIU received a request from a government agency requesting financial background checks on a senior government official, Person X. There was an allegation that Person X had received FJ$377,000 from a foreign businessman and invested these funds for his son's university tuition.

106. Fiji FIU conducted checks and established significant international remittances sent by one of Person X's staff/colleague to individuals related to Person X. The ultimate beneficiaries of these remittances were the wife and children of Person X. Investigations are currently underway.

HONG KONG, CHINA

107. The Joint Financial Intelligence Unit (JFIU) received confidential information that a man, Person A, took out a life insurance product and paid HK$8 million premium in one go via transfer

from his personal bank account. Shortly afterwards, Person A requested to terminate his insurance policy and suffered a penalty of HK$2 million. It was believed that Person A attempted to launder suspected proceeds of crime through the service of an insurance company. Enquiries revealed that Person A was allegedly involved in a corruption investigation in Jurisdiction X. The information was shared with FIU in Jurisdiction X to facilitate the investigation.

INDIA

108. There is a case of misappropriation of government funds against a retired civil servant wherein the amount sanctioned for a public function organized by the State Government were misappropriated through an event management company. The funds allocated by the government were fully withdrawn by the public servant, but only a small portion of it was utilized for the function. Proceeds of corruption were attached under the Prevention of Money Laundering Act.

INDONESIA

109. Ms. X, a People's Representative Council (PRC) member, was charged for corruption and money laundering totalling USD625,000 related with abuse of authority in deciding the region to receive local infrastructure funds. According to INTRAC's analysis, the total value in Ms. X's bank account was USD5 million. The funds were suspected to be the result of criminal action. Most of the funds were used to purchase assets such as insurance policy, time deposits, houses, apartments and gold jewellery. Ms. X also used a credit facility and transferred the funds to a third party. Some of Ms. X's assets totalling USD1 million were seized. Ms. X was indicted to six years in prison and USD50,000 in fines.

JAPAN

110. The offender, a municipal official, engaged in bid-rigging on civil engineering work of the city. He designated a civil engineering business company to be the bid winner for taking a bribe. The chief executive of the company who succeeded in the illegal bidding gave a third party's cash card to the said municipal official. The chief executive had his wife, who didn't know the circumstances of the matter, deposit hundreds of thousands of JPY into the account for the cash card as a bribe. They were arrested for bribery and the chief executive was charged with violating the Act on Punishment of Organized Crime (concealment of criminal proceeds).

4.3 Abuse of charities for terrorist financing

INDIA

111. Based on the allegation that a banned terrorist organisation received funds through front organisations to commit terrorist activities in India by using non-banking channels, a case was registered. A charity registered under the Charities Act in the United Kingdom used Western Union money transfer/Money Gram/MO/banking and cash channels as the transaction mode. The motive for sending money was to support sleeper cells, jailed terrorists and families of terrorists, so that they remain committed to the terrorist cause. A total amount of about of INR1,000,000 was reported to be transferred as per the available records.

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

AUSTRALIA

Complex tax avoidance scheme hid funds in Samoa and New Zealand

112. AUSTRAC information assisted authorities to identify offshore bank accounts and international funds transfers in relation to a complex tax avoidance scheme involving funds transfers between Australia, Samoa and New Zealand. The scheme involved the use of an offshore superannuation fund and a loan arrangement to avoid tax.

113. Authorities ultimately issued amended tax assessments to the individuals involved, resulting in approximately AUD2 million in additional tax, penalties and interest.

114. This complex case is presented in four parts:

- Part 1 covers international transfers made to an offshore superannuation fund and the rapid return of these funds to Australia.
- Part 2 covers the ongoing international transfers of funds under a fictitious loan arrangement over ten years.
- Part 3 describes the transfer of this loan arrangement to another Australian company when the original company went into liquidation. This covers a further four years' worth of activities.
- Part 4 shows how a charity became involved in the loan arrangement.

115. Individuals A and B were family members who owned and controlled a group of Australian-based companies. The companies undertook motor vehicle repairs and sold automotive products in Australia.

Arrangement 1 – Offshore superannuation fund

116. Individuals A and B received advice from an accountant about the purported benefits of offshore superannuation funds. As a result, individual A instructed his accountant to establish a superannuation fund in Samoa. The superannuation fund was established and a Samoa-based company acted as trustee of the fund.

117. Company 1 was owned and controlled by individuals A and B, and formed part of the Australia-based group. Company 1 made two contributions of AUD100,000 each to the superannuation fund in Samoa. The two international funds transfers were undertaken over an eight-day period and the funds were subsequently provided to a private bank in Samoa.

118. The Samoa-based private bank returned the AUD200,000 to company 1 in Australia in two international funds transfers of AUD100,000. The transfers were made within one month of the initial contributions being made to the superannuation fund. The two transfers of AUD100,000 were described as a 'loan' from the bank to company 1. There was no loan agreement in place to support the transfer of these funds.

119. Company 1 subsequently claimed deductions for the AUD200,000 offshore superannuation contribution in its tax return and was assessed as liable for less tax than it should have been, thereby avoiding its tax obligations.

120. The deductions were later disallowed and deemed not deductible under the Income *Tax Assessment Act 1936*. An amended tax assessment was issued to company 1 by the Australian Taxation Office (ATO).

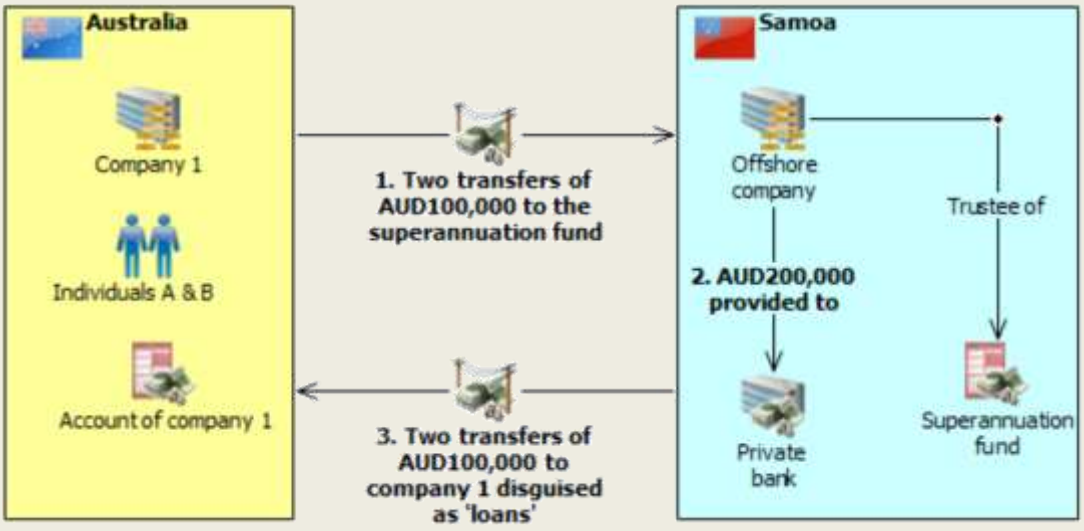


Figure – Transfers to offshore superannuation fund in Samoa (Arrangement 1)

Arrangement 2 – Loan arrangement (years 1 to 10 of the scheme)

121. Individuals A and B entered into a loan agreement on behalf of company 1 with the Samoa-based private bank. This arrangement was separate to the AUD200,000 'loan arrangement' described above in 'Arrangement 1'. This second loan arrangement remained in place for more than 10 years and was later transferred to other companies in the group.

122. A subsidiary company of the Samoa-based private bank held a bank account in New Zealand. The subsidiary was instrumental in facilitating payments between the Samoa-based private bank and company 1, or companies and individuals associated with the Australia-based group.

123. In subsequent years, in accordance with the loan agreement, companies controlled by individuals A and B made annual 'interest' payments on the loan to the bank or its subsidiary, by way of international funds transfer.

124. The interest payments were then borrowed back from the Samoa-based private bank or its subsidiary, with funds transferred back to Australia to either company 1 or other companies and individuals associated with the group. The returned funds were generally described as 'draw downs' or 'loans'.

125. This complex 'round robin' tax avoidance arrangement aimed to disguise the funds movements as legitimate transactions associated with the loan. In reality, any funds sent overseas ultimately returned to the original beneficiary, either company 1 or other companies in the Australia-based group.

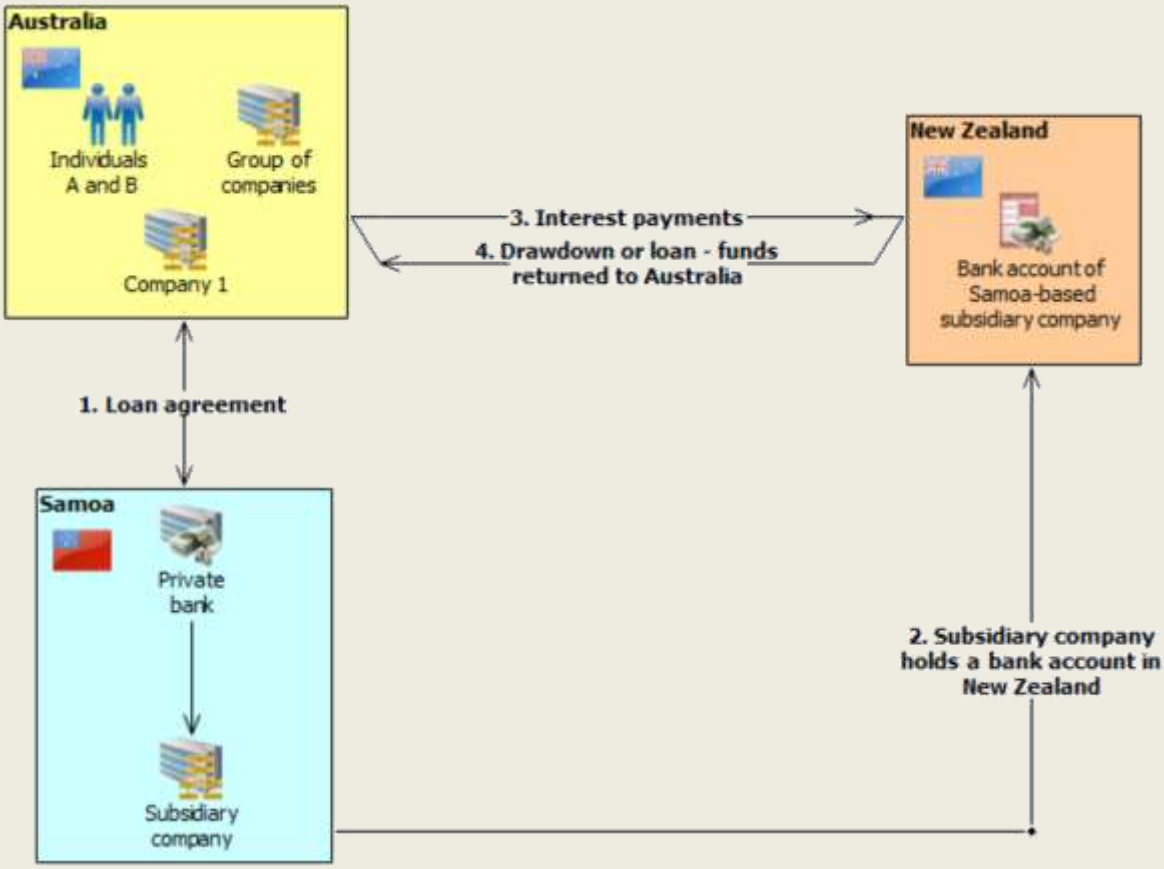


Figure – Transfers to and from the subsidiary's New Zealand bank account disguised as loan payments (Arrangement 2)

Transfer of the loan arrangement from company 1 to company 2 (years 11 to 14 of the scheme)

126. Company 1 changed its name and subsequently went into liquidation. As a result, the ATO was forced to write off a tax debt of AUD800,000 which had accrued on the income tax account of the company.

127. After company 1 went into liquidation the loan liability was transferred to company 2. Company 2 was incorporated in Australia and was associated with company 1 and individuals A and B. The loan liability at this time was approximately AUD3 million.

128. Company 2 continued to utilise the tax avoidance arrangement by making interest payments on the loan to the Samoa-based private bank via its subsidiary. Each time company 2 made interest payments to the bank, the bank's subsidiary subsequently transferred funds into company 2's bank accounts in Australia. These transfers were described as 'loan draw downs'.

129. Information in IFTIs, combined with information received by authorities, revealed four years worth of incoming and outgoing international fund transfers between company 2 in Australia and the bank's subsidiary company, which held a bank account in New Zealand.

130. Company 2 claimed that the funds received as 'loan draw downs' were lent to companies in the Australian group of companies by way of interest-free loans.

Introduction of an Australian charitable organisation (years 15 to 16 of the scheme)

131. To further complicate the loan arrangement, another Australian organisation (a trust) was introduced to the transaction activity. This organisation was unrelated to the main group of companies and was described as a charitable organisation. The organisation facilitated the transfer of funds between the bank's New Zealand subsidiary and the Australian group of companies.

132. AUSTRAC information, combined with other information received by authorities, showed:

- company 2 sent funds representing 'interest payments' to the New Zealand bank account of the bank's subsidiary
- the subsidiary transferred funds, in similar amounts to the 'interest payments', from its New Zealand bank account to the bank account of the Australian charitable organisation. The transfers were described as 'draw downs' and 'transfer of funds'
- four to five days later, the charitable organisation conducted a domestic transfer for a similar amount into the bank account of company 2, described as a 'loan draw down'.

133. The figure below shows the direction and value of incoming and outgoing IFTIs between company 2, the subsidiary's New Zealand-based bank account and the Australian charitable organisation.

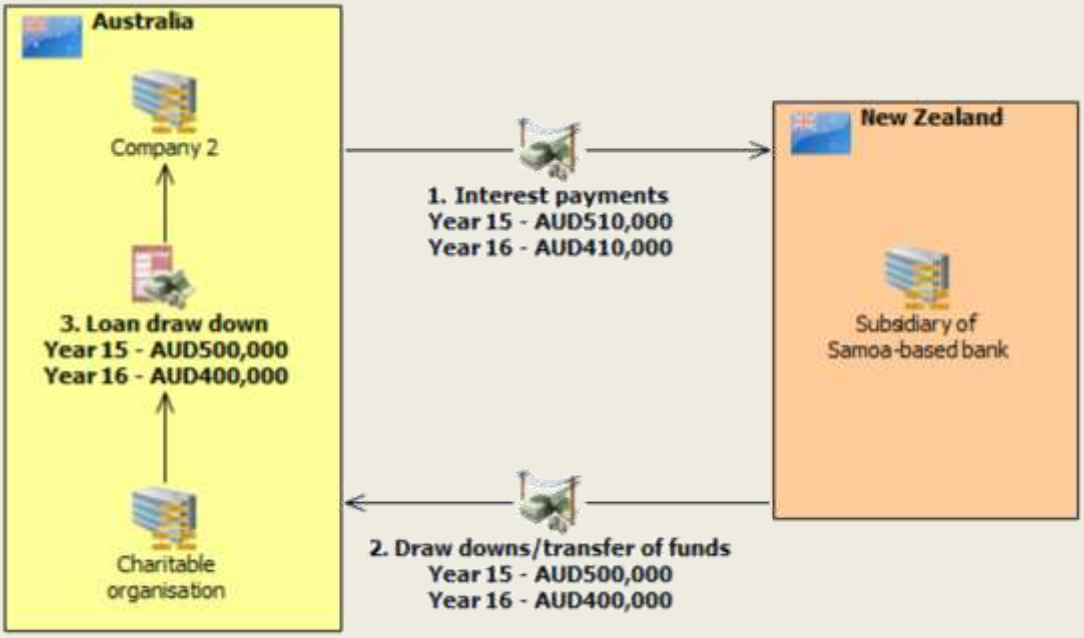


Figure – Use of Australian charitable organisation to facilitate payments

134. In its tax returns, company 2 claimed deductions for interest expenses and fees paid to the Samoa-based private bank. As a result of claiming these deductions, company 2 reduced its taxable income and was assessed as liable for less tax than it should have been, thereby avoiding its obligations.

135. It was later determined that these expenses were not deductible and the deductions were disallowed. Amended assessments for company 2 were issued resulting in approximately AUD2 million in additional tax, penalties and interest.

Offence	Tax avoidance
Customer	Business Foreign entity Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI

Jurisdiction	International – Samoa, New Zealand
Designated service	Account and deposit-taking services
Indicators	Customer receives international funds transfers described as 'loan draw down' or 'loan advance' Customer undertaking complicated transfers without a business rationale International funds transfers to and from a high-risk jurisdiction Multiple high-value international funds transfers to and from Australia with no apparent logical reason Outgoing funds transfers sent to offshore entities followed soon after by incoming funds transfers of similar amounts from the same offshore entities Use of charitable organisation with a lack of business rationale Use of third-party company accounts in an attempt to complicate transaction activity Use of third-party or family member accounts

CHINESE TAIPEI

136. In March 2012, the Anti-Money Laundering Department (AMLD) received a STR from a bank indicating that the customer Ms. Z often conducted deposit and withdrawal transactions with a large amount of cash from her bank account in a short period of time. Most funds were from the settlement of securities.

137. Ms. Z avoided giving a clear answer to the source and the purpose of the funds and refused the suggestion of the bank to conduct the transaction by remittance. The bank considered that the transactions were suspicious and filed the STR to the AMLD.

138. After receiving the STR, the AMLD initiated analysing procedures and found the suspicious transactions conducted by Ms. Z were used to buy/sell the stock of a listed Company, Company A. It is possible that Ms. Z's bank account was used as a dummy account to manipulate stock price and the real controller of the stock trade was Mr. C.

139. Further investigation found that Mr. C was involved in economic crime. Company A issued 3,000 shares of convertible bond by book building in December 2011. In order to gain the profit from the price difference between the issuing price and the market price, the president Mr. W, the CFO Mr. H, the market speculator Mr. C, and the vice president Mr. Ch of the Security Company B, conspired to use dummy accounts to allocate 2,280 shares to Mr. W, Mr. H, and Mr. C and allocate 300 shares to Mr. Ch that held about 40% shares of Company A in total with lower cost.

140. To lure investors to buy Company A's shares to elevate its share price, they intentionally window dressed the financial reports. In order to artificially inflate income, the market speculator Mr. C arranged fake trading between Company A and the shell companies which were incorporated in Chinese Taipei and foreign countries.

141. Mr. W instructed his employees to cooperate with Mr. C's employees to deal with the vouchers and the financial transactions of the fake trades. Mr. C also arranged for his sister in law, Ms. Z, the subject reported in this STR, to be the director of Company A.

142. The investors therefore were led to believe Company A had had good profit and bought its shares and the convertible bonds.

143. In order to more aggressively lift the share price, Mr. C used dummy accounts including Ms. Z's to wash trade Company A's shares in a short period of time. Mr. W and other related people

could benefit from selling their shares with higher price and made redemption of the options. Mr. W et al. gained about NTD 110 million through the market fraud and stock manipulation.

144. To continue to elevate Company A's share price, Mr. C instructed several fund managers to buy Company A's shares with higher price, but Mr. C took advantage of the occasion to simultaneously sell the shares he held and gained more profit.

145. The transactions that the fund managers made caused public investors to misunderstand that Company A was successful in its business and continuously bought its shares in the stock market. After that, Mr. C gave the fund managers rewards in cash. The shares that the managers bought at a higher price sold with lower price caused a loss to fund investors.

146. Besides this, Company A has paid around NTD 990 million to these shell companies for completing the money flow of the above mentioned fake trading. Based on the agreement, these shell companies should have returned the payment of the NTD 990 million back to Company A. However, Mr. C embezzled part of the funds and transferred the rest of funds to Mr. W and Mr. H.

147. In order to embezzle more money from Company A, Mr. H instructed the employees to remit money of Company A to those shell companies as the prepayment of purchase. The money was embezzled by them as well. The total embezzlement caused about NTD 450 million losses to Company A.

148. Mr. W was indicted on the charges of violating the Securities Exchange Act and the Business Entity Accounting Act by the Taipei District Prosecutors Office in May 2013.

COOK ISLANDS

149. In July 2014, a report was received from a trustee company about a client (trust) owned by an individual who had been indicted in the United States for five counts of making false statement to an Insurance Regulator for the total value of US$5million. The alleged period of the offending was from June 2012 and April 2014. The matter was investigated by the Federal Bureau of Investigation, Homeland Security, and Internal Revenue Services and, by the Immigration and Customs Enforcement.

150. As at 1st September 2014, the balance in the trust account with a local bank was US$8,208.00. An instruction to freeze the remaining funds was issued by the FIU on 9 September 2014.

INDIA

151. In one case a terrorist organisation used a foreign based trust for raising, collecting and transferring funds to India through banking/cash couriers/non-banking channels for its distributions to active cadres, other beneficiaries of the terrorist organization and families of terrorists. In this case extensive use of e-mail network was cracked and evidence collected. A charge sheet has been filed against 10 accused persons in the court. Two accused persons have been arrested.

4.5 Use of virtual currencies

AUSTRALIA

Suspect used black market website and digital currencies for drug trafficking

152. AUSTRAC assisted an investigation which led to the arrest of a suspect who used a digital currency to purchase, import and sell illicit drugs through a black market website.

153. The suspect was sentenced to three years and six months imprisonment and fined AUD1,000 for possessing controlled weapons.

154. Law enforcement intercepted a number of packages sent to Australia from Germany and the Netherlands via the postal system. The packages were addressed to the suspect. Authorities found that the packages contained cocaine and methylenedioxymethamphetamine (MDMA), with a combined weight of 60 grams.

155. AUSTRAC information identified that the suspect had sent funds to a digital currency exchange to purchase a digital currency. Analysis of AUSTRAC information showed that over a six-month period the suspect undertook 13 outgoing international funds transfer instructions (IFTIs) totalling approximately AUD28,000. The funds were transferred via banks to an online digital currency exchange based overseas. The payments enabled the suspect to purchase an amount of digital currency.

156. AUSTRAC information showed that the suspect gradually increased the value of IFTIs sent to the digital currency exchange from approximately AUD600 to AUD3,500 per transaction over the six-month period. The suspect also received two incoming IFTIs totalling approximately AUD2,000 from the same online digital currency exchange.

157. Law enforcement executed a search warrant on the suspect's home and seized a quantity of illicit drugs including cannabis, MDMA, cocaine, amphetamine and methylamphetamine. Additionally, law enforcement seized a number of items associated with drug trafficking, namely digital scales, clip seal bags and a money counter. Authorities also seized approximately AUD2,300 cash, computers, mobile phones and a number of stun guns.

Computers and mobile phones revealed drug trafficking

158. Analysis of the suspect's mobile phones identified text messages that suggested the suspect was trafficking drugs. On one phone law enforcement identified 150 such messages sent during the week prior to the suspect's arrest.

159. Analysis of the suspect's computers revealed that he registered an online account with a black market website. The website allows users to purchase and sell illicit goods and conduct transactions using a digital currency. The use of digital currencies provides a degree of anonymity for users. The suspect used this online account to purchase, import and sell illicit drugs.

160. The suspect was convicted of two charges of importing a marketable quantity of a border controlled drug and one charge of trafficking a controlled drug contrary to the *Criminal Code Act 1995*. He also pleaded guilty to possessing a controlled weapon contrary to the *Control of Weapons Act 1990*.

161. The suspect was sentenced to three years and six months imprisonment. He was also fined AUD1,000 for possessing controlled weapons.

Offence	Drug importation Drug trafficking
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	Domestic International
Designated service	Account and deposit-taking services

Indicators	Increase over time in the value of transactions with a digital currency exchange Multiple low-value international funds transfers

Digital currencies and the regulated AML/CTF sector

162. Financial activity relating to the use of digital currencies may be indirectly visible to AUSTRAC via the regulated sector. For example, when digital currency-related transactions intersect with the mainstream regulated AML/CTF sector they can generate reportable transactions such as:

- reports of IFTIs between Australian accounts and foreign accounts for the purchase/sale of digital currencies
- threshold transaction reports (TTRs) for cash deposits/withdrawals of AUD10,000 or more involving the bank accounts of digital currency exchange providers
- suspicious matter reports (SMRs) submitted where reporting entities consider financial activity involving a digital currency exchange to be suspicious.

4.6 Use of professional services (lawyers, notaries, accountants)

AUSTRALIA

Accountant jailed for laundering money via Hong Kong and New Zealand

163. An Australian law enforcement agency conducted an investigation into a suspect believed to be involved in laundering money. AUSTRAC information linked the suspect to multiple companies and structured cash deposits. The suspect was charged with providing incomplete information in relation to a financial transaction.

164. The suspect pleaded guilty and was sentenced to nine months imprisonment and received a two-year good behaviour bond.

165. Over a two-year period an account held by the main suspect received more than 80 'structured' cash deposits, as a well as a small number of cheque deposits. The cash and cheques were deposited into an account held by the suspect. The suspect, an accountant, regularly consolidated the funds from the various deposits and transferred the funds electronically to third-party domestic accounts. Authorities believed the suspect received a percentage of the funds he transferred as a commission for his services.

166. Although the exact source of the funds laundered by the suspect is unknown, authorities identified possible links between the funds and the importation of drugs into Australia. AUSTRAC information linked the suspect to approximately 50 companies and revealed that the structured cash deposits into the suspect's account were made on behalf of both companies and individuals.

167. AUSTRAC also received four suspicious matter reports (SMRs) from reporting entities detailing structured cash deposits undertaken by the suspect.

168. Further analysis by AUSTRAC identified that the suspect also undertook international funds transfer instructions (IFTIs) worth more than AUD700,000 to Hong Kong and New Zealand. The funds were transferred from accounts held in the suspect's name to overseas business accounts in amounts ranging from AUD400 to AUD50,000. In some instances the offshore recipient businesses shared the same name as businesses operated by the suspect in Australia.

169. The suspect was charged under section 31 of the *Financial Transaction Reports Act 1988* and section 142(1) of the *Anti-Money Laundering and Counter-Terrorism Act 2006* for providing incomplete information in relation to a financial transaction. He pleaded guilty and was sentenced to nine months imprisonment and received a good behaviour bond for a period of two years.

Offence	Money laundering
Customer	Individual Business
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	Domestic International – New Zealand, Hong Kong
Designated service	Account and deposit-taking services Remittance service (money transfer)
Indicators	Multiple domestic transfers to third-party accounts Multiple international funds transfers which are inconsistent with the established customer profile Structured cash deposits into a bank account from third parties Structured financial transactions in personal and business names

INDONESIA

170. Mrs. ST was a lawyer and an ex-subordinate of Mr. AM, a public official (PEP). In 2010, Mrs. ST received USD50,000 from a pair of regional heads, which was given gradually, firstly USD30,0000, then USD10,000 and the last was given as a cheque valued USD10,000. The case was uncovered by the investigators after a development from INTRAC's analysis of Mr. AM's transactions. It was proved that Mrs. ST acted as an intermediary of the money handout to Mr. AM so that the pair would win a regional election. Mrs. ST firstly transferred USD25,000 to Mr. AM's account with transaction description as "Payment for Palm Tree", and then transferred to Mr. AM's wife's account. Mrs. ST was sentenced to 5 years in prison and fined for USD15,000.

JAPAN

171. An administrative scrivener in Japan received JPY850,000 in cash, in nominal terms, as a consulting fee from an underground club manager.

172. The offender, knowing that the funds were proceeds from unauthorized entertainment business, was arrested for violating the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

NEW ZEALAND

Operation Rock

173. Two offenders involved in the importation of ecstasy laundered large amounts of cash through a lawyer's trust account. A total of $400,000 cash was given to the lawyer who banked it into his trust account on behalf of the two offenders. The lawyer had conducted no due diligence on the offenders and did not report an STR. However, the bank that held the lawyer's trust account submitted suspicious transaction reports when the lawyer deposited $100,000 on four occasions. The offenders had instructed the lawyer the cash was being held on behalf of their company registered in Gibraltar. This alleged company was a shell company that "lent" one of the offenders the $400,000 in order to purchase a property in Auckland. Another lawyer was engaged by the offender to facilitate this "loan" and the purchase of the house in the offender's name. The funds for the purchase of the house therefore looked legitimate (a loan from a company). Effectively, two lawyers from different law firms had been involved in the money laundering process.

UNITED STATES OF AMERICA

Attorney Who Helped Owner of Marijuana Stores Launder Illegal Proceeds Pleads Guilty in Federal Money Laundering Case

U.S. Attorney's Office December 18, 2014 Central District of California (213) 894-2434

SANTA ANA, CA—An attorney who engaged in a conspiracy that allowed the owner of a chain of marijuana stores to hide some of his income has pleaded guilty to federal financial offenses.

Guilty pleas by Richard C. Brizendine, 59, of Long Beach, were entered Monday by United States District Judge James V. Selna. Monday's action concludes proceedings in which Brizendine pleaded guilty to two counts: money laundering and conspiracy to structure cash deposits to avoid federal reporting requirements.

Brizendine was an attorney for John Melvin Walker, who operated marijuana stores across Los Angeles and Orange counties and generated approximately $25 million in income over a six-year period. Brizendine conspired with Walker and others to accept cash from the marijuana operation and invest the funds into several corporations. According to court documents, Brizendine agreed to accept more than $10,000 in cash and then make smaller deposits into different bank accounts so as to not trigger federal requirements that financial institutions report currency transactions of more than $10,000 (this process is called structuring cash transactions). By pleading guilty, Brizendine specifically admitted that he structured approximately $389,700 for Walker.

The case against Brizendine was announced today after Judge Selna unsealed documents associated with the case.

Last year, Walker was sentenced to nearly 22 years in federal prison for operating a chain of marijuana and failing to reporter millions of dollars in revenues was on his taxes (see: http://www.justice.gov/usao/cac/Pressroom/2013/096.html).

Judge Selna is scheduled to sentence Brizendine on May 4, 2015. At that time, Brizendine will face a statutory maximum sentence of 10 years in federal prison. Until that time, he will remain free on a $500,000 bond.

The investigation of Brizendine and the marijuana operation was conducted by the Orange County Sheriff's Department; the Drug Enforcement Administration; the Bureau of Alcohol, Tobacco, Firearms and Explosives; IRS-Criminal Investigation; the California Board of Equalization; the Orange County District Attorney's Office; and the Federal Bureau of Investigation.

This content has been reproduced from its original source.

http://www.fbi.gov/losangeles/press-releases/2014/attorney-who-helped-owner-of-marijuana-stores-launder-illegal-proceeds-pleads-guilty-in-federal-money-laundering-case

4.7 Trade based money laundering and transfer pricing

FIJI

174. Fiji FIU received a Suspicious Transaction Report on Company X. The nature of business for this company was hiring of trucks and transportation of sand and gravel. Fiji FIU established that Company X was instructing overseas suppliers to split invoices for goods imported by Company X. Fiji FIU was able to verify the amounts remitted and customs duty paid by Company X. When paying for customs duty, Company X was only showing the amount on a single invoice and was avoiding paying duty on the full amount.

INDONESIA

175. AAG Company, one of Asia's largest crude palm oil (CPO) producers, was the parent company of RGS group which was owned by Mr. ST. AAG Co. had 200 thousand hectares of palm tree, rubber, and cacao plantations in Indonesia, the Philippines, Malaysia, and Thailand. A tax evasion suspicion was exposed when Mr. V, a whistle blower, reported the case that AAG Co. was selling its CPO to their affiliated company overseas under the market price, and then the CPO was sold to real customers with a higher price, to avoid paying income taxes and value added taxes in the country. The investigators found that AAG Co.'s affiliated companies were mostly shell and paper companies. The tax evasion was estimated to cause a loss to the State for about USD130 million. AAG Co. was then forced to pay USD250 million in fines.

MACAO, CHINA

176. A foreign trading company A which was incorporated in a remote overseas country Z in 2012, recorded millions of dollars of business activities and had opened a bank account locally. However none of its businesses had direct relationships in the local market. The bank account was used for payment receipts. In addition, company A and its overseas "business partners" were all located in the same city in another country.

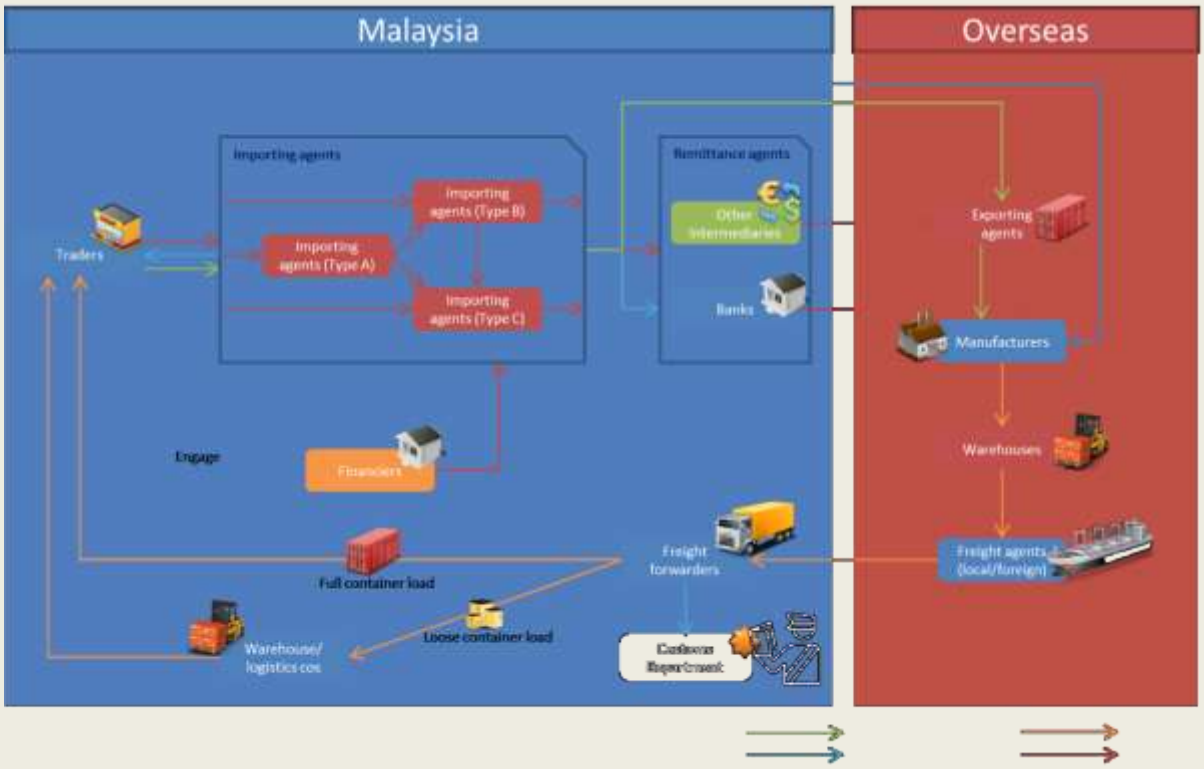
177. The FIU during the analysis process found out that company A was a suspected shell company with massive business volume and huge amount of loan agreements with its partners. All the loan agreements had a fixed repayment date of 3 months with no interest rate clause. Further analysis showed that one of the companies that did business with company A was related to overseas money laundering case. The other three companies on the other hand were being monitored by foreign FIUs. The case was submitted to Public Prosecutions Office for further investigation.

MALAYSIA

Trade-Based Money Laundering

178. Methods used:

- Use of nominees, family members or third parties, etc.
- Wire transfer/use of foreign bank accounts
- Use of shell companies/corporations
- Underground banking/alternative remittance services/hawala



179. Background of subjects:

- Mr. K acts as an importing agent to local traders by providing services to these traders to import goods from overseas. Mr. K and his associates control a number of companies/businesses which were set up mainly to facilitate fund movements. The financial accounts of these companies/businesses were generally controlled (as signatories) by individuals (believed to be Mr. K's associates) with no apparent relationship with the companies/businesses.

- These companies/businesses offer various services, such as transportation, hardware, sea products, garments and etc. with a majority being located in the north of Peninsular Malaysia, in an area well-known for import/export businesses. Some of these companies/businesses share the same business address while being registered under the ownership of different sole proprietors/directors.

- In order to pay a substantially lower amount of customs duties, Mr. K falsified documentation and declaration of goods and services traded. Moreover, Mr. K either did not file tax declaration or significantly understated the revenue in the companies/businesses books.

180. Source of information:

- STR and CTR records

- Sharing of intelligence from foreign FIUs

181. Preliminary assessment & findings (modus operandi):

- Mr. K used nominees to set up companies/businesses to facilitate the opening of bank accounts. To avoid any suspicious activity detection by the authorities, the companies/ businesses or bank accounts usually existed for a short period of time only.

- The most common ground for suspicion reported in STRs on these companies/businesses accounts were frequent deposits from large number of domestic companies/businesses

involved in various type of businesses. The deposited funds were then either transferred among them or withdrawn via foreign remittances to various foreign companies.

- These companies play the importing agent role which can be classified into three distinctive types.

  (i) Type A importing agent normally receives funds from traders and subsequently transfer the funds to other importing agents in Malaysia.
  (ii) Type B importing agent normally receives funds from traders and Type A importing agents before depositing the funds to other importing agents or remitting the funds overseas.
  (iii) Type C importing agent receives funds from traders and other importing agents before remitting the funds overseas directly.

- Mr. K also controls several foreign companies acting as exporting agents and warehouses as part of his business operation in receiving orders and handling finished goods overseas respectively. In certain instances, some of these freight forwarders would act as importing agents and participate in this trade-based money laundering activity instead of just acting as genuine transporters.

- In addition, some of the third parties that transacted with these subjects were reported in STRs as they were suspected to be involved in illegal money lending or illegal remittance activities. It is believed that some of these parties acted as financiers to the traders' imports and remittance intermediaries to facilitate trade settlements.

- The total amount of cash transactions captured in CTRs of these subjects amounted to RM26 billion, including RM12 billion which was remitted overseas over a period of 9 years.

182. Actions taken to date:

- Information in FIU's database was analysed together with the intelligence received from foreign FIUs, and was subsequently disclosed to law enforcement agencies.

- Given the involvement of large number of entities coupled with the complexity of the case which involves offences that cut across multiple agencies, a multi-agency task force was set up to review this case.

- The case is currently being investigated by local law enforcement agencies.

<u>Smuggling and Customs Duties Evasion</u>

183. Methods used:

- Smuggling of goods

- Use of nominees, trusts, family members or third parties, etc.

- Trade-related ML & TF

184. ABC Enterprise is a company located in the Free Trade Zone (FTZ) and fully owned by Director Y who has several businesses involved in importing and exporting. Customs intelligence branch had conducted analysis on the records of customs export declarations, which exported beer to a neighbouring country. Based on the analysis conducted it was suspected that such exports did not take place and that the beer stated in the export documents had been smuggled from the FTZ back into the country for domestic consumption.

185. RMCD had used the e-Tracking System (an internal intelligence tool) to examine port activities which include the tracking of transhipment port ship loading, inward & outward manifests

and invoices from shippers. This investigation led to the discovery that the beer was never loaded in containers destined for export to the neighbouring country.

186. Financial investigations on the movement of funds revealed suspicious activities in the bank account of director Y, where the monies were deposited from banks located in various places within Malaysia. ABC Enterprise and director Y could not provide any evidence to prove that the suspicious deposit transactions identified in her bank account are from a legitimate source.

187. RMCD investigations indicated a strong inference that the monies deposited into the account of director Y were derived from the sales of beer that was smuggled back into Malaysia without the payment of import duties even though the export declarations indicated otherwise. There were very strong suspicions that ABC Enterprise had gained large profits from the smuggling and the sale of contraband consisting of duty unpaid beers. The case was investigated for the offence under section 133(1)(c) of the Customs Act 1967, related to the making of incorrect declarations and submitting false documents to RMCD, and money laundering offence under section 4(1) of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. The case is currently under trial.

REPUBLIC OF KOREA

188. After a foreign currency account titled to Person Y who is a representative of a trading company received some funds remitted in advance for imported goods many times, the funds were deposited into a foreign currency account titled to the company. Then, the funds were repeatedly moved to Person Y's personal account, his sister-in-law's account and his younger brother's account. Finally, the funds were transferred to the company's account.

- The company exports processed food including coffee to China, Vietnam, Cambodia, Kazakhstan, etc. While the amount of exported goods is 1.3 million dollars and 30 million dollars, foreign exchange receipt for exported goods only amounts to 1.27 million dollars. Thus, it is not confirmed whether 30 million dollars were remitted to the Republic of Korea.

- The company received part of 30 million dollars using false name accounts and the rest of the funds were not moved to the Republic of Korea which could constitute illegal movement of domestic property. It was determined that Person Y received money for clothing smuggling from domestic companies through accounts titled to his younger brother and his wife's sisters-in-law. Thus, this case was referred to the Republic of Korea Customs Service on the suspicion of smuggling and illegal movement of domestic property.

189. The investigation by the Republic of Korea Customs Service revealed that Person Y smuggled in items worth 2.3 billion KRW on 250 occasions and sold the items domestically. Then he disguised payment as receipt for exported goods. He later was prosecuted for the offences of smuggling and illegal flight of property abroad at Prosecutors Office.

4.8 Underground banking/alternative remittance services/hawala

AUSTRALIA

Director of remittance business jailed for laundering cash for criminals

190. AUSTRAC provided financial intelligence to assist law enforcement with their investigation into a remitter suspected of laundering illicit funds for crime syndicates.

191. AUSTRAC analysis identified additional entities, bank accounts and telephone numbers associated with the remitter. The remittance company director was charged and pleaded guilty to dealing with money reasonably suspected to be the proceeds of crime. He was sentenced to three months imprisonment and given an 18-month good behaviour bond.

192. Law enforcement commenced an investigation into a remittance company and its directors who were suspected of laundering illicit funds for criminal syndicates and individuals. The company also operated as a legitimate remitter sending funds primarily to individuals in Iran and Iraq.

193. Through its regular financial transaction reporting to AUSTRAC, the remittance company reported sending AUD6 million to Iran and Iraq on behalf of its legitimate customers. However, according to transaction data submitted by banks which dealt with the remittance business as a customer, the remitter sent AUD3.66 million to overseas beneficiaries over the same period. This resulted in an AUD2.34 million shortfall between the amount of money the remitter company claimed to have sent overseas and the amount the company actually remitted. The bank transaction data also showed that the remitter made significant cash deposits (cash deposits of AUD10,000 or more) totalling AUD3.14 million.

194. Along with the company director, a number of other individuals also played a key role in the company, including an associate and his son.

195. The company director was charged and pleaded guilty to dealing with money reasonably suspected to be the proceeds of crime contrary to section 400.9(1) of the *Criminal Code Act 1995*. He was sentenced to three months imprisonment and given an 18-month good behaviour bond. He also received a forfeiture order under section 48 of the *Proceeds of Crime Act 2002* allowing for the seizure of AUD225,000. The other two men were not charged.

Offence	Money laundering
Customer	Individual Business
Industry	Remittance services
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Iran, Iraq
Designated service	Remittance services (money transfers)
Indicators	International funds transfers to high-risk jurisdiction Large cash deposits used to pay for IFTIs Third-party cash deposits

CHINESE TAIPEI

196. Since 2011, Mr. K has used his son's accounts to conduct an underground banking system. Mr. K used the middle value between buying and selling rate of RMB and NTD as the exchange rate to provide underground banking services. Customers who want to use underground banking could remit the funds to his son's accounts. After the funds were remitted into his son's accounts, Mr. K informed the contact point in Mainland China to remit funds to the designated accounts. The total value of the undergrounding banking system that Mr. K conducted was more than NTD222M. The MJIB initiated a criminal investigation and then referred this case to Taipei District Prosecutors Office in October 2014 for prosecution.

197. Mr. Z hired Mr. K to operate an underground banking system from June to July 2012. In order to facilitate his underground banking system, Mr. Z used his unwitting relatives' bank accounts, and rented Mr. C and others' accounts at the price of NTD 5,000 per month. He also opened accounts with financial institutions in Mainland China. In Chinese Taipei, people remitted money to the accounts held by Mr. Z and subsequently Mr. Z instructed an associate in China to transfer equivalent value in RMB to the accounts designated by the remitters. Mr. Z charged NTD 2,000 for each remittance of RMB 1,000,000. The amount through underground exchanges in total reached NTD

779,624,478 (about USD 25,497,088). This case was referred to the Taichung District Prosecutors Office by the Criminal Investigation Bureau (CIB) on July 29, 2014.

HONG KONG

198. In March 2010, two males were found operating an unlicensed remittance business. Subsequent investigation revealed that their company accounts had received HK$2.2 billion between January and March 2010. The males were subsequently arrested and admitted under caution that they had no knowledge of the source of the funds in the accounts and just carried out instructions given by their unidentified boss. In October 2014, both males pleaded guilty to three counts of money laundering. Assets worth HK$16.7 million were restrained pending confiscation.

JAPAN

Case 1

199. Offenders, Thai women, using underground banking transferred money in Thailand. They had their clients transfer a remittance and commission fee into a bank account, in Japan, under the name of a third party. They were arrested for violating the Act on Punishment of Organized Crimes (concealment of proceeds).

Case 2

200. A member of a Vietnamese shoplifting group obtained money by mainly selling cosmetic products which were shoplifted in Japan and made unlawful remittances to Vietnam through underground banking established by fellow Vietnamese citizens.

201. Based on the suspect's statement, the police arrested Vietnamese citizens managing underground banking for violating the Banking Act.

SAMOA

Case 1

202. Ms NH of country C, remitted approximately USD$13,645.00 to Ms JS (a local resident), as payment for lawyer's accommodation and airfare. This is suspected to be an inheritance scam, given that, Ms NH was told to meet all the costs before receiving her inheritance of USD$1.6 million from a dying nun in country U. Ms NH was instructed to remit the said funds to Ms JS.

Case 2

203. Ms VS was reported by one of the money transfer operators due to her unusual behaviour and her involvement in a suspected scam operation. Accordingly, Ms VS received numerous transfers from Mr GH in country N, whom she claimed is her husband. Ms VS asked about the limit to remit funds and also if she could send funds using her children's names. However, Mr GH stated that Ms VS is just a business partner and she owed him NZD$100,000.00.

Case 3

204. Mr JR is suspected to be involved in a scam operation. According to the information provided, he received approximately SAT$105,392.44 (USD$45,822.00) from five different senders in country N. Mr JR is connected to Ms VS (as stated in Case 2 above), given that, Ms VS usually withdrew money on behalf of Mr JR. Also, Mr GH is one of the remitters who sent monies to Mr JR.

UNITED STATES OF AMERICA

Unlicensed Money Transmitters Charged with Money Laundering

U.S. Attorney's Office October 17, 2014 Southern District of California (619) 557-5610

SAN DIEGO—San Diego-based business attorney Richard Medina Jr. and alleged co-conspirator Omar Trevino Caro Del Castillo appeared in federal court today to face allegations that they laundered almost $12 million via international financial transactions in an attempt to promote their unlicensed money transmitting business.

According to an indictment unsealed this afternoon, the defendants are charged with operating as a commercial enterprise, willing and able to transfer cash on behalf of third parties without registering with the Secretary of the Treasury, as required by Title 31, United States Code, Section 5330. In turn, the defendants' customers availed themselves of the defendants' ability to collect cash anywhere throughout the United States, and transmit it anywhere in the world. According to the indictment, the defendants obtained commissions for their services, extracting a fee from the millions of dollars transmitted abroad.

The indictment alleges that in an effort to mask the transmission of currency, Medina opened several "Interest on Lawyers Trust Accounts," known as IOLTA accounts, at national financial institutions. Other co-conspirators picked up cash at various locations throughout the United States and deposited the cash into one of Medina's IOLTA Accounts.

By depositing the money into the IOLTA Accounts, the defendants, along with their clients abroad, intended to avoid financial institutions from filing accurate Department of Treasury FinCEN Form 104, Currency Transaction Reports. Financial Institutions must file Currency Transactions Reports for all currency transactions exceeding $10,000 during any one banking day. The defendants sent their clients' funds internationally through an informal and unlicensed transfer network, in furtherance of the conspiracy to promote the operation of the unlicensed money transmitting business.

The criminal case is assigned to U.S. District Court Judge Roger T. Benitez.

During today's hearing, the government asked that Caro Del Castillo be held without bond based on risk of flight, and U.S. Magistrate Judge Bernard G. Skomal agreed; Medina was ordered released on $200,000 bond.

DEFENDANT

Case Number: 14cr2936

Richard Medina, Jr. Age: 38

Omar Trevino Caro Del Castillo Age: 37

CHARGES

Money Laundering Conspiracy—Title 18, U.S.C., Section 1956(h) Maximum penalty: 20 years' imprisonment, $500,000 fine, and forfeiture

Operating an Unlicensed Money Transmitting Business—Title 18 U.S.C., Section 1960 Maximum penalty: Five years' imprisonment, $250,000 fine, and forfeiture

Conspiracy—Title 18, U.S.C., Section 371 Maximum penalty: Five years' imprisonment

Money Laundering—Title 18, U.S.C., Section 1956(a)(2)(A) Maximum penalty: 20 years'

imprisonment, $500,000 fine, and forfeiture

Cause or Attempt to Cause Financial Institution to File CTR that Contains Material Omission or Misstatement of Fact—Title 31, U.S.C., Section 5324(a)(2) Maximum penalty: 10 years' imprisonment, $500,000 fine, and forfeiture

INVESTIGATING AGENCY

Federal Bureau of Investigation Drug Enforcement Administration Internal Revenue Service

*Indictments and complaints are not evidence that the defendant committed the crime charged. All defendants are presumed innocent until the United States meets its burden in court of proving guilt beyond a reasonable doubt.

This content has been reproduced from its original source.

http://www.fbi.gov/sandiego/press-releases/2014/unlicensed-money-transmitters-charged-with-money-laundering

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

AUSTRALIA

AUSTRAC data helped capture international cybercriminal

205. Suspicious matter reports submitted to AUSTRAC led to the arrest of an international fugitive wanted for cybercrime and fraud offences. The suspect pleaded guilty to conspiracy to commit bank fraud, conspiracy to commit money laundering and computer fraud.

206. The suspect was sentenced to five years and 10 months imprisonment and also agreed to assist United States authorities to recover the stolen funds.

207. The suspect was an international fugitive who was wanted in the United States for cybercrime and fraud-related offences. United States authorities alleged that the suspect was part of an organised crime group that stole more than USD30 million from United States victims through an elaborate home equity line-of-credit fraud. United States authorities seeking the suspect's arrest published information about him online to alert the public and international authorities.

208. Australian authorities analysed three SMRs submitted by reporting entities, which included detailed information about multiple aliases used by the suspect. The SMRs prompted AUSTRAC to conduct further analysis, which ultimately assisted Australian law enforcement to identify the suspect.

209. Initial analysis of AUSTRAC information identified that the suspect held multiple Australian bank accounts in a false name, a joint bank account with a third-party and a business account for a cafe he operated. The SMRs detailed a range of transactions, described below, which reporting entities considered to be suspicious.

International funds transfer instructions (IFTIs)

210. The SMRs detailed high-value incoming IFTIs sent to the suspect's Australian bank accounts. The suspect received incoming IFTIs in USD totalling approximately AUD1.5 million. These funds were sent from Hong Kong by different individuals and businesses over a one-month period. The suspect also received two incoming IFTIs for AUD90,000 and AUD95,000 from Canada.

211. Further analysis identified incoming IFTIs into the suspect's accounts totalling approximately AUD6.6 million over a one-year period. The IFTIs were sent from Canada, Hong Kong, Indonesia, Nigeria and the United Arab Emirates. The individual IFTIs were for amounts between AUD30,000 and AUD765,000.

212. Of the AUD6.6 million transferred into the suspect's accounts, AUD2.6 million was sent to the suspect's personal account, mostly from Hong Kong, Canada and Nigeria. The suspect's business account received approximately AUD4 million from Hong Kong, Indonesia, Nigeria and the United Arab Emirates. The high-value IFTI activity was inconsistent with the café's established customer profile.

213. The SMRs reported that the suspect withdrew the funds received via the incoming IFTIs shortly after receiving them, using a range of withdrawal types:

- cash withdrawals at different bank branches in two Australian states
- cash withdrawals from automatic teller machines (ATMs) at gaming venues
- use of a debit card to purchase high-value goods including: AUD50,000 purchase at a luxury car dealer
- AUD95,000 purchase at a high-end jeweller
- withdrawal of a bank cheque for AUD195,000 made payable to a real estate agent.

214. Over the same period the suspect sent IFTIs totalled approximately AUD318,000. The IFTIs were sent to the United States, Canada, Germany, Luxembourg and Malaysia. The value per transaction ranged between AUD20 and AUD245,000. An outgoing IFTI to Canada for AUD245,000 was described by the suspect as 'pay out of mortgage'.

215. An SMR noted that the high-value incoming IFTIs and withdrawals were inconsistent with the customer's established profile, and therefore grounds for suspicion.

Cash withdrawals

216. The SMRs identified a large number of high-value cash withdrawals from accounts operated by the suspect:

- eight cash withdrawals totalling AUD94,000 conducted at multiple bank branches over a 10-month period in amounts ranging between AUD1,000 to AUD57,000
- cash withdrawals undertaken within a short time frame at multiple bank branches including: three cash withdrawals totalling AUD25,000 over an eight-day period in amounts ranging between AUD6,500 and AUD9,500 more than 15 cash withdrawals undertaken at multiple bank branches totalling AUD128,000 over a two-month period in amounts ranging between AUD5,000 and AUD9,700.

217. The above withdrawals appeared to be structured into amounts of less than AUD10,000 to avoid the threshold transaction reporting regime

- eight cash withdrawals of AUD1,000 each on the same day at the same branch
- more than 100 cash withdrawals at ATMs totalling AUD105,000 over a three-month period in amounts of between AUD80 and AUD2,000

Cash deposits

218. The SMRs detailed a high volume of high-value cash deposits at multiple bank branches, including:

- two cash deposits of AUD8,500 and AUD32,000 made at two bank branches on different days
- cash deposits totalling AUD56,000 over a three-month period with each deposit ranging between AUD3,000 and AUD23,000

- cash deposits for amounts between AUD45 and AUD65,000 totalling AUD105,000 made at multiple bank branches over a 10-month period.

Domestic electronic transfers

219. The SMRs also detailed high-volume and high-frequency domestic electronic transfers between the suspect's accounts:

- numerous transfers totalling AUD1.3 million over a two-month period between the suspect's accounts
- transfers from the joint bank account to the suspect's own accounts totalling AUD1.5 million over a three-month period
- transfers to and from unrelated third parties including: approximately 75 transfers totalling AUD7.2 million ranging in value between AUD140 and AUD1.2 million over a three-month period from the suspect's accounts to unrelated third parties
- transfers received from unrelated third parties totalling AUD7.2 million over a three-month period, ranging in value between AUD400 and AUD1.2 million.

Dissemination of SMRs to partner agencies

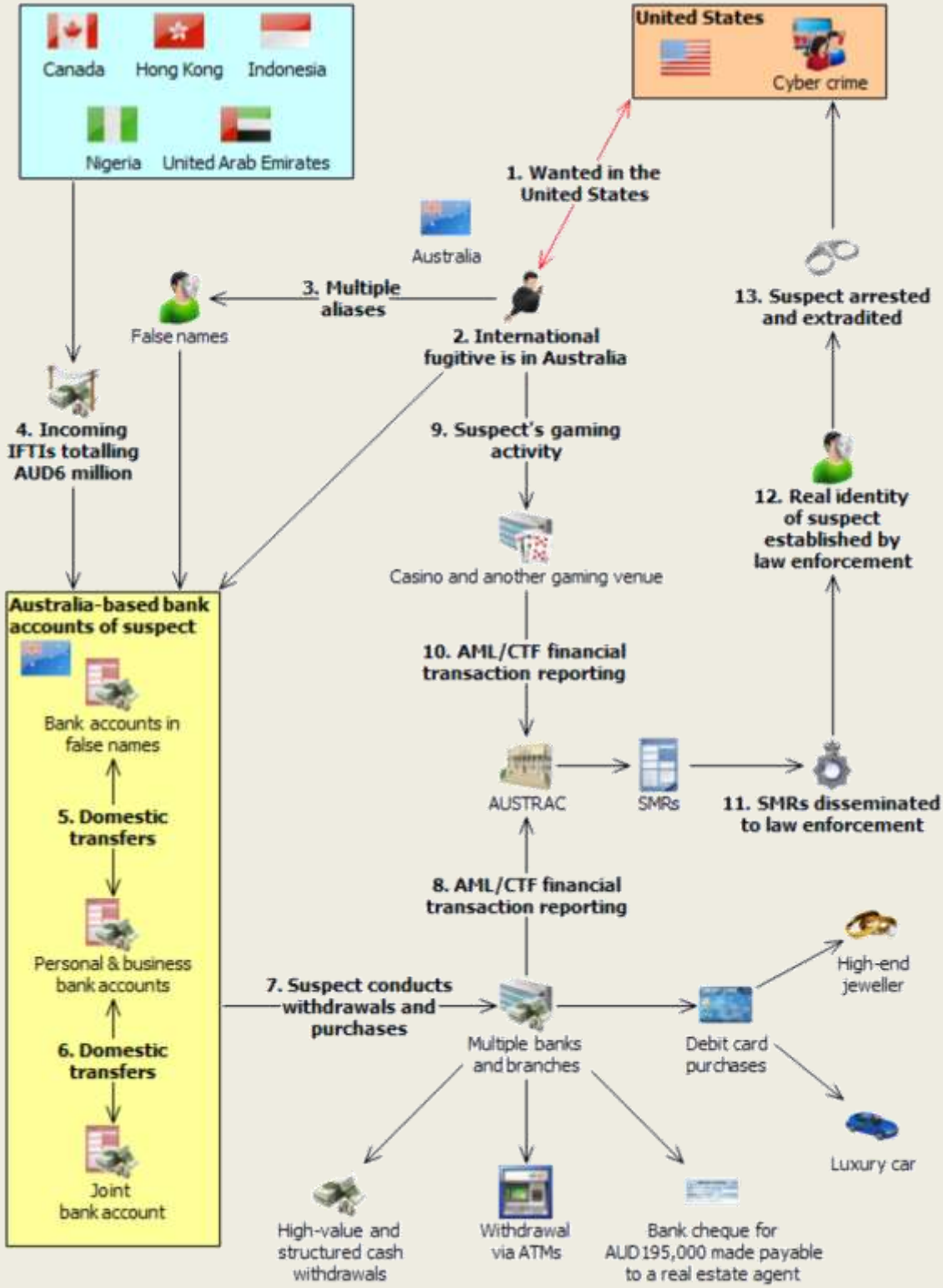
220. After analysing the SMRs, AUSTRAC disseminated them to law enforcement partner agencies, who used them to identify additional false names used by the suspect.

221. A further five SMRs submitted by reporting entities triggered AUSTRAC's monitoring system and were also disseminated to law enforcement. The financial transaction activity reported to AUSTRAC in the SMRs was consistent with the activity outlined above. Reporting entities detailed additional financial activity of the suspect including:

- two domestic electronic funds transfers conducted on consecutive days for AUD25,000 and AUD60,000 to bank accounts held by a casino and another gaming venue
- cash buy-ins of gaming chips totalling AUD275,000 during six visits to a casino, amounting to a total annual loss of AUD53,7006
- multiple structured cash buy-ins of gaming chips worth AUD9,000 and the suspect's refusal to show identification at a casino
- cash totalling AUD175,000 used to place bets at multiple gaming venues over a two-month period.

222. AUSTRAC information combined with analysis undertaken by law enforcement confirmed the identity of the suspect. AUSTRAC data identified phone numbers and address details used by the suspect which ultimately led to his arrest. AUSTRAC data also provided authorities with detailed information about the suspect's financial activities.

223. The suspect was arrested and extradited to the United States. He pleaded guilty to conspiracy to commit bank fraud, conspiracy to commit money laundering and computer fraud. He was sentenced to five years and 10 months imprisonment. The suspect also agreed to assist United States authorities to recover the stolen funds.



Offence	Money laundering Fraud
Customer	Business Individual
Industry	Banking (ADIs)

	Gambling services
Channel	Electronic
	Physical
Report type	IFTI
	SMR
Jurisdiction	Domestic
	International – Canada, Germany, Hong Kong, Indonesia, Luxembourg, Nigeria, the United Arab Emirates
Designated service	Account and deposit-taking services
	Gambling services
Indicators	Account activity inconsistent with customer/business profile
	High-value cash deposits at multiple bank branches over a short period of time
	High-value or structured casino chip cash buy-ins
	High-value transfers to accounts held in the name of a casino and gaming venue
	High-volume and high-value incoming international funds transfers to Australia for no apparent logical reason
	High-volume and/or high-value cash withdrawals at multiple bank branches and ATMs
	Incoming international funds transfers from a high-risk jurisdiction
	Large amount of cash used to place bets at a casino over a short period of time
	Multiple cash withdrawals below the AUD10,000 reporting threshold (that is, structured cash deposits)
	Multiple same-day cash withdrawals conducted at ATMs and the same bank branch
	Outgoing international funds transfers to pay out a mortgage
	Refusal to show identification when undertaking cash buy-ins of gaming chips
	Significant cash withdrawals over a short period of time
	Third-party transfers to and from accounts for no apparent logical reason
	Use of debit cards to purchase high-value goods

BANGLADESH

224. A company took its license from the Registrar of Joint Stock Companies & Farms for the business of export-import and general suppliers. Multi-Level Marketing (MLM) based business was another scope of business among the other activities according to the Memorandum of Article of Association of the organization, but did not obtain related permission from the competent authority.

225. After registering, they started a MLM based outsourcing business. In the name of a web based marketing business, they collected thousands of members who paid either $100 or $200 equivalent BDT each as per the subscription packages. Their products were known as “pay to click/click to earn” and “investment on websites”.

226. The company told the members that they would get $1 per day for the $100 package and $2 for the $200 package through the next 6 months of membership, if they had clicked 100 links of advertisements per day from some listed websites. Thus the members would have been able to double their investments in just 6 months according to the company’s commitment. Furthermore, the company used to give incentives if a member can recruit more members.

227. This became very popular among the general public, especially young people and students as they were getting an outrageous yield by almost doing nothing. As a result, the company was able to collect hundreds of thousands of members within just 6 months of starting business.

228. In this stage the company started to show reluctance to repay their members. Members came to know that the chairman and managing director of the company were preparing to fly away with all the money. Agitated people vandalized the company's office and caught the chairman and MD red handed and handed over the culprits to the police.

229. BFIU came to know about the crime when this was published in various popular daily newspapers and other electronic media. Meanwhile, transactions made by the company, its chairman along with the introducer of company seemed to be suspicious to a bank and it lodged an STR to BFIU. After an investigation, BFIU came to know that the directors of the company were involved in illegal pyramid scheme/MLM business and collected a huge amount of money from the general public fraudulently.

230. BFIU also suspected that the real beneficiary of the company was the introducer of the company's account and his wife. They also layered funds to hide the source of the money in their numerous related bank accounts. BFIU froze the accounts in exercising the power conferred by the section 23(1) (c) of the MLPA, 2012 and sent the case to the ACC for investigation and to initiate further legal action.

Offence	Fraud, Embezzlement of public fund
Customer	Individual, Business
Industry	Banking
Channel	Electronic
Report type	STR
Jurisdiction	National
Designated Services	Internet based Services
Indicators	Unusual transaction, Transaction did not match with the nature of business

FIJI

Case 1

231. Fiji FIU received a Suspicious Transaction Report on Person X who was allegedly arranging work and visas for individuals in Fiji to work in New Zealand. INTERPOL checks revealed that Person X and his de-facto partner, Person Y, were charged in New Zealand for an employment and visa scam. Person X and Person Y had absconded to Fiji and failed to appear in the NZ court for charges laid. Analysis of the bank account maintained by Person X in Fiji revealed significant deposits made to the account by third parties in Fiji with the purpose of the deposits being 'visa fees'. There were subsequent withdrawals conducted on Person X's bank account via international debit card in New Zealand and USA.

232. Fiji FIU established that Person X and Person Y had conducted another employment and visa scam in Fiji after absconding New Zealand. Person X and Person Y then departed for USA. The case was disseminated to Fiji Police Force and investigations are currently underway.

Case 2

233. Fiji FIU received a complaint from a local company, Company X, regarding an order for grass cutters which they had placed with an overseas supplier. Company X was communicating with a known overseas supplier, Company Y based in Chinese Taipei, via email and placed the order. In response, Company Y's bank account details were provided to Company X for the payment.

Company X made the first payment of US$43,368 to Company Y. Before the second payment was made, Company X received an email that appeared to be from Company Y instructing Company X to make the second payment to a company based in UAE. Company X remitted US$65,052 to the company in UAE and when advising Company Y, Company X was informed that the beneficiary in UAE was not known to Company Y.

234. Fiji FIU also received a similar complaint from another local company. Fiji FIU liaised with Chinese Taipei FIU, UAE FIU and UK FIU for these companies. A press release was also issued in April 2014 advising members of the public to beware of email spoofing or impersonations, this press release is available on the Fiji FIU website at http://www.fijifiu.gov.fj/getattachment/8f146dee-68bd-49f2-bad8-7f462cb471a6/Press-Release-09-2014-Beware-of-Email-Spoofing.aspx

235. The case was reported to Fiji Police Force and is currently under investigation.

INDONESIA

236. Mr. RG was an online seller active in Indonesia's biggest online forum and also had his own online shop. He was also the administrator of several blogs. In May 2012, he was arrested and his assets amounting to about USD870.000 was seized. Mr. RG was a skilled hacker, having learned how to hack from his colleague, Mr.CF. Together they broke through a virtual forex trading site (SPEEDLINE), cashed out the money, and used it to buy some assets and financed several terrorism acts in 2010-2011. Mr.CF also was proven guilty of hacking the www.speedline.com, website that enabled him to get funds illicitly and used them to finance terrorists in order to support their military training in Poso, Central Sulawesi.

SAMOA

Case 1

237. Mr YZ is a non-resident and works in an Embassy. He opens a Samoan Tala account with bank A. Bank A in country T reported that they received instructions via internet banking from one of their clients, Mr DS, to remit USD4,400 to Mr YZ's Tala account. Mr DS confirmed that he did not issue such instruction; hence, bank A stopped the transaction. Furthermore, the hacker sent instructions via internet banking to local bank A, to transfer SAT$4,400.00 from Mr & Mrs CS account to Mr YZ's Tala account. Bank A contacted Mr & Mrs CS for confirmation of transfer and discovered that the couple didn't issue such instruction. Bank A cancelled the transfer.

Case 2

238. Bank W received an email from Mr AN about his account balance. The bank released the balance and later on, received another email from Mr AN to debit his account with SAT$24,000 and remit to country A. Bank W did not action the transfer because they still need confirmation from Mr AN. Mr AN visited the bank and confirmed that he did not send the emails. The transfer was then cancelled.

UNITED STATES OF AMERICA

Ross Ulbricht, the Creator and Owner of the Silk Road Website, Found Guilty in Manhattan Federal Court on All Counts. Silk Road was Used by More Than 100,000 Users to Buy and Sell Hundreds of Kilograms of Illegal Drugs and Other Unlawful Goods and Services.

U.S. Attorney's Office February 05, 2015 Southern District of New York (212) 637-2600

Preet Bharara, the United States Attorney for the Southern District of New York, announced today that ROSS WILLIAM ULBRICHT, a/k/a "Dread Pirate Roberts," a/k/a "DPR," a/k/a "Silk Road," was found guilty yesterday on all seven counts in connection with his operation and ownership of Silk Road, a hidden website designed to enable its users to buy and sell illegal drugs and other unlawful

goods and services anonymously and beyond the reach of law enforcement, following a four-week trial before U.S. District Judge Katherine B. Forrest.

Manhattan U.S. Attorney Preet Bharara said: "As a unanimous jury has found, Ross William Ulbricht operated Silk Road—a clandestine global marketplace that offered buyers and sellers of illegal goods and services a promise of anonymity. Ulbricht built this black market bazaar to exploit the dark web and the digital currency Bitcoin to allow users to conduct illegal business beyond the reach of law enforcement. Ulbricht's arrest and conviction—and our seizure of millions of dollars of Silk Road Bitcoins—should send a clear message to anyone else attempting to operate an online criminal enterprise. The supposed anonymity of the dark web is not a protective shield from arrest and prosecution."

According to the Complaint, the Superseding Indictment, and the evidence presented at trial:

ULBRICHT created Silk Road in approximately January 2011, and owned and operated the underground website until it was shut down by law enforcement authorities in October 2013. Silk Road emerged as the most sophisticated and extensive criminal marketplace on the Internet, serving as a sprawling black-market bazaar where unlawful goods and services, including illegal drugs of virtually all varieties, were bought and sold regularly by the site's users. While in operation, Silk Road was used by thousands of drug dealers and other unlawful vendors to distribute hundreds of kilograms of illegal drugs and other unlawful goods and services to well over a hundred thousand buyers, and to launder hundreds of millions of dollars deriving from these unlawful transactions.

ULBRICHT deliberately operated Silk Road as an online criminal marketplace intended to enable its users to buy and sell drugs and other illegal goods and services anonymously and outside the reach of law enforcement. ULBRICHT sought to anonymize transactions on Silk Road in two principal ways. First, ULBRICHT operated Silk Road on what is known as "The Onion Router," or "Tor" network, a special network of computers on the Internet, distributed around the world, designed to conceal the true IP addresses of the computers on the network and thereby the identities of the networks' users. Second, ULBRICHT designed Silk Road to include a Bitcoin-based payment system that served to facilitate the illegal commerce conducted on the site, including by concealing the identities and locations of the users transmitting and receiving funds through the site.

The vast majority of items for sale on Silk Road were illegal drugs, which were openly advertised as such on the site. As of September 23, 2013, Silk Road had nearly 13,000 listings for controlled substances, listed under such categories as "Cannabis," "Dissociatives," "Ecstasy," "Intoxicants," "Opioids," "Precursors," "Prescription," "Psychedelics," and "Stimulants." From November 2011 to September 2013, law enforcement agents made more than 60 individual undercover purchases of controlled substances from Silk Road vendors. These purchases included heroin, cocaine, ecstasy, and LSD, among other illegal drugs, and were filled by vendors believed to be located in more than ten different countries, including the United States, Germany, the Netherlands, Canada, the United Kingdom, Spain, Ireland, Italy, Austria and France.

In addition to illegal narcotics, other illicit goods and services were openly bought and sold on Silk Road as well. For example, as of September 23, 2013, there were: 159 listings under the category "Services," most of which offered computer hacking services, such as a listing by a vendor offering to hack into social networking accounts of the customer's choosing; 801 listings under the category "Digital goods," including malicious software, hacked accounts at various online services, and pirated media content; and 169 listings under the category "Forgeries," including offers to produce fake driver's licenses, passports, Social Security cards, utility bills, credit card statements, car insurance records, and other forms of false identification documents.

Using the online moniker "Dread Pirate Roberts," or "DPR," ULBRICHT controlled and oversaw every aspect of Silk Road, and managed a staff of paid, online administrators and computer programmers who assisted with the day-to-day operation of the site. Through his ownership and

operation of Silk Road, ULBRICHT reaped commissions worth over $13 million generated from the illicit sales conducted through the site. ULBRICHT also demonstrated a willingness to use violence to protect his criminal enterprise and the anonymity of its users. ULBRICHT even solicited six murders-for-hire in connection with operating the site, although there is no evidence that these murders were actually carried out.

* * *

ULBRICHT, 30, of San Francisco, California, was found guilty of: one count of distributing narcotics, one count of distributing narcotics by means of the Internet, and one count of conspiring to distribute narcotics, each of which carries a maximum sentence of life in prison and a mandatory minimum sentence of 10 years; one count of engaging in a continuing criminal enterprise, which carries a maximum sentence of life in prison and a mandatory minimum sentence of 20 years in prison; one of count of conspiring to commit computer hacking, which carries a maximum sentence of five years in prison; one count of conspiring to traffic in false identity documents, which carries a maximum sentence of 15 years; and one count of conspiring to commit money laundering, which carries a maximum sentence of 20 years in prison. The maximum sentences are prescribed by Congress and are provided for informational purposes only, as the sentence will be determined by the judge. ULBRICHT is scheduled to be sentenced on May 15, 2015.

Mr. Bharara praised the outstanding investigative work of the Federal Bureau of Investigation and its New York Special Operations and Cyber Division, as well as the outstanding investigative work of the DEA's New York Organized Crime Drug Enforcement Strike Force, which comprises agents and officers of the DEA, the IRS, the New York City Police Department, U.S. Immigration and Customs Enforcement's ("ICE") Homeland Security Investigations ("HSI"), the New York State Police, the Bureau of Alcohol, Tobacco, Firearms and Explosives, the U.S. Secret Service, the U.S. Marshals Service, Office of Foreign Assets Control, and NY Department of Taxation. Mr. Bharara also thanked the ICE-HSI Chicago-O'Hare office for its assistance and support, as well as the Department of Justice's Computer Crime and Intellectual Property Section and Office of International Affairs. Additionally, Mr. Bharara praised the foreign law enforcement partners whose contributions to the success of the investigation and prosecution have been invaluable, namely, the Reykjavik Metropolitan Police of the Republic of Iceland, and the French Republic's Central Office for the Fight Against Crime Linked to Information Technology and Communication.

Mr. Bharara also noted that the investigation remains ongoing.

The prosecution of this case is being handled by the Office's Complex Frauds and Cybercrime Unit. Assistant United States Attorneys Serrin Turner and Timothy Howard are in charge of the prosecution, and Assistant United States Attorney Christine Magdo is in charge of the forfeiture aspects of the case.

This content has been reproduced from its original source.

http://www.fbi.gov/newyork/press-releases/2015/ross-ulbricht-the-creator-and-owner-of-the-silk-road-website-found-guilty-in-manhattan-federal-court-on-all-counts

4.10 Use of new payment methods / systems

INDONESIA

239. LL Co. was a company producing plastic ores. In 2009, it created IDR and USD accounts in M Bank. LL Co. was reported by its customers because it were deceiving customers by marketing its goods on a website and asking customers to pay upfront before the goods were sent, but never actually sent the goods after the customers paying. Based on the reports, INTRAC traced LL Co.'s transaction and found that there were flows of funds from overseas totalling USD225,668. Mr. ER (Finance Staff of LL Co.) then transferred the money several times using Real Time Gross Settlement

(RTGS) to his account in B Bank. There was also USD1.53 million of money that entered his account via internet banking that came from Mr. TW, a colleague of Mr. ER. Mr. TW was also in involved in the fraud case of LL Co.

MACAO, CHINA

240. Police, during a house search, found over a thousand bank cards from visitors D & E who were not the card holders of those bank cards. After preliminary investigation, the police found that suspects D and E used those debit cards to conduct cash transactions in different local shops. Documents seized from the scene indicated that over MOP20million (USD2.5million) worth of cash was being cashed out by using those debit cards within a one month period.

241. It was confirmed that the two suspects used debit cards from a third party and carried out a large number of cross-border money transfers. Police will further investigate the source of the funds.

4.11 Laundering of proceeds from tax offences

AUSTRALIA

Accountant's overseas tax evasion scheme landed clients in jail

242. AUSTRAC information assisted authorities to investigate a tax evasion scheme promoted and facilitated by an accountant in Australia. The scheme used false invoices and loans to avoid tax. Authorities identified that a client of the accountant defrauded the Commonwealth of AUD2 million over a five-and-a-half year period.

243. The accountant was sentenced to six years imprisonment. The accountant's clients were sentenced to prison terms ranging from two to four years.

244. Authorities commenced an investigation into the accountant and a number of his clients, including suspect A.

245. Investigating authorities identified that suspect A operated an import business in Australia and was a participant in the tax evasion scheme operated by the accountant.

246. Suspect A and his wife were directors and shareholders of an Australian company (company 1). Suspect A was also a director and shareholder of another Australian company (company 2). An associate of suspect A was the co-director of company 2.

247. Authorities identified that the accountant controlled company 3, which was registered in Hong Kong and operated a bank account in Australia. This company was used to issue false invoices to companies 1 and 2.

False invoices

248. Over a five-and-a-half year period company 3 issued false invoices to companies 1 and 2 for supposed 'brokering services'. Suspect A paid the false invoices, which totalled more than AUD2 million, by directing companies 1 and 2 to pay company 3. Over the five-and-a-half year period, at suspect A's direction:

- company 1 paid company 3 a total of AUD1 million
- company 2 paid company 3 a total of AUD1 million.

249. The payment of the false invoices was made by either domestically transferring funds to company 3, or by company 2 issuing cheques made payable to company 3. For example, company 1 domestically transferred AUD50,000 to company 3 in one transaction, and company 2 issued cheques totalling AUD1 million made payable to company 3 over a six-month period.

250. The payments were supposedly for 'commissions' on commercial deals brokered by company 3. Enquiries revealed that company 3 was not a broker and no service had been provided to warrant the payments.

251. Companies 1 and 2 falsely claimed deductions in their tax returns for the 'commissions' paid to company 3, which reduced their taxable income**.**

False loan

252. The funds paid to company 3, less the accountant's 10 per cent fee, were returned to suspect A and individuals associated with him.

253. Over the five-and-a-half year period, company 3 and other companies controlled by the accountant returned approximately AUD1.8 million of the funds originally paid by companies 1 and 2. The funds were distributed at suspect A's direction as follows:

- AUD100,000 by way of a loan to suspect A's business associate and co-director of company 2
- AUD200,000 to suspect A's wife
- AUD1.5 million to suspect A disguised as a 'loan'.

254. Analysis of AUSTRAC information identified two outgoing international funds transfer instructions (IFTIs) totalling AUD270,000 each, sent from company 3 to suspect A's bank account in Japan. The transfers represent part of funds returned to suspect A disguised as a 'loan'.

255. Suspect A claimed that the AUD1.5 million received from company 3 and other companies controlled by the accountant were a 'loan' from another company (company 4), which was registered in the British Virgin Islands and owned and controlled by the accountant. However, authorities found no evidence to support this claim: there was no record of any payments from company 4 to the suspect's personal bank accounts, company 4 did not have any bank accounts in Australia and it had not deposited any funds into any Australian banks.

256. Analysis of AUSTRAC data showed that suspect A and company 2 were both the ordering and beneficiary customers of international funds transfers from Australia to Japan totalling AUD1 million, sent over a period of three years.

257. Authorities believed these transfers were the proceeds of the tax evasion which were sent to Japan for the benefit of suspect A. In essence, suspect A directed companies 1 and 2 to make payments to company 3 in order for the funds to be transferred back to him tax free.

258. Authorities identified that suspect A spent approximately AUD400,000 of the funds received from companies controlled by the accountant on the demolition and rebuilding of his home, mortgage payments and living expenses.

Income tax inconsistencies

259. Authorities analysed the personal income tax returns of suspect A and identified that in one financial year he reported his gross income as AUD30,000. During the same financial year, AUD400,000 was deposited into a personal bank account held by suspect A, and AUD450,000 was withdrawn from the account.

260. Over the next three years, suspect A reported his gross personal income as AUD30,000 per year. Suspect A did not declare the AUD1.5 million he received from company A.

261. Authorities executed more than 20 search warrants on properties including the accountant's Australian accountancy business and suspect A's residential property, from which large quantities of documents were seized.

Charges and sentencing

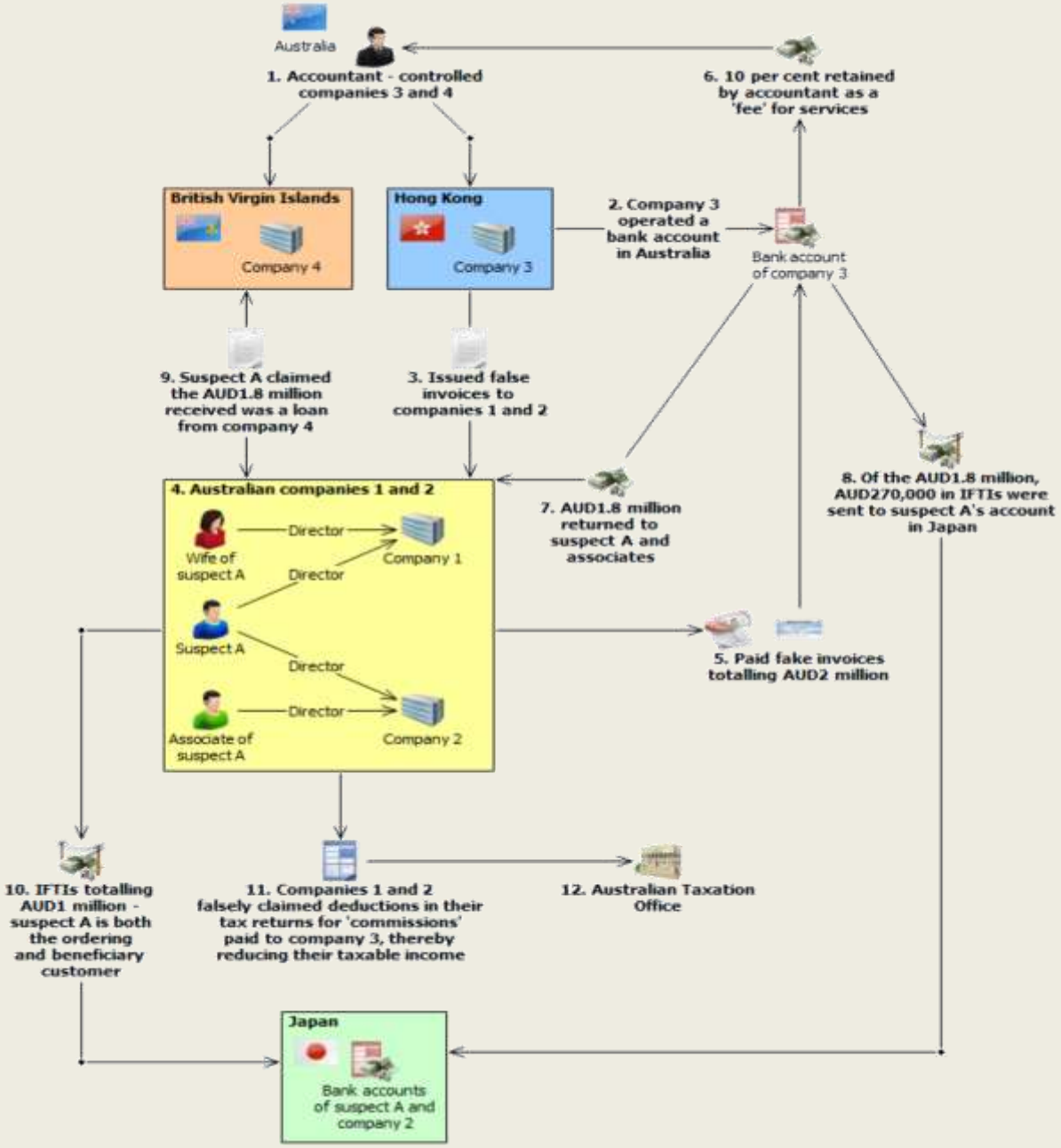
262. Suspect A was charged with:

- three counts of being knowingly concerned in defrauding the Commonwealth under the *Crimes Act 1914*
- one count of aiding in general dishonesty causing a loss under the *Criminal Code Act 1995*
- one count of aiding in obtaining a financial advantage by deception under the Criminal Code Act
- four counts of obtaining a financial advantage by deception under the Criminal Code Act.

263. Suspect A was convicted and sentenced to four years imprisonment and required to pay a penalty of AUD1 million.

264. The accountant was convicted of aiding and abetting the commission of fraud against the Commonwealth and was sentenced to six years imprisonment.

265. A further three clients of the accountant were convicted of obtaining a financial advantage by deception. Two of the clients were sentenced to three years imprisonment and the third client was sentenced to two years imprisonment.



Offence	Tax evasion
Customer	Business Foreign entity Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – British Virgin Islands, Hong Kong, Japan
Designated service	Account and deposit-taking services

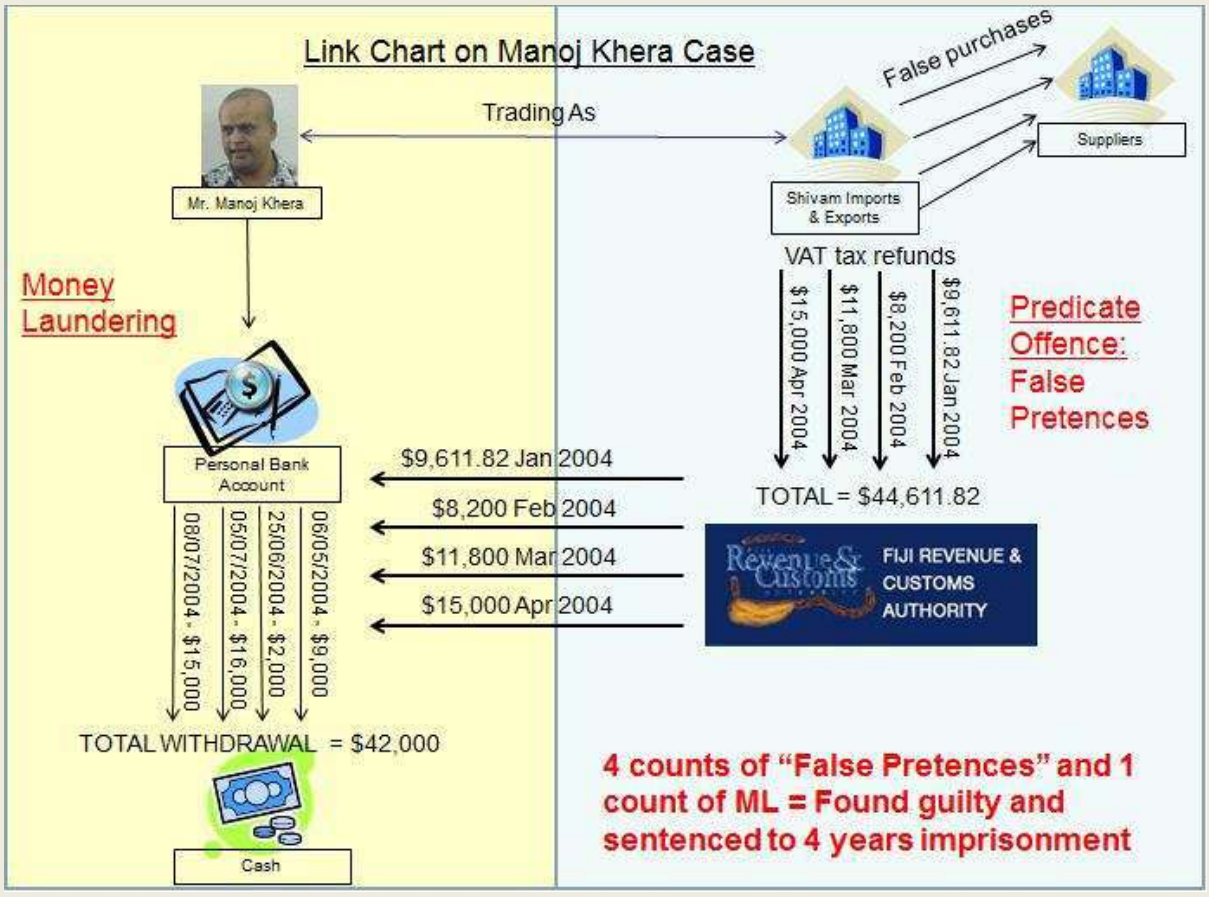
Indicators

- Customer is both the ordering and beneficiary customer for multiple outgoing international funds transfers
- Customer receives international funds transfers described as 'loan'
- Customer undertaking complicated transfers without a business rationale
- High-value international funds transfers from Australia with no apparent logical reason
- Use of an accountant to facilitate unusually complicated transactions
- Use of tax secrecy jurisdictions

FIJI

266. In 2004, a commercial bank reported a case to Fiji FIU regarding a businessman, Person X, receiving large Inland Revenue cheques into his account. The case was scrutinized by Fiji FIU and it was established that Person X had fraudulently obtained VAT refund cheques.

267. In July 2014, Mr. Manoj Kumar Khera (brother of Person X) was convicted for money laundering and false pretences. He was sentenced to four years imprisonment. A copy of the court rulings including judgment and sentencing is available on the Fiji FIU website (http://www.fijifiu.gov.fj/Pages/Case-Laws/2014.aspx). The following diagram illustrates this case.



INDONESIA

268. Mr. DA was a staff in the Directorate of General Taxes. The development of the case was started by the Analysis Result by INTRAC that was sent to the Attorney General. Mr. DA was revealed to own several bank accounts holding billions of Rupiah. From the investigation it was known that the money came from the criminal act of tax evasion. Mr. DA helped KTU Co. to reduce its outstanding tax payment in 2002 and asked for a USD100,000 fee. Mr. DA also asked MV Co. a total of USD20.8 million. M r. DA, other than holding money in his bank account, also purchased

some assets such as land, property, precious metals, and vehicles. Mr. DA was then evicted to 13 years in prison.

4.12 Real Estate, including roles of real estate agents

CHINESE TAIPEI

269. Mr. T was a manager of Security Company K. In 2000, Mr. T claimed that he was operating an additional business which is to provide loans for investors, assistant investors to buy new shares issued for cash, and produce certificate of financial status to K Security Company's customers but he needed capital to run his business. Therefore, he collected money from the customers of Security Company K and friends with the promise of high return. However, Mr. T didn't use the funds to operate the claimed business. Instead, he used funds received from the investors to pay the interest and capital to previous investors. Then, he used the rest of the funds amounting to about NTD 50 million for his personal investment in the stock market and about NTD 7.1M for the purchase of real state in the name of his wife. The Investigation Bureau initiated a criminal investigation and then referred this case to Hsinchu District Prosecutors Office in August 2014 for prosecution.

FIJI

270. In January 2014, the Fiji FIU received a Suspicious Transaction Report on an inward remittance of FJ$0.7 million from Company X based in the British Virgin Islands to a foreigner, Person X's bank account in Fiji. Soon after this remittance, Person X withdrew significant amounts of money to purchase a prime real estate property and a luxury motor vehicle.

271. The Fiji FIU had established that Company X also made remittances to Person Y, an adversely reported individual known to Fiji FIU. Person Y was previously investigated by the Fiji Police for alleged illegal gambling activities.

INDIA

272. A NIA investigation has revealed that the accused persons belonging to a banned terrorist organization had utilised the proceeds of terrorism to purchase/acquire land, flats and vehicles for terrorist activities. This case relates to criminal conspiracy to wage war against the government by extremists by recruiting youths and procuring arms/ammunition using funds extorted from the general public. All the movable/immovable properties created out of proceeds of terrorism as investigated and identified in the case have been attached under the provisions of Unlawful Activities (Prevention) Act, 1967 (UAPA).

4.13 Gems and Precious Metals

BHUTAN

273. Customs Officials at the International Airport Paro, during their normal routine baggage check of passengers arriving from Bangkok, intercepted passengers carrying gold beyond the permissible quantity on four different instances. As the passengers were in possession of gold beyond the permissible quantity, they were handed over to the Royal Bhutan Police, Paro for investigation and prosecution.

274. The first incident occurred on 22/02/2014 involving seven Indian nationals with total of 8 kgs gold biscuits. While the four were travelling from Bangkok with 8 kgs gold biscuit, one person was caught who had come to receive them, and another two from a hotel in Thimphu, as they were also found involved in the racket.

275. On investigation, they revealed that they were couriers only and the man behind the racket was an Indian citizen based at Bangkok. They were paid Rs. 5,000 each for carrying one kg gold biscuits, free air ticket, free accommodation, food, taxi charges etc. One of them was responsible for

receiving the people at the airport, gold consignment, arranging taxi, accommodation and arranging road permit. Further, he receives Rs. 5,000 each per person for the job, besides his personal expenses.

276. They smuggled the gold biscuits by concealing it in their underwear and the final destination was supposed to be India.

277. They were charge sheeted to the Royal Court of Justice, Paro on the following charges:

i. Section 279 of Bhutan Penal Code, 2004
ii. Section 16 Kha of Sales Tax, Customs and Excise Act of the Kingdom of Bhutan, 2000.
iii. Section 281 of Bhutan Penal Code, 2004
iv. Section 120 (281) of Bhutan Penal Code, 2004
v. Section 127 (279) of the Penal Code of Bhutan, 2004

278. However, the Royal Court of Justice, Paro amended the charge of aiding and abetting smuggling to that of attempt to aiding and abetting smuggling and passed judgment, convicting three defendants to three years each and other four for one year and six months each. Further, two defendants were ordered to restitute Nu. 30,55,000 each to the Government of Bhutan within one month from the date of judgment as the price of two kgs of gold smuggled and sent to India.

INDIA

279. Fraudsters opened several companies in India and fraudulently remitted foreign exchange amounting to INR 54000 million to firms based in Hong Kong & Dubai. They forged the signatures of the custom officials of India and presented the said forged bills of entry before the Bank with the help of his accomplices. The funds were brought back to India in the guise of export proceeds of various exporters who over invoiced. The kingpin was manipulating this by charging 0.45 million per 10 million INR. The investigation reveals involvement of DNFBP of gold bullion industry. The case is under the Prevention of Money Laundering Act (PMLA) investigations.

UNITED STATES OF AMERICA

Former Jeweler Faces Federal Money Laundering Charges for Pawning Diamonds Falsely Reported Stolen in 2004

U.S. Attorney's Office October 03, 2014 Northern District of Alabama(205) 244-2001

BIRMINGHAM—Federal prosecutors today charged a Vestavia Hills man with money laundering for pawning a 3-carat diamond in 2013 that was among a cache of jewels he collected $2.6 million in insurance money on in 2004 after reporting them stolen in a Mountain Brook Jewelry store robbery.

U.S. Attorney Joyce White Vance, FBI Special Agent in Charge Richard D. Schwein Jr., U.S. Secret Service Special Agent in Charge Craig Caldwell, Vestavia Hills Police Chief Dan Rary and Mountain Brook Police Chief Ted Cook announced the charges against JOSEPH HAROLD GANDY.

The U.S. Attorney's Office charged Gandy, 64, with one count of money laundering for pawning property worth more than $10,000 that he obtained through a criminal act, wire fraud, which he committed when he submitted an insurance claim on diamonds that had not been stolen. Prosecutors also charged Gandy with one count of being a convicted felon in possession of firearms for the 99 weapons seized at his Vestavia Hills home in November 2013. Gandy is prohibited from possessing weapons because of a 1989 federal mail fraud conviction.

The FBI recovered jewelry during the search of Gandy's home and, as part of a plea agreement with the government, he also turned over a portion of the approximate $1.5 million worth of diamonds and jewelry he falsely reported stolen in 2004. Among those jewels is a rare Blue Diamond worth at least $620,000.

"This defendant revealed decade-old criminal acts, and committed a new crime when he brought forth valuable, but fraudulently obtained diamonds to pawn," Vance said. "Thanks to the committed and cooperative efforts of the Mountain Brook and Vestavia Hills police departments, the FBI and the Secret Service, Mr. Gandy avoided, but did not escape justice."

"This case illustrates the great cooperation among law enforcement at all levels," Schwein said. "I want to extend my personal appreciation to the Vestavia Hills and Mountain Brook police departments, the U.S. Secret Service, and my agents for their outstanding work. It was their diligent investigative efforts that brought this case to where it is today," he said.

"I commend the cooperative between the FBI and our investigators," Rary said. "Interagency cooperation is essential in today's environment, especially in complex investigations such as these."

Prosecutors filed the charges and the plea agreement with Gandy in U.S. District Court.

According to the plea agreement, Gandy's crime unfolded as follows:

Gandy was an owner and the operator of Denman-Crosby Jewelry Store in Mountain Brook in 2004. In December of that year, he reported that two unidentified men robbed the store at gunpoint. At the time, Denman-Crosby was promoting a loose diamond sale for Christmas. It had many diamonds and other jewelry in on consignment from jewelers in New York and elsewhere. The store carried a $2.6 million insurance policy. Gandy had increased the coverage amount with XL Specialty Insurance Company a few weeks before the robbery.

In January and March of 2005, Gandy used interstate wire transmissions to submit insurance claims from the robbery. He included a detailed inventory of jewelry worth about $2.8 million that he reported stolen. XL Specialty paid the policy's limit of $2.6 million.

In July 2013, Gandy began sending a friend to jewelry stores in Jefferson County to pawn diamonds he had reported stolen in 2004. The first effort ended when the jeweler requested documentation on a 1.59-carat diamond, mounted in a platinum setting, and attempted to examine the stone closely. The concern was that the diamond might bear a laser inscription useful in tracing its history. Subsequently, Gandy examined 10 to 12 diamonds under a microscope and selected stones that bore no inscription.

On July 26, 2013, Gandy sent his friend to a Birmingham jewelry store to pawn a 3.01-carat emerald-cut diamond he said was worth about $43,000. Gandy said he wanted at least $15,000 for the stone. The store accepted the diamond in exchange for a $12,000 loan. The diamond was one Gandy reported stolen in the Denman-Crosby robbery. He gave his friend $2,000 for making the transaction.

Between August and November of 2013, Gandy's friend pawned two more diamonds: a 3.45-carat cushion-cut diamond for $8,000; and a 2.16-carat round diamond for $2,000. Both stones were on the stolen inventory list Gandy provided the insurance company in 2005. Gandy gave his friend $1,880 after receiving the $8,000 for the 3.45-carat diamond.

Gandy's plea agreement is a "binding plea agreement" in which the government and Gandy stipulate that a 45-month prison sentence is appropriate. If the court rejects the plea agreement, either party may declare it null and void.

As part of the agreement, the government would recommend Gandy be required to pay $20,000 in restitution to the jewelers where he pawned the diamonds, and that he forfeit to the U.S. government all the jewels seized and recovered in the case. Vestavia Hills Police seized the 99 weapons at Gandy's house and has state charges pending against him. The city police are handling forfeiture of the firearms.

The government acknowledges in the plea agreement that it has no evidence or information to suggest Gandy is violent or has been engaged in previous violent behavior. The agreement notes that Gandy, through his lawyer, related that, except for older firearms he bought before his 1989 conviction or that were passed down from his father and grandfather, the firearms at his house belonged to his son who died in 2004.

The FBI, Secret Service, Vestavia Hills and Mountain Brook police departments investigated the case. Assistant U.S. Attorney George A. Martin Jr. is prosecuting the case.

This content has been reproduced from its original source.

http://www.fbi.gov/birmingham/press-releases/2014/former-jeweler-faces-federal-money-laundering-charges-for-pawning-diamonds-falsely-reported-stolen-in-2004

4.14 Association with human trafficking and people smuggling

AUSTRALIA

Suspect jailed after forcing trafficking victims to work in Australian brothels

280. AUSTRAC information contributed to a law enforcement investigation into a syndicate involved in the trafficking of women from Thailand to Australia. The suspect pleaded guilty to conducting a business involving sexual servitude and making a false statement to an immigration official.

281. The suspect was sentenced to two years and three months imprisonment.

282. The syndicate used a bank account to conduct a range of transactions to facilitate the trafficking. The investigation ultimately disrupted the Australia-based syndicate.

283. Australian law enforcement identified an Australia-based suspect who organised for foreign women to work in brothels in Australia. The suspect organised the placement of 11 women in brothels, where they were forced to work to pay off a large debt owed to the suspect. They incurred the debt in return for being brought to Australia.

284. A broker recruited the women in Thailand and organised passports, visas and other travel arrangements. Each of the women agreed to repay a 'debt' of approximately AUD53,000 after arriving in Australia. Some of the women were made aware that they would be working in the sex industry, while others were misled as to the nature of the work they would be required to perform.

285. Each Australian brothel deducted its fee and paid the remainder of the earnings to the women. The women used these funds to repay their debt to the suspect by transferring funds electronically into the suspect's bank account or by depositing cash into the suspect's account. In the case of one brothel, the repayments were made by giving cash directly to the suspect.

286. At the request of the law enforcement agency, AUSTRAC produced financial intelligence assessments which analysed various aspects of the suspect's financial activities.

287. AUSTRAC identified that:

- the suspect used aliases and variations of her address when conducting transactions
- significant cash transaction reports (SCTRs) revealed the suspect had withdrawn AUD53,000 cash from a bank account over a one-month period
- over an eight-year period the suspect, using her own name and a number of aliases, sent 90 international funds transfer instructions (IFTIs) to individuals in Thailand, totalling approximately AUD455,000.

288. Analysis of AUSTRAC information identified an individual in Thailand who was suspected of being a broker who arranged the trafficking of women from Thailand into Australia as part of the sexual servitude syndicate.

289. Over a 12-month period the suspect in Thailand received 37 IFTIs from Australia totalling approximately AUD320,000. The IFTIs were made through banks and were sent by Australia-based employees of the main suspect in Australia, as well as the 11 women. The IFTIs showed the women shared common addresses. Authorities suspect the cash payments were structured into amounts of less than AUD10,000 to avoid the cash transaction reporting threshold. AUSTRAC disseminated information to a Thai law enforcement agency to assist its investigations into the syndicate's operations in Thailand.

290. On average, it took approximately six months for each woman to pay off their debt to the suspect. Enquiries revealed that of the AUD53,000 each woman was required to pay back to the suspect, the broker in Thailand was paid AUD20,000. The main suspect made a profit of approximately AUD10,000 to AUD18,000 per woman.

291. As part of the arrangement, after the women arrived in Australia the suspect assisted them to apply for a protection visa. To substantiate a claim for refugee status the suspect provided the women with false information about the conditions they had each experienced in their home country. The suspect also coached the women on how to answer questions from Australian authorities about their visa application.

292. The suspect pleaded guilty to:

- conducting a business involving sexual servitude over a three-year period contrary to section 270.6(2) of the Criminal Code Act 1995
- making a false statement to an immigration official in connection with an application for a protection visa contrary to section 234(1)(b) of the Migration Act 1958.

293. The suspect was sentenced to two years and three months imprisonment.

Offence	People trafficking Sexual servitude
Customer	Individual
Industry	Banking (ADIs)
Channel	Electronic
Report type	IFTI
Jurisdiction	International – Thailand
Designated service	Account and deposit-taking services
Indicators	International funds transfers to a country of interest to authorities Large cash withdrawals within a short time frame Multiple customers linked by common addresses, conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers below AUD10,000

<u>People smuggling operation shut down by joint Australian– Indonesian investigation</u>

294. A joint investigation between Australian and Indonesian authorities identified two Australian suspects (a father and son) who were facilitating a people smuggling venture. AUSTRAC analysis of

financial transaction reports assisted the investigation. Authorities restrained approximately AUD60,000 as the proceeds of crime.

295. The main suspect was sentenced to a suspended nine-month jail sentence.

296. Australian authorities alleged that approximately 70 foreign nationals had paid the two suspects to facilitate their passage from Indonesia into Australia. The voyage was not undertaken due to intervention by Indonesian police. The father, suspect A, was identified as a people smuggler operating in Indonesia and Malaysia.

297. Suspect A originally arrived in Australia as an asylum seeker and was granted a visa. Suspect A was linked to numerous Afghan nationals who were detained in Indonesia and Christmas Island. Suspect A travelled to Pakistan, Malaysia and Indonesia and was approached by Afghan nationals to arrange their safe passage to Australia. The Afghan nationals were willing to pay between AUD8,000 and AUD10,000 each for the journey.

298. Suspect B assisted his father (suspect A) to transfer funds relating to the people smuggling operation. In Indonesia the foreign nationals paid cash up-front before being transported to Australia. Some of the funds were sent to Australia. Money was also sent from Australia to Indonesia to assist the suspects' people smuggling associates in Indonesia.

299. Over a two-month period, three suspicious matter reports (SMR) were submitted by reporting entities which identified the following:

300. While in Australia, suspect B received multiple incoming international funds transfer instructions (IFTIs) from suspect A in Indonesia. The transfers appeared to be deliberately structured3 into amounts below AUD10,000.

- Suspect A provided multiple, conflicting identification details when sending separate IFTIs from Indonesia to Australia.
- Suspect B received significant cash deposits into his personal account from multiple third parties in different Australian states.
- Suspect B transferred approximately AUD40,000 from his personal everyday account to his debit card account via internet banking. On the same day suspect B conducted three significant cash withdrawals from the debit card account in amounts of AUD10,000, AUD20,000 and AUD10,000. These cash withdrawals were made at three different bank branches in a major metropolitan area. On a separate occasion, suspect B attempted to withdraw a significant amount of cash. Upon being questioned by the branch manager regarding the purpose of the funds suspect B provided conflicting information and then became irate. Suspect B did not withdraw the funds and proceeded to close all accounts at this major bank.

301. AUSTRAC staff analysed financial transaction reports submitted by reporting entities and identified the following:

- Over a one-month period suspect B conducted one cash deposit of AUD11,000 and five cash withdrawals in amounts between AUD5,000 and AUD20,000. Suspect A also conducted one cash deposit of AUD13,000.
- Over a six-day period suspect A used remittance services in Indonesia to transfer approximately AUD40,000 to suspect B in Australia in amounts between AUD1,900 and AUD7,600.
- Over an eight-month period suspects A and B conducted 10 outgoing IFTIs from Australia to Indonesia. The suspects used the remittance services to transfer the funds to

third-party accounts and accounts held in their names in amounts between AUD150 and AUD5,000.

302. Both suspects were charged with people smuggling and money laundering offences, and suspect B was charged with possessing a drug of dependence. Suspect A did not face trial. Authorities restrained as the proceeds of crime approximately AUD60,000 held in a bank account operated by suspect A's daughter. Suspect B was sentenced to a suspended nine-month jail sentence after pleading guilty to receiving and dealing with money from the proceeds of crime.

Offence	Money laundering Fraud People smuggling
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	SCTR IFTI SMR
Jurisdiction	Domestic International – Indonesia
Designated service	Account and deposit-taking services Remittance service (money transfers)
Indicators	Conflicting or incomplete identification details provided for different transactions Customer becomes irate when questioned over financial transactions Customer undertaking transactions that appear to be inconsistent with their customer profile and transactional history International funds transfer from an individual account to several offshore accounts held in the names of third parties International funds transfer to high-risk jurisdictions Large cash withdrawals from multiple bank branches on the same day Structured international funds transfers within a short period of time Use of overseas bank accounts

BANGLADESH

303. A gang of Bangladeshi human traffickers got some young men fly to Iran on the promise of providing them better jobs and attractive salary. Traffickers lured the men mostly from Dubai and Sharjah in the United Arab Emirates (UAE) at different times with the promise of lucrative jobs in Saudi Arabia, Iraq and Greece. These men were picked up separately and taken to Iran where they were confined inside a house secretly, their passports, documents and other valuables were confiscated.

304. The traffickers then forced the hostages to contact their families in Bangladesh to get them to pay a ransom for their release. Each hostage were forced to pay between BDT 0.15 million (USD1948) to BDT 0.3 million (USD3896) through a popular mobile financial service provider for their release. Investigation reveals that 23 mobile banking accounts were used to collect the ransom. Some of these accounts were opened by using fake IDs and some transactions were conducted by using 20 unique mobile banking customer accounts under an agents name within a short period of time and facilitated most of the ransom (BDT 2.1 million) on behalf of the traffickers. According to the existing directive, an agent should not open mobile banking customer accounts on behalf of others

under his/her name and should not transact for others through either his/her mobile banking agent account or personal mobile banking account. The case was forwarded to CID of Bangladesh Police who filed a case in this regard. With the help of Iranian Authority, Bangladesh Authority rescued 13 kidnapped persons from Iran.

Offence	Human trafficking, Hostage taking
Customer	Group of Individuals
Industry	Banking
Channel	Physical Mobile Financial Service
Report Type	Complaints from different sources
Jurisdiction	Transnational
Designated Services	Mobile banking agents account and customer account
Indicators	Human trafficking, unlawfully open and operate mobile accounts

FIJI

305. In June 2014, Mr. Inoke Raikadroka and Mr. Mohammed Sagaitu were found guilty for domestic trafficking in children and slavery. Mr. Raikadroka was sentenced to 16 years imprisonment and Mr. Sagaitu was sentenced to 12 years imprisonment. These two individuals had recruited three sisters who were aged 18, 17 and 15 to work as sex workers for Mr. Raikadroka. During the trial, it was established that Mr. Raikadroka would traffic these girls between central and west Fiji to provide services to clients. Mr. Raikadroka in this case was found to be the "controller" or pimp.

306. Further details of the case are available on the link: http://www.paclii.org/cgi-bin/sinodisp/fj/cases/FJHC/2014/409.html?stem=&synonyms=&query=raikadroka

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

AUSTRALIA

International crime syndicate used underground banking to launder massive drug profits

307. AUSTRAC assisted an investigation which disrupted a global crime syndicate involved in money laundering and the importation of more than 30 kilograms of methamphetamine into Australia.

308. Three suspects were arrested and charged with importing a commercial quantity of a border controlled drug.

309. The syndicate operated a 'hawala'-type remittance system with cells based in Australia, the United Arab Emirates (UAE) and Nigeria. The syndicate head was located in Lebanon.

310. The cells in Australia were headed by an Iranian national (suspect A) and an Iraqi-born Australian citizen (suspect B).

311. The head of the syndicate coordinated the distribution of cash payments from drug trafficking networks operating in Australia to suspects A and B.

312. Suspect A operated a business in the Iranian community facilitating the immigration of Iranian nationals to Australia and other countries. Most of suspect A's financial activity involved large cash deposits (reported to

313. AUSTRAC as threshold transactions reports, or TTRs) and regular incoming international funds transfer instructions (IFTIs) from companies in Canada, Iran, Slovenia, the UAE and Turkey.

314. TTRs received by AUSTRAC showed that, over a six-year period, suspect A received AUD715,000 in large cash deposits, while AUD63,000 cash was withdrawn from bank accounts

associated with the suspect. Over that same period, the suspect and his company were the beneficiary of 41 incoming IFTIs totalling AUD521,000.

315. Suspect A was also the subject of two suspicious matter reports (SMRs) submitted by a bank. The SMRs described the various activities observed that gave it grounds for suspicion:

- suspect A's unusual account activity
- funds being sent to/received from high-risk jurisdictions
- large cash deposits made at different bank branches on the same day
- third parties making cash deposits into suspect A's account.

316. Over a one-year period suspect B was the ordering customer for 56 outgoing IFTIs totalling AUD244,000. Suspect B sent the funds to approximately 38 overseas-based beneficiary customers in 12 different countries, with the top five countries being the United States, Lebanon, China, Luxembourg and Syria. All but six IFTIs were conducted through remittance dealers. Over the one-year period suspect B conducted multiple 'same-day' IFTIs, on the majority of occasions conducting the transactions through different remitters.

317. Suspect B was also the subject of two SMR reports submitted by a bank, detailing the following activity:

- Suspect B deposited cash into third-party bank accounts, with one beneficiary account holder identified to be an Iranian national without any work entitlements in Australia.
- The suspect's trading account received regular large cash deposits, which were followed by cheque withdrawals issued to third parties.
- Suspect B's mortgage account exhibited unusual transaction behaviour, being used for very large cash deposits and withdrawals (worth hundreds of thousands of dollars).
- The suspect made many large cash deposits; behaviour which was inconsistent with the suspect's claimed occupation as a shop assistant.

318. Law enforcement also investigated the activities of a third suspect, suspect C, because of his involvement with a suspected money launderer. Authorities believe that suspect C arranged to transfer AUD300,000 to Mexico using the unregistered remittance service provided by suspect B. Suspect B was not registered with AUSTRAC as a remittance service provider.

319. Suspect C was arrested as he was departing Australia on a flight to Mexico. In his possession was USD9500, AUD660, two diamonds valued at AUD50,000 each and casino chips valued at AUD170,000.

320. A search of the AUSTRAC database showed that suspect C had a gambling turnover of AUD11 million over a three-month period. Suspect C was also the subject of four SMRs, which detailed his unusual gambling activity and practice of making cash deposits in amounts just below the AUD10,000 reporting threshold. The suspect conducted multiple, same-day gambling-related transactions on a regular basis. The gambling-related transactions were in close succession, which suggested the suspect was undertaking a bare minimum of gambling in between transactions.

321. The three suspects were arrested and charged with importing a commercial quantity of a border controlled drug contrary to the Criminal Code Act 1995. Suspect C was also charged with dealing in money or property valued in excess of AUD100,000, which is believed to be the proceeds of crime, contrary to section 400.4 of the Criminal Code Act.

Offence	Drug trafficking Money laundering
Customer	Individual Business
Industry	Banking (ADI) Gambling services Remittance services
Channel	Electronic Physical
Report type	IFTI SMR TTR
Jurisdiction	International – primarily Canada, Iran, Lebanon, Mexico, Nigeria, Slovenia, Syria, Turkey, United Arab Emirates
Designated service	Account and deposit-taking services Gambling services Remittance services (money transfers)
Indicators	Cash deposits into third-party accounts High-value transactions inconsistent with customer profile High-value/volume gambling transactions with minimal gambling activity International funds transfers to high-risk jurisdictions Large cash deposits made at different bank branches on the same day Multiple same-day gambling activity Unusual transaction activity through business accounts, suggesting the account is being used for unregistered remittance activity

FIJI

Case 1

322. Fiji FIU received Suspicious Transaction Reports on significant transactions occurring in the personal bank accounts of Person X. Analysis of these reports found that Person X was a government official and also owned an excavation works company. Person X and his wife maintained several term deposit accounts for themselves and on behalf of their children.

323. Fiji FIU established significant transfers from the business account of Person X's company to personal accounts maintained by him and his wife.

324. The total amount involved in this case was FJ$0.8 million. This case was disseminated to Fiji's tax authority for possible tax evasion offences. Investigations are currently underway.

Case 2

325. Person X was reported for receiving large amounts of money into his personal account. Checks on the FIU database revealed that Person X was sharing the same postal address as Person Y and Person Z. These three individuals were linked to a business, Business A, which was investigated for possible illegal gambling operations.

326. Person X stated that he was a chef at Business A. We had also established that Person Y was a chef at Business A. Between 2011 and 2014, total of FJ$118,000.00 was deposited into the personal bank account of Person X. We had noted that funds were accumulated in Person X's bank account and a lump sum withdrawal was made from the account.

327. The case was disseminated to Fiji Police Force and investigations are currently underway.

Case 3

328. A Suspicious Transaction Report on unauthorised transactions conducted in the bank accounts of Person A and Person B were reported to Fiji FIU. Investigations found that 2 bank officers (Person C and Person D) had colluded with 2 other individuals (Person E and Person F) to obtain access to the bank accounts of Person A and Person B.

329. Person E and Person F used social engineering techniques on social networking sites to extract personal information, including telephone numbers, of Person A and Person B who both had signed up for telephone banking. Once Person E and Person F obtained the personal information, they were able to change the telephone banking login details of Person A and Person B. Person E and Person F then proceeded onto transferring funds (total of FJ$24,000) from the bank accounts of Person A and Person B to their own bank accounts and the bank accounts of the 2 bank officers.

330. Person E and Person F have been charged with money laundering and the case is still before the Court.

HONG KONG, CHINA

331. In May 2013, a journalist (who acted as an undercover agent) was recruited by a foreign male Person B in jurisdiction Y to set up front companies and open bank account in Hong Kong in order to launder crime proceeds. In June 2013, the journalist had set up two companies as instructed and made a report to Hong Kong Police leading to the arrest of Person B. Person B was charged with one count of "incitement to money laundering" and was sentenced to four years imprisonment in September 2014.

INDIA

332. Mr. S along with his parents was involved in cheating different persons to the tune of 40 million INR and made huge cash deposits into his bank accounts. On the complaint an offence of cheating was booked against him by the Law Enforcement Authorities. On investigation he tried to show the receipts from various friends and sale of motor vehicles. It has since been revealed that all these claims were exaggerated to conceal the actual source of funds. The funds so sourced were mainly invested in properties. However, the same were attached under the Prevention of Money Laundering Act (PMLA).

INDONESIA

333. Mrs. IMD was a Relationship Manager in C Bank. Mrs. IMD embezzled her customers' fund totalling USD4.7 million. To obscure the origin of her wealth, Mrs. IMD founded 4 companies, and transferred the funds to her husband (Mr. AG), her sister (Mrs. VL), and her brother-in-law (Mr. I). Mrs. IMD was indicted to 8 years in prison and USD1 million in fines.

JAPAN

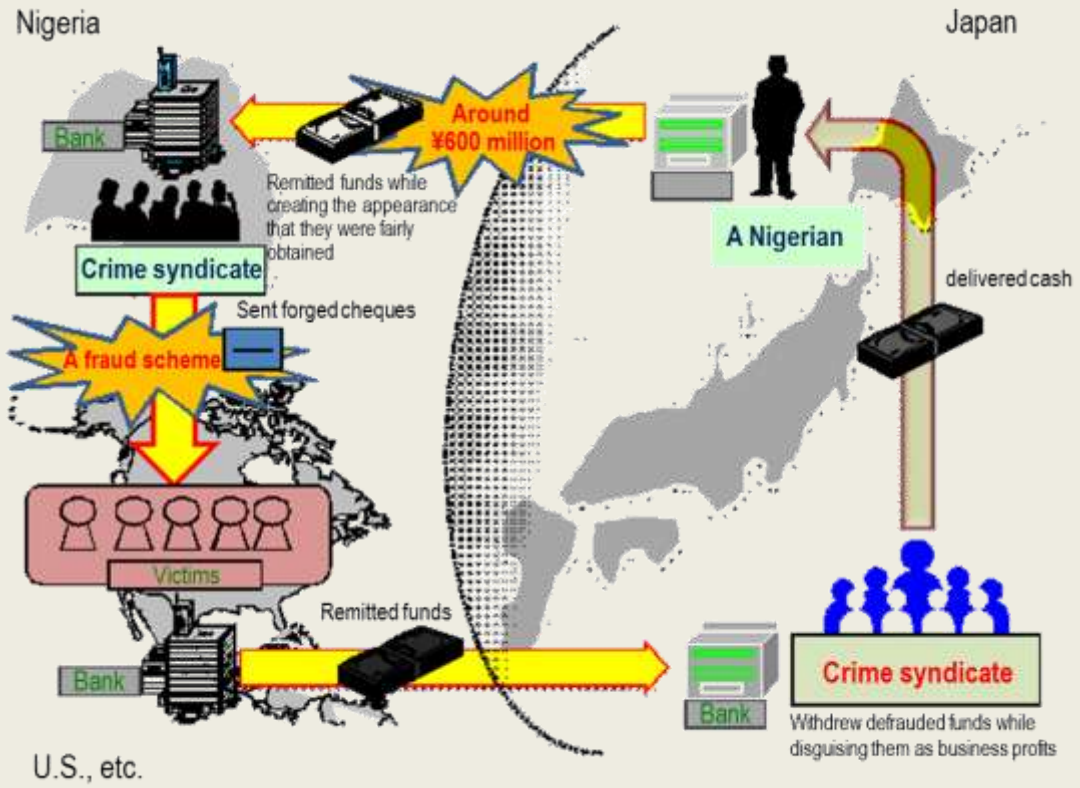
Case 1

334. A few women engaging in loan sharking had borrowers remit a total of around 225 million dollars including illegally high interest to multiple accounts opened in the names of third parties. They were arrested for the violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds, etc.).

Case 2

335. A Nigerian crime syndicate, using forged cheques in the United States, had people remit funds into accounts of Boryokudan members in Japan, submitting a false transaction sheet, pretending that the funds were legally-earned profits. The Boryokudan members and Nigerians involved were

arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds). The funds defrauded by the Nigerian crime syndicate were transferred via the Boryokudan crime syndicate to a Nigerian who was a resident in Japan and who filled the role of remitting the funds out of Japan. The Nigerian remitted a total of around 600 million dollars 45 times from Japan to Nigeria through such means as remittance from an account opened in Japan to an account at an overseas bank.

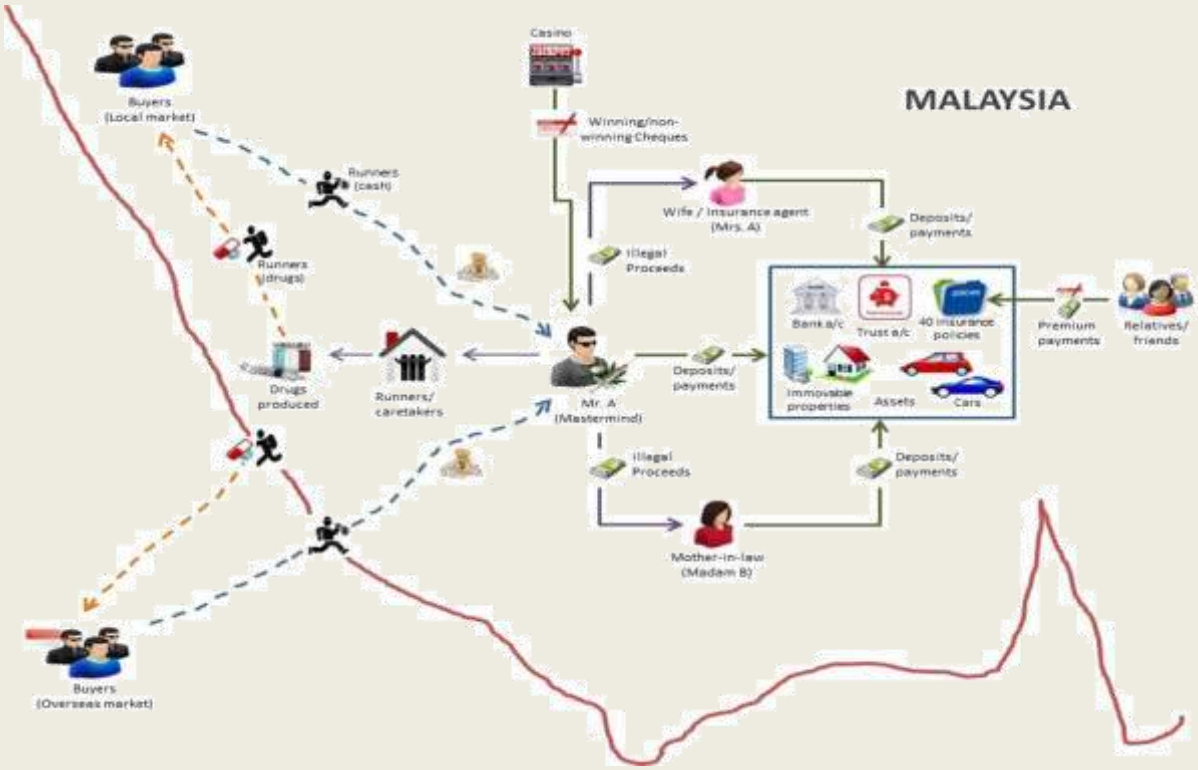


MALAYSIA

Case - Drugs Trafficking

336. Methods used:

- Use of nominees, trusts, family members or third parties etc.
- Purchase of valuable assets (properties, vehicles)
- Use of casino value instruments-cheques
- Mingling (business investment)



337. Background of subjects:

- An investigation was conducted upon the arrest of several individuals under Section 39B[5] of Dangerous Drugs Act 1952 (DDA), suspected to be related to Mr. A for their involvement in drugs trafficking activities in the southern state of Malaysia.
- Mr. A was suspected to be involved in drugs trafficking activities since 2011 which is connected to an international syndicate. The drugs were meant for local as well as overseas market. Mr. A started his activities in one of the districts in the southern state of Malaysia but he managed to evade the police search, and started drugs trafficking activities in another district, which subsequently resulted in his arrest.
- The individuals that were arrested due to possible involvement in Mr. A's drugs trafficking activities, i.e. runners/caretakers, were reported to be formerly employed as a Guest Relations Officer (GRO) while the male accomplice as a tow truck driver.
- An investigation was conducted under the Dangerous Drugs (Forfeiture of Property) Act 1988 to trace and seize properties belonging to Mr. A, the 3 individuals who were arrested, their relatives and associates.

338. Source of information:

- STR and CTR records
- Internal intelligence from Royal Malaysia Police (RMP)
- Documents recovered from the crime scene

339. Preliminary assessment & findings (modus operandi):

[5] 39B. (1) No person shall, on his own behalf or on behalf of another person, whether or not such other person is in Malaysia—
(a) traffic in a dangerous drug;
(b) offer to traffic in a dangerous drug; or
(c) do or offer to do an act preparatory to or for the purpose of trafficking in a dangerous drug.

- Mr. A and his wife (Mrs. A) were noted to be involved in several business activities. In addition, Mrs. A was also working as a part-time insurance agent, while Mr. A's mother-in-law (Madam B) is a housewife.
- To avoid detection of their activities, most of their transactions were on cash terms.
- There were no significant assets seized from Mr. A as most of the assets were owned by Mr. A's wife, mother-in-law and relatives.
- The 3 subjects maintained several bank accounts, i.e. individual, joint, business, foreign currency and fixed deposit accounts.
- As reported by an insurance company, Mr. and Mrs. A held a total of 40 insurance policies within a 4 year period. During that period, Mrs. A had also sold insurance policies to Madam B.

340. The red-flag indicators noted in this case include:

- Large cash payments were paid for the insurance policies. Payments were also made by 3rd parties such as relatives and friends into the insurance policies by way of cash and cheques.
- Some of Mr. A's insurance policies were assigned to Mrs. A.
- Monthly premium for one of the insurance policy was increased extensively by RM10,000 or 52%. It was noted that multiple withdrawals were made from the existing insurance policies. The withdrawal cheques were subsequently cancelled and the money from the withdrawals was reapplied into different existing insurance policies as premium payments. Most of the premiums were made one year in advance.
- Mr. A was also noted to be performing gambling activities in the casinos.

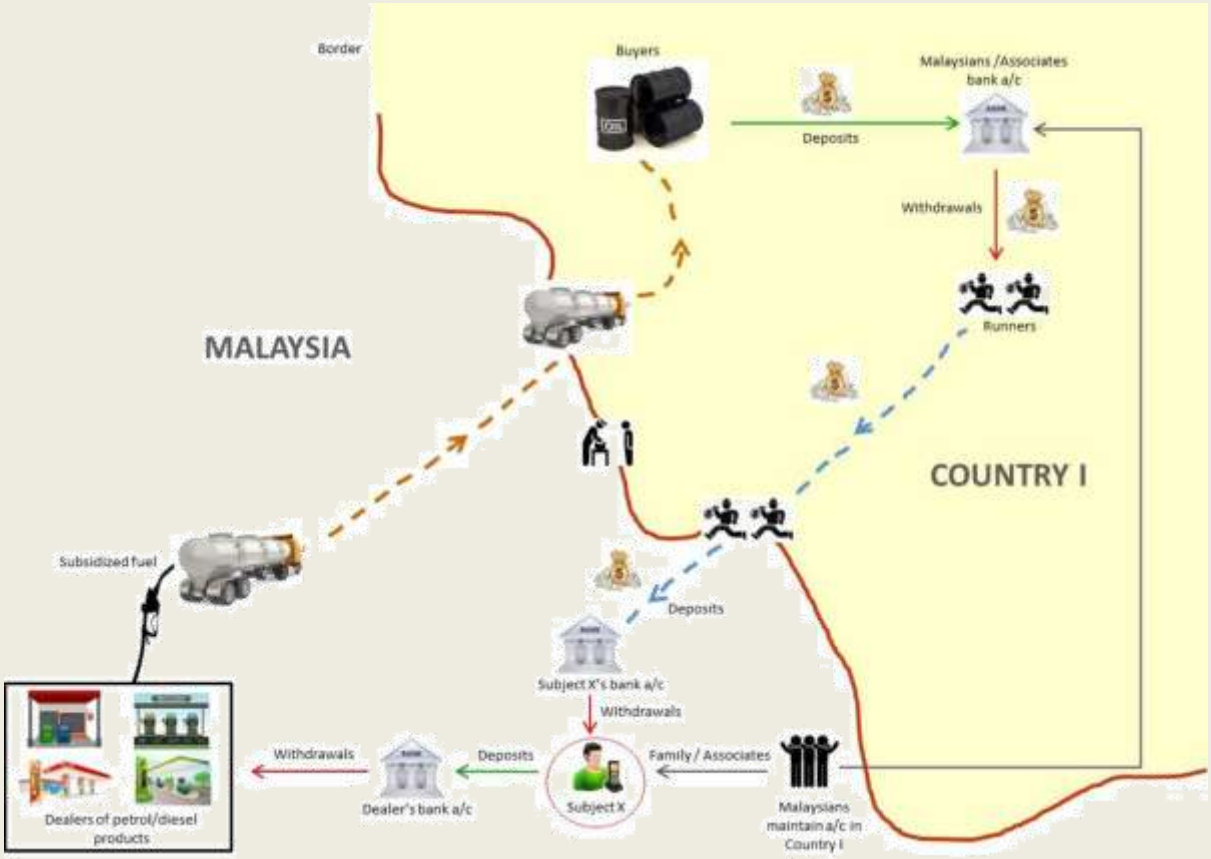
341. Actions taken to date:

- Mr. A has been charged for trafficking in dangerous drug.
- RMP managed to seize assets belonging to 5 entities related to Mr. A. Majority of the properties seized were subsequently referred to the Court under Section 32(2) Dangerous Drugs (Forfeiture of Property) Act 1988for a forfeiture order, whereby 80% of the properties including insurance premiums of their policies, funds in bank and unit trust accounts were forfeited.

<u>Case - Diesel Smuggling</u>

342. Methods Used:

- Underground banking/alternative remittance services / hawala
- Smuggling – currency and goods
- Wire transfers/Use of foreign bank accounts
- Structuring
- Use of nominees, trusts, family members or third parties etc.



343. Background of subject:

- Mr. X is a businessman residing and conducting businesses at a border town in the northern state of Malaysia. Mr. X owns several business entities which are either directly or indirectly under the name of his family members, staff and friends. These entities are involved in various businesses, including food products wholesaler and direct selling business.
- Funds were frequently deposited into bank accounts of these entities including Mr. X's individual account and were mostly cash deposits. Mr. X received multiple deposits from traders located near a border town and various other locations throughout the country. Subsequently, transfers/cash deposits were made into the accounts of several dealers of petroleum/diesel products.
- Accounts belonging to Mr. X's associates (e.g. family, friend and staff) were also active and showed similar modus operandi.

344. Source of information:

- STR and CTR records
- Sharing of intelligence from foreign FIU
- Initial surveillance from law enforcement agencies confirming the occurrence of multiple offences

345. Preliminary assessment & findings (modus operandi):

- A number of Malaysians who were suspected to be linked / associated with Mr. X had opened accounts with several banks in the neighbouring country. It is likely that these accounts were used to collect funds possibly for payments into Malaysia.

- It was suspected that the payments made were for subsidised petrol/diesel smuggled into the neighbouring country. To avoid detection of their activities, transactions performed via accounts there were properly structured and below the CTR reporting requirement.

- The funds were subsequently channelled from Mr. X's Malaysian associates' individual accounts in the neighbouring country to local individuals who are suspected to be the cash couriers, one of which owns a licensed money changing business, where our foreign counterpart had indicated possible hawala type illegal remittance business by the said local individual.

- The funds were believed to be smuggled cross-border and deposited into Mr. X and his associate's accounts at border towns in Malaysia. Funds accumulated were withdrawn in lump sum and paid mostly to dealers of petroleum/diesel products.

- Between July 2007 and July 2013, more than 6,000 deposits were received into 3 accounts belonging to Mr. X, one of which recorded more than 1,000 deposit transactions totalling more than RM30 million within 6 consecutive months in 2013.

346. Actions taken to date:

- Information in FIU's database was analysed together with the intelligence information received from foreign FIU, and subsequently disclosed to the law enforcement agencies.

- Mr. X has been charged in court for 68 counts of money laundering involving millions of ringgit as well as 7 counts of charges for running an illegal money remittance service.

Case - Tax Evasion

347. Methods used:

- Use of nominees, trusts, family members or third parties, etc.

348. The investigation showed that Mr. D acted as an agent for a birds nest business and as an agent for receiving payments and remittances on behalf third parties. Mr. D used his three personal bank accounts namely Account 1, Account 2 and Account 3 in his role as an agent. Mr. D received commission from those activities but did not declare this commission income to the IRBM. This is an offence under Section 113 of the Income Tax Act, 1967. It is also a predicate offence under the Second Schedule of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

349. To determine the amount of tax evaded, two mechanisms were used, which are the Bank Deposit Method as well as the Capital Wealth Method. The Bank Deposit Method showed that non-reporting amounted to RM 989,000, whereas, the Capital Wealth Method established an understatement of RM991,000. As the variance is only 0.2%, the Capital Wealth Method was used as it is more accurate and was supported by documents. The total amount of tax evaded was RM426,000 (with a penalty of 60% levied under Section 113(2) of Income Tax Act, 1967). Due to insufficient evidence, the case was not prosecuted under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. The case was settled as a civil settlement under the Income Tax Act 1967. The total amount of tax evaded (inclusive of penalties) of RM426,000 has been paid.

NEW ZEALAND

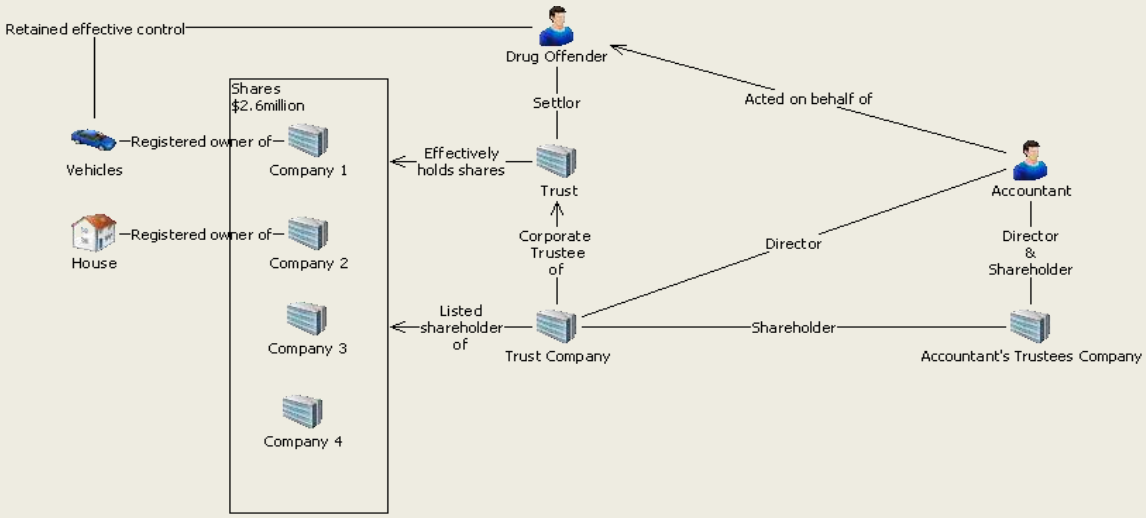
Operation Ark

350. In Operation Ark, drug offenders engaged an accountant to set up a complex structure of legal entities including a trust. This case demonstrates many of the principal ways trusts are used to launder proceeds, in particular:

- layering entities, in particular hiding the beneficial control of companies controlling assets,
- use of professional service provider to access complex structures and intermediary
- use of trust to hide criminal involvement in transactions.

351. The drug offender used the trust to buy shares in a fitness magazine business and a company with the proceeds of drug offending. Vehicles owned by the drug offender were then registered in the name of the company, ostensibly distancing the offender from ownership of the vehicles.

352. The offender also used his accountant as an intermediary and additional layer in the legal structure of his finances. Ultimately, as was the case in his layering of entities to hide ownership of the magazine and vehicles, the offender used the accountant and the trust to hide his own beneficial ownership of property. For example, the offender's house was put in the name of the name of a company whose nominee shareholder was the accountant's trust company. The accountant trust company was in turn holding the shares on behalf of the offender's trust.



SAMOA

Case 1

353. Ms KKY is a non-resident and owns an offshore company registered through one of the local trustees. Ms KKY was reported as being charged and convicted for conspiracy to defraud country H. She is now serving an imprisonment term of 17 months in country H.

Case 2

354. Mr B resides in country A and owns an offshore company registered through one of the local trustees. Mr B has been an intermediary for the trustee for quite a while. He instructed senior officers of the trustee to buy foreign currencies and sell it again. The trustee declined his request, given that; this is outside their normal business activity. The trustee reported the matter to their head office, the SFIU and the regulator of offshore companies.

THAILAND

355. A high level politician was accused of tax evasion. He created several "paper" companies to hold assets in place where he had to sell the shares before taking office. Then the company sold it back to his relatives at par value which at that time the price had gone up over 40 times. This amount was subject to tax, total of BT5.67 billion (U.S.$170,989,144). He was acquitted of a similar charge of asset transfers to his maid, driver, relatives and others to evade conflict-of-interest laws.

UNITED STATES OF AMERICA

Head of International Narcotics Trafficking and Money Laundering Organization Sentenced to 150 Years in Prison
Organization Spanned Three Continents, Distributed More Than Eight Tons of Cocaine, and Laundered More Than $14 Million in Narcotics Proceeds

U.S. Attorney's Office September 29, 2014 Southern District of Florida (313) 226-9100

Wifredo A. Ferrer, United States Attorney for the Southern District of Florida, George L. Piro, Special Agent in Charge, Federal Bureau of Investigations (FBI), Miami Field Office, and Donnell Young, Acting Special Agent in Charge, Internal Revenue Service, Criminal Investigation (IRS-CI), announce that Alvaro López Tardón, 39, of Miami Beach and Madrid, Spain, was sentenced by U.S. District Judge Joan A. Lenard to 150 years in prison. In addition to the term of imprisonment, a $14 million forfeiture money judgment and $2 million fine were entered against Tardón. Tardón was also ordered to forfeit a significant number of assets, including luxury real estate, cars and bank accounts.

After a seven-week trial, Tardón was convicted on one count of conspiracy to commit money laundering and 13 substantive counts of money laundering, in violation of Title 18, United States Code, Sections 1956 and 1957, respectively.

Tardón was the head of an international narcotics trafficking and money laundering syndicate which distributed over 7,500 kilograms of South American cocaine in Madrid and laundered over $14,000,000 in narcotics proceeds in Miami by buying high-end real estate, luxury and exotic automobiles and other high-end items. The proceeds were smuggled into Miami by couriers through Miami International Airport, wire transferred to South Florida by co-conspirators via MoneyGram and Western Union, wire transferred to third parties internationally on behalf of Tardón, and wire transferred directly to Tardón and his co-conspirators in Miami through Tardón's exotic car dealership and other companies controlled by him located in Madrid, Spain.

Following the guilty verdicts, the jury found that a significant portion of the Tardón's assets should be forfeited. Those assets involved real estate and cars. The real estate purchased by Tardón included condominium units in Miami Beach and Coconut Grove areas of Miami-Dade County. The exotic automobiles included a Bugatti Veyron and Ferrari Enzo, each worth over $1 million, a Mercedes-Benz Maybach 57S, two Mercedes-Benz G55, a Rolls Royce Ghost, and a Land Rover Range Rover. The government also seized three bank accounts.

The seven-week trial included the introduction of over 36,000 pages of financial and corporate documents from Spain and the United States. The trial also included testimony from six members of the Spanish National Police, a member of the Spanish national wiretapping agency (SITEL), and the Spanish taxing authority (Agencia Estatal de la Administración Tributaria).

The investigation and prosecution of Tardón was the result of the ongoing efforts by the Organized Crime Drug Enforcement Task Force (OCDETF), a partnership between federal, state and local law enforcement agencies to identify, investigate and prosecute high level narcotics traffickers and money launderers.

"For over a decade, Tardón oversaw a narcotics trafficking and money laundering organization that spanned three continents, distributed over 8 tons of cocaine and laundered over $14 million," said U.S. Attorney Wifredo A. Ferrer. "Today's sentencing, which includes the forfeiture of millions of dollars in assets acquired with the proceeds of the narcotics trafficking, ensures not only that Tardón will spend the rest of his life in prison, but the dismantlement of this criminal organization."

"With this term of imprisonment, rest assured Alvaro Lopez Tardon's days as an international drug kingpin are over," said George L. Piro, Special Agent in Charge, FBI Miami. "This was most

certainly a team effort with the Spanish National Police and our partners in the Organized Crime Drug Enforcement Task Force."

"Today's sentencing of Tardon is a decisive blow against the drug trafficking and money laundering network. It also sends a clear message to those who attempt to hide their ill-gotten gains through investment in real estate and cars," said Donnell Young, Acting Special Agent in Charge, IRS Criminal Investigation. "The success of this case can be attributed to the partnership of local, federal and international partners, and IRS Criminal Investigation is proud to be part of such a dedicated group of agencies who were committed to putting Tardon in prison and taking away assets he acquired from the proceeds of his illegal international organization."

Mr. Ferrer commended the investigative efforts of the FBI, IRS-CI and members of the South Florida High Intensity Drug Trafficking Area Task Force (HIDTA) for their extraordinary work in this multi-agency, multi-jurisdictional investigation. Mr. Ferrer also thanked Customs and Border Protection, Tactical Analytical Unit, Drug Enforcement Administration, Miami Police Department and Monroe County Sherriff's Office. This case was prosecuted by Assistant U.S. Attorneys Tony Gonzalez, Cristina Maxwell, Daren Grove and Evelyn B. Sheehan.

A copy of this press release may be found on the website of the United States Attorney's Office for the Southern District of Florida at www.usdoj.gov/usao/fls. Related court documents and information may be found on the website of the District Court for the Southern District of Florida at www.flsd.uscourts.gov or on http://pacer.flsd.uscourts.gov.

This content has been reproduced from its original source.

http://www.fbi.gov/miami/press-releases/2014/head-of-international-narcotics-trafficking-and-money-laundering-organization-sentenced-to-150-years-in-prison

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

AUSTRALIA

Mothballed cash stash led to drug trafficker's arrest

356. AUSTRAC intelligence assisted law enforcement with an investigation into drug trafficking. The suspect was charged with attempting to traffic a controlled drug and sentenced to two-and-a-half years' imprisonment.

357. AUSTRAC disseminated an intelligence assessment report to law enforcement regarding the financial activities of a suspect attempting to launder the proceeds of crime raised through drug-related activity. The suspect used bank and casino accounts to launder the funds.

358. The suspect was the subject of five suspicious matter reports (SMRs) submitted to AUSTRAC. Over a four-day period the suspect made five structured cash deposits of between AUD8,000 and AUD9,000 into his personal bank account. The structured cash deposits totalled AUD41,500. Bank staff reported in the SMRs that the deposited cash smelled of mothballs. After the deposits, the suspect undertook a domestic electronic transfer to move AUD40,000 from his bank account into an account with an Australian casino. The suspect deposited an additional AUD40,000 cash directly into the casino account.

359. An additional SMR submitted by the bank reported that the suspect received a deposit via domestic electronic transfer of AUD131,000 from the casino. Following this deposit into his bank account, the suspect withdrew AUD9,000 in cash.

360. The casino submitted an SMR indicating that the suspect was known by two aliases and that he would become aggressive when casino staff requested identification as part of the casino's normal

identification procedures for customers cashing out gaming chips. The casino also reported that the suspect was known to cash out chips in amounts under the AUD10,000 cash reporting threshold, presumably to avoid the requirement to present identification to staff.

361. The suspect was arrested at a domestic Australian airport after a drug detector dog reacted to his suitcase. The suitcase contained 10 vacuum-sealed plastic bags containing a total of 4.5 kilograms of cannabis. The suspect was charged with attempting to traffic a controlled drug, contrary to sections 11.1 and 302.4 of the *Criminal Code Act 1995* and was sentenced to two-and-half years' imprisonment.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Gambling services
Channel	Electronic Physical
Report type	SMR
Jurisdiction	Domestic
Designated service	Account and deposit-taking services Gambling services
Indicators	Cash has a distinct or unusual odour Customer unwilling to produce identification when requested by reporting entity staff Structuring of multiple cash deposits below AUD10,000 to avoid reporting obligations Structuring of gaming chip cash outs to avoid reporting obligations Use of false identification

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

AUSTRALIA

Welfare recipients found with $75,000 cash and 15 kilograms of cannabis

362. AUSTRAC information helped initiate an investigation that resulted in the arrest of three suspects and the seizure of approximately 15 kilograms of cannabis. Authorities restrained a number of assets, including AUD100,000 in cash suspected to be the proceeds of crime, a property and numerous vehicles.

363. One suspect was sentenced to four years and 10 months imprisonment. The other suspect received a suspended sentence of two years and nine months imprisonment.

364. Information held by authorities indicated that a woman (suspect A) and husband (suspect B) had accumulated substantial assets, which was inconsistent with their declared income.

365. Additionally, a credit union submitted a suspicious matter report (SMR) detailing the financial activities of the suspects. AUSTRAC forwarded the SMR to authorities, which detailed the following:

- suspects A and B held a joint account with the reporting entity

- suspect A telephoned the credit union and indicated that she wanted to withdraw AUD15,000 cash from her personal account
- credit union staff advised the suspect that withdrawing AUD15,000 cash required the completion of a significant cash transaction report (SCTR)
- over two consecutive days, suspect A attended the credit union branch and withdrew AUD9,800 and AUD5,200 respectively.

366. The cash withdrawals totalled AUD15,000 and appeared to be 'structured' into two separate transactions to avoid the SCTR requirement. Subsequent investigation of the account activity by social welfare investigators identified that:

- suspects A and B received government welfare payments
- a large number of transactions were made at a casino
- the account received large cheque deposits.

367. Analysis of AUSTRAC information identified additional SMRs submitted by a credit union. The SMRs included the following information:

- suspect A was a signatory to a credit union account held in a relative's name
- suspect A periodically deposited cash into the relative's account. Over a one-month period the relative's account received four cash deposits totalling AUD20,000 structured into amounts ranging from AUD2,000 to AUD9,000
- suspect A attended a branch of the credit union with her relative and they deposited AUD9,000 and AUD6,000 cash respectively into their personal accounts, at different counters
- credit union staff observed that the relative appeared 'nervous' while conducting cash deposits
- a cheque for AUD50,000 was withdrawn by the relative from his account to purchase a motor vehicle.

368. Enquiries conducted by authorities identified that:

- over a six-year period approximately AUD1.37 million was deposited into the accounts of suspects A and B
- the suspects purchased numerous assets including a house, two motor vehicles and three motorcycles
- suspect B frequently travelled overseas.

369. Analysis of AUSTRAC information showed that in the same year the SMRs were reported to AUSTRAC, suspect B completed an international currency transfer report (ICTR), which indicated he was carrying cash worth approximately AUD16,000 when he departed Australia for the Philippines.

370. Enquiries showed that suspects A and B's income did not support their lifestyle. The SMRs, combined with information held by authorities, prompted law enforcement to investigate the suspects' unexplained wealth.

371. Further law enforcement investigations revealed that suspects A and B had obtained approximately 15 kilograms of cannabis and were arranging for a courier (suspect C) to transport the cannabis interstate.

372. Law enforcement officers intercepted a motor vehicle and found the cannabis concealed in the side panels of the vehicle. Suspect C was arrested and charged with possessing cannabis for sale or supply.

373. A search warrant was executed at suspect A and B's home. Authorities seized approximately AUD75,000 cash, numerous receipts for goods worth AUD400,000 purchased using cash, and various documents that indicated suspects A and B were trafficking in cannabis. Suspects A and B were arrested.

374. Suspect A pleaded guilty to:

- aiding, abetting or procuring another to traffic in a substance that is a controlled drug under the Criminal Code Act 1995
- jointly possessing approximately AUD75,000 being the proceeds of crime under the Criminal Code Act
- jointly dealing with approximately AUD330,000 being the proceeds of crime under the Criminal Code Act
- possessing a motor vehicle being the proceeds of crime under the Criminal Code Act.

375. Suspect A was sentenced to four years and 10 months imprisonment.

376. Suspect B died and court proceedings against him were discontinued.

377. Suspect C pleaded guilty to possessing cannabis for sale or supply and received a suspended sentence of two years and nine months imprisonment.

378. Law enforcement restrained a house, two motor vehicles, three motorcycles, approximately AUD75,000 in cash and AUD25,000 in a bank account.

379. The social welfare investigation revealed both suspect A and B had each accumulated debts of AUD69,944.45 for welfare payments they were not entitled to.

Offence	Drug trafficking Money laundering Welfare fraud
Customer	Individual
Industry	Banking (ADIs)
Channel	Physical
Report type	ICTR SMR
Jurisdiction	Domestic and international – Philippines
Designated service	Account and deposit-taking services
Indicators	Account activity inconsistent with customer profile Customer and relative(s) attend the same branch and make structured cash deposits into their own accounts at the same time Customer is a signatory to a relative's account and makes large cash deposits to the account High-value cash deposits Regular or multiple deposits below the AUD10,000 reporting threshold

(that is, structured cash deposits)

Third-party or relative appears to be nervous while conducting transactions

FIJI

380. A Suspicious Transaction Report was flagged to the Fiji FIU by a local company on possible involvement in fraud, theft, embezzlement activities by 11 of its employees.

381. It was alleged by the local company that the employees had colluded, stole and sold products of the company for their personal gain without the authorization of the company.

382. The Fiji FIU conducted checks on the employees' assets, financial and credit history. Fiji FIU established that the head cashier, Person X, had purchased a vehicle in April 2014 and another vehicle in 2013. There was no evidence according to the analysis of the head cashier's bank statements that he had the funds to finance the motor vehicle purchases. I in addition to these motor vehicles, he also owned two properties. Deposits made to Person X's personal bank account between 2013 and 2014 exceeded FJ$1000 but his income showed that his annual salary was FJ$10 000. There was no recent disposal of any of his motor vehicles and assets thus the deposits in his account could not be justified and were suspicious.

383. The father of Person X also owned two motor vehicles; a third motor vehicle which had a public service registration had been disposed of.

INDONESIA

384. In March 2013, Mr. F, a narcotics dealer, was arrested by the National Narcotics Agency. From the investigations, Mr. F had conducted his business since 2004. He accumulated USD4 million from his crimes. He mostly used other parties' names for his assets, which were spread around Malaysia, Aceh, and Jakarta. He purchased 3 units of luxurious cars, 1 gas station, 4 shophouses, a piece of land, 1 hotel, bank account with the value of USD1 million, and 22 building ownership certificates using Mr. F's name. Mr. F was evicted to 10 years in prison and USD200,000 in fines.

SRI LANKA

385. On 05/11/2013, the Sri Lanka Customs Unit at Katunayake International Air Port arrested a Liberian national with 30 kilograms of heroin based on information received from the Police Narcotic Bureau. Upon the investigation of individuals related to the Liberian national (his telephone records), it was revealed that a Sri Lankan national Mr. X is directly involved with the Liberian national in a large drug trafficking scheme and owned an unexplainable amount of wealth in movable and immovable properties. Further, the Narcotic Bureau arrested several other individuals with drugs in their possession, who were identified as associates of Mr. X. Based on the information available, the Narcotic Bureau commenced investigations on the offence of drug trafficking relating to all individuals identified.

386. The case was referred to the Criminal Investigations Division (CID) to conduct investigations relating to the money laundering aspect as well. At the search of the residence of Mr. X, the investigation team found a copy of document extracts relating to land of a third party which was taken for clearance checking. Thereafter, the records of that land were examined at the Land Registry and it was found out that Mr. X has later purchased the land. Then, all the land registered under Mr. X's surname/family name were searched and it was revealed that he had purchased two parcels of land under his name, five parcels of land under his relatives names, two parcels of land under his wife's name and six parcels of land under a private limited company where Mr. X is the Managing Director of that company. Suspension orders were issued preventing selling or transferring the properties under the Criminal Procedure Code Act No. 15 of 1979. The total value of the immovable properties

identified so far is around LKR 5 Billion. However, it has been revealed that there are more properties belonging to Mr. X which are currently owned by his associates who are yet to be traced.

387. In addition, the CID has traced most of vehicles registered to Mr. X, his relatives and his company's names. A suspension order was issued to the Commissioner General of Department of Motor Traffic to prevent selling or transferring the vehicles to any third party. Following are the list of vehicles traced so far. However the values of the movable properties were not yet estimated.

i. Two Jeeps
ii. Two Lorries
iii. Three vans
iv. Five motor cars
v. One bus
vi. Two Lorries

388. Further, the individuals who were identified as parties involved in this drug scheme (his wife, sister in law etc.), suspension orders were issued to suspend all banking transactions under the Sec. 15 (2) of the Financial Transactions Reporting Act No 06 of 2006 and under the Sec. 66 (1) and 124 of Criminal Procedure Code Act No. 15 of 1979.

389. The CID is still continuing their investigations to trace properties belongings to Mr. X and his associates/relatives.

4.18 Investment in capital markets, use of brokers

MACAO, CHINA

390. The bank accounts of 6 shell companies sharing the same address were opened and they received wire transfers of millions of dollars from 15 companies overseas. Upon receipt of theses wire transfers, these shell companies issued cashier's orders to company T.

391. Further analysis revealed that the funds received by the shell companies through wire transfers was finally deposited into company T's accounts were then passed to Mr. A as cash for depositing into Mr. X and Ms. Y's accounts. A, X and Y are employees of company T. Upon receiving the deposits, Mr. A, X and Ms. Y immediately purchased the shares of company F, a 3rd-tier listed company. It was found that the major shareholder of listed company F was controlled by company G. The purchase of shares by Mr. A, X and Ms. Y manipulated the share price of F to a higher level, so as to facilitate the subsequent share repurchase program in favour of company G without getting the attention of the stock exchange supervisor. The case was submitted to the Public Prosecutions Office for further investigation.

4.19 Mingling (business investment)

MALAYSIA

<u>Fraud</u>

392. Method used:

- Mingling (Business Investment)

393. Mr. G 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 an investment return. In addition, all the investors were required to pay substantial amount of member fees to the company annually.

394. Initially, the investment scheme was carried out in accordance to the law. However, as the number of members grew, Mr. G and his team could not obtain sufficient optional-properties to meet the demand of the increasing numbers of investors. Mr. G 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 with 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 investment multiplying tremendously.

395. Eventually, the monies that the investors invested were then partially paid as return to the other investors but the majority of it was siphoned out by Mr. G. The investigation revealed that the investment scheme had lured a total of 500 investors who suffered losses of RM250 million. A money laundering investigation was also carried out in parallel with the predicate offence investigation under section 420 Penal Code in relation to cheating.

396. The investigation subsequently managed to trace of 288 properties around the country purchased from the ill-gotten gain obtained via investors. Following tracing of the properties which registered mainly under proxies and suspects, the Royal Malaysia Police (RMP) issued an order to freeze and thereafter, seizure under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

397. Despite the absconded suspect in this case, RMP decided to pursue the case under section 56 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001. The properties and several bank accounts worth RM26 million belonging to the suspect and his family was subsequently forfeited and returned to bona fide third parties to compensate the partial losses suffered by the victims.

NEW ZEALAND

Operation Ark

398. Christopher Chase and Lee Vincent, a New Zealand citizen resident in Thailand, jointly owned a New Zealand 'legal high' business. In addition to selling unrestricted party drugs, the business was used as a front for distribution of illicit drugs. Money generated by both the licit and illicit activity was mingled and the cash generated by these businesses was taken on a regular basis to Vincent's mother's home for temporary storage. The cash was packed into boxes, generally in the form of bundles of $20 and $50 notes. The boxes were then picked up by couriers, who transported the cash to Hong Kong where it was deposited in the bank accounts of three companies beneficially owned by Vincent. Bank statements for these Hong Kong accounts were sent to Vincent's mother's address in New Zealand. The money laundering process was completed by loans made by one of the Hong Kong companies to another New Zealand company. Chase controlled a trust that was a 50 per cent shareholder in the New Zealand company. A small portion of the cash, around $184,000, was retained by Vincent's mother for her own purposes.

399. Court proceedings are ongoing and to date around NZD23 million has been restrained.

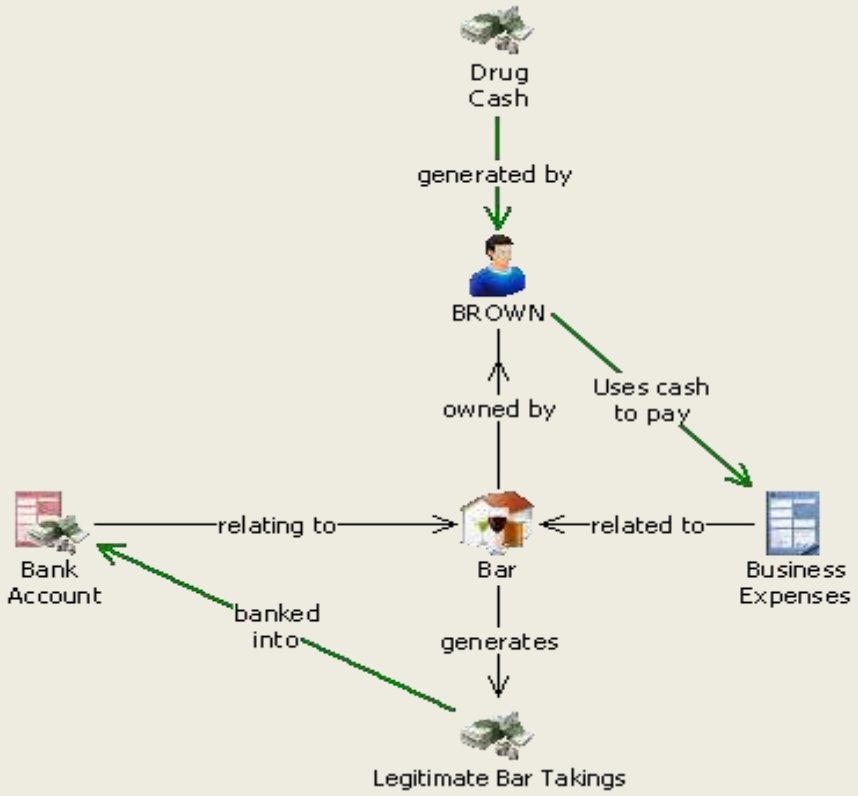
Operation Keyboard

400. A bar was used to mingle cash proceeds in the Operation Keyboard case:

- drinks are often purchased in cash, in multiple small untraceable and easily forged transactions; and
- takings may be variable providing an opportunity to explain unusual cash deposits.

401. In Operation Keyboard, a central figure of a drug supply ring used a central Auckland bar to co-mingle the proceeds of drug sales. Ron Brown's declared source of income was an unemployment and later sickness benefit. However, in 2007, Brown was able to purchase the K' Rd Pool Bar & Lounge.

402. While the business was run at a loss, the bar was an effective mechanism for Brown to place the proceeds of his drug offending without having to deposit cash from drug sales at financial institutions. Placement was achieved by paying business expenses with drug cash and banking the bar takings as per a legitimate bar in the business account that Brown maintained beneficial ownership of. This relatively simple mechanism allowed Brown to effectively swap the drug cash for the ostensibly clean bar takings.



Abuse Of Road Contracting And Forestry Businesses (Currently Before Courts)

403. In 2013 the High Court restrained around $1.8 million worth of assets related to a drug supply network connected to a roading contractor. Court proceedings are ongoing and no indication of settlement and no resolution date has been set.

404. The Crown alleges that the principle offender and a number of associates were involved in a national drug supply network that used the roading contractor's roading and forestry businesses to facilitate offending. The businesses provided ideal fronts for drug distribution and/or manufacture, providing the principle offender with a reason for local and domestic travel required for drug related transactions. While Police is aware of extensive movement ostensibly related to these businesses, Police has not been able to substantiate corresponding legitimate business activity.

405. The offenders also appear to have used these companies to co-mingle the proceeds of the offending. Such businesses provide an opportunity to explain the illicit earnings from drug supply. The principle offender ensured that his businesses maintained good records of apparent earnings by using professional accountants. In addition to facilitation of predicate offending, the nationally dispersed business interests also would have provided an opportunity to select professional service providers which may have allowed the offenders to select professionals who would be unable to detect illicit activity. These types of arrangements could also allow criminals to seek remote professional services and/or to change professional service providers so as to prevent professionals gaining a full appreciation of any unusual business activity.

406. In this case, maintaining professionally facilitated business records and declaring earnings for tax helped the offenders to maintain an air of legitimacy.

407. Using such businesses as fronts for criminal activity may also make law enforcement investigation to establish illicit earnings more complex. However, despite the extensive and well documented earnings, corresponding legitimate business has not been established giving a strong indication that the illegitimate earnings from drug supply were co-mingled with whatever legitimate earnings the businesses made.

Operation Acacia

408. A methamphetamine manufacturer operated a business buying and selling building materials supplied from demolitions.

409. Police financial analysis of the business accounts showed that approximately $150,000 cash had been deposited over a five and a half year period. Over half of the cash deposits were banked in 2008 and 2009; a period where the business declared it was making a loss and where evidence showed the offender was manufacturing methamphetamine. It is therefore likely that some of the cash was the proceeds of drug sales as this level of legitimate deposits would have been sufficient to nullify the loss. In addition, the offender did not declare all the cash deposits as income for tax purposes.

410. Later, in the civil criminal-proceeds case, the offender argued that the cash deposits were the proceeds of legitimate business sale; however, he could not substantiate this because he did not keep proper business records. The offender's business, therefore, created the ideal opportunity to launder drug proceeds because it was a cash business and he could disguise the drug cash as legitimate income.

411. Partial payments were made from the business account towards personal bonus bonds, a marina berth and property thus converting the criminal proceeds into assets and completing the money laundering process. Cash withdrawals were also made from the business account, potentially to conduct further illicit transactions without an audit trail.

412. Outcome: The offender was sentenced to 17 years prison for the manufacture and supply of methamphetamine. His residential home, rural land, cars, a digger, a marina berth and bank accounts were forfeited to the crown in order to repatriate an estimated $1.6million that he earned from selling methamphetamine.

4.20 Use of shell companies/corporations

CHINESE TAIPEI

413. Mr. L is the former Senior Vice Director General of HH Technology Group, a famous international technology corporation, and the vice chairperson of the Committee of Surface Mount Technology (SMT) under the Group. SMT Committee is in charge of making decisions for all business procurements. It is alleged that Mr. L and other members of SMT Committee took advantage of their duty in the Committee to collect kickbacks from the suppliers of HH for a long time.

414. In order to qualify as a supplier for the Group, the suppliers reportedly had to pay 2.5% of procurement values as kickbacks and then pay an additional commission to secure orders. After Mr. L's retirement in 2011, the rate of kickbacks was increased even further to 3% and the extra 0.5% was charged by Mr. L. Mr. L set up shell companies and opened bank accounts abroad as places where the bribes were placed and then transferred the kickbacks back to Chinese Taipei. After the investigation, the Taipei District Prosecutors Office timely seized the funds in Mr. L's and other members' accounts. The AMLD received the information from foreign counterparts regarding the abnormal overseas financial activities of Mr. L and other suspects, and the information was disseminated to the prosecutor's office for further investigation. The amount of seized funds of this

case has reached NT$41 million up to now. The Taipei District Prosecutors Office charged Mr. L and other committee members with breach of trust in May 2014.

INDONESIA

415. Mr. DW and Mr. HI was Directorate General of Tax officials. In 2012, firstly they placed the proceeds of their crime in mutual funds. They also bought land, properties, precious metals, and placed the money in a bank account. They created a shell company (X Company) to launder money. They purchased cars from their proceeds of crime and made it as if the cars were for sale by X Company.

JAPAN

Case 1

416. The offender, a loan shark, lent money to debtors, pretending it was for payment of a purchase.

417. The offender had the debtors transfer money, including illicit interest, between the debtors and a shell company the offender had set up, in instalments to a bank account opened under the name of the shell company. The offender pretended, using false order forms for commodities, that a fictitious wholesale company sold commodities to the shell company and had the shell company transfer around 49.4 million JPY from its bank account to a bank account opened under the name of the wholesale company, and then had the wholesale company transfer the same amount to the offender's bank account.

418. The offender was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceed)

Case 2

419. The offenders subscribed to shares issued in the incorporation of a stock company by paying around USD10,000, which was a part of around USD3,000,000 they swindled through a fraudulent investment fund. They then obtained status as directors-at-incorporation, and one of the offenders, having other directors-at-incorporation exercise the power of directors-at-incorporation, elected himself as a representative director-at-incorporation. The offender (representative director-at-incorporation), in conspiracy with other directors-at-incorporation, carried out the registration of the incorporation, formed a stock company and then elected himself the representative director of the stock company. They were arrested for violating the Act on Punishment of Organized Crimes (management control through illicit proceeds).

SINGAPORE

420. Jay Alan Thierens (Jay), a UK national, incorporated Fairwind Pte Ltd in Singapore through a corporate service provider and opened bank accounts in Singapore in the name of Fairwind. Investigations revealed that an account of Fairwind received money from victims of investment scams. The victims, residing in various jurisdictions, received cold calls from an individual, purporting to offer exclusive pre-initial-public offering shares of foreign companies with the promise of attractive returns. They then received invoices via email with instructions to remit funds to various overseas bank accounts, including the said account of Fairwind in Singapore.

421. The funds deposited by the victims into Fairwind's account were remitted overseas soon after they were received. From June to September 2011, Fairwind's account received more than EUR400,000 while more than EUR350,000 was remitted out of the same account during the same period. These transactions were not consistent with Fairwind's registered business activity of building and repairing pleasure crafts, lighters and boats, and general wholesale trade.

422. As this case involved various countries, the Police collaborated closely with its foreign counterparts to exchange information, which was very useful in furthering the investigation.

423. Jay was convicted of criminal offences and sentenced to a total of 15 months' imprisonment.

UNITED STATES OF AMERICA

Six Corporate Executives and Six Corporate Entities Indicted for Orchestrating a $500 Million Offshore Asset Protection, Securities Fraud, and Money Laundering Scheme
Defendants Created Three Brokerage Firms in Belize to Assist U.S. Citizens in Fraudulent Manipulation Schemes of Publicly Traded Companies, Including Cannabis-Rx Inc. (CANA)

U.S. Attorney's Office September 09, 2014 Eastern District of New York(718) 254-7000

A multi-count indictment was unsealed this morning in federal court in Brooklyn, New York, against six individual defendants: Robert Bandfield, a U.S. citizen; Andrew Godfrey, a citizen of Belize; Kelvin Leach, a citizen of the Bahamas; Rohn Knowles, a citizen of the Bahamas; Brian De Wit, a citizen of Canada; and Cem Can, a citizen of Canada; and six corporate defendants: IPC Management Services, LLC; IPC Corporate Services Inc.; IPC Corporate Services LLC (collectively, IPC Corp); Titan International Securities, Inc. (Titan); Legacy Global Markets S.A. (Legacy); and Unicorn International Securities LLC (Unicorn).1 The charges include conspiracy to commit securities fraud, tax fraud, and money laundering. Bandfield's initial appearance for removal proceedings to the Eastern District of New York is scheduled for tomorrow at the Wilkie D. Ferguson Jr. United States Courthouse, 400 North Miami Avenue, Miami, Florida. The government will seek extradition for the other individual defendants.

The indictment was announced by Loretta E. Lynch, United States Attorney for the Eastern District of New York; George Venizelos, Assistant Director-in-Charge, Federal Bureau of Investigation, New York Field Office (FBI); Shantelle P. Kitchen, Acting Special Agent-in-Charge, United States Internal Revenue Service, Criminal Investigation, New York (IRS-CI); and James T. Hayes, Jr., Special Agent-in-Charge, U.S. Immigration and Customs Enforcement (ICE), Homeland Security Investigations (HSI), New York.

"As alleged, Bandfield and his co-conspirators devised not only a fraudulent scheme but an elaborate corporate structure based on lies and deceit designed to enable U.S. citizens to evade and circumvent our securities and tax laws. They set up sham companies with figureheads at the helm in an attempt to deceive U.S. law enforcement and regulators and bragged about their scheme to their clients," stated United States Attorney Lynch. "Today's sweeping indictment, charging the individuals and companies responsible for this $500 million scheme, closes this fraudulent offshore safe haven and sends a strong message to those who seek to abuse the financial markets in order to enrich themselves that we will investigate and prosecute them no matter where they set up shop." Ms. Lynch expressed her grateful appreciation to the United States Securities and Exchange Commission for its significant cooperation and assistance in the investigation.

"As alleged, the defendants concocted an intricate scheme using sham companies to make money while repeatedly evading and violating U.S. securities and tax laws. The indictment of these defendants should serve as a stern reminder that such greed-based behavior comes at a cost. The FBI will continue to use its investigative expertise in working with law enforcement partners to identify, disrupt, and dismantle sophisticated fraud schemes to ensure the integrity and transparency of our financial markets," stated FBI Assistant Director-in-Charge Venizelos.

"The investigation of offshore tax evasion and money laundering are top priorities for IRS-Criminal Investigation, and we are committed to using all of our enforcement tools to stop this abuse. The enactment of the Foreign Account Tax Compliance Act (FATCA) is yet another example of how it is becoming more and more risky for U.S. taxpayers to hide their money globally. Moreover, this partnership of IRS-CI, the FBI, HSI, and the U.S. Attorney's Office demonstrates the government's resolve to combat international crime," stated IRS-CI Acting Special Agent-in-Charge Kitchen.

"Today's arrests and charges disrupt an illicit offshore operation that was allegedly laundering money for corrupt clients and cheating the U.S. government out of half a billion dollars in tax revenue," said HSI New York Special Agent-in-Charge Hayes. "The collaboration between HSI and its federal law enforcement partners serves as an example of law enforcement's global reach to dismantle criminal organizations."

As alleged in the indictment, between January 2009 and September 2014, this group of conspirators, masquerading as financial professionals, concocted three interrelated schemes to: (a) defraud new investors in various U.S. publicly traded companies through, among other things, fraudulent concealment of the defendants' corrupt clients' ownership interests in the U.S. publicly traded companies and their fraudulent manipulation of artificial price movements and trading volume in the stocks of those companies; (b) aid the corrupt clients to circumvent the IRS's reporting requirements under, among other statutes, the Foreign Account Tax Compliance Act (FATCA); and (c) launder money for the corrupt clients through financial transactions to and from the United States involving proceeds of fraud in the sale of securities. As part of this fraudulent offshore scheme, the defendants laundered approximately $500 million for the corrupt clients—who included more than 100 U.S. citizens and residents.

To facilitate these interrelated schemes, the defendants created shell companies in Belize and Nevis, West Indies, for the corrupt clients and placed nominees at the helm of these companies. This structure was designed to conceal the corrupt clients' ownership interest in the stock of U.S. public companies, in violation of U.S. securities laws, and enable the corrupt investors to engage in trading under the nominee's names through brokerage firms also set up in Belize. For example, this structure enabled the defendant De Wit and a U.S. corrupt client to manipulate the stock of Cannabis-Rx, Inc., a microcap or penny stock company which traded under the ticker symbol CANA, through a series of orchestrated transactions between March 27, 2014 and April 16, 2014. On March 28, 2014 alone, De Wit received at least five telephone calls from the corrupt client with specific instructions to fraudulently orchestrate the trading of CANA's stock. That day, CANA's stock, which had not traded since July 2, 2013, had a trading volume of 189,800 shares. Ultimately, CANA's stock price plummeted from $13.77 per share on March 27, 2014 to $0.50 per share on April 16, 2014.

The defendants' scheme also enabled the U.S. corrupt clients evade reporting requirements to the IRS by concealing the proceeds generated by the manipulated stock transactions through the shell companies and their nominees. For example, in response to a request received by a U.S. corrupt client from a U.S. transfer agent who had to determine whether the proceeds from manipulative stock trading transaction were taxable under U.S. law, the defendant Bandfield forwarded an IRS Form signed by co-defendant Godfrey as the nominee for the shell company which had been set up at the request of the client. At one point during the government's investigation, Bandfield boasted to an undercover law enforcement agent that he had specifically designed this "slick" corporate structure to counter President Barack Obama's new laws, a reference to FATCA.

An example of how the defendants' scheme enabled U.S. corrupt clients to launder the proceeds from their fraudulent trading in U.S. public companies was the production of unidentifiable debit cards for the clients allowing them to freely transfer their proceeds back into the United States.

The government's case is being prosecuted by Assistant United States Attorneys Jacquelyn M. Kasulis, Winston M. Paes, and Brian D. Morris.

Today's announcement is part of efforts underway by President Obama's Financial Fraud Enforcement Task Force (FFETF) which was created in November 2009 to wage an aggressive, coordinated and proactive effort to investigate and prosecute financial crimes. With more than 20 federal agencies, 94 U.S. attorneys' offices, and state and local partners, it is the broadest coalition of law enforcement, investigatory, and regulatory agencies ever assembled to combat fraud. Since its formation, the task force has made great strides in facilitating increased investigation and prosecution of financial crimes; enhancing coordination and cooperation among federal, state, and local

authorities; addressing discrimination in the lending and financial markets; and conducting outreach to the public, victims, financial institutions and other organizations. Over the past three fiscal years, the Justice Department has filed more than 10,000 financial fraud cases against nearly 15,000 defendants. For more information on the task force, visit www.stopfraud.gov.

This content has been reproduced from its original source.

http://www.fbi.gov/newyork/press-releases/2014/six-corporate-executives-and-six-corporate-entities-indicted-for-orchestrating-a-500-million-offshore-asset-protection-securities-fraud-and-money-laundering-scheme

4.21 Financing the proliferation of weapons of mass destruction (WMD)

424. No cases submitted

4.22 Association with illegal logging

425. No cases submitted

4.23 Currency exchanges/cash conversion

CHINESE TAIPEI

426. Ms. Z established a radical religious group. In May 2013, Ms. Z considered Ms. H's son as misbehaving. Ms. Z assembled her followers, Ms. H and other members, to question the child, assaulted and battered him, and then took him into custody for more than 10 days. Eventually, multiple blunt knife wounds, rhabdomyolysis, and acute tubular necrosis resulting in multiple organ dysfunction syndromes found on the child's body that caused his death.

427. On December 6, 2013, the media disclosed the above information but the chairperson of the religious group, Ms. Z, denied that the group was involved when she was interrogated by the public prosecutor. The AMLD received an STR from one bank on the same day when this news was disclosed. The STR indicated that Ms. Z's account received several inward remittances from other banks on November 27, 2013, and Ms. Z terminated her Certificates of Deposits prematurely and immediately withdrew about NTD10 million in cash. Besides this, Ms. Z sold USD from her foreign currency saving account and withdrew about NTD1.7 million in cash. The clerk of the bank questioned Ms. Z about the purpose of these transactions, but she refused to explain. The bank evaluated Ms. Z's financial transactions were suspicious and then filed the STR to the AMLD.

428. After receiving this STR, the AMLD initiated analysis procedures and found that the purposes that Ms. Z withdrew her accounts in cash were very possible for concealing the funds that might be seized and confiscated for civil compensation in the future. The AMLD determined to immediately disseminate the information to the Changhua District Prosecutors Office, which was in charge of this case, for further reference. Considering that Ms. Z continuously withdrew huge amounts of cash, the Changhua District Prosecutors Office strongly suspected Ms. Z might intend to abscond so that the Prosecutors Office requested the court to detain her. In December 2013, the Changhua District Court decided a detention ruling and held incommunicado. In January 2013, Ms. Z et al were indicted for committing the offence of causing injury resulting in death. The public prosecutor specifically indicated in the indictment that the defendant Ms. Z might abscond due to the fact that she withdrew the huge amounts of cash from her own accounts shortly before the case was disclosed.

INDONESIA

429. Mr. X was the head of Y Agency, an agency that manages the trading contracts of oil and gas in Indonesia. Mr. X was bribed by Mr. Y, Mr. Z, and Ms. A, Directors of Company B, Company C, and Company D, respectively, in order for him to manipulate oil and gas contracts. Among other methods, Mr. X ordered his golf trainer Mr. E (also an accomplice in his crime) to buy a luxurious

car, whose down payment was paid with money exchanged from USD (USD 50 thousands). He also ordered Mr. E to buy house using exchanged currency from SGD. In total, Mr. X exchanged foreign currency amounting to USD 298,900.

JAPAN

430. An unemployed man murdered a woman and robbed her of around HKD 1,400,000 in cash in the Special Administrative Region of Macau, and had an acquaintance who didn't know the circumstances of the matter exchange around HKD 140,000 which was a part of what the offender had robbed her of into Japanese currency at a financial institution in Japan in the name of the said acquaintance. The offender was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

4.24 Currency smuggling (including issues of concealment and security)

FIJI

431. A foreigner, Person X, was offloaded from an international flight for a body search by Fiji Customs. It was revealed that Person X had concealed the following foreign currencies in his shoes packed in his check-in luggage: AU$2,110, CA$1,175, £485, NZ$1,510 and €2,150.

432. Profiling of Person X established that an anonymous complaint was received on Person X alleging that he was smuggling currency to his overseas bank accounts. Investigations are continuing.

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

AUSTRALIA

Crime syndicate recruited Malaysian nationals for major credit card fraud

433. AUSTRAC information was used to verify the identities of an organised crime syndicate undertaking credit card fraud. A number of suspicious matter reports also assisted authorities to unravel the group's illicit financial activities.

434. Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment and the other to 12 months imprisonment.

435. A Melbourne-based Asian organised crime syndicate operated a company arranging for overseas students to migrate to Australia. This company was also used to facilitate a credit card shopping fraud scheme. The syndicate recruited Malaysian nationals with significant gambling debts to assist in fraudulently purchasing high-value portable goods which could be resold easily.

436. The syndicate used false identity documents to create fake identities for the recruits. These documents were either fraudulently produced or were genuine documents obtained in false names. The false identities were used to obtain legitimate identity documents – for example, drivers' licences – which were then used to set up bank accounts and apply for bank loans.

437. The syndicate provided the recruits with fraudulently obtained items such as credit cards. The recruits were then taken to several shopping centres around Australia to purchase portable high-value goods such as laptops, navigation devices, personal music devices, jewellery, department store gift cards and premium alcohol. The recruits provided the goods to the syndicate who on-sold the items to unwitting third parties for cash. The recruits were given a portion of the proceeds to pay off personal gambling debts.

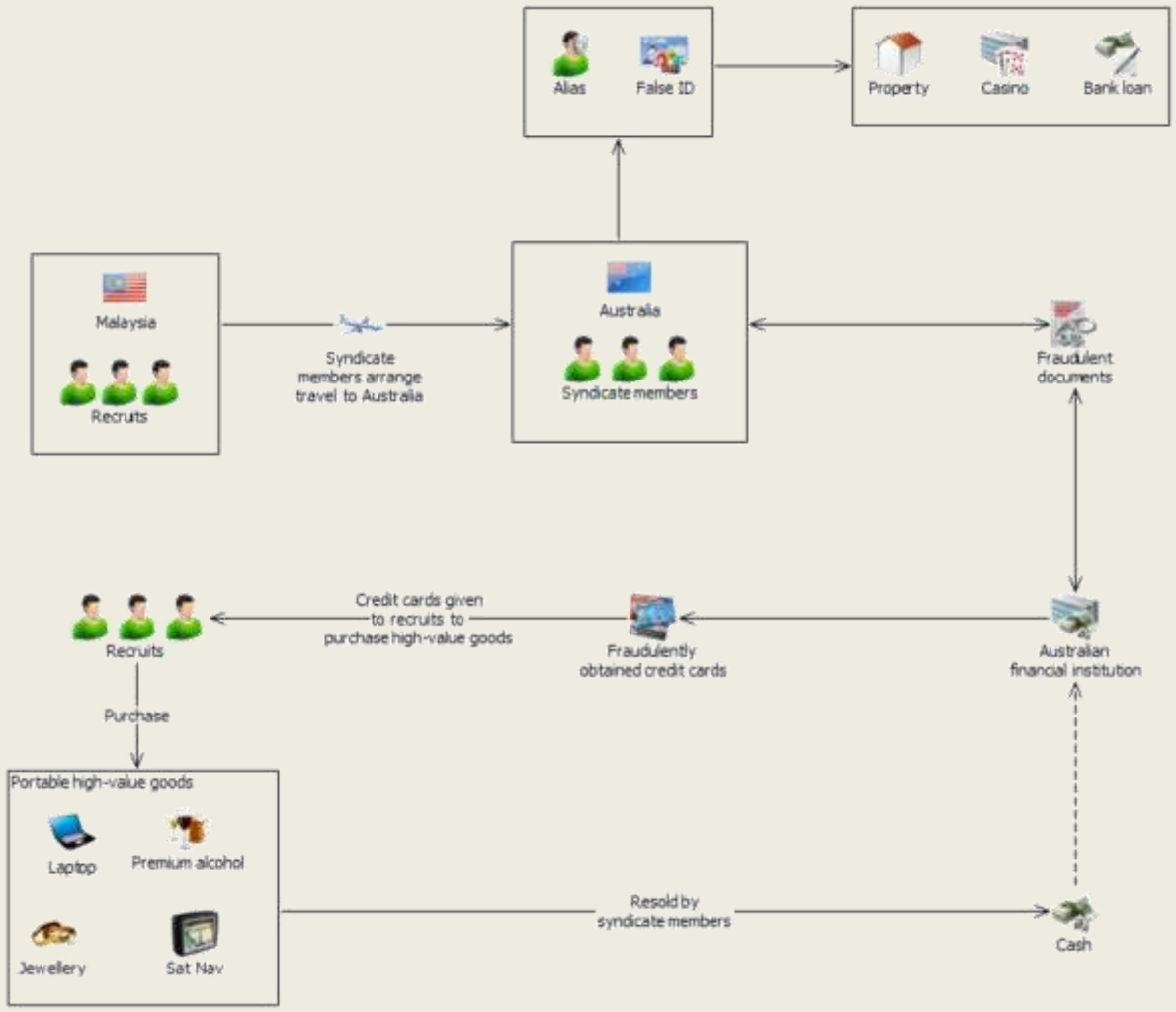
438. AUSTRAC information was used by authorities to verify identities used by the syndicate and to identify related international funds transfer instructions (IFTIs). A number of suspicious matter reports (SMRs) also assisted authorities to unravel the group's illicit financial activities. AUSTRAC

analysis and law enforcement investigations suggested that syndicate members used a portion of their criminal proceeds to purchase property, while other funds were laundered through Australian casinos.

439. One SMR submitted by a casino revealed that a member of the syndicate had converted AUD32,000 of gaming chips for cash, providing a casino identity card that was not linked to any 'rated play' (gambling activity), at the casino.

440. Further investigation by the casino found that the same person had previously supplied a different casino identity card for other transactions on the same day. Significant cash transaction reports (SCTRs) submitted to AUSTRAC also linked the syndicate member to four other gaming chip cash-outs totalling AUD59,000 over a 14-month period. The cash-outs were either conducted on the same day, or in the same week.

441. Two members of the syndicate were charged with fraud-related offences. One was sentenced to two years and three months imprisonment and the other to 12 months.



Offence	Fraud Money laundering
Customer	Individual Business
Industry	Banking (ADIs) Gambling services

Channel	Electronic Physical
Report type	IFTI SCTR SMR
Jurisdiction	Domestic International – Malaysia
Designated service	Account and deposit-taking services Gambling services
Indicators	Multiple chip cash-out occurring on the same day Significant chip cash-out with minimal play at a casino Use of false identification

CHINESE TAIPEI

442. In order to cut production costs and acquire more profit, the chairman of TC Foodstuff Factory Co. Mr. K, and employees Mr. W and Mr. C adulterated virgin olive oils, grape seed oils and other high quality oils with cheap oil products but labelled them as 100% pure oils and had sold them with a high price since 2007. Subsequently, since March 2013, they also added illegal additive copper chlorophyllin for forging the colour of high quality oils but labelled as 100% pure oils and sold them at high prices. The above processed products caused consumers to mistake the adulterated oils as pure oils due to the intentional mislabelling and paid more for them. The TC Foodstuff Factory Co. therefore gained the illegal profit in total of more than NTD1.9 billion.

443. The Changhua District Prosecutors Office charged Mr. K, Mr. W and Mr. C with fraud in October 2013. In November 2013, the AMLD found the TC's employee withdrew NTD12 million in cash from a checking account and delivered the cash to Mr. K. The checking account's holder is a company which has a business relationship with TC. The cash has been identified as the payment from that company to TC. But Mr. K took the money away. The AMLD immediately informed the Changhua District Prosecutors Office of this information for further reference. During the trial process, the presiding judge decided to increase Mr. K's bail up to NTD11 million considering that the prosecutor stated that Mr. K intended to conceal the property of the company through the money laundering method as mentioned above. Furthermore, the AMLD found Mr. K instructed his employees to notice the TC's retail dealers to make payments in cash or with cheques.

444. After receiving the payments, the employees immediately delivered the funds to Mr. K or his family members. The sum of funds reached up to NTD $95 million. Because Mr. K refused to disclose the funds flow of disposition, the Changhua District Court decided to take Mr. K into custody after considering that he might abscond due to the fact of concealing the funds. On December 16, 2013, Mr. K was sentenced to 16 year imprisonment.

FIJI

445. A suspected credit card fraud was reported by a commercial bank to the Fiji FIU. A merchant, Hotel X, advised the bank that Person A emailed the hotel for accommodation bookings. Person A provided credit card details and instructed Hotel X to deduct the following from the credit card:

- Accommodation Fee (for Hotel X) = FJ$400
- Flight Tickets (for Travel Agent) = FJ$3,500
- Compensation (for Hotel X) = FJ$300

446. Person A instructed Hotel X to inform him once the money was credited to the hotel's account so he could provide details of the travel agent to whom Hotel X would transfer FJ$3,500. The commercial bank advised Hotel X not to process these transactions.

447. Once Hotel X informed Person A that the transactions would not be processed from the given credit card, Person A provided details of another 2 credit cards with similar instructions to Hotel X. The commercial bank found that there was a block on the credit cards provided by Person A.

4.26 Structuring (smurfing)

AUSTRALIA

Cash courier transferred millions of dollars to Hong Kong for money laundering syndicate

448. A law enforcement agency identified a suspect believed to be working as a cash courier for a suspected money laundering syndicate. AUSTRAC data revealed that the suspect and additional cash couriers were laundering millions of dollars internationally for the syndicate.

449. Three suspects were arrested and received sentences ranging from 11 months imprisonment, a 12-month intensive corrections order and a 12-month good behaviour bond. Authorities also seized AUD543,000 cash.

450. Analysis of AUSTRAC data revealed that suspect A and additional cash couriers were depositing and transferring millions of dollars internationally for the syndicate.

451. The syndicate used the following method to move funds:

- Suspect B instructs suspect A to open two business accounts. Suspect A is made the sole signatory for the accounts.
- When suspect B takes possession of illicit cash, she contacts suspect A, who then flies interstate to meet her.
- Suspect A meets suspect B at a designated location where suspect B provides suspect A with the cash to be deposited and instructions on where the funds are to be transferred overseas.
- Suspect A deposits the cash into one of the business accounts. She makes several deposits across a number of different bank branches on the same day.
- On suspect B's instructions, suspect A transfers the funds overseas to accounts in Hong Kong.
- Afterwards, suspect A gives the receipts for the deposits and transfers to suspect B.

452. AUSTRAC information identified a significant spike in suspect A's financial activity over a six-month period:

- During the first month of activity, the business accounts held by suspect A received more than AUD430,000 in cash deposits, by third parties in various states.
- In the first two months of activity, suspect A sent international funds transfer instructions (IFTIs) totalling more than AUD2.3 million to businesses located in Hong Kong.
- Although suspect A's business accounts appeared to be receiving significant amounts of money from various sources and then transferring the funds overseas on their behalf, the business was not registered with AUSTRAC as a remittance dealer.

453. Prior to the transaction activity described above, AUSTRAC had recorded minimal financial transaction activity undertaken by suspect A.

454. The subsequent three months saw the business account set up by suspect A receive cash deposits worth more than AUD4.8 million.

455. Suspicious matter reports (SMRs) submitted to AUSTRAC highlighted the extent of financial activity related to suspect A and his business account. Some of these details included:

- Each month suspect A's business account received hundreds of cash deposits and electronic domestic transfers. Some cash deposits were undertaken by third parties. These deposits and transfers totalled more than AUD1 million per month.
- Typically, around AUD200,000 of the total deposits each month was deposited in structured cash amounts of less than AUD10,000. The remainder of the cash deposits were for larger amounts ranging from AUD10,000 to AUD70,000.
- A small portion of the funds was then debited from the accounts through cash withdrawals or domestic transfers.
- The majority of the funds were transferred via IFTIs to businesses located in Hong Kong, some of which were thought to be foreign exchange companies. These IFTIs ranged in value from AUD10,000 to AUD98,000
- The cash withdrawals, domestic transfers and IFTIs were usually conducted soon after a deposit was made into the account. This activity appeared to be inconsistent with the customer's established profile.

456. Three suspects were arrested by law enforcement and AUD543,000 cash was seized. Suspect A and B pleaded guilty to dealing in property reasonably suspected to be the proceeds of crime greater than AUD100,000.

457. Suspect A was sentenced to 11 months imprisonment, suspect B was given a 12-month intensive corrections order, and an additional suspect was given a 12-month good behaviour bond.

Offence	Money laundering
Customer	Business Individual
Industry	Banking (ADIs)
Channel	Electronic Physical
Report type	IFTI SCTR SMR
Jurisdiction	Domestic International – Hong Kong
Designated service	Account and deposit-taking services
Indicators	Frequent cash deposits occurring at different branches on the same day International funds transfers to overseas businesses similar in total value to recently received cash deposits Structuring of cash deposits below AUD10,000 to avoid reporting obligations Sudden increase in financial activity inconsistent with individual's transaction history

Third parties making regular cash deposits into a business account
Withdrawals conducted quickly after deposits

FIJI

458. A Suspicious Transaction Report was received on Person X, a foreigner, who was allegedly receiving international remittances of similar amounts from six different individuals on the same day. The purpose given for these remittances was "student allowance".

459. The Fiji FIU established that Person X was the wife a businessman in Country X. It was further established that the businesses of Person X's husband would buy supplies from companies in Fiji.

460. The remittances to Fiji appeared to be for business payments. The case was disseminated to the FIU of Country X for possible tax evasion offences, possible non-compliance by the sending institution in Country X and possible exchange control breaches in Country X. Investigations are currently underway.

4.27 Wire transfers/Use of foreign bank accounts

AUSTRALIA

Case - Suspicious million dollar transfers undid major methamphetamine operation

461. Multiple law enforcement agencies worked together to dismantle a major drug syndicate operating in Australia and Vietnam. The investigation uncovered one of the most elaborate methamphetamine operations in Victoria's history and led to the arrest of eight suspects.

462. AUSTRAC information detailed international funds transfers undertaken by the syndicate.

463. Law enforcement targeted the drug syndicate after monitoring the financial activity and assets belonging to the suspects, most of whom were operating from Vietnam.

464. Analysis of AUSTRAC information by law enforcement showed that over a 12-month period, approximately AUD24 million was sent via international funds transfer instructions (IFTIs) to Vietnam. All IFTIs were paid for entirely with cash. The syndicate mainly used remittance dealers to send the outgoing IFTIs. Law enforcement also believed that the individuals sending the funds were using false driver licences and credit cards.

465. The syndicate was the subject of 53 suspicious matter reports (SMRs). The majority of these were submitted by the remittance providers facilitating the outgoing IFTIs to Vietnam. The grounds for suspicion mainly related to the large amounts of cash possessed by the network and the transfer of funds to common beneficiaries in Vietnam.

466. Banking institutions also submitted four SMRs related to the syndicate, with the nominated grounds for suspicion including suspicious cash activity undertaken by the syndicate members, including apparent 'structuring' of account deposits and withdrawals. The SMRs noted that some of the beneficiary customers in Vietnam shared the same address and the large amounts of cash sent by the syndicate were inconsistent with the stated occupations of many of its members.

467. Eight members of the syndicate were arrested and charged with trafficking a large commercial quantity of methamphetamine. They were remanded in custody.

Offence	Drug trafficking
Customer	Individual
Industry	Banking (ADIs) Remittance services
Channel	Electronic Physical
Report type	IFTI SMR
Jurisdiction	International – Vietnam
Designated service	Account and deposit-taking services Remittance services (money transfers)
Indicators	Financial activity does not match established customer profile Large international funds transfers to common beneficiaries Large amounts of cash to pay for international funds transfers Multiple customers conducting international funds transfers to the same overseas beneficiary Multiple international funds transfers to a high-risk jurisdiction Multiple international funds transfers to beneficiaries with same address Structuring of cash deposits and withdrawals over a period of time to avoid reporting requirements Use of false identification to conduct transactions

FIJI

468. Suspicious Transaction Reports were received on two brothers, Person X and Person Y. Both individuals were unemployed, however analysis found significant financial transactions conducted by both of them. While profiling the two individuals, the FIU liaised with Police and established that Person X and Person Y were under investigation for supplying illegal drugs.

469. Analysis of the financial transactions conducted by Person X and Person Y established the following:

- Numerous cash deposits made into personal bank accounts. The source of funds for the deposits could not be clearly supported;
- Overseas cash withdrawals via international debit cards were conducted from the bank accounts of Person X and Person Y, although both individuals were in Fiji during the date of the overseas withdrawals;
- Large amount of funds were being remitted to relatives residing overseas although both individuals did not have a regular source of income;
- Purchases made at hardware stores were believed to be for house renovations;
- Purchases and payments made at hotels and expensive stores showed the lavish lifestyles of Person X and Person Y.

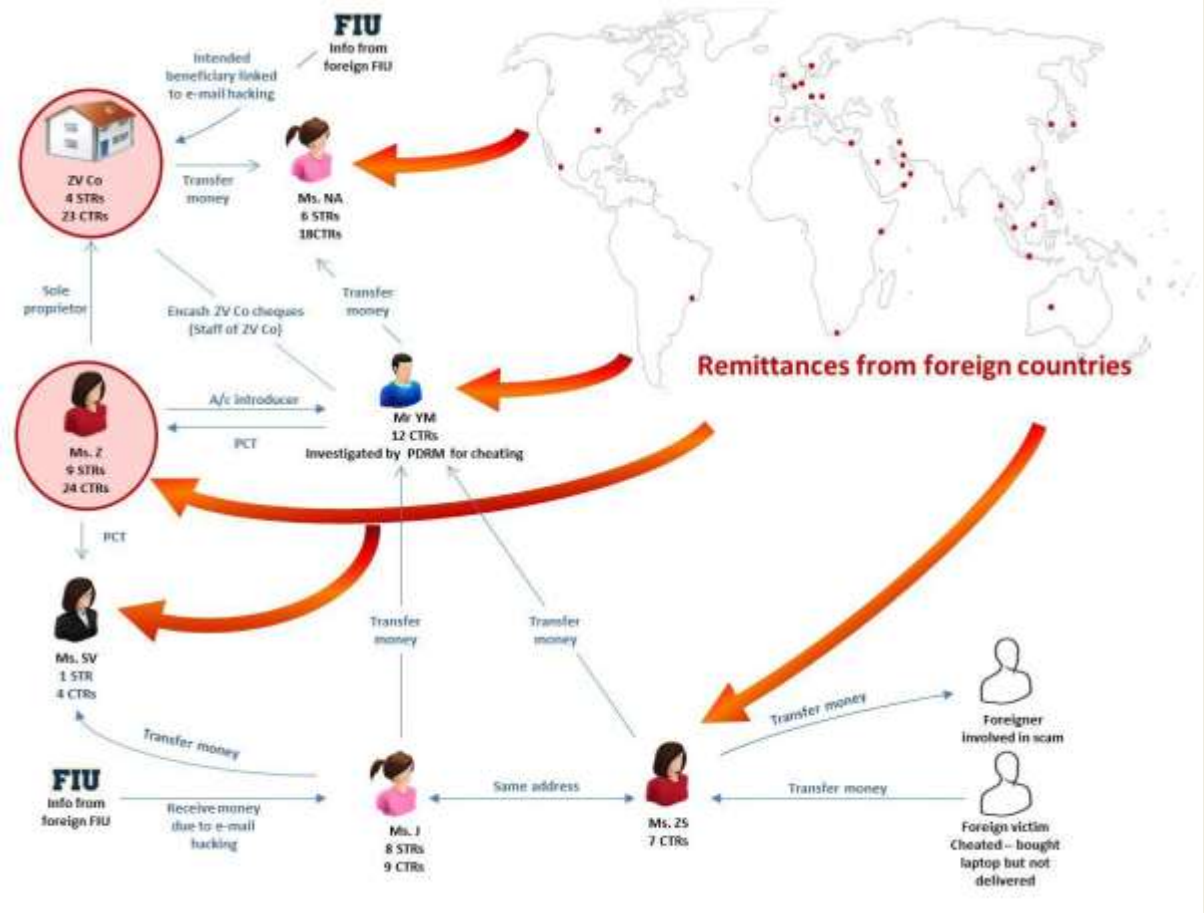
470. The case was disseminated to Police for their formal investigation. Investigations are currently underway.

MALAYSIA

Scam Related Money Laundering

471. Methods Used:

- Use of wire transfers/foreign bank accounts
- Use of the internet



472. Background of subjects:

- This case was triggered from STRs and CTRs reported on ZV Co. and Ms. Z. The STRs were reported due to frequent remittances received from overseas via banks and remittance agents which appear to be the main source of Ms. Z's income.
- Ms. Z owns ZV Co., a trading company dealing in fashion accessories and apparel, as per the business registration records. Other information indicates that ZV Co. is involved in providing engineering architecture technical services.
- Direct relationship among other subjects is unknown and could not be established although there are financial transactions performed between them.
- The subjects tend to open multiple accounts with various banks and the accounts were mostly closed within short period of time, i.e. within one year.

473. Source of information:

- STR and CTR records
- Sharing of intelligence from foreign Financial Intelligence Units

- Media source

474. Preliminary assessment & findings (modus operandi):

- Further analysis of accounts revealed that the subjects (i.e. ZV Co and Ms. Z) are linked to a wider network of people with the same modus operandi, i.e. receive numerous remittances from overseas. Upon receiving the remittances, funds were withdrawn via ATM, cash cheques or transferred to other accounts locally.

- These subjects were also seen to be transferring funds among each other, suspected to be involved in similar activities. It is likely that the activities of the subjects are linked to a scam activity as we have identified that Ms. ZS has transferred funds to an individual suspected to be involved in those activities.

- Proactive disclosures were received from foreign FIUs on ZV Co and a related individual named Ms. J as their accounts were used to receive funds following an e-mail hacking activity.

- Fund recall notifications in the form of SWIFT message i.e. MT199 were received from remitters banks that the subject's accounts were being used for fraudulent wire transfer scam. Based on the above case, FIU was able to identify that the subjects were involved in the following type of scams:

1. Career opportunity scam

475. Potential victims are contacted or recruited as a response to their online resume. The career scheme varies from invitation to become models, actors, engineers, hotel employees for which the victim has to pay a fee purportedly as administrative fees.

2. Love scam

476. Online dating sites were used to create fictional profiles for the purpose of securing monies from victims.

3. Advanced fee fraud/Inheritance scam

477. Fraudster uses mail, e-mail or faxes to target potential victims by creating fake scenarios; i.e. that they are currently holding a large sum of money and often need a fee to help facilitate the transfer'.

4. E-mail hacking

478. Fraudster will infiltrate e-mail accounts of overseas suppliers, (usually free e-mail accounts like Hotmail and Yahoo), and will send fake e-mails to customers, i.e. importers. These e-mails, which tend to target importers with an existing relationship with overseas suppliers, would direct the customer, i.e. importer to pay deposit for goods into a different bank account than that usually used.

479. In cases where the scam was successful, the importer believed the validity of the request for payment of deposit into a different account has been verified with the overseas supplier, however, the verification request was sent to the fake contact information provided in the fake e-mails.

480. Actions taken to date:

- Information in FIU's database was analysed together with the intelligence received from foreign FIUs, and subsequently disclosed to the Royal Malaysia Police (RMP) for investigation.

4.28 Commodity exchanges (barter – e.g. reinvestment in illicit drugs)

481. No cases reported.

4.29 Use of false identification

AUSTRALIA

Suspect used casinos, remitters and airline pilots to launder proceeds of crime

482. A law enforcement agency conducted an investigation into a suspect believed to be part of an international money laundering scheme. AUSTRAC information revealed the syndicate's financial activities and assisted authorities to identify the suspect.

483. The suspect was charged with dealing with property reasonably suspected of being the proceeds of crime and received a 12-month good behaviour bond.

484. Authorities alleged that the suspect was part of a scheme to launder approximately AUD2.4 million from the proceeds of crime. AUSTRAC information provided an insight into the financial activities of the syndicate and assisted in identifying the suspect.

485. The investigation was initiated following the identification of three Chinese airline crew who attempted to depart Australia while carrying a total of more than AUD100,000 of undeclared currency. Authorities identified that two of the airline crew were found to be carrying both Australian and foreign currency equivalent to more than AUD40,000 and AUD30,000 respectively. The third crew member was in possession of foreign currency equivalent to more than AUD30,000.

486. Following the identification of the three crew members, law enforcement authorities obtained information that prompted them to begin investigating a number of Australian-based individuals, believed to be part of the international money laundering scheme.

Suspicious casino gambling activity

487. Law enforcement officers began investigating the suspect after AUSTRAC received a suspicious matter report (SMR) concerning the suspect's activities. The SMRs highlighted inconsistent gaming activity at a casino by the suspect. One SMR described how the suspect had lost more than AUD3 million in one year while gambling in the casino. The suspect's losses in other years were comparatively smaller, ranging from approximately AUD3,000 to AUD30,000.

488. During further investigations, authorities observed the suspect take possession of a bag. Authorities intercepted the suspect and found approximately AUD200,000 cash inside the bag. Law enforcement officers seized the cash and the suspect was arrested.

489. Law enforcement officers subsequently established that the suspect had previously given the three airline crew large amounts of cash for them to 'courier' from Australia to China as part of the money laundering scheme.

Suspicious transfers to China and huge cash deposits

490. Authorities established that the suspect was a known associate of an individual employed by a remittance service provider. On several occasions the individual received a commission for transferring a significant amount of funds to China on behalf of the suspect. Authorities suspected that the individual used false names and altered records to the international funds transfers.

491. An Australian bank submitted an SMR about this individual's activities after she made two unusually large cash deposits totalling AUD600,000 on the same day to the same bank account.

AUSTRAC also received two significant cash transaction reports (SCTRs) for the two large deposits. Authorities also alleged that the individual deposited a further AUD800,000 on a different day.

492. The suspect was charged under the Criminal Code Act 1995 with dealing with property reasonably suspected of being proceeds of crime. The suspect received a 12-month good behaviour bond.

Offence	Money laundering Undeclared currency
Customer	Individual Business
Industry	Remittance services Banking (ADIs) Gambling services
Channel	Physical Electronic Agent/third party
Report type	SMR IFTI SCTR
Jurisdiction	International – China
Designated service	Remittance services (money transfers) Account and deposit-taking services Gambling services
Indicators	Multiple cash deposits on the same day into the same bank account Multiple high-value international funds transfers Sudden large increase in gambling activity inconsistent with customer's established gambling profile Third-party individuals making large cash deposits into accounts Use of cash couriers Use of third parties to deposit funds

FIJI

493. The Fiji FIU received an allegation that a licensed foreign exchange dealer, Company X, was involved in illegal foreign currency sales. Checks established that foreign currency sales recorded in Company X's books were conducted by foreigners who were not in Fiji during the date of the transaction. Documents provided for the transactions included copies of passports and electronic tickets. The Fiji FIU also ran checks with the airline that reportedly issued the e-tickets and found that the e-tickets were fake. Further checks established that the compliance officer of Company X was the main person facilitating the suspicious foreign currency sales.

494. The total amount involved in this case was FJ$0.7 million. The case was disseminated to Police and investigations are currently underway.

INDONESIA

495. In April 2014, the National Narcotics Agency arrested Mr. E and Mr. M who were proved laundering money from the narcotics trade. The narcotics was sourced from Mr. Mu and Mr. A (residents of M country). To obscure the source of wealth, Mr. E used false identifications to create several bank accounts and purchased luxurious goods. Mr. E also invested the proceeds from

narcotics trade to his brother's (Mr. M) property business. Mr. E's assets were seized, with the total value of USD100,000, which included money in bank accounts, vehicles, and houses. Mr. M's assets was also seized, with the total value of USD2.6 million, which included USD700,000 in bank accounts, time deposits with the value of USD200,000, 2 units of truck, 3 units of luxurious cars, 3 units of apartment, and 1 unit of house.

4.30 Others

SRI LANKA

496. As per the information received by Deputy Inspector General of Police (in 2012.01.14), the CID initiated investigations on several individuals who maintained close relationships with Mr. X (who has been identified as a main drug dealer). Upon investigations it was revealed that Mr. X's wife Mrs. X are now continuing the drug trade in the absence of her husband. Mr. X left the country using a forged passport to evade arrest in 2011. Mrs. X also possesses a forged passport which has been used to leave the country. However, she was arrested on her return on 30/01/2012.

497. Further it was revealed that a relative of Mrs. X, Ms. M had rented out a building purported to be used for a business of packaging toys (teddy bears). Based on the information received from Mrs. X, CID searched the house and there was evidence to prove that heroin was packed at the premises.

498. With the records obtained from Mrs. X and Ms. M, the CID raided the business premises. Physical cash of LKR 9,071,680.00 and a motor vehicle were seized. Books of accounts which were used to record the daily collection of their drugs trade and how the profit had been divided between Mr & Mrs. X were also seized. Six individuals who were at the premises were arrested. Further, investigations revealed that Ms. M has frequently deposited cash to an account of Mrs. X. one of the drivers of Mrs. X has testified that he, on the order of Mrs. X frequently transported some parcels to Ms. M which could be assumed as cash. Assistance from the FIU was obtained to trace the financial transactions of the individuals concerned.

499. Further investigations revealed that they conducted the business from rented buildings using rented motor vehicles and buildings have been obtained on short term rent.

500. Mr. and Mrs. X and Ms. M were prosecuted under the Prevention of Money Laundering Act No. 05 of 2006, Dangerous Drugs and Emigration Laws.

501. Followings are the list of properties identified relating to the case where total value of suspended properties is approximately LKR 1.7 billion.

1. 5 Real Estate Properties
2. 2 Condominium Properties
3. Motor Vehicles
   BMW Car - 1
   Jeeps - 2
   Motor Bicycle
4. Cash – LKR 18,200,000 and Fixed Deposit Certificates
5. Gold Jewellery – 2851g

UNITED STATES OF AMERICA

Large-Scale Law Enforcement Effort Targets Downtown Los Angeles Businesses Linked to Money Laundering for Drug Cartels
Fashion District Store Using 'Black Market Peso Exchange' Scheme Allegedly Took Ransom Money for Hostage Being Held and Tortured by Sinaloa Drug Cartel

U.S. Department of Justice September 10, 2014 Central District of California (213) 894-2434

LOS ANGELES—Approximately 1,000 law enforcement officials this morning fanned out across the Fashion District in downtown Los Angeles to execute dozens of search warrants and arrest warrants linked to businesses suspected of using "Black Market Peso Exchange" schemes to launder narcotics proceeds for international drug cartels.

Authorities today arrested nine defendants and seized what is estimated to be at least $65 million in cash and from bank accounts around the world in relation to asset forfeiture actions filed as part of the ongoing investigations.

One case unsealed today alleges that the Sinaloa Drug Cartel used a Fashion District business to accept and launder ransom payments to secure the release of a United States citizen who was kidnapped by that narcotics organization, held hostage, and tortured at a ranch in Mexico.

Two other indictments also unsealed today involve alleged money laundering by other Fashion District stores using the Black Market Peso Exchange (BMPE) scheme.

In a BMPE scheme, a peso broker works with an individual engaged in illegal activity, such as a drug trafficker, who has currency in the United States that he needs to bring to a foreign country, such as Mexico, and convert into pesos. The peso broker finds business owners in the foreign country who buy goods from vendors in the United States and who need dollars to pay for those goods. The peso broker arranges for the illegally obtained dollars to be delivered to the United States-based vendors, such as the stores in the Fashion District, and these illegally obtained dollars are used to pay for the goods purchased by the foreign customers. Once the goods are shipped to the foreign country and sold by the foreign-based business owner in exchange for pesos, the pesos are turned over to the peso broker, who then pays the drug trafficker in the local currency of the foreign country, thus completing the laundering of the illegally obtained dollars.

This BMPE scheme—which is also known as Trade-Based Money Laundering—is often used by Mexico-based drug trafficking organizations to collect money from their drug sales in the United States without having to take the risk of smuggling bulk amounts of U.S. currency across the Mexican border and without having to convert and wire the U.S. currency through established financial institutions, which not only carries transaction fees, but also a threat their illegal activity will be detected.

"We have targeted money laundering activities in the Fashion District based on a wealth of information that numerous businesses there are engaged in Black Market Peso Exchange schemes," said Robert E. Dugdale, the Assistant United States Attorney who oversees the Criminal Division in the Central District of California. "Los Angeles has become the epicenter of narco-dollar money laundering with couriers regularly bringing duffel bags and suitcases full of cash to many businesses. Because Los Angeles is at the forefront of this money laundering activity, law enforcement in Los Angeles is now at the forefront of combatting this issue."

In the criminal case related to the laundering of ransom money to the Sinaloa Cartel, three people were arrested today for their roles in a BMPE scheme based at a Fashion District wholesaler named QT Fashion, Inc., (which did business under the names QT Maternity and Andres Fashion). The indictment in this case also alleges that a Sinaloa, Mexico-based business, Maria Ferre S.A. de C.V.,

was involved in the scheme to launder ransom money. Following the kidnapping of a United States Citizen by the Sinaloa Drug Cartel, QT Fashion allegedly accepted bulk cash and funneled the money through 17 other Fashion District businesses at the direction of Maria Ferre.

The indictment alleges that the Sinaloa Drug Cartel ordered the kidnapping of the victim after authorities in the United States seized more than 100 kilograms of cocaine that he was responsible for distributing. The victim was held at a ranch in Culiacan, Sinaloa, where he was beaten, shot, electrocuted and water boarded. The hostage was released after relatives paid $140,000 in ransom, and he is currently in the United States.

"Today's arrests and searches should send a message to international drug cartels that the FBI and our partners won't tolerate the exploitation of American businesses for the purposes of illicit financial transactions that fund hostage-taking and the distribution of narcotics," said Bill L. Lewis, the Assistant Director in Charge of the FBI's Los Angeles Division. "In addition, today's actions should send a warning to American businesses who turn a blind eye to the crime they facilitate, while avoiding reporting requirements, transaction fees and law enforcement scrutiny."

Three defendants related to QT Fashion were arrested this morning—Andrew Jong Hack Park (aka Andres Park), 56, of La Canada-Flintridge; Sang Jun Park, 36, of La Crescenta; and Jose Isabel Gomez Arreoloa (aka Chabelo), 49, of downtown Los Angeles.

Three defendants linked to Maria Ferre are wanted by authorities. They are Luis Ignacio Orozco Munoz (aka Nacho), 50, of Culiacan, Sinaloa; Armando Arturo Chavez Gamboa, 43, of Culiacan, Sinaloa; and Daisy Corrales Estrada, 30, of Culiacan, Sinaloa.

The six individual defendants were charged in a three-count indictment returned under seal by a federal grand jury on June 19. The indictment, which was unsealed this morning, accuses the defendants of conspiracy to launder money, conspiracy to operate an unlicensed money transmitting business, and operating an unlicensed money transmitting business. If they are convicted of the charges in the indictment, each defendant would face a statutory maximum penalty of 30 years in federal prison.

The investigation into the money laundering scheme related to the kidnapping was conducted by the FBI, IRS—Criminal Investigation and the Drug Enforcement Administration. The case is being prosecuted by Assistant United States Attorney Angela Scott (213-894-6683).

"Today's Fashion District takedown sends a clear message that law enforcement will not tolerate the actions of those who use the cover of legitimate business to conceal bulk cash obtained directly from drug trafficking and associated acts of violence," said DEA Associate Special Agent in Charge Stephen G. Azzam. "These indictments and arrests deal a massive blow to complex trade-based money laundering schemes in general, and will therefore severely impair the ability of drug cartels to realize profits and further entrench themselves in our nation's socioeconomic fabric."

In the second case announced today, three members of a Temple City family—Xilin Chen, 55; Chuang Feng Chen (aka "Tom"), 24, who is Xilin Chen's son; and Aixia Chen, 28, who is Xilin Chen's daughter—have been charged with conspiring to launder monetary instruments, money laundering, and various immigration offenses for their roles in running various businesses in the Fashion District that were used in BMPE schemes. During this morning's operation, Xilin Chen and Chuang Chen were arrested. Aixia Chen is a fugitive currently being sought by authorities.

The indictment related to the Chens' businesses—Yili Underwear and Gayima Underwear—alleges that they received bulk cash from a narcotics trafficker in Los Angeles and from an undercover agent posing as a drug trafficker. The Chens allegedly laundered the money to drug trafficking organizations outside of the United States through use of the BMPE scheme, and "structured" the

deposits of the bulk cash they received at their businesses to avoid currency reporting requirements that would have alerted law enforcement to their criminal conduct.

IRS—Criminal Investigation's Special Agent in Charge Erick Martinez said, "Through our collective efforts, we are gaining access to more and more information on the abusive practices of individuals and businesses involved in the laundering and structuring of drug proceeds through the Los Angeles Fashion District, and you can expect us to use all of our enforcement tools to stop this abuse. IRS—Criminal Investigation is working hard to ensure criminals do not use the United States financial system to legitimize their illegal profits."

If they are convicted, Xilin Chen would face a statutory maximum sentence of 100 years in federal prison, Chuang Chen would face up to 40 years, and Aixia Chen could be sentenced to as much as 80 years.

The case naming the Chens was investigated by the Drug Enforcement Administration and IRS—Criminal Investigation under the auspices of the Southwest Border Initiative. The case is being prosecuted by Assistant United States Attorney John Kucera (213-894-3391) and Assistant United States Attorney Vicki Chou (213-894-8692).

In the third case announced today, a business in the Fashion District named Pacific Eurotex, Corp. and four individuals connected to that business have been charged with conspiracy to launder money, conspiring to illegally structure currency transactions to avoid a currency transaction reporting requirement, structuring currency transactions to avoid currency transaction reporting requirements, and failing to file reports of currency transactions over $10,000. This Indictment alleges that the defendants utilized Pacific Eurotex as a repository to receive bulk cash that they knew or believed consisted of drug money, that they later laundered those drug proceeds to foreign countries through a trade-based money laundering scheme; that they failed to report the receipt of this bulk cash, as required; and that they structured deposits of this bulk cash into bank accounts by making frequent deposits of the cash in amounts less than $10,000 to avoid a bank reporting requirement that would have drawn the scrutiny of law enforcement to their actions.

"These arrests and seizures should serve as a sobering warning to companies that seek to bolster their bottom line by doing business with drug traffickers—you will pay a high price for your complicity," said Claude Arnold, special agent in charge for Homeland Security Investigations in Los Angeles. "Unscrupulous companies that help cartels cover their financial tracks by laundering their illicit funds are contributing to the devastation wrought by the international drug trade."

The four individual defendants named in the Pacific Eurotex indictment were arrested this morning. Those taken into custody are: Hersel Neman, 55 of Beverly Hills, the chief financial officer of Pacific Eurotex; Morad Neman, 54, of the Westwood District of Los Angeles, the chief executive officer of Pacific Eurotex and brother of Hersel Neman; Mehran Khalili, 45, of Beverly Hills, who is a brother in law of the Nemans; and Alma Villalobos, 52, of Arleta.

This indictment alleges that Pacific Eurotex received, laundered and structured approximately $370,000 in bulk cash delivered on four separate occasions by an undercover agent posing as a money courier. The indictment alleges that defendants laundered the money after being specifically advised by Homeland Security Investigations agents that bulk cash payments were frequently derived from illegal activity and that they were required to report cash transactions involving more than $10,000 in currency. According to the indictment, the defendants laundered money, despite the fact that, on one occasion, some of the bulk currency appeared to be spattered with blood.

California Attorney General Kamala D. Harris stated: "Transnational gangs are the number one threat to California's public safety. These predatory criminal organizations destabilize our communities with drugs, guns and human trafficking. Today marks a major victory in our ongoing fight to keep California safe from these predators."

The investigation into Pacific Eurotex was conducted by U.S. Immigration and Customs Enforcement's Homeland Security Investigations and IRS—Criminal Investigation. Substantial assistance was provided by the Los Angeles Interagency Metropolitan Police Apprehension Task Force (LA IMPACT); the Los Angeles, Long Beach, Gardena, Torrance, El Segundo, and Monterey Park police departments; along with the Westside High Tech Task Force. This case is being prosecuted by Assistant United States Attorney Julie Shemitz (213-894-5735).

The defendants arrested today are scheduled to be arraigned this afternoon in United States District Court.

An indictment contains allegations that a defendant has committed a crime. Every defendant is presumed to be innocent until proven guilty in court.

This content has been reproduced from its original source.

HTTP://WWW.FBI.GOV/LOSANGELES/PRESS-RELEASES/2014/LARGE-SCALE-LAW-ENFORCEMENT-EFFORT-TARGETS-DOWNTOWN-LOS-ANGELES-BUSINESSES-LINKED-TO-MONEY-LAUNDERING-FOR-DRUG-CARTELS

5. USEFUL LINKS

Anti-Corruption Research Network

502. 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

503. 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)

504. 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

505. 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

506. For FIU information and links to FIUs with websites.
http://www.egmontgroup.org/

Global Financial Integrity

507. 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
GAFILAT - Grupo de Acción Financiera de Latinoamérica (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

ADB - Asian Development Bank
AGD - Attorney General's Department
AML - Anti-Money Laundering
AMLD - Anti-Money Laundering Department
APG – Asia/Pacific Group on Money Laundering
ATM - Automatic Teller Machine
AUSTRAC - Australian Transaction Reports and Analysis Centre
CFT - Countering the Financing of Terrorism
CRA – Canada Revenue Agency
CTED - Counter Terrorism Executive Directorate
CTR - Cash Transaction Report
DNFBP - Designated Non-Financial Businesses and Professions
EAG – Eurasian Group
ECOWAS - Economic Community Of West African States
EDD - Enhanced Due Diligence
EFT - Electronic Funds Transfer
FATF - Financial Action Task Force
FEMA – Foreign Exchange Management Act (India)
FinCEN - Financial Crimes Enforcement Network
FINTRAC - Financial Transactions Reports Analysis Centre (Canada)
FIU - Financial Intelligence Unit
FMU – Financial Monitoring Unit (Pakistan)
FSRB – FATF-Style Regional Bodies
FTZ – Free Trade Zone
GIF – Financial Intelligence Office (Macao, China)
GAFILAT - Financial Action Task Force of Latin America
HOSSP - Hawala and Other Similar Service Provider
ICRG – International Cooperation Review Group
IFTI - International Funds Transaction Instruction
INTERPOL - International Criminal Police Organisation
INTRAC – Indonesian Financial Transaction Reports and Analysis Centre
LEA - Law Enforcement Agency
JIB - Investigation Bureau, Justice (Chinese Taipei)
ML - Money Laundering
MLA - Mutual Legal Assistance
MOU - Memorandum of Understanding
NGO – Non-Government Organisation
NPO – Non-Profit Organisations
NRA – National Risk Assessment
PCA - Principal Customs Areas
PEP - Politically Exposed Person
RCMD - Royal Malaysian Customs Department
RCMP – Royal Canadian Mounted Police
SALW – Small Arms and Light Weapons
SAR – Suspicious Activity Report
SCTR - Significant Cash Transaction Report
SECP – Security Exchange Commission of Pakistan
SMR – Suspicious Matter Reports
STR - Suspicious Transactions Report

SUSTR - Suspicious Transactions Report
TBML - Trade Based Money Laundering
TCSP - Trust and Company Service Providers
TF - Terrorism Finance
TTR – Threshold Transaction Reports
UN - United Nations
UNSCR – United Nations Security Council Resolution
VAT - Value Added Tax
WG – Working Group