APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2016

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

Approved and adopted, 8 September 2016

APG Yearly Typologies Report 2016

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 APG Yearly Typologies Report is provided for under the APG's Strategic Plan and the APG Typologies Working Group Terms of Reference and 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 indicators included in this report will assist front-line financial institutions and non-financial businesses and professions (casinos, accountants, lawyers, trust and company service providers, real estate agents, etc.) involved in implementing preventative measures, including customer due diligence and suspicious transaction reporting, to detect and combat ML and TF.

3 Each year APG members and observers provide information on ML and TF cases, trends, research, regulatory action and international cooperation. The information collected 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.

4 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. Many cases cannot be shared publicly due to their sensitive nature or to ongoing investigative or legal processes. 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.

Typologies in 2015-2016

5 The Typologies Working Group continued its work in 2015-16, initially under the leadership of Mongolia and Fiji as Co-Chairs. In November 2015, at the annual APG typologies workshop, Fiji stepped down as Co-Chair and India subsequently took up the position. The APG would like to express its gratitude to Fiji for its support of the APG's typologies work.

6 In July 2015 the Typologies Working Group met at the APG Annual Meeting to determine the work program for the year, including the conduct of a joint MENAFATF and APG Typologies Workshop, which will be held in November 2016 hosted by Saudi Arabia.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2015 - 2016

7 This section of the report provides a brief overview of typologies related work undertaken by the APG between July 2015 and June 2016.

1.1 2015 APG Typologies Workshop

8 Each year the APG typologies workshop brings together AML/CFT practitioners from investigation and prosecution agencies, financial intelligence units (FIUs), regulators, customs authorities and other relevant organisations to consider priority ML and TF risks and vulnerabilities. In recent years the APG has taken the opportunity to combine the typologies workshop with capacity building/technical seminars to share practitioners' experience on priority topics related to ML and TF.

9 APG typologies and capacity building/technical workshops are designed to achieve a number of objectives, as follows:

- 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 FATF-Style Regional Body (FSRB) led typologies projects;
- Share best practices and strategies for practical application of AML/CFT measures related to previous typologies studies and other implementation issues;
- Expand partnerships between the public and private sectors on AML/CFT issues; and
- Enhance industry cooperation on AML/CFT issues and draw on industry experience in the selection and conduct of studies of ML and TF typologies.

10 The 2015 APG Typologies Workshop was held in Kathmandu, Nepal from 16 – 20 November 2015. The workshop involved approximately 230 delegates from 38 jurisdictions and ten international organisations, as well as 39 representatives from the private sector. The workshop was co-chaired by the Typologies Working Group Co-Chairs from Fiji and Mongolia.

11 On the first day of the workshop the United Nations Counter-Terrorism Executive Directorate gave the keynote address on emerging global terrorism risks. On subsequent days delegates attended one of three breakout sessions, as follows:

- *TF*. This breakout session was on TF trends in a changing regional context including the use of social media as a tool for financing terrorism. Case studies included how the Islamic State of Iraq and the Levant and its fighters are being financially supported in the Asia-Pacific region. This breakout session complemented and fed into the FATF's work on coordinating TF related typologies by sharing regional experience and considering opportunities to deepen international cooperation in assessing and responding to TF risks.
- *Developing the necessary infrastructure of a FIU*. This breakout session was led by the Egmont Group and was designed to assist FIUs improve their security arrangements. Egmont Group's Information Technology Working Group gave guidance on developing and implementing security policies and procedures in the areas of physical, personnel, document and information security.
- *Wildlife crime and ML*. This breakout session raised awareness on the need to use financial investigations to enhance wildlife and environmental crime investigations, and was facilitated by the United Nations Office on Drug and Crime (UNODC), the American Bar Association and Nepal Money Laundering Investigation Department. Presenters from the APG membership, non-government organisations involved in tracking wildlife crime and from members of the Eastern and Southern Africa Anti-Money Laundering Group

(ESAAMLG) provided information as to the scale of the problem, the benefits of using the concept of 'following the money' and the types of financial enquiries that can support this process. This breakout session was open to the private sector. As a result of this session, the UNODC and the American Bar Association's Rule of Law Initiative are currently working with the APG to scope a project to enhance the detection and investigation of illicit financial flows from wildlife crime through developing good practice guidelines and relevant typologies.

1.2 Status of current and possible new typologies projects

12 In 2015–16, two of the APG's four on-going typologies were completed and one new project was commenced, as follows:

- The Recovering the Proceeds of Corruption in the Pacific was a joint project undertaken between the Pacific Island Law Officers' Network (PILON) and the APG and was co-led by PNG and Tonga. The report was finalised in April 2016 (see below);
- Frauds and Money Laundering in the Pacific report co-lead by Fiji and Vanuatu was finalised in June 2016 (see below);
- The development of guidance and best practices on following the financial flows related to wildlife crime is a project that was initiated at the 2015 APG typologies workshop hosted in Nepal and is due to commence in July 2016. This project is being led by the UNODC (supported by the American Bar Association's Rule of Law Initiative and the APG secretariat);
- Risks and Vulnerabilities of Trans-Pacific Drug Routes is an on-going project being co-led by Tonga and Vanuatu. This project is due for competition by December 2016; and
- Scoping Money Laundering Risks Associated with Offshore Financial Centres is an on-going project being co-led by Cook Islands and Samoa.

PILON/APG Typologies Project: Recovering the Proceeds of Corruption in the Pacific

13 This report compiles relevant regional case studies on corruption and related money laundering and highlights key challenges and successes. It draws on regional and global experiences to provide recommendations for Pacific countries to improve responses to corruption through effective money laundering and proceeds of crime frameworks. Countries in the Pacific report corruption as one of the most common predicate offences for money laundering in the region. Countries around the world have sought to implement anti-money laundering and proceeds of crime regimes in their fight against corruption. However, these regimes are under-utilised across the Pacific.

Fraud & Money Laundering in the Pacific

14 This report compiles relevant regional case studies on fraud and related money laundering and highlights key challenges and successes. The case studies illustrate that for most money laundering cases which result in successful convictions and prosecutions, fraud appears to be the underlying predicate offence. The scale of fraud can take many forms. The case studies showcase the methods and techniques used by criminals and fraudsters to derive proceeds of crime. Emerging fraud and money laundering techniques and in particular the extensive use of internet and technology enabled crimes possess challenges for financial institutions, law enforcement agencies, financial intelligence units (FIUs), regulators and the judiciary. The challenges are especially in the timely identification of the fraud, it's location and the movement of proceeds of crime.

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

15 This section of the report provides a brief overview of typology reports published by FATF and several other FSRBs between July 2015 and June 2016.

2.1 FATF Typology Projects

FATF/MENAFATF Money Laundering through the Physical Transportation of Cash

16 This joint FATF/MENAFATF report highlights that despite the availability of a range of non-cash payment methods and the continuous development of new and innovative alternatives for cashless payments, cash remains an important means of payment across the globe, with an estimated USD 4 trillion in various currencies in circulation.

17 The report also highlights that cash is still widely used in the criminal economy. The physical transportation of cash across international borders is one of the oldest forms of ML and is still widely used today – criminals remove their illicit assets from the banking system as cash, transport it to another country and then spend it or reintroduce it into the banking system.

18 This report analysed input provided by over 60 countries to identify methods and techniques use by criminals to transport funds across the border. The report contains a number of case studies that illustrate techniques, such as the transportation of large quantities of cash in small denominations by cargo or mail, and the transportation of low quantities of cash in high denominations by cash couriers. The report identifies the main challenges that law enforcement, customs and other agencies face in detection and disruption of illicit cross-border transportation of cash. Finally, to assist agencies stop this criminal activity, the report also provides 'red flags' and other information for use by law enforcement agencies.

19 This report is available on the FATF's website http://www.fatf-gafi.org/.

FATF Report on Emerging Terrorist Financing Risks

20 In the light of recent global developments, terrorist financing has been a major focus of the FATF in the last year, including in its typologies work. *The Emerging Terrorist Financing Risks Report*, the result of the call for further urgent research into terrorist financing, provides an overview of the various financing mechanisms and financial management practices used by terrorists and terrorist organisations. It explores emerging terrorist financing threats and vulnerabilities posed by foreign terrorist fighters (FTFs), fundraising through social media, new payment products and services, and the exploitation of natural resources, as follows:

- The issue of FTFs is not a new phenomenon, but the recent scale of the issue in relation to the conflict in Syria and Iraq is disturbing. FTFs are now considered one of the main forms of material support to terrorist groups. The report sets out the funding needs, sources and methods of FTFs and the challenges associated with combatting them.
- New technologies have also introduced new terrorist financing vulnerabilities. The broad reach and anonymity associated with social media and new payment methods makes these attractive tools for terrorists and terrorist organisations to use in their financial activities. The report discusses fundraising through social media, new payment products and services.
- The exploitation of natural resources for TF was raised as a substantial concern in the context of the Islamic State of Iraq and the Levant but this report has confirmed that it is also relevant for other terrorist organisations and regions. The ability to reap high rewards from the natural resources sector, coupled with the weak institutional capability, particular in or near areas of conflict, creates a significant vulnerability for terrorist organisations to

capitalise on. This report finds that this issue is linked with criminal activity including extortion, smuggling, theft, illegal mining, kidnapping for ransom, corruption and other environmental crimes.

21 The report also highlights that all terrorists and terrorist groups, particularly large terrorist organisations, require a financial management strategy to allow them to obtain, move, store and use their assets. Understanding these financial management strategies is essential in developing effective measures to counter TF.

22 Furthermore, the report emphases the need to develop private/public partnerships to enhance awareness of, and responses to, emerging terrorist financing risks. Such a partnership will facilitate the identification of FTFs and their facilitation networks. In addition, accurate and forward-looking guidance to the private sector will further improve their monitoring and screening processes and reporting-time on sensitive transactions which may relate to terrorist financing.

23 This report is available on the FATF's website http://www.fatf-gafi.org/

2.2 EAG – Eurasian Group on Combating Money Laundering and Financing of Terrorism

24 In 2015 EAG continued working on several Typologies projects, as follows:

- The Republic of Tajikistan is leading the project *ML typologies in Ponzi schemes* (financial pyramids) and presented preliminary results of the research at the EAG plenary meeting in June 2016. This project is scheduled for completion in June 2016; and
- The Russian Federation, leader of the project *ML typologies in corruption*, presented preliminary results of the research at the EAG plenary meeting in November 2016. EAG members determined next steps, including cooperating with the Egmont Group on further research, drafting and dissemination of an additional questionnaire to EAG members.

25 The EAG decided at its 23rd EAG Plenary held in Moscow to conduct two typological studies in 2016:

- Russia will lead a project on illegal expatriation of assets of the credit institutions; and
- Kazakhstan will lead a project on structural analysis of financial flows related to the use of cash in committing predicate offence and/or money laundering.

2.3 ESAAMLG – The Eastern and Southern Africa AML Group

Typology Report on the Study on Money Laundering through the Securities Market in the ESAAMLG Region

26 This report analysed the main sources of funds being invested in the ESAAMLG securities markets, and the possible linkages to ML/TF activities. The report aims to raise awareness of the ML/TF risks in the securities market to local, regional and international stakeholders by identifying possible methodologies used by money launderers in the securities market. The report highlights measures being undertaken by countries to mitigate identified ML/TF risks in securities markets, and also makes recommendations on appropriate measures to combat ML/TF in the securities market in the ESAAMLG region.

27 This report concludes that the clearing and settlement frameworks in almost all ESAAMLG member jurisdictions do not address AML/CFT issues and that the most common predicate offence related to the sector is the fraudulent change of ownership of shares, which has potential to create proceeds that can be laundered. The report did not find any incidences of TF related to the securities market.

28 The report revealed AML/CFT risks in the securities market that render the sector vulnerable; however, these can be mitigated. The report also proposed recommendations to assist members to mitigate the risks identified and encouraged member countries to adopt regional and international best practices.

29 This report is available on the ESAAMLG website www.esaamlg.org

2.4 MONEYVAL – The Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism

Typologies Report on Laundering the Proceeds of Organised Crime

30 The report examines the methods used by organised criminal groups to launder proceeds of crime and the challenges faced by financial intelligence units, law enforcement agencies and prosecutors in investigating ML linked with organised crime groups. The report analyses the main reasons for, and obstacles to, successful prosecution of organised crime groups and those who launder money on their behalf, as well as to final confiscation of the proceeds from organised crime. With a view to assisting relevant authorities, the report sets out possible measures that can be taken to improve the investigation and prosecution of organised crime and support the confiscation of proceeds. Specific typologies and trends are also included, together with red flag and other indicators, for use by FIUs in identifying cases where organised criminal groups might be involved.

31 This report is available on the MONEYVAL website www.coe.int/moneyval.

2.5 The Egmont Group

Global Money Flows in International Mass-Marketing Fraud Project Report

32 The report highlights that mass-marketing fraud (MMF) is a global problem and suggests governments need to work multilaterally to combat this criminal activity. The methods of MMF and its ML components are similar to drug trafficking. MMF scams are perpetrated through mass communications media offshore, usually by a criminal organization, and MMF proceeds are often remitted via different jurisdictions to conceal the source. Criminal organizations involved in MMF recruit “employees” and place them in countries around the world to perpetrate schemes and move the illicit proceeds.

33 The methods used by fraudsters include targeting victims in numerous countries on multiple continents, and using international borders to hinder legislative authorities prohibiting the schemes. Fraudsters can perpetrate their schemes from anywhere in the world, making identification difficult and time consuming.

34 Furthermore, the guilt, shame, and embarrassment often felt by victims in relation to these crimes take a psychological toll. The impact on victims of MMF includes loss of personal savings or homes, physical risks or threats of violence, depression or health issues, and even contemplated, attempted, or actual suicide.

35 The project report includes:

- Indicators of the multiple types of MMF as well as patterns and trends of MMF to help FIUs conduct their analysis of this financial crime; and
- Specific country experiences of MMF and a compendium of MMF cases.

3. TRENDS IN MONEY LAUNDERING & TERRORISM FINANCING

36 This section of the report provides a brief overview of trends in ML and TF including open source information on research conducted by APG member and observers.

3.1 Research or Studies Undertaken on ML/TF Methods and Trends by APG members and observers

AUSTRALIA

37 Individual government agencies within Australia produce a number of different research products on ML/TF methods and trends as follows.

Australian Crime Commission (ACC)

38 *The Organised Crime in Australia 2015 Report* provides a comprehensive overview of serious and organised crime in Australia. The report provides the context in which organised crime operates in Australia and gives an overview of each of the key illicit markets and activities that enable serious and organised crime. The report is intended to provide government, industry and the public with information needed to better respond to the threat of organised crime. The report is available at https://www.crimecommission.gov.au/publications/intelligence-products/organised-crime-australia/organised-crime-australia-2015.

Australian Transaction Reports and Analysis Centre (AUSTRAC)

39 AUSTRAC produces research on current and emerging ML and TF vulnerabilities in Australia. This research is a valuable resource for industry and AUSTRAC's partner agencies as it reveals the diversity and seriousness of organised crime and TF threats facing industry and the wider community. AUSTRAC publishes case studies, strategic analysis briefs and methodology briefs.

40 *Case Studies.* AUSTRAC uses case studies to highlight how criminals are seeking to misuse Australia's financial system, and how AUSTRAC intelligence and analysis products are effectively combating these illicit activities. The case studies also demonstrate the intelligence value of financial transaction and suspicious matter reports AUSTRAC receives from industry, and the important role industry partners play in combating serious and organised crime and TF. AUSTRAC has recently developed an online searchable case studies database available on its website http://www.austrac.gov.au/case-studies.

41 *Strategic Analysis Briefs*. AUSTRAC produces strategic analysis briefs on topics of strategic relevance to the ML/TF risks in Australia. In 2015, AUSTRAC released five briefs. The briefs, which relate to ML methods and trends, are:

- *Money Laundering Through Real Estate Brief.* This brief is designed to provide information about ML methods, vulnerabilities and indicators associated with ML through real estate in Australia. The brief is available on AUSTRAC's website http://www.austrac.gov.au/money-laundering-through-real-estate, and contains 20 indicators that may assist in the identification of potential ML and in-depth discussion of 10 common methods of ML through real estate, as follows:
    - Use of third parties;
    - Use of loans and mortgages;
    - Manipulation of property values;
    - Structuring of cash deposits to buy real estate;
    - Rental income to legitimise illicit funds;

- Purchase of real estate to facilitate other criminal activity;
- Renovations and improvements to property;
- Use of front companies, shell companies, trust and company structures;
- Use of professional facilitators or *gatekeepers*; and
- Overseas-based criminals investing in Australian real estate.

- *Money Laundering Through Legal Practitioners Brief*. This brief is designed to provide information about ML methods, vulnerabilities and indicators associated with ML through legal practitioners in Australia. The brief is available on AUSTRAC's website http://www.austrac.gov.au/money-laundering-through-legal-practitioners, and it contains 15 indicators that may assist to identify potential ML and in-depth discussion of five common methods of ML through legal practitioners, as follows:
  - Use of legal practitioners to conduct transactions;
  - Use of legal practitioners' trust or investment accounts;
  - Use of legal practitioners to recover fictitious debts;
  - Buying and selling real estate; and
  - Establishing corporate structures.

- *Politically Exposed Persons (PEPs), Corruption and Foreign Bribery Brief*. This brief is designed to provide information about ML methods, vulnerabilities and indicators associated with PEPs and laundering the proceeds of corruption including foreign bribery. The brief is available on AUSTRAC's website http://www.austrac.gov.au/peps-corruption-and-foreign-bribery, and it contains 15 indicators that may assist to identify potential ML and in-depth discussion of five common methods of ML through legal practitioners, as follows:
  - Use of corporate vehicles and trusts;
  - Use of third parties;
  - Use of professional facilitators;
  - Use of international funds transfers; and
  - Use of international trade in services payments.

- *Use of Business Express Deposit Boxes to Avoid Reporting Requirements Brief*. This brief is designed to inform reporting entities about the use of business express deposit (BED) boxes and internet banking facilities by serious organised crime groups (SOCGs) to avoid 'know your customer' and ongoing customer due diligence requirements. The brief is available on AUSTRAC's website http://www.austrac.gov.au/use-business-express-deposit-boxes-avoid-reporting-requirements, and it contains five common BED boxes ML methods used by a SOCG and 10 indicators that may assist to identify potential ML, as follows:
  - Accounts opened in company names with foreign nationals on student visas as signatories;
  - Business receiving very large volumes of cash compared to businesses of a similar type, size or location;
  - Frequent bulk cash deposits using BED boxes followed by multiple international funds transfers;
  - Identities of individuals making cash deposits are not established;
  - Account activity inconsistent with customer profile;
  - The customer does not have a legitimate business reason to use BED boxes;
  - Numerous deposits occurring each day at a number of different bank branches;
  - Deposits occurring in a different state to where the accounts are held;
  - There is no building located at the business or residential address provided by the customer (for example, as checked on Google Maps); and

- International funds transfers from business account are not related to the actual payment of goods or services for the business.

42 *Bank De-Risking of Remittance Businesses Brief.* This brief is designed to provide information on bank de-risking in the Asia/Pacific region including:

- Remittance sector in Australia;
- Remittance sector access to banking services;
- Impact of bank de-risking on remittance network providers;
- Impact of bank de-risking on international funds flows through the remittance sector; and
- Case studies relating to the Pacific, Asia and Africa.

43 This brief is available from http://www.austrac.gov.au/bank-de-risking-remittance-businesses.

44 *Methodology Brief*. In 2015 AUSTRAC published a methodology brief on *Financial Characteristics Associated with Known Foreign Terrorist Fighters and Supporters*. The brief is designed to assist industry in identifying behaviours of foreign terrorist fighters and their supporters. The brief includes key indicators and guidance on suspicious matter reporting. The brief is available at http://www.austrac.gov.au/building-profile-financial-characteristics-associated-known-ftf-fts.

CANADA

45 In July 2015, Canada published *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. The report can be accessed at http://www.fin.gc.ca/pub/mltf-rpcfat/index-eng.asp

46 In June 2015, Canada published *Terrorist Financing in Canada and Abroad: Needed Federal Actions.* This report sets out the findings of a study into the costs, economic impact, frequency and best practices to address the issue of terrorist financing both in Canada and abroad. Chapter two of this report identifies terrorism and terrorist financing costs, sources of revenue and methods to transfer funds. The report is available at http://www.parl.gc.ca/HousePublications/Publication.aspx?DocId=8048561&Language=E&Mode=1&Parl=41&Ses=2&File=9

47 In May 2015, Canada published *National Action Plan to Combat Human Trafficking - 2013-2014 Annual Report on Progress*. This is the second annual report on implementation progress of *Canada's National Action Plan to Combat Human Trafficking* (National Action Plan), which was launched on June 6, 2012. The report is available at https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/2014-ntnl-ctn-pln-cmbt-hmn/index-en.aspx

48 In May 2015, FINTRAC issued an advisory to reporting entities on terrorist financing indicators.

CHINA

49 Since 2014, the People's Bank of China has issued the *Notice on further strengthening financial institutions counter-terrorism work*, the *Notice on strengthening the work related to financing of terrorism transaction monitoring* and other regulations, to strengthen CFT efforts. In addition, investigations have been undertaken on major banking institutions' CFT work in order to actively explore effective preventive measures related to the financing of terrorism transaction monitoring and to study and establish monitoring and analysis models of transactions involving financing of terrorism.

FIJI

50 The Fiji Financial Intelligence Unit *2014 Annual Report*, which was published in July 2015, includes analysis of suspicious transaction reports and a major case study on a successfully prosecuted ML case in Fiji. The report also included discussion of emerging, continuing and declining money laundering trends. A copy of this report is available at http://www.fijifiu.gov.fj

FRANCE

51 France produces a number of reports on ML and TF trends and case studies which are available in English. These include the following:

- Annual activity report 2014
  http://www.economie.gouv.fr/files/rapport_tracfin2014_tome1_en.pdf
- ML/TF risk, trends and analysis 2014
  http://www.economie.gouv.fr/files/rapport_tracfin2014_tome2_en.pdf

KOREA

52 In 2015, Korea FIU published the *Money Laundering Trends Review*, which was provided to law enforcement agencies and institutions. This report provides an explanation of the amendments and policy direction of Korea's AML/CFT laws, comparison of the Information Analysis Office's 2015 analysis with previous years, and information on how STRs were analysed in 2015.

MONGOLIA

53 Mongolian authorities note the publication of recent research on ML of human trafficking proceeds and comparative study of different organized crime groups from China, Russia, and the Balkans. The citation of this research is Enkhchimeg Sengee *Unique Features of Different Nationalities of Transnational Organized Crime Groups, Especially Human Trafficking, and Their Money Laundering Methods* (in Mongolian), Criminology Journal, 2014.No.3 (49). The publication is available from http://criminology.mn/index.php?option=newsm&id=202&lang=1

NEW ZEALAND

54 The New Zealand FIU publishes quarterly typology reports which are available at http://www.police.govt.nz/about-us/publication/fiu-assessments-reports. The last three reports are:

- *Quarterly Typology Report Fourth Quarter (Q4) 2014/2015*, which includes an in-depth examination of ML methods, vulnerabilities and indicators associated with the real estate sector, including five cases studies;
- *Quarterly Typology Report First Quarter (Q1) 2015/2016*, which includes an in-depth examination of ML methods, vulnerabilities and indicators associated with Capital Markets, including six domestic and international case studies; and
- *Quarterly Typology Report Second Quarter (Q2) 2015/2016*, which includes an in-depth examination of TF methods, vulnerabilities and indicators, including one domestic and three international case studies.

THAILAND

55 Thailand's Anti-Money Laundering Office (AMLO) produces monthly reports on STRs to highlight current ML/TF trends. The latest report shows the four most commonly filed STRs which relate to: (i) transaction not consistent with customer profile, (ii) smurfing, (iii) criminal conduct related to the news or lists of persons whose information is requested, and (iv) irregularly frequent asset transactions. The reports are disseminated to relevant internal authorities and are not available for distribution externally.

3.2 Association of Types of ML or TF with Predicate Activities

AUSTRALIA

56 In Australia, numerous crime types can be identified with links to ML activity. These typically include:

- Illicit drug importations;
- Importations of prohibited goods;
- Identity theft and/or fraud;
- Visa fraud; and
- Revenue evasion.

57 Many of the above crimes are conducted by organised crime groups. AUSTRAC (Australian FIU) participates in a number of multi-agency taskforces aimed at combating serious national crime including drug importation, outlaw motor cycle gangs, ML and fraud. Two examples of AUSTRAC's contribution to multi-agency task forces include the Serious Financial Crime Task Force and the Eligo 2 National Task Force.

58 *Serious Financial Crime Task Force*. The Australian Serious Financial Crime Task Force targets serious and financial crimes including fraud, manipulation of the stock market and ML. The task force combines the intelligence and specialist capabilities of eight Commonwealth agencies including the Australian Taxation Office (ATO), the Australian Federal Police (AFP), the Australian Crime Commission (ACC), the federal Attorney-General's Department, the Commonwealth Director of Public Prosecutions, the Australian Securities and Investments Commission, the Australian Border Force, and AUSTRAC.

59 Key operational priorities for the task force include investigations into serious international tax evasion and criminality related to trusts and 'phoenix' activity (when companies deliberately and repeatedly liquidate to avoid paying creditors, employee entitlements and taxes).The task force works closely with international partner agencies, governments and organisations around the world to remove wealth from criminal activity, prosecute facilitators and promoters of serious financial crime and deploy deterrent and preventative enforcement strategies.

60 *Eligo 2 National Task Force*. The Eligo 2 National Task Force was established in December 2012 to address criminal vulnerabilities and the potential for exploitation by Serious and Organised Crime (SOC) within the Alternative Remittance Sector (ARS). The principal objective of Eligo 2 is to take coordinated collective action against money launderers. The task force consists of members of the ACC, AUSTRAC, the AFP, and the ATO, with additional support from State and Territory law enforcement agencies.

FIJI

61 Examples of methods of ML through financial institutions in Fiji include significant cash deposits detected in personal bank accounts linked to possible fraud, corruption and tax evasion.

62 Fiji does not have any incident or report on TF cases; however there have been reports of a foreign businessman remitting business funds from Fiji to individuals in a high risk country.

LAO PDR

63 Cases identified relate to the following predicate offences: illicit trafficking in narcotic drugs, corruption, counterfeiting currency, illegal logging, illicit trafficking of war arms and explosives, human trafficking, robbery, and hostage taking.

MONGOLIA

64 In Mongolia, 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 including arms; and
- Drugs and psychotropic substance trafficking.

NEPAL

65 Tax evasion, foreign exchange abuse, hundi and corruption are the major predicate offences associated with ML in Nepal. Nepal is also investigating a TF case.

PAKISTAN

66 Suspicious transaction reports received relate to terrorism, including TF, illicit trafficking in narcotic drugs, corruption and bribery/unexplained assets, fraud, smuggling, extortion, hawala/hundi, illegal trade in financial instruments, grey telephony and virtual currencies.

THAILAND

67 Insurgency groups in southern Thailand source their funds from several activities, including goods smuggling, drug trafficking and illegal oil trade. In an effort to block the funds, the Excise Department, Royal Thai Police and the military have launched a joint operational campaign to suppress the illegal oil trade.

3.3 Emerging Trends; Declining Trends; Continuing Trends

AUSTRALIA

68 As identified above, AUSTRAC has released four analysis briefs and one methodology brief on various topics relating to ML trends and TF. These can be considered emerging or continuing trends and include:

- ML through real estate;
- ML through legal practitioners;
- Politically exposed persons, corruption and foreign bribery;
- Use of business express deposit boxes to avoid reporting requirements; and
- Financing of foreign terrorist fighters and supporters.

BRUNEI DARUSSALAM

69 In Brunei Darussalam there is a continuing trend of predicate offences associated with unlicensed financial activity and the smuggling of contraband goods. In addition, the FIU notes a continuing trend of scams conducted from neighbouring countries involving local victims.

CHINA

70 In 2014, based on monitoring and analysis, China's FIU, the China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) provided 282 suspicious transaction reports (STRs) and 135 suspicious transaction leads to law enforcement. Among the 282 STRs, according to the categories of ML offences and predicate offences defined by Criminal Law, 245 related to unlawful activities such as underground banking, internet gambling, multi-level marketing, 25 related to crimes of disturbing financial administrative order, 14 required further investigation, seven related to drug crimes, six related to terrorist activities, six were connected with PEPs, four related to smuggling, and

one related to fraud concerning raising funds (some STRs are connected with several categories of offences).

FIJI

71 The FIU has identified the following emerging, declining and continuing trends:

- *Emerging trends:* large telegraphic transfers from foreign nationals offshore to recently opened local bank accounts and subsequent investment in real estate and income/business tax fraud.
- *Declining trends:* use of minors' accounts and currency smuggling.
- *Continuing trends:* advance fee fraud.

FRANCE

72 France has identified the following STR trends:

- The banking sector remains the leading source of STRs with 86% of total financial sector STRs submitted by the banking sector. The sector's involvement in AML/CFT efforts increased by nearly 35% in 2014.
- Insurance sector: overall the percentage of total financial sector STRs submitted by the insurance sector (insurance companies, insurance intermediaries, mutual insurance companies and benefits institutions) fell slightly in 2014 to 4.7% (4.9% in 2013). Insurance companies continue to lead the insurance sector in terms of STRs submitted with 1,423 STRs submitted in 2014. Insurance intermediaries' submissions, which are historically low, increased to 43 STRs in 2014 (25 in 2013). There was another sharp increase in submissions by mutual insurance companies with 139 STRs submitted in 2014 compared with 60 in 2013.
- Within the financial professions there was a steep increase in the reporting flow from banks and payment institutions. However, reporting by money changers is low; over the last three years less than half of the reporting entities registered with Tracfin (France FIU) have submitted an STR.
- The reporting flow of non-financial entities subject to reporting obligations has doubled in the last two years.
- The number of STRs submitted in 2014 by the casino sector must increase. The FIU received twice the volume of STRs relating to alleged ML through gambling than the number received from gambling sector reporting entities alone.
- Of the sectors considered to be high risk by the reporting entities, labour intensive sectors with a high business turnover rate continue to account for a large share of STRs. The increase in reports regarding the logistics and transport, and medical and paramedical sectors, already noted in previous years, continued this year. There has also been a rise in reports relating to the industrial sector, in areas such as trafficking in metals and waste recycling and management.
- While the number of legal entities reported compared with the number of natural persons reported was around one fifth, a ratio which is down slightly versus 2014, the ratio of legal entities to subject to disclosures was around one third. This observation is proof of the effectiveness of the FIU's investigations, which led to the identification of 30% more legal entities, some of which should have been reported to Tracfin, a fact that it would like to draw reporting entities' attention to.
- The average amounts per STR, which may cover several transactions over highly varied time periods, were under €500,000 (~USD570,000) in 85% of cases. The anti-money laundering system monitoring indicators, which show that the distribution of STRs by range of amounts, has been relatively stable in recent years, show that in 2014 STRs concerning amounts under €100,000 (~USD114,000) grew more than the flow as a whole. However, these reported amounts should not be taken at face value, as the reporting entity is rarely aware of the entire scope of the financial transaction.

- Out of all of the transactions reported, while cash transactions, transfers and cheques remain the most commonly reported payment methods, the first two methods experienced the most growth in 2014.
- In 2014 STRs relating to financial flows using digital currencies did not maintain their growth of previous years. The anonymity that surrounds some digital currency instruments creates a particular risk, which is increased by the fact that there is nothing guaranteeing that a prepaid card's buyer will be its final user, as the payment instrument is linked to the holder.
- STRs relating to attempts to reduce wealth tax or repatriate undeclared foreign assets rose in 2014. Around a fifth of Tracfin's referrals to the tax authorities in 2014 concerned accounts held abroad and attempts to repatriate undeclared foreign assets. Reports regarding the operating of an undeclared, or under-declared, professional activity, remain significant. The rise in the intermediate VAT rate applicable to renovation works has probably also helped to keep the reporting level high.
- Since 2009, Tracfin has noted an increase in the use of cash in the shadow economy, which showed no sign of decreasing; between a quarter and a third of the STRs received by Tracfin involved cash withdrawals and/or deposits. Like the reporting flow as a whole, reports relating to cash deposits and withdrawals rose by more than a third between 2013 and 2014. STRs on gambling involving cash transactions grew particularly strongly over the same period. These STRs refer, for example, to cash withdrawals from bank accounts in which gambling winnings are deposited, and which are held by individuals linked to companies operating in labour intensive sectors.
- More generally speaking, transactions may be conducted in cash so that companies or individuals can avoid paying various forms of tax, or criminals can inject this cash into the financial system. The STRs received by Tracfin show, when analysed, the role played by cash as a channel for tax fraud, for example by reducing a company's revenue, through withdrawals for a lower wealth tax base or undeclared donations. They also reveal how cash is used in social security fraud, in practices such as the payment of wages to undeclared workers.
- Cash, and especially small denomination notes, are the main form in which funds of illegal origin are generated. These funds can be manipulated and transported more easily following conversion into large denomination notes, confirming the use of the €500 note in illicit financial flows. Notes with a high face value are used by organised criminal groups both as stores of value and as a means of paying for assets. Large denomination notes make it easier to move cash around in large-scale ML schemes. Such notes may also be requested in connection with financial activities that are legal but are fraudulent in tax terms, as €500 notes can be easily transported to offshore financial centres, for example, to be integrated into the financial system through tax evasion schemes.
- The many different types of gaming and the high rates of return naturally attract those who wish to recycle money from dubious sources into the legal economy. There was an across-the-board increase in the number of STRs received by the FIU from the gaming sector, an increase that was particularly high in the area of online gaming. In 2014, submissions by online gaming operators reached 450, compared with 181 in 2013

INDIA

73 India has identified the following trends related to TF.

74 *Emerging trends:* self-funding; abuse of charities for terrorist financing; utilization of proceeds of terrorism to purchase/acquire land, flats and vehicles for terrorist organizations; and use of money transfer services by terrorist organizations for funding.

75 *Declining trends:* use of legitimate banking channel for financing of terrorist activities.

76 *Continuing trends:* use of counterfeit currency and proceeds of counterfeit currency for funding of terrorism; extortion by extremists from local transporters, general public, government officials, businessmen, professionals and civilians to fund terror activities; smuggling and trafficking counterfeit currency along with drugs and weapons through international border; involvement of public servants and contractors in misappropriation of Govt. funds and their criminal misconduct, which facilitates the funding of terrorist activities; use of formal and non-formal banking channels, trade based routes, cash couriers by trusts acting as frontal organization for terrorist groups; transactions without national boundaries; widespread use of Hawala for movement of terror funds; and widespread transactions involving inconspicuous sums.

JAPAN

77 Japan has identified the following continuing trends:

- Fraud and theft are common predicate offences;
- The illicit sale of drugs is also common; and
- Phishing and computer viruses continue to be used to steal IDs and passwords of internet banking, credit cards etc. These IDs or passwords are used to transfer money and purchase merchandise.

78 Furthermore in Japan 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. This is a major technique used in ML crimes. For example, a male company employee made an acquaintance an offer to purchase bank passbooks, and purchased for JPY 40,000 (~USD365.00) multiple passbooks that the acquaintance defrauded from financial institutions. As a result, the company employee was arrested for purchasing stolen goods with compensation and violating the Act on Punishment of Organized Crimes (receiving of criminal proceeds).

LAO PDR

79 Lao, PDR has identified that the illicit trafficking in narcotic drugs and human trafficking have increased in 2015 by 35% and 41%, respectively, and illegal logging has decreased by 60%.

MACAO, CHINA

80 During the period January to June 2015, a total of 910 STRs were received by the financial intelligence unit, with 75% of STRs from the gaming sector, 24% from the financial sector (including banking, insurance and financial intermediaries) and 1% from other sectors.

81 Common ML methods detected from STRs received are as follows:

- Chips conversion without/with minimal gambling activities;
- Chips conversion/marker redemption on behalf of a third party;
- Irregular large cash withdrawals;
- Suspicious wire transfer;
- Use of cheques/promissory notes/account transfer to transfer funds;
- Suspected underground banking/alternative remittance services;
- Significant cash deposit with non-verifiable source of funds;
- Unable to provide ID/important personal information;
- Suspected PEP related transaction; and
- Use of ATM, phone banking, cash deposit machines.

82 From January to June 2015, 60 STRs were disseminated to the Public Prosecutions Office. These cases were mainly related to fraud and encashment with the use of debit cards. The Judiciary

Police processed 143 investigations which were mainly related to use of debit cards and cross-border cash smuggling. Some of the suspicious cases found are related to a few individuals using numerous different valid credit/debit cards to withdraw cash from ATMs. Moreover, there is also a trend of using third parties' bank accounts for transfers of illicit fraud proceeds across different jurisdictions.

MALAYSIA

83 Analysis of STRs revealed that geographically, for the banking sector, 72% of STRs were submitted by branches operating in areas identified to be of high risk as follows:

- Crime hot spots as identified by the police, which are mostly main cities or town of various states.
- Border towns near with neighbouring jurisdictions.

84 Based on STRs submitted to FIU in 2014, the top three suspected offences are tax-related, fraud offences including internet scams/wire transfer fraud, and smuggling offences.

85 The continuous trends identified from the STR analysis include the following:

- Increasing trends with regards to internet/wire transfer fraud with the following characteristics:
    - Active inward remittance transactions received from various overseas entities on a continuous basis without valid justification;
    - Funds received would be withdrawn nearly in full amount on an immediate basis via the ATM and over the counter, leaving a minimal balance in the account, an action undertaken to avoid further monetary trails against the subject; and
    - Profile of the sender and recipient seemed to be ambiguous and no relationship can be established.
- Usage of transit accounts (mule accounts) with large, rapid movement of funds:
    - Funds were actively transferred in and out of the account on the same day or within a short period of time with no absolute reason; and
    - Immediate withdrawals upon receiving large amount of funds.
- Unverified banking transactions:
    - Abnormal deposits and withdrawals which are deemed inconsistent with the profile of the customer;
    - Large number of transactions conducted near border towns, ports and high risk areas where smuggling activities are rampant; and
    - Large amounts of funds transferred into unverified third parties accounts located overseas on a frequent basis.

MARSHALL ISLANDS

86 Inquiries regarding suspected ML offences were received by the FIU from the Egmont Group of Financial Intelligence Units as well as INTERPOL via the Marshall Islands Police Department. Without exception, all inquiries related to non-resident corporations registered with the Marshall Islands trust company providers. These inquiries demonstrate that certain non-resident corporations operating in high risk jurisdictions are using Marshall Islands trust company providers to facilitate ML schemes.

MONGOLIA

87 Mongolia has identified the following trends:

- *Emerging trends:* sale of drugs and psychotropic substances, especially ice; credit card fraud; new technology, including fraud and embezzlement of assets through disrupting online payments during online shopping or online settlements.

- *Continuing trends:* association of ML with corruption, embezzlement and bribery of state funds; real estate – purchase of valuable assets in foreign countries, especially luxury houses, apartment, vehicles in foreign jurisdictions; ML through establishing legal entity and building a service sector real estate in Mongolia; trade-related ML through invoice manipulation, trade mispricing in the purchase of goods from abroad, either through legal persons or state institutions responsible for public procurement; use of gatekeepers/professional services: accountants, bankers, legal entities, and company service providers; use of shell companies; wire transfers; use of credit cards; use of offshore banks/companies; use of family members, third parties; identity fraud-use of false identification; and use of foreign bank accounts.

88 According to the Police, a new trend is that company service providers seem to open legal entities under the names of their relatives and friends with the purpose to conceal and launder illegally obtained assets.

NEPAL

89 In Nepal, identified trends are physical cash transfers, wire transfers, foreign exchange embezzlement, and an emerging trend is misuse of ATMs.

THAILAND

90 Thailand has identified the following trends:

- *Emerging trends:* use of nominee to hold asset or accounts, especially by corrupt politicians, and religious schools producing false documents to gain financial support from the government.
- *Declining trends:* smurfing has declined because money launderers now know that authorities are monitoring these types of transactions;
- *Continuing trends:* buying precious metal or stone and real estate.

3.4 Criminal knowledge of and response to law enforcement / regulations

AUSTRALIA

91 Like in other parts of the world, organised crime groups (OCGs) in Australia are sophisticated and profit driven. It is highly likely they have a thorough understanding of the regulatory framework and law enforcement practices, including techniques used by law enforcement. Given OCGs' understanding of the regulatory framework, low risk predicate offences are likely to appeal to certain OCGs and it is likely some groups will pursue these options in order to avoid prosecution. The following case illustrates how criminal knowledge of regulations was used to obscure drug trafficking.

Drug trafficking, Money laundering and Identity Fraud Case

A suspect used false identification to lease a number of privately owned mailboxes. Drugs were imported into Australia in letters and packages, addressed to false identities at these mailboxes.

AUSTRAC (Australia FIU) analysis revealed that the suspect used multiple aliases to transfer funds overseas, via remittance service providers, with correlations between these money transfers and drug importations.

Suspicious matter reports (SMRs) from remittance service providers revealed that the suspect made multiple International Funds Transfer Instructions (IFTIs), paid for in cash amounts below the 10,000 Australian dollar threshold for transaction reporting. This MLtechnique is used in an attempt to prevent the transfers attracting scrutiny from authorities.

The suspect was sentenced to 10 years and six months imprisonment with a total non-parole period of six years and 10 months.

The full version of this case study is available on the AUSTRAC case studies hub http://www.austrac.gov.au/case-studies/international-drug-importation-scheme-cracked-trafficker-convicted

CHINA

92 China highlights that new types of financial services including third-party payment and online banking systems can be taken advantage of by the criminal suspects. The third-party payment can split the funds chain while online banking enables people to make quick transfers of funds and control the accounts of other people conveniently. With the lack of face-to-face communication for online banking services, it is hard for the financial institution to conduct customer identification.

93 Third-party payment systems bring convenience to customers, but also provide criminals with more opportunities and make AML funds monitoring challenging. The supervision and regulatory authorities should actively pay attention to the development and changes of the new types of financial services and make necessary and timely adjustments to regulatory policies to improve the capability of management and control and prevent the risk of crimes.

94 Moreover, it is necessary and important to strengthen law-enforcement cooperation among various agencies, and research mechanisms between the FIU and the public security authorities as well as to enhance intelligence exchange and information feedback among different agencies.

4. CASE STUDIES OF ML AND TF

4.1 Association with corruption (corruption facilitating ML or TF)

CANADA

95 In December 2014, an individual pleaded guilty to two counts of ML in connection with the laundering of bribes paid to assist a large Canadian engineering firm to secure a public contract to build a new hospital. The Crown confiscated CAD5.5 million (~USD 4.2 million) in property and a small amount of cash from the individual. Sentencing in this case is pending.

CHINA

96 When investigating the case of person K involving bribery in March 2014, the People's Procuratorate of Yongchun County, Quanzhou, Fujian Province suspected his relative, person L, of ML. In December 2014, the People's Court of Yongchun County convicted person L for ML. Person L was sentenced to 6 months' imprisonment and a fine of RMB 20,000 (~USD3,000).

97 *Case details.* Person L, a local farmer, was K's brother in law. In 2013, K took the position as head of management station of agricultural machinery of Yongchun County. Person K received bribes of RMB 200,800 (~USD31,000) from an agricultural machinery company. Under the instruction of person K , L transferred bribe money to the value of RMB 160,000 (~USD25,000) and also lent money to others in order to register companies. Loan repayments were then made into person L's bank account. In February 2014, person L transferred RMB 198,000 (~USD30,500) to an automobile sales & service company in Xiamen and provided his identification for the purchase of a car for person K.

FIJI

98 Fiji FIU received a STR on person X, an employee of a government department. Person X was reported for making large deposits of government cheques into his personal bank account. Fiji FIU established that person X falsified three government cheques totalling FJ$57,000 (~USD27,600) over a period of four months. The cheques issued were supposedly for payments to an overseas supplier but the payee details were altered so that the funds were deposited into person X's bank account. The case was disseminated to the Fijian Anti-Corruption Agency. Person X was charged with two counts of abuse of office, one count of falsification of documents and one count of obtaining financial advantage. The matter is currently under trial.

INDIA

99 There are a number of cases registered under the Prevention of Money Laundering Act 2002, where corruption is a predicate offence. In one case the accused, who was a public servant, had amassed a huge sum of money through criminal misconduct. He had adopted a novel modus-operandi to launder black money. He gave black money to certain operators in the market and arranged cheques/RTGS credits favouring entities under his control. The payments received were shown as investments in equity shares and the shares were issued at high premium.

KOREA

100 *Case 1.* The joint government investigation team for defense industry corruption, arrested former Minister of Patriots and Veterans Affairs on the charge of accepting bribes in relation to the procurement of AW159, maritime helicopters.

101 The former minister was suspected of accepting USD 1.2 million in bribes in exchange for exerting his influence on the procurement of the helicopters. The former minister claimed that he

made a legitimate contract with AW for an advisory role and provided consulting services to help AW enter into the Korea's defence industry. However, the court did not accept this argument, and investigations into the procurement of the helicopters are on-going.

MONGOLIA

102 There was a case which involved a head of a branch office of one of the well-known Mongolian banks involved in conspiracy to launder money derived from embezzlement of funds of a state-owned aviation company in Mongolia.

PAKISTAN

103 During a bank's ongoing review of an account holder, who declared himself as a landlord, it was noticed that funds aggregating to PKR 8.6 Million (~USD82,000) were credited in his account through online transfers in a month. Subsequently a sum of PKR 3.2 Million (~USD30,500) was withdrawn from the account without disclosing the purpose. Moreover, structured cash withdrawals were also observed in the account. On a query by the bank, the customer was reluctant to disclose the sources of funds credited in the account or to provide any documentary evidence to substantiate the credits/debits in the account.

104 During analysis, it was observed that the suspect had also previously served as a provincial legislator. The suspect's account was credited with high value funds through online transfers. The funds were then withdrawn through cash and clearing. Average monthly turnover in the account was PKR 2.08 Million (~USD20,000). During the period of 2.5 years PKR 56.22 Million (~USD537,000) was deposited in the account while PKR 54.88 Million (~USD 524,000) was withdrawn. Most of the funds were transferred from the account of an individual maintaining account in a branch situated in an area adjacent to the suspect's constituency.

105 Due to the high volume of funds credited in the personal account, it was suspected that he might be involved in abusing his authority as a legislator. Therefore, the financial intelligence was shared with LEAs for investigation in the matter.

PHILIPPINES

106 *Large-scale corruption through the use of Non-Government Organizations (NGOs), Dummy Corporations and Foreign Exchange Dealers.* This ML case is based on one of the biggest corruption cases in recent Philippine history. It stemmed from complaints filed by the National Bureau of Investigation (NBI) for plunder, malversation, direct bribery, and graft and corrupt practices act before the Office of the Ombudsman (Ombudsman) related to the use of the legislators' Priority Development Assistance Fund (PDAF) allocation.

107 The PDAF, popularly called "pork barrel", is well-entrenched in Philippine political history and often used as a means to generate majority legislative support for the programs of the executive. Since the 1920s, it has been a lump-sum discretionary fund granted to each member of Congress for spending on priority development projects of the Philippine government, mostly at the local level. Every member of the House of Representatives usually receives an annual PDAF allocation of Php70 million (~USD1.5 million), while every Senator receives an annual allocation of Php200 million (~USD4.4 million).

108 The PDAF scam, also called the pork barrel scam, is the alleged misuse of the PDAFs of several members of the Congress. The scam involved the funding of agricultural "ghost projects" using the PDAF of participating lawmakers. These agricultural projects were primarily concocted by person N and purportedly implemented through her companies, with the projects producing no tangible output. Funds would be processed through fake foundations and NGOs established under the wing of the person N's Group of Companies (holding company of person N), with her employees named as incorporators or directors. Each foundation or NGO served as an official recipient of a

particular legislator's PDAF, and each organization had a number of bank accounts where PDAF funds would be deposited for the supposed implementation of these projects. The funds would then be withdrawn by person N's employees and eventually split among person N, the lawmaker, the official of the implementing agencies responsible for facilitating the transfer of funds and the local mayor or governor. Person N's Group of Companies received a commission of 10-15% against funds released to local government units and recipient agencies of PDAF, while a legislator would receive a commission of between 40-60% against the total value of his/her PDAF.

109 Some of person N's employees eventually became whistle-blowers, agreeing to expose the scam and testify against Ms. N. They alleged that the legislators who were complicit in the scam were usually paid in cash, through their Chiefs of Staff or other representatives.

110 As a result of the discovery of this scam, plunder and corruption charges were filed against person N, her employees, officials of the implementing agencies and lawmakers, including three prominent Senators.

111 Financial investigation conducted by the Anti-Money Laundering Council (AMLC) showed, among others, that for one of the Senators, cash deposits were made to his various bank accounts and investments from 2006 to 2010 totalling more than PhP87.6 million (~USD1.95 million) within 30 days from the dates they allegedly received commissions from their PDAF in cash. During the same period, cash deposits totalling more than PhP27.7 million (~USD615,000) were also made to NCDR Corporation, a company owned and controlled by the Senator's wife which apparently had no operations as it did not file financial statements with the Philippine Securities and Exchange Commission (SEC).

112 In relation to the funds received by person N from the scam, investigation revealed that aside from the use of bank deposits, investments in variable-life insurance policies, prime real estate properties and expensive motor vehicles, person N also laundered the funds by using two money changers, to remit more than USD5.26 million to Country S in favour of two companies owned by her daughter and brother.

113 In August and November 2013, the Court of Appeals granted the Petitions filed by the AMLC for the Issuance of Freeze Orders against the bank accounts, investments, real properties and motor vehicles of person N, her companies and employees. In 2014, the AMLC filed Petitions for Civil Forfeiture before the Regional Trial Court (RTC) in Manila against the said properties. The said Petitions led to the issuance of Asset Preservation Orders to cover the following:

- Peso funds and investments totalling more than PhP155 million (~USD3.4 million);
- USD bank accounts totalling approximately USD697,000;
- 47 real properties; and
- 16 motor vehicles.

114 In addition, AMLC Secretariat investigators have been called as expert witnesses in proving the plunder and corruption cases filed against the three Senators involved in the scam.

HONG KONG, CHINA

115 Arising from a corruption investigation, it was revealed that between October 2011 and February 2012, the proprietor of a trading company applied to a bank for six import invoice financing loans totalling HK$3.3 million (~USD425,000). To support the loan applications, the proprietor of the trading company submitted to the bank bogus delivery notes and invoices issued by the sole director and shareholder of a diamond company, who was also a merchandiser of the trading company. The bogus delivery notes and invoices purportedly showed that the diamond company had sold and delivered various merchandises to the trading company. As a result, the bank approved the loan applications and transferred a total of over HK$3.3 million (~USD425,000) to the bank account of the diamond company to settle the invoices. Upon receipt of the loan proceeds, the funds were reverted

by the diamond company to the trading company. The diamond company withdrew monies from its bank account and paid the proprietor of the trading company either in cash or funds transfer to the bank accounts of the trading company and another related company. The proprietor of the trading company pleaded guilty to six counts of fraud and was sentenced to 28 months' imprisonment. The merchandiser was convicted of ML and sentenced to 20 months imprisonment.

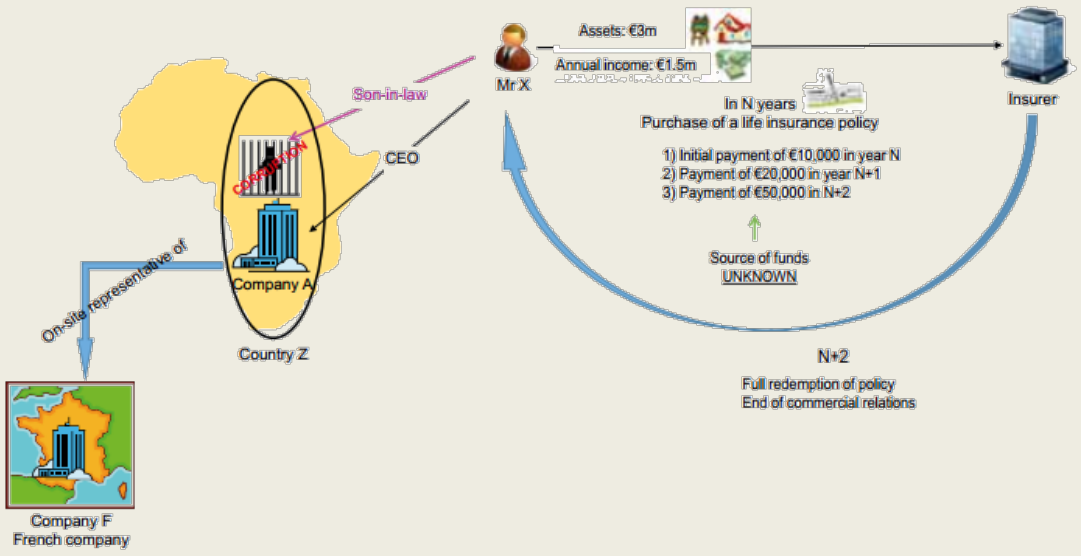
4.2 Laundering proceeds from corruption

FIJI

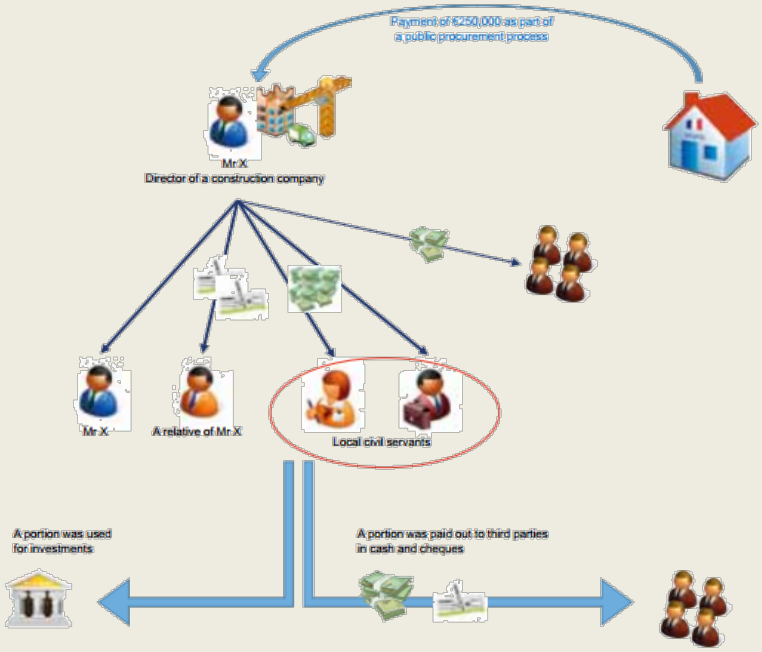
116 Fiji FIU received a request from a law enforcement agency to conduct financial background checks on an individual who was employed by a statutory body. Person X was alleged to have received a loan of FJD4,000 (~USD2,000) and a motor vehicle amounting to FJD30,000 (~USD15,000) as a bribe from person Y who was a car dealer. It was alleged that the bribe was to assist person Y's company/business obtain certain concessions from the statutory body. FIU information was released to the local law enforcement agency. Person X and person Y have been charged for bribery and official corruption.

FRANCE

117 *Life insurance sector – Suspected laundering of the proceeds of corruption.* Mr X, a non-European resident, was CEO of Company A, registered in non-European jurisdiction Z, and representative of Company F, with headquarters in France. According to his tax returns, Mr X had annual earnings of more than €1.5 million (~USD1.6 million), with assets estimated at more than €3 million (~USD3.3 million). He took out a life insurance policy and made an initial payment of €10,000 (~USD11,200). Subsequently, over a two-year period, he made two additional payments of €20,000 (~USD22,500) and €50,000 (~USD56,300). The money came from Mr X's earnings and dividends – the client provided no documentation. At the end of the second year, the client fully redeemed his policy (€80,000). The insurance company observed that Mr X's transactions took place within a specific context. As it turned out, an article in the international press stated that Mr X and Company A were involved in a corruption case involving jurisdiction Z. According to the intelligence collected, Mr X was the son-in-law of a former finance minister for Country Z who had been jailed several years earlier for corruption. Company A was a shell company that served as an intermediary between the French Company F and the non-European country for manufacturing machines to cancel tax stamps.



118 *Case involving the misuse of company assets, corruption and influence peddling as part of a public procurement process*. Tracfin (France FIU) analysed a series of unusual transactions in connection with the bank accounts of a specialised construction firm that submitted bids for public procurement contracts. Within a six-month period, the company had received more than €250,000 (~USD281,500) from a local authority. The investigation revealed that the company's director, Mr. X was related to the local official at the head of the municipal council that was the source of the suspicious transfers. Concurrent with the transfers, the director withdrew cash, issued cheques and made bank transfers to individuals, some of whom exercise activities that were hardly compatible with the public works in question. Most of the cheques were deposited by the director, a member of his family and two local civil servants. The suspicious outflows totalled more than €210,000 (~USD236,500). The beneficiaries of these amounts then made investments, withdrew cash or wrote cheques to third parties. To justify the receipt of public monies, the director of the beneficiary company submitted various documents concerning the award of a public contract. These documents, however, contained inconsistencies, such as mismatches between the payment instalments and the corresponding invoices, and a payment made prior to the issuance of the corresponding accounting document. The case was handed over to the judicial authorities. The FIU underscored its persistent doubts about the awarding of the contract and its financing conditions, as well as the subsequent financial transactions carried out by the director of the beneficiary company.



INDIA

119 In one case, Government funds meant for a specified community were siphoned by a public servant by misusing his official position. These funds were used for personal gain and immoveable properties were acquired.

KOREA

120 Person J who is a former representative of the Anti -Financial Speculation Center is suspected of accepting hundreds of millions of Won from the former CEO of LS Funds Korea who was accused of stock market manipulation.

121 The charge that the Public Prosecutors' Office (PPO) is investigating is breach of trust and bribery. The PPO believes that person J submitted documents in favor of the former CEO to the court after receiving hundreds of millions Won when the ex-CEO was on trial on the charge of stock market

manipulation. The PPO assumes that person J is guilty of breach of trust and bribery by soliciting special favors and receiving money in violation of his duty as the head of a watchdog group.

MONGOLIA

122 Laundering proceeds from corruption remains a substantial problem in Mongolia. These tend to be grand corruption cases involving current or former state officials at senior or decision making levels of the government or state-owned enterprises. Suspects tend to conceal their illegally derived money in banks overseas, and seem to purchase properties in foreign countries. Therefore, obtaining evidence and documents from abroad through mutual legal assistance remains a vital step to successfully trace stolen assets, and eventually convict the case.

PAKISTAN

123 *ML by a Government Official laundered through an integrated scheme involving winning prize bonds, Term Deposit Receipts, Running Finance Facility, and Asset Acquisition.* Person A, a Government Official, opened a savings account in XYZ Bank in 2015. Two high value transfers were made by the suspect from his own account maintained in PQR Bank, out of which half of the amount was placed Term Deposit Receipts (TDRs). Later on, the suspect received prize money which was cleared via cheque and also placed in TDR. The prize money remained invested in TDRs for five months.

124 The suspect also got a Running Finance facility (loan) from XYZ Bank against security of term deposits. The suspect was issued a high value demand draft in favour of person D from his running financing facility. After 10 months of utilizing running financing facility, the entire bank's loan liability was paid off in one go through liquidation of TDRs.

125 This appeared a typical ML arrangement for routing of apparently illegitimate funds through acquisition of winning prize bonds, investing in TDRs, seeking running finance facility, and asset acquisition. The illegitimate funds were suspected to be kickbacks or embezzled public funds, since the suspect was holding a government office entrusted with district management powers. The suspicious transaction was shared with LEA for further proceedings.

THAILAND

126 A high ranking police officer and his associates committed the following:

- Demanded and received bribes, ranging from 3 to 5 million baht (~USD85,000 to ~USD142,500), for application to highly influential positions and successfully appointed to the position, 10 thousand to 2 million baht per month (~USD285.00 to ~USD57,000);
- Demanded and received bribes for facilitating offshore illegal oil trade through sub-ordinate officers; and
- Organized an illegal casino in a rental space in a massage parlour and received 40 percent of income, totalling 110 million baht (~USD3.1 million).

127 Proceeds were then used to buy foreign currency, arts, antiques, jewellery, as well as real estate in nominees' names.

4.3 Abuse of charities for terrorist financing

FRANCE

128 *Case 1.* This case relates to the charity "Perle d'espoir", which led to the first prosecution of a charity for TF. This charity was created in 2012 to raise funds for humanitarian projects in foreign jurisdictions. After a donation campaign, in August 2013, this charity brought two ambulances with medical material to build a hospital: pictures were posted on Facebook to attest the reality of the project and communicate with donors. At the same time, one of the main members of this association

was claiming on his personal Facebook profile that he had met with jihadist and got training to fire weapons. A month later, a new call for funds was made on social networks: this time it was a campaign to buy sheep for the 'Eid celebration. Three members of the association were planning to deliver the funds raised. French customs control at the airport revealed that each of the three members was carrying €9,900 (below the declaration threshold) – basically, the members were acting as cash couriers. In January 2014 assets of the association and four other members were frozen by an administrative order for six months. But two days after this order was issued, one of those individuals left France, and wrote on his Facebook wall that he had joined a terrorist organisation. He kept on posting about his daily life there on Facebook, for six months, before returning. In November 2014, the association was dissolved, and two members were arrested for TF and criminal conspiracy in connection with a terrorist enterprise – most funds raised were used to support foreign terrorist fighters. Facebook public messages and pictures were used as evidence by law enforcement authorities.

129 *Case 2*. The other case involves a charity set up in 2010 to support humanitarian projects in Africa and the Middle-East. Its Chairman was a webmaster for another humanitarian association who specializes in e-marketing. The website displays numerous pictures of all projects, and the page offers several options to make donations via credit card, PayPal, cash transfers, checks. The Facebook page displays two links: one to directly make a donation and one below to share the call for donations. Over a year and a half, bank accounts of this charity received numerous donations by checks and wire transfers below €500 – almost €2 million was received in total. A quarter of those funds were collected in personal PayPal accounts, and then withdrawn by cash, or wire transferred to accounts of other charities. In this case, authorities could not prove TF.

INDIA

130 The National Investigation Agency (NIA) has investigated a case in which terrorist organization HM, a proscribed terrorist organization, has been found to be receiving funds originating from jurisdiction X through different channels for supporting its terrorist activities in India. In this case approximately USD 11.822 million has been transferred into India to support terrorist activities since 2008. J Trust, a front organization of HM, with its Head Office in jurisdiction X, is actively involved in raising and collecting funds in jurisdiction X and transferring it to India for its distribution to active cadres and other beneficiaries of terrorist organizations. It has been found that banking channels were extensively used for transfer of funds to various bank accounts in India. Investigations have disclosed that the accused recruited and trained persons for terrorist acts, organized training camps, trained cadres of the organizations, supplied arms, ammunitions, explosives, and means of communications. Further, for investigation, collection and transfer of evidence, a Letter of Rogatory/Letter of request has been sent to jurisdiction X under section 166-A of Code of Criminal Procedure, 1973. Interpol Red Notices have been published against 8 absconding accused. Presently, the case is under further investigation.

THAILAND

131 Community helmsmen in the southern border provinces collected religious donations from community members. Use of the funds is totally at the discretion of the helmsmen. Some helmsmen are sympathizers or have links to insurgency groups and are suspected of channelling some of the funds to these groups.

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

BELARUS

132 The efforts undertaken by the Financial Monitoring Department, Belarus jointly with the law enforcement agencies disrupted the operation of a criminal group where members used business entities controlled by them for misappropriating and laundering funds on a large scale.

133 The attention of the Financial Monitoring Department was drawn to a group of business entities that transferred large amounts of funds among themselves and also to non-resident entities. Detailed examination of the operations of these business entities indicated their potential involvement in activities intended for falsifying and disguising the true origin of funds. This information was disseminated to the law enforcement agencies.

134 The investigation revealed that bank T represented by its board chairman person V, and private company F, represented by its director person S, signed the contract, under which Bank T placed an order with Company F for designing and constructing the real estate property (new building for the bank) in the city of Minsk and undertook to pay for this work.

135 Under the said contract, Bank T transferred, in two instalments (20 billion rubles ~USD1 million on September 2014 and 80 billion rubles ~USD4 million on September 2014), a total of 100 billion rubles (~USD5 million) to the account of Company F. Most of these funds were used for acquisition of 5, 286 bonds worth a total of 78.7 billion rubles (~USD3.8 million) of company A at the agreed price.

136 In order to convert these securities into foreign currency by trading them under the sale and purchase contracts signed between the business entities controlled by person S, the said bonds were transferred by Company F to Tr Ltd (jurisdiction R), which, in turn, transferred them to S LLP (jurisdiction U) and further to T Limited (jurisdiction C). However, these transactions involved just transfer of the securities and generated no cash flows.

137 Funds used for payment for the bonds were transferred only after the bonds were actually paid for by their ultimate purchaser – Bank T. These transactions were intended for falsifying and disguising the true origin of the funds. For this purpose, the funds used in these transactions were transferred through the accounts of the aforementioned companies opened with banks in three different jurisdictions.

138 Under the securities sale and purchase contract of signed between T Limited (jurisdiction C), controlled by person S and Bank T, represented by the deputy chairman of the board person G, T Limited (jurisdiction C) sold 5 286 bonds worth a total of 5.3 million euro (~USD5.9 million) to Bank T (at 1,000.36 euro per bond). Immediately after that, almost the same amount (5.3 million euro) was transferred from the account of T Limited (jurisdiction C) to S LLP (jurisdiction U) as payment for the bonds.

139 On the same day, the funds received by T Limited (jurisdiction C) for the sale of the bonds, funds were transferred to the account of Tr Ltd (jurisdiction R). A portion of the received funds was converted from US dollars into euro and transferred from the account of Tr Ltd to the account of S LLP (jurisdiction U).

140 According to the Financial Monitoring Department it was established that the director and founder of Company F person S was the beneficial (actual) owner of Company F (Belarus), Tr Ltd (jurisdiction R), S LLP (jurisdiction U) and T Limited (jurisdiction C).

141 The investigators found out that person S carried out the aforementioned transactions under the preliminary agreement with person M for further contribution of the involved funds into the authorized capital of Bank B. Person M required to transfer 5.5 million euro (~USD6.2 million) to R Ltd (jurisdiction C) controlled by him as the obligatory condition. In order to obtain the needed amount, person S arranged for additional sale of 994 bonds worth a total of USD 996.5 thousand (at USD 1002.47 per bond) to Bank T through the company T Limited in jurisdiction C controlled by him.

142 Thus, 5.5 million euro (~USD 6.2 million) from the funds allocated by Bank T for construction of the real estate property in Minsk was transferred to the account of Seam LLP (UK).

After those finds were credited to the account of Seam LLP (UK) on 20.10.20111, they were immediately transferred to the account of Rose Ltd (Cyprus) as the contribution into the authorized capital.

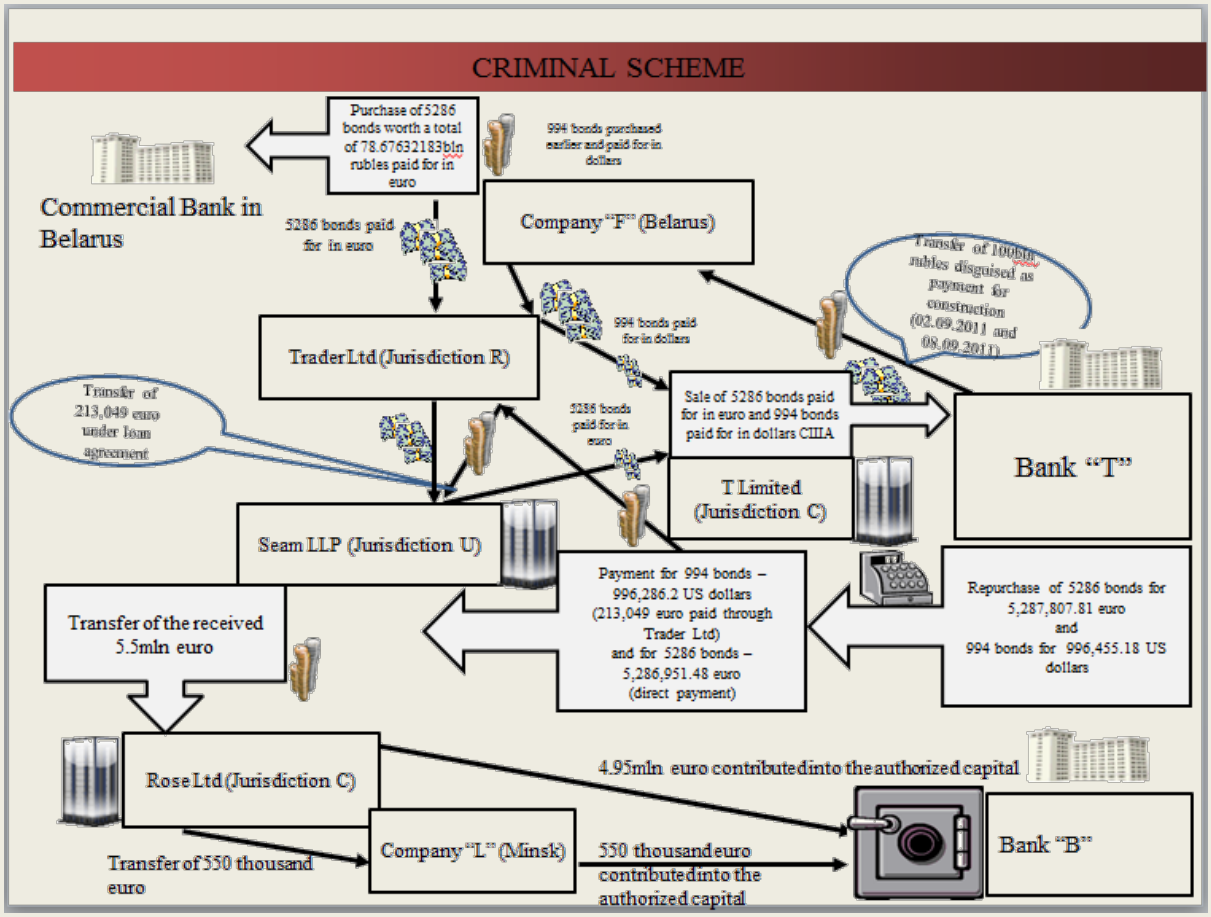
143 In December 2011, R Ltd (jurisdiction C) carried out two debit transactions:

- Euro 4.95 million (~USD5.5 million) were transferred as the contribution into the authorized capital of Bank B (the purpose of payment was indicated as the contribution into the authorized capital of Bank B under the Bank B incorporation agreement of December 2011) in compliance with the bank registration procedure;
- Euro 550 thousand (~USD621 thousand) were transferred as the loan to Company L under the loan agreement of December 2011, and were further contributed, on the same day, into the authorized capital of Bank B in compliance with the bank registration procedure.

144 The Financial Monitoring Department sent the requests for information on the said companies to the FIUs of the jurisdiction U and C. The received responses indicated that Ro Ltd (jurisdiction C) and Company L were controlled by the foreign national person M. Besides that, the undertaken investigative and other efforts revealed that Company L was established in 2011 as a result of reorganization of Company T, which shares were repurchased from person M (755) and person V (25%). It was also established the person M was the former director of Company T and the authorized representative of R Ltd (jurisdiction C). Pursuant to the decision of July 2011, Company T was renamed as Company L. This document was signed by person M acting in the capacity of the authorized representative of Rose Ltd (jurisdiction C).

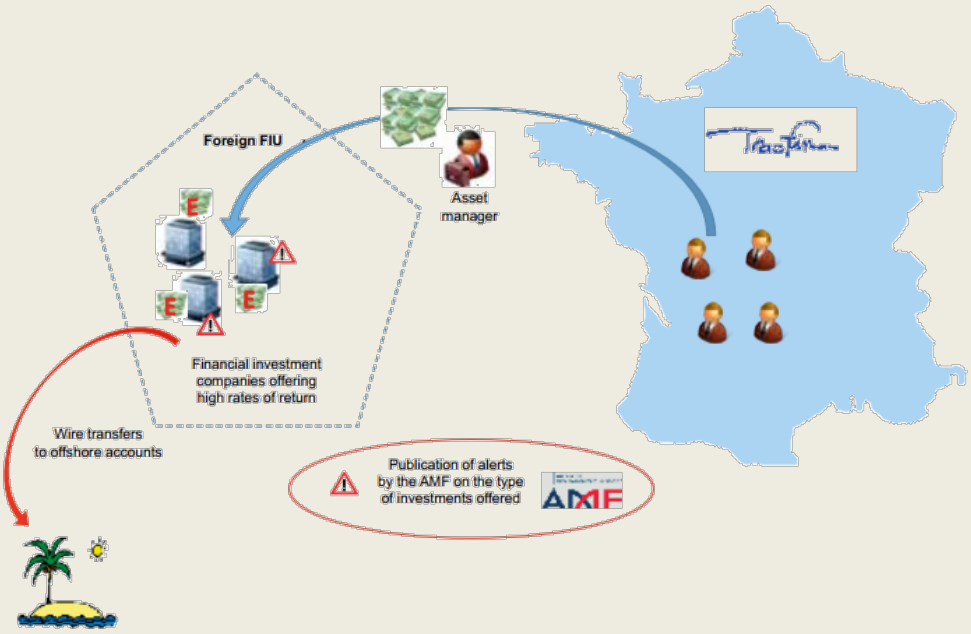
145 Thus, in September – October 2011, the chairman of the board person V and the deputy chairman of the board person G of Bank T, being the executive officers of this bank and acting upon prior conspiracy with the secretary and authorized member of the board of directors person M and with the support of the director and founder of Company F person S, abused their official job positions for carrying out various financial transactions through the accounts of the business entities controlled by person S and person M, through which they misappropriated at least 80 million rubles (~USD4 million) that belonged to Bank T. The actions committed by the said persons constitute the offence covered by Article 210 (4) (Misappropriation through abuse of powers) of the Belarusian Criminal Code.

146 In December 2011, after the misappropriated funds were converted into 5.5 million euro (~USD6.2 million) and transferred to the account of R Ltd (jurisdiction C), person M carried out transactions through the accounts of the companies controlled by him (R Ltd and Company L) and laundered these criminal proceeds by contributing them into the authorized capital of Bank B. The actions committed by the foreign national person M constitute the offence covered by Article 235 (3) (Legalization (laundering) of proceeds obtained through crime) of the Belarusian Criminal Code.



FRANCE

147 *Conspiracy to defraud, breach of trust and money laundering – Investigations undertaken based on reports from foreign FIUs.* A foreign FIU reported to Tracfin (France FIU) that they had blocked funds possibly connected with a fraud (some of the funds had originated in France). The blocked funds totalled more than €1 million (~USD1.1 million). At the same time, Tracfin became aware of transfers by individuals in France to companies established in the same foreign country, which were presented as high-return financial investments. Some of these companies were the subjects of alerts, issued by Autorité des Marchés Financiers (France stock market regulator), concerning the type of investments they offered. These transactions included an asset manager, who was an employee of the insurance company, and who played the part of intermediary in the purchase of these products. Investigation quickly determined that these investments were fraudulent, offering unrealistic returns and involving wire transfers to several offshore bank accounts.

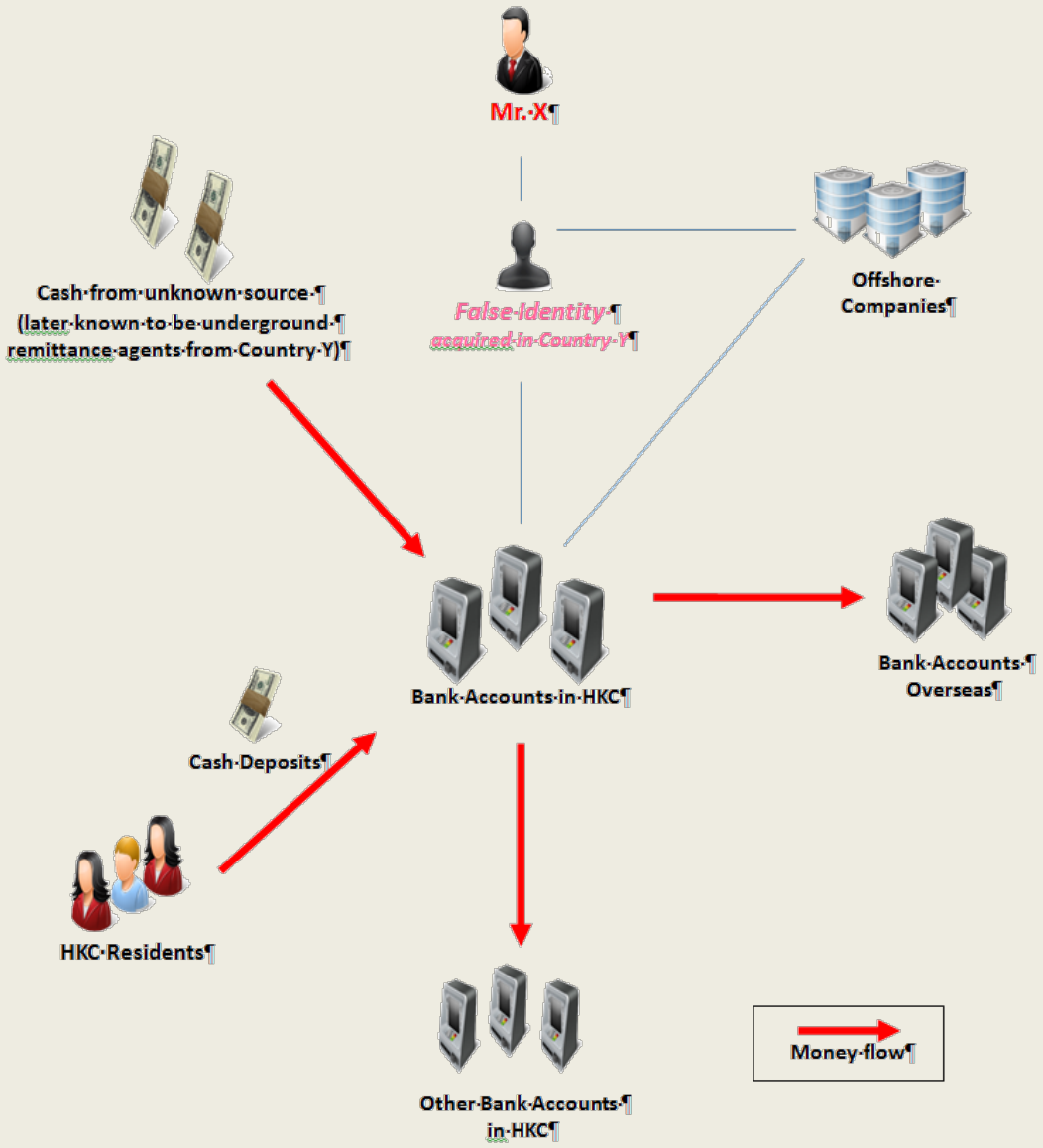


HONG KONG, CHINA

148 The Customs and Excise Department (C&ED) investigated a transnational ML scheme in Hong Kong, China (HKC) and other jurisdictions involving Mr. X who was wanted by jurisdiction Y for misappropriation of public funds. See diagram below which illustrates the case.

149 C&ED's investigation unveiled that Mr. X had acquired a false identity in jurisdiction Y. Between 2008 and 2012, he used his false identity to set up several offshore companies and opened a number of personal and company bank accounts in HKC to receive large amounts of funds via cash deposits from unidentified sources and bulk deposits from local residents. After accumulation to a certain threshold, he transferred the funds in large amounts to other local and overseas accounts under his control. To conceal the origin of the crime proceeds, person X engaged an insurance agent and three property agents to help him receive and divert the money using the same structuring modus operandi. Moreover, he used deposited funds to purchase a real estate in HKC and five pieces of real estate overseas. Furthermore, person X's overseas bank accounts recorded a large amount of remittances from HKC. Investigations confirmed that the money originated from underground remittance agents in Country Y. Over HK$330 million (~USD42.5 million) was laundered during the period.

150 In August 2014, the C&ED mounted a joint operation in collaboration with the relevant authorities in four other jurisdictions to track down the assets held by person X. Through cooperation with the counterparts, the C&ED successfully restrained HK$112 million (~USD14.4 million) worth of assets held by person X in HKC and in another jurisdiction. In December 2014, the assets were ordered for confiscation in HKC.



INDIA

151 In one of the cases under a Prevention of Money Laundering Act 2002 investigation, an amount of USD 1.5 million has been siphoned off to jurisdiction U from an account held in Jurisdiction S by the accused.

152 In a second case, a banned terrorist organization in Punjab received funds to commit terrorist activities by using banking/non-banking channels, since May, 2011. There were several instances where established money transfer operators and other cash channels were used to transfer funds. The money was transferred by the intermediaries to terrorists in jail or their relatives. The money has been transferred primarily through money orders or by cash. The case is under investigation.

CHINESE TAIPEI

153 Person H was the chairman of company A, established in jurisdiction X, and company P, established in jurisdiction Y. Both A and P had no actual business activities. In July 2013, person H advertised the investment with the following deceptive information: (i) company A held 100% shares of company P which was in charge of the land development business of company T in jurisdiction Y, (ii) company A had spent USD 44 million for purchasing land, (iii) the development and construction would be finished in 3 years, and (iv) therefore, this investment would have high rate of return.

154 In order to win the trust of investors, person H forged three remittance vouchers of HSBC to falsely prove that company A had transferred USD 44 million for the investment. Several investors transferred funds to company A's account. The total amount of investment funds was about USD 15 million.

155 Person H only transferred USD 5.38 million to jurisdiction Y for purchasing land and for the development. The rest of funds were remitted to person H's accounts or foreign legal persons' accounts controlled by person H. Chinese Taipei authorities initiated a criminal investigation and then referred this case to the Kaohsiung District Prosecutors Office in 2015 for prosecution.

4.5 Use of virtual currencies

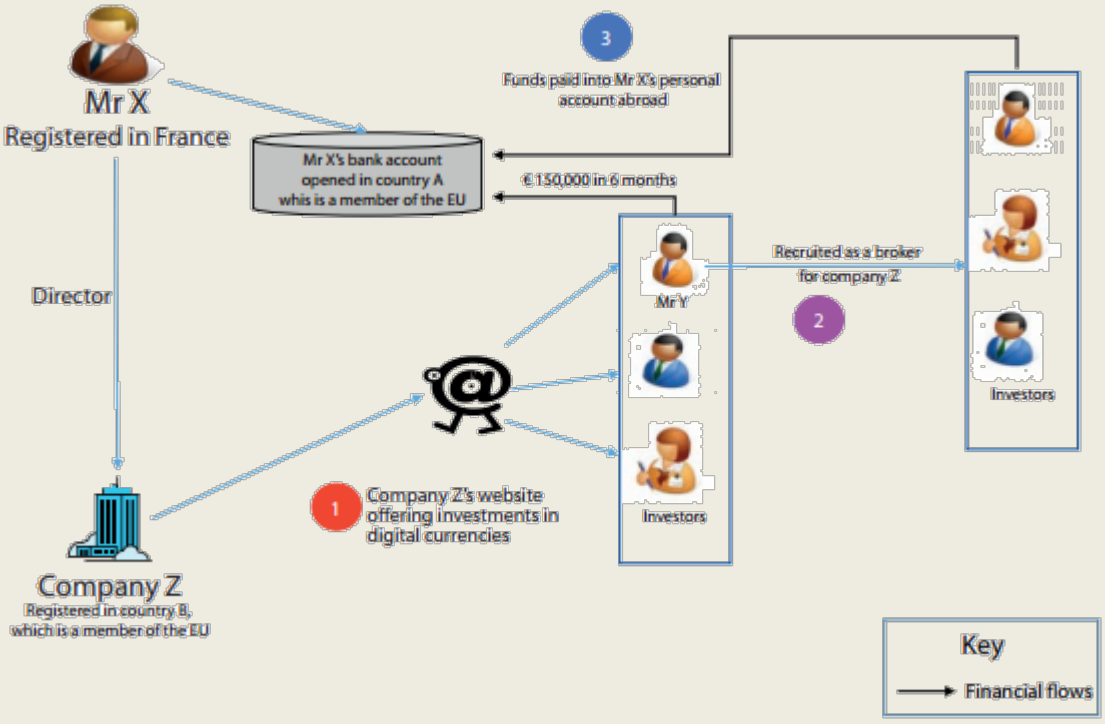
FRANCE

156 *Presumed case of financial fraud on the internet based on the use of virtual currencies.* Clients were offered the chance to invest in products linked to virtual currencies, although there was no proof of the actual existence of these investments.

157 *Flows leading to the suspicion of wrongdoing:* company Z was registered in jurisdiction B as a fund management company specialised in products linked to virtual currencies. No information was given about the investments offered by company Z, which was recently created and managed by Mr X. There was also no proof of the investments' actual existence. The so-called investment products offered by company Z were advertised on a website and dedicated pages on social networks.

158 The funds invested by clients, some of whom may have been victims of an abuse of weakness, were not paid into company Z's accounts, but directly into Mr X's foreign account. Some clients were invited to become brokers for company Z in order to receive commissions on the funds collected and referrals of new brokers. Generally, the contracts offered by company Z were poorly drafted, with clauses that were extremely unfavourable to company Z's clients.

159 The circumstances in which Mr X offered his fund manager services to his clients, some of whom were invited to become brokers, and the fact that he collected funds in his personal account, opened in jurisdiction A, suggested that he was possibly guilty of abuse of trust, and abuse of weakness in the case of some clients, conspiracy to defraud and laundering of the subsequent proceeds. This type of financial fraud on the internet, using the speculative nature of virtual currencies to attract investors, is comparable to the Ponzi schemes set up by conmen who use the pull of new technologies to draw in investors.



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

HONG KONG, CHINA

160 Arising from a corruption investigation, it was revealed that a partner of a solicitors firm and the wife of a former executive director of a listed company in Hong Kong, China (HKC) had laundered HKD230 million (~USD29 million) in crime proceeds.

161 Between December 2009 and February 2010, a HKC listed company raised HKD790 million (~USD101 million) through the issue of convertible notes for acquiring dairy farms in another jurisdiction. Of the amount received by the vendor of the dairy farms, HK$73.7 million (~USD9.5 million) was remitted back to a company owned by the former executive director of the listed company, who then transferred HK$68.95 million (~USD8.8 million) to a solicitors firm in HKC. Soon after, the partner of the solicitors firm transferred HK$68.95 million (~USD8.8 million) to the bank account of the wife of the former executive director of the listed company. Between March 2010 and October 2011, the wife of the former executive director of the listed company also dealt with a further HK$161 million (~USD20.7 million) in crime proceeds.

162 The partner of the solicitors firm and the wife of the former executive director of the listed company were convicted of ML and were respectively sentenced to six years and six and a half years imprisonment. Following appeals lodged by both defendants, the Court of Appeal quashed their convictions and ordered that a retrial be held on a date to be fixed.

MALAYSIA

163 *Background of subjects & modus operandi:*

- Mr. A was a lawyer-turned-businessman where he established a property investment company which offered services to investors to buy auctioned properties which normally sold at a lower price and an option to re-sell the properties at a 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 are required to pay substantial amounts of membership fees to the company on annual basis;

- Mr. A also set up companies that are related to real estate management, renovation and auction house to lure investors to invest in the scheme. Free investment courses were offered to prospective investors conducted at well- known hotels; and
- Mr. A's modus operandi was to search and secure auctioned properties especially and sell these properties to prospective investors through a specially created website.

164 *Method used:* Abnormal number of properties purchased/acquired during short period of time; disposal and recycling of properties on active and frequent basis; utilisation of lawyers (client's account) to disguise the investment activity is valid and legal.

165 *Source of information:*

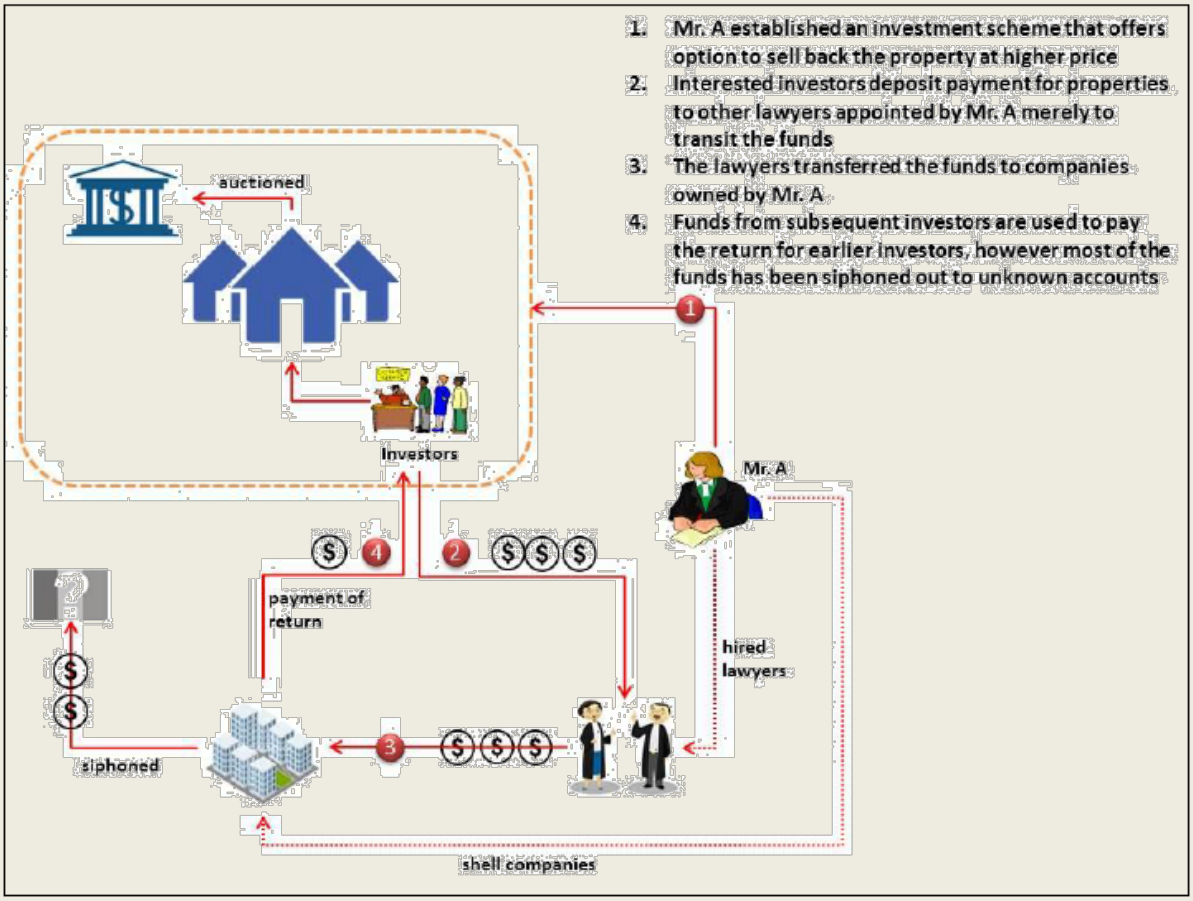
- STR and cash transaction reports (CTR) records;
- Complaint from investors; and
- Internal surveillance conducted by the Royal Malaysia Police (RMP).

166 *Facts of the case:*

- Initial investigation carried out by RMP discovered that the investment scheme had gain huge popularity and received large number of responses from interested investors from across the country. The investment scheme had lured around 500 investors nationwide;
- Lawyers were engaged to solicit the investment scheme transaction by receiving investment money from potential investors into the client's account in order to portray that the investment scheme was conducted legitimately;
- Mr. A was found to have given instruction to the lawyers to withdraw the collected funds and credit into Mr. A's companies accounts;
- As the number of investors continued to grow, Mr. A could not obtain sufficient properties to meet the demand of the increasing investment funds. As a result, Mr. A started to recycle the same properties among the existing investors, and resold the same properties to new investors;
- Profit would be distributed back to the investors to gain their trust and confidence for further investment which resulted in the value of investment continued to multiply tremendously; and
- Although some of the profits were distributed back to the investors, the majority of the profits was siphoned out by Mr. A.

167 *Actions taken to date:*

- RMP had conducted ML investigations in parallel with the predicate offence investigations under section 420 Penal Code in relation to cheating;
- The investigation managed to trace 288 properties across the country that were purchased for the said investment scheme, and freezing and seizure procedures were initiated against these 288 properties which have a market value of RM25 million (~USD6.2 million), together with several personal accounts maintained by Mr. A and his immediate family members, which were later forfeited; and
- As Mr. A had absconded and could not be traced, RMP had pursued the case for non-conviction based forfeiture (civil forfeiture) under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA).



MONGOLIA

168 A professional accountant of a state-owned enterprise was involved in a conspiracy to launder embezzlement money through multiple transactions to offshore companies and banks. The defendant was also an Executive Director of a non-bank financial institution in Mongolia.

NEW ZEALAND

169 *Case study - asset forfeiture from dishonest accountant*. In March 2014, assets valued at an estimated NZD1.4 million (~USD.95 million) were forfeited from accountant person X, who used funds stolen from the trust accounts of his clients to fund a lavish lifestyle. For years person X was considered 'one of the family' but behind their back the Hamilton-based accountant siphoned off funds and used them to build a mansion complete with hydro-slide and to fund purchases such as vehicles, company shares, boats and a holiday home in Fiji. His actions were concealed by a complex set of entities that were used to hide his fraud, often under the guise of legitimate transactions. Person X was caught when Inland Revenue noted discrepancies between his assets and his declared income. He has been sentenced to more than five years imprisonment and his status as a chartered accountant has been suspended by the Institute of Chartered Accountants.

170 This case study is published in FIU Quarterly Typology Report Q3 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2013-2014.pdf

171 *Case study - Operation Rock.* Two offenders involved in the importation of ecstasy laundered large amounts of cash through a lawyer's trust account. A total of NZD400,000 (~USD270,000) 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 a suspicious transaction

report. However, the bank that held the lawyer's trust account submitted suspicious transaction reports when the lawyer deposited NZD100,000 on four occasions. The offenders had instructed the lawyer the cash was being held on behalf of their company registered in jurisdiction X. This alleged company was a shell company that 'lent' one of the offenders the NZD400,000 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.

172 This case is published in FIU Quarterly Typology Report Q3 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2013-2014.pdf

4.7 Trade based money laundering and transfer pricing

MALAYSIA

173 *Background of subjects & modus operandi:*

- Investigation of company BSPSB arising from the audit performed by Post Clearance Audit of State Compliance Division of the Royal Malaysian Customs Department (RMCD).
- Investigation conducted found there is a relationship between BSPS's directors and company ZCT and their involvement in importation of kitchenware and hardware from Country C.
- The value of declaration by ZCT to RMCD was below real transaction value as the product sold by ZCT to BSPSB was at a higher price. For example, a unit of chest freezer was declared to RMCD at RM62.08 (~USD15.50) and sold to BSPSB at RM384.00 (~USD95.20).
- Such action portrays possible offences of under-declaration of imported goods committed by parties involved.

174 *Method used:* use of front companies that do not physically exist; active international fund transfers within short period of time; inter-linkages with other company operating the same modus operandi; appointment of 3rd party/proxy to execute payment to avoid money trail detection.

175 *Source of information:*

- STR and CTR records;
- Internal intelligence from RMCD; and
- Documents recovered from the crime scene.

176 *Facts of the case:*

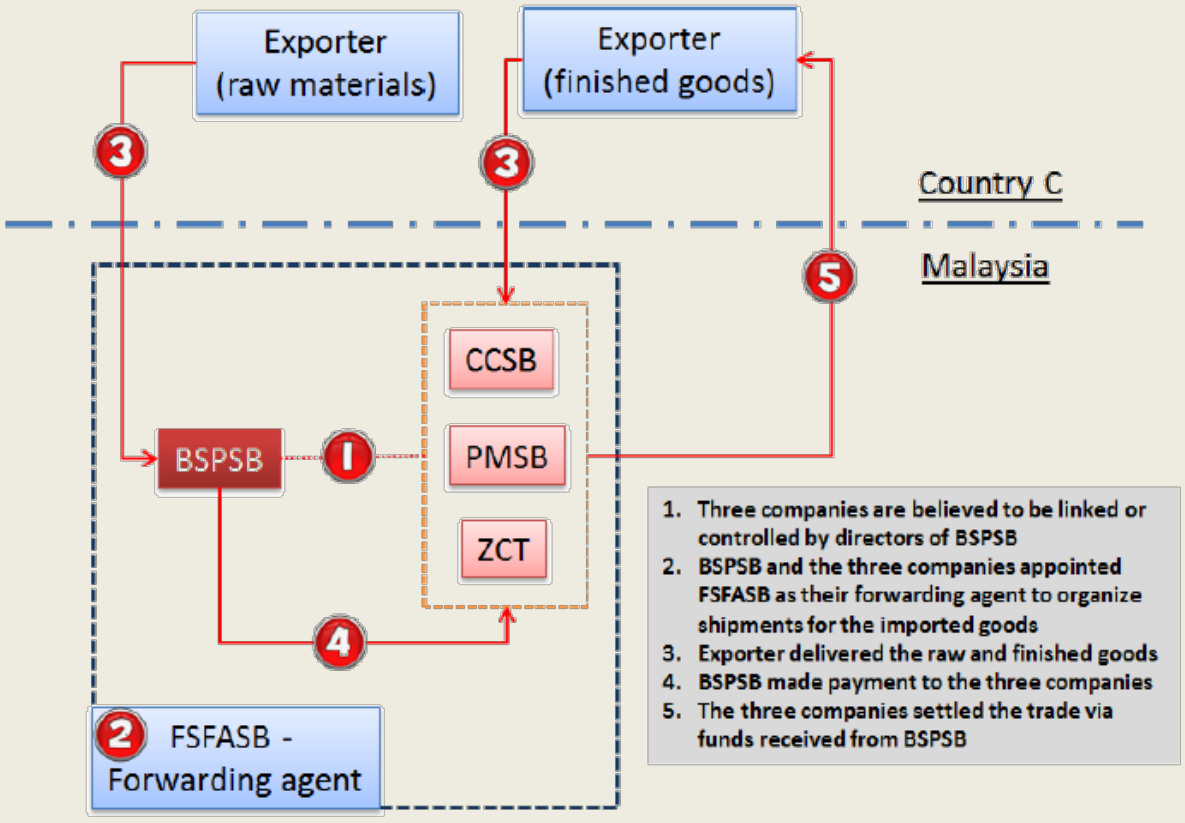
- ZCT was found to be the proxy of BSPSB as the directors of BSPSB, i.e. person CWC and his wife person CSL were given mandate by person L, the director of ZCT, to approve payments to overseas supplier using local bank account;
- ZCT business did not physically exist;
- Person CWC was also found to be involved in the business operation of ZCT, as he was responsible in approving all payment transactions on behalf of ZCT;
- All Telegraphic Transfer (TT) forms for overseas payment were signed by person CWC and not by person L;
- Similar to ZCT's business operation, BSPSB is also involved in importation of kitchenware and hardware from the same supplier. Besides that, BSPSB also manufactured kitchenware and hardware in smaller quantity;
- Audit conducted by RMCD found that BSPSB had committed tax deficiency fraud amounting to RM1.6 million (~USD.396 million). BSPSB denied having any connection with ZCT thus, refused to pay the said tax deficiency. As a result of this, money laundering investigation was

conducted against BSPSB in relation to the offence under section 135(1)(g) under Customs Act 1967 concerning fraudulent evasion of customs duty;

- Findings from investigation showed that, aside from ZCT, there are two other companies related to BSPSB namely, company PMSB and company CCSB, which conduct similar business transactions;
- Person S, manager and accountant of BSPSB admitted to be involved in the operation of ZCT, PMSB and CCSB on behalf of BSPSB. A statement was also recorded from person CWC and he admitted that all the 3 companies. i.e. ZCT, PMSB and CCSB had relationship with company BSPSB;
- Person L admitted there was tax deficiency paid to RMCD and claimed that BSPSB is solely responsible on its action;
- Tax deficiency amounting to RM1.6million (~USD.396 million) was detected against ZCT while RM1.7million (~USD.421 million) detected against PMSB; and
- There is strong evidence indicating that BSPSB was involved in tax deficiency fraud involving ZCT and PMSB.

177 *Actions taken to date:*

- Bill of Demand was issued by RMCD for tax deficiency offence committed by BSPSB; and
- The case under section 135 Customs Act has been closed upon the settlement of duty claimed including compound by RM3.3 million (~USD.818 million).



SRI LANKA

178 *Defrauding Foreign Exchange in the Guise of Outward Remittances.* Sri Lanka Customs submitted an STR to the FIU relating to the activities of several individuals and entities which had violated the Customs Ordinance by defrauding foreign exchange amounting to approximately USD 7.5 million in the guise of outward remittances meant for imports.

179 Company PS and the company BM were registered for importation of fabric from country U. Bulk cash deposits were been made to the accounts of above companies at Bank H by company employees. The deposits were then remitted to Country U on the same day or the following day to settle dues in connection with imports of fabric.

180 Investigations by Sri Lanka Customs revealed that both company PS and BM were non-existent and the import documents submitted to banks for remitting money were forged. Further, individuals identified as proprietors were also non-existent. Forged national identification documents had been presented to the bank to open bank accounts.

181 On the receipt of STR and Customs Investigations report, all related accounts of above individuals and entities were suspended by the FIU and the case was immediately referred to the LEAs for further investigations. It was further revealed that several other companies which were also connected to the main suspects of this case were engaged in importing fabric and purposefully had understated the value of import consignments.

INDIA

182 *Case 1.* A person who is accused of the offence of cheating and ML has transferred USD 103.9 million to Jurisdiction X in the guise of payments against the import of software.

183 *Case 2.* The accused who is a public servant has apparently laundered black money and received an amount of USD 2.4 million as Foreign Direct Investment in his front company from abroad.

184 *Case 3.* The accused for the offences of cheating and ML has received USD 10.5 million as an inward remittance by diverting money from India.

4.8 Underground banking/alternative remittance services/hawala

AUSTRALIA

185 *Case Study of European Syndicate using cash couriers and remittances to facilitate drug imports.* A sophisticated and well established offshore syndicate was identified as targeting Australia for import of cocaine and MDMA. The syndicate was using multiple streams to import drugs, including passenger, air cargo and international mail. The syndicate had well established links in Australia and facilitated imports using the remittance of funds offshore. It is also likely that the syndicate instructed drug couriers arriving in Australia to collect physical currency and conceal the currency when departing Australia.

FIJI

186 Fiji FIU received a STR on company X. Company X is involved in the export of agricultural produce and other commodities. Fiji FIU established that company X supposedly instructed its overseas buyers to remit payments through foreign exchange dealers, instead of paying directly into company X's local bank account which is known to the tax authorities. Fiji FIU was able to verify that company X had reportedly collaborated with its overseas buyers, in order to hide the revenue from its business records. Company X directors deposited most of its export revenue in alternative bank accounts and did not fully declare the total revenue for tax purposes. The amount involved in the case was FJD 6 million (~USD2.6 million). A case dissemination report (CDR) was provided to the Fijian tax authority and investigations are currently underway.

INDIA

187 *Case 1.* A person who is accused of cheating and ML offences has sent USD 10.5 million through a hawala channel to Jurisdiction X for receiving inward remittance against a purported business transaction.

188 *Case 2.* The proscribed terrorist organization X based in Jurisdiction X sent money through hawala to fund terrorism and secessionist activities. Large amounts of money were delivered to various places in Delhi through hawala channels, which was then used to support secessionist activities. Interpol Red Notices have been issued against the accused persons. The case is under further investigation.

JAPAN

189 *Case 1.* Foreign nationals from jurisdiction X who operated underground banking in Japan, transferred money to jurisdiction X. They had their clients transfer around JPY 1.4 million (~USD12,700) concerning a remittance and commission fee into a bank account under the name of third party. They were arrested for violating the Banking Act and the Act on Punishment of Organized Crimes (concealment of proceeds).

190 *Case 2.* Foreign nationals from jurisdiction X, operated an underground banking scheme in Japan, and transferred around JPY 4.3 billion (~USD.03 billion) to jurisdiction X via cash mule. They were arrested for violating the Banking Act.

PAKISTAN

191 *Case 1.* The transfer of funds via cheques from and to the inter-connected accounts maintained in the border towns by a network of individuals/entities. Moreover, a significant proportion of funds were moved from the accounts maintained at Bank A's border town branches to accounts maintained at Bank A's tribal area branch. The individuals involved were young and unlikely to have such large transactions. The movement of funds to the tribal region without any plausible justification made the transactions suspicious in respect to hawala and other criminal activities including terrorism financing. Further, CTRs reported on the individuals indicated that the suspects also held accounts with other banks in the region as well. The case was report to LEA for further investigation.

192 *Case 2.* Multiple STRs were reported on foreign individuals residing in Pakistan suspected to be involved in activities related to hundi/hawala. Some foreign individuals maintained account with ABC Bank. Some of these accounts were personal accounts while others were Sole Proprietorship accounts. The transactional pattern in all these accounts did not match with the profile of the customers. The turnover was very high and very frequent transactions took place in the accounts. The transactions were also being carried out with unrelated counter-parties. All these individuals conducted inter-linked transactions in each other's accounts. Most of these individuals were not registered with tax authorities.

193 During analysis of STRs, it was revealed that one of the suspects was already involved in hawala/hundi activities. Accordingly, the financial intelligence on all the connected individuals was forwarded to the LEA to assist them in apprehending the illegal network of hawala/hundi operators.

194 *Case 3.* The suspects opened their accounts in XYZ Bank Limited and routed funds from their accounts were likely to be associated with the business of hawala/hundi. Some accounts were reported to the FIU due to heavy turnover noticed in the accounts which did not match with the profiles of the account holders. Furthermore, investigation releveled transactions from the accounts were conducted with unrelated counterparties and there were high-value online transactions with the accounts maintained in the branches located in high-risk regions of Pakistan.

195 During analysis of the accounts, it was revealed that none of the suspects were registered with tax authorities despite having heavy turnover in their accounts. Further, it was noticed that suspects opened accounts in the area located a long way from their residential addresses. Various other accounts maintained by the suspects were also identified using the CTRs database and through positive matches of contact information. It appeared that the funds routed from the accounts of the suspects were likely to be related to the illegal business of hawala / trade of smuggled goods. Therefore, the matter was referred to LEA for further investigation.

196 *Case 4.* The accounts of D-Trading Company (person DK), S-Fruit Merchant (person SSK), K-Trading Company (persons KK and JK) and A-International Corporation (person AK) were reported by XYZ Bank. The accounts were either opened as proprietorship or partnership concerns. The accounts were reported to the FIU due to heavy turnover in the accounts and transactions with individuals / entities unrelated to the nature of business of the account holders.

197 During analysis, the accounts of D-Trading Company, S-Fruit Merchant, K-Trading Company and A-International Corporation were found to be linked by the transfer of funds. The accounts were being maintained in XYZ Bank at the same branch located in tax exempted region. An identical pattern of transactions was noticed in all these accounts. Additional accounts of suspects were identified via CTRs. Furthermore, different businesses were mentioned by the suspects in the accounts maintained at different banks and the suspects were not registered with tax authorities, except for AK.

198 From the activity in the accounts and the location of the accounts, it was suspected that the suspects were engaged in the business of illegal hawala/hundi. Therefore, the financial intelligence was disseminated to LEA for investigation.

199 *Case 5.*A STR was reported on account of news aired on a local TV Channel. According to the news, a local businessman had received a threatening call from a foreign jurisdiction asking him to deposit an amount into an account maintained by person X in a local bank. A search of the FIU's database revealed a link between the account numbers and other individuals maintaining accounts with the same and other banks.

200 Analysis of all the linked accounts identified a nexus of Hawaladars who were suspected to be facilitating the network. Analysis of statement of account reflected frequent transfers of funds from/to different accounts. The matter was referred to LEA for investigation.

SAMOA

201 Mr T was reported by a money transfer operator (MTO) due to significant incoming transfers in his name. When he was interviewed by the MTO, he stated that the funds were to meet operational costs of his employer/business. Information obtained revealed that Mr T was sacked from his job. Mr X was convicted of fraud and jailed for two years.

CHINESE TAIPEI

202 *Case 1.* Since 1997, person L has operated an underground banking system. In order to avoid the detection by law enforcement agencies, person L used 14 accounts under his name and relatives and thereby reduced the number and size of remittance transactions in each account. Customers who used the underground banking system could remit the funds to L's and his relatives' accounts. After receiving funds, person L informed the contact points in a foreign jurisdiction to give Hong Kong Dollars, CNY or USD with equal value to appointed persons or remit to appointed accounts. Between August 1997 and July 2014, the 14 accounts that person L used have received about NTD 3.6 billion (~USD110 million). Chinese Taipei authorities initiated a criminal investigation and then referred this case to the Taipei District Prosecutors Office in January 2015 for prosecution.

203 *Case 2.* Person A (foreign national), person B (foreign national), person C (foreign national), person D engaged in underground money exchange between the Chinese Taipei and jurisdiction X

since 2013. The subjects collected cash in NTD from clients, who wished to transfer money back to designated accounts in jurisdiction X. The money was hidden in secret compartments in luggage or hand carried to jurisdiction X then exchanged into local currency and deposited into designated accounts. The underground remittance business was profited by exchange differences. The criminal proceeds exceeds around NTD 44,179,000 (~USD1.36 million). The case was investigated by Criminal Investigation Bureau and transferred to the Nantou District Prosecutors Office for further investigation in 2015.

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

AUSTRALIA

204 *Case Study of European Syndicate laundering the proceeds of cyber-related malware activity.* A European syndicate was identified as using sophisticated malware and malicious spam software in order to compromise a victim's computer and gain access to their bank account details. Once the bank account details were known to the syndicate, funds were funnelled out of the account and on-forwarded to members of the syndicate through bank accounts that they had opened in Australia. Once the transfer was received, the funds were either:

- Withdrawn;
- Remitted offshore;
- Used to purchase cash-passports (using the credit/debit card associated to the account); or
- Used to purchase foreign currency.

BRUNEI DARUSSALAM

205 The FIU disseminated STRs relating to a short messaging system (SMS) scam which was particularly prevalent in the first half of 2015. The scam involved the use of a known beverage company where unknown persons using a foreign registered phone number sent text messages randomly to local victims informing them that they had won prizes. These victims would then be asked to deposit funds or to release those prizes, to a local intermediary. This intermediary would then either remit the collected funds from various victims overseas (the scammer) or transfer the funds to other victims to gain their trust and endorsement of the scam. The relevant law enforcement agency is currently investigating this case.

HONG KONG, CHINA

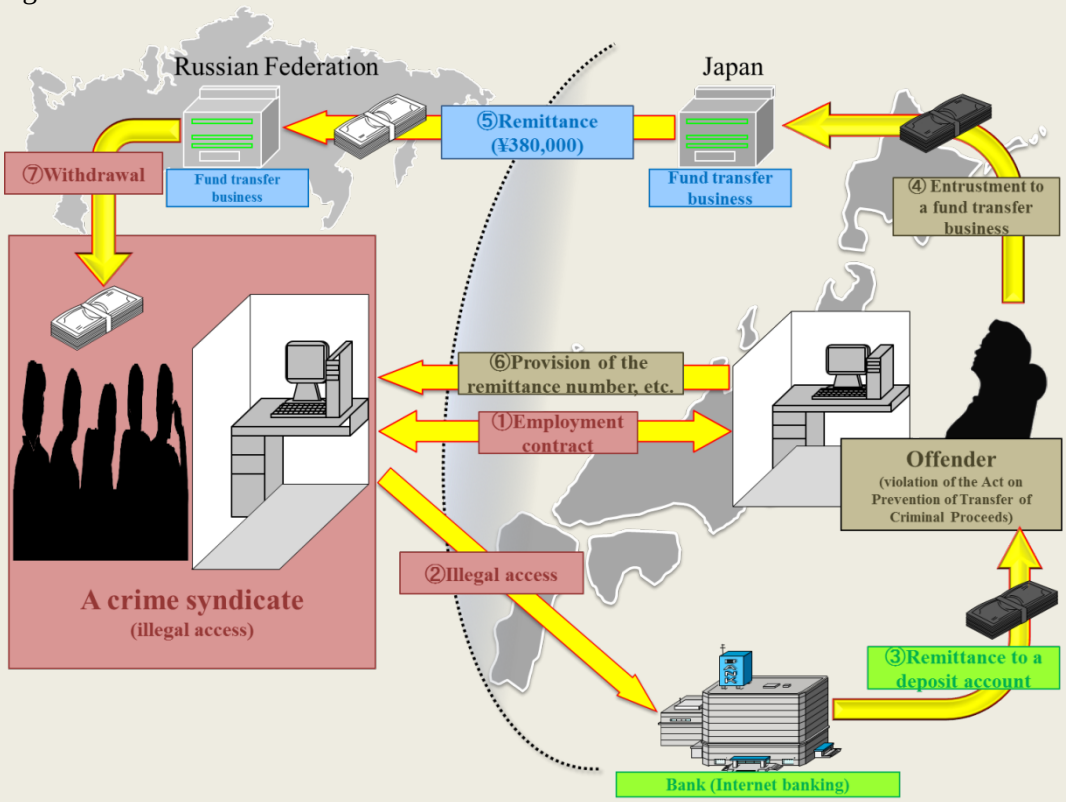
206 Between 2011 and 2012, financial investigations by the Hong Kong Police Force (HKPF) revealed that a group of 135 residents from Country X used false bank statements and documents showing the same residential address as proof of address to open 135 accounts in 42 branches of a bank in HKC. A total of eight different addresses were used by the stooges who sold their accounts to a money laundering syndicate for HK$500 to HK$3,000 (~USD65.00 to ~USD385.00). Some of the account holders also applied for credit cards to obtain cash advances. The total transactions in these 135 accounts were HK$145 million (~USD18.6 million). The syndicate operated the stooge accounts via internet banking. Between 2013 and 2015, a total of 19 syndicate members were convicted of money laundering or various fraud-related offences with imprisonment from three months to three years.

INDIA

207 A terrorist organization used a foreign based trust for raising, collecting, and transferring funds to India through banking/cash couriers/non-banking channels for its distribution to active terrorists units and other beneficiaries of the terrorist organization and families of terrorists. In this case extensive use of email network was cracked and evidence collected. The case is presently under further investigation.

JAPAN

208 A foreign man from jurisdiction X who is a resident in Japan registered with a job search site for foreigners living in Japan and concluded an employment contract concerning remittance work with a person claiming to represent a foreign consulting company and other persons. At the instruction of those persons, the man remitted to an individual in Russia via a fund transfer business in Japan around JPY 380,000 (~USD3,465), the amount remaining after the subtraction of his own fee and the remittance fee from the JPY 400,000 (~USD3,645) in proceeds. The man provided, via email, information necessary for the receipt of the remittance (remittance number, etc.) to the person claiming to represent the consulting company. As a result, the man was arrested for violating the Act on Prevention of Transfer of Criminal Proceeds (sale of exchange cards, etc.). Further investigation revealed that the remitted funds were withdrawn in Russia on the day of the remittance, see below figure.



MALAYSIA

209 *Background of subjects & modus operandi:*

- Person X, while not having a capital market license to carry out regulated capital market activities, set up an internet-based investment scheme to solicit investments from the public through several websites;
- The investment scheme misrepresented itself as having investment portfolios in capital market products such as equities and commodities. Investors are offered returns of up to 300% within 15 months; and
- An investor is required to place a minimum investment of US$100. An additional US$30 is required to activate an investor's trading account. The cash is then converted into *e-points*; in which US$1 is equivalent to 1 e-point. This e-point can be exchanged for cash through the investor's trading account or sold to other investors. Similar to a pyramid scheme, existing investors (known as up-liners) who bring in new investors (known as down-liners) will receive lucrative commissions and incentives.

210 *Method used:* regular transfers of funds to tax haven jurisdiction; unjustifiable occurrence of back-to-back deposits and withdrawals in bank accounts; utilization of high risk business entity such as money changers where unjustifiable fund transfers were sighted.

211 *Source of information:*

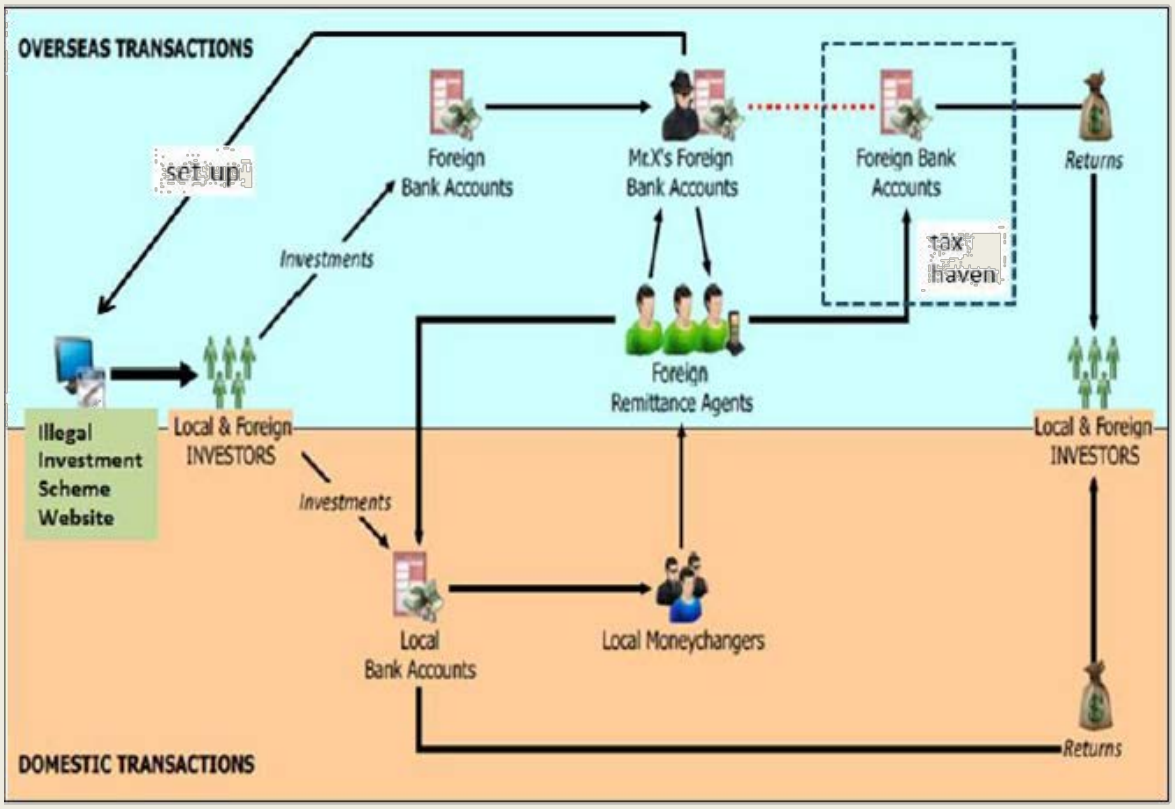
- STR and CTR records;
- Complaints from public; and
- Exchange of information with foreign securities commissions.

212 *Facts of the case:*

- Financial investigations revealed that monies collected from investors were dissipated across numerous local and foreign bank accounts controlled by person X;
- Monies were also transferred through several illegal moneychangers in Malaysia and illegal remittance agents located in several foreign jurisdictions. It was suspected that cash from local licensed and unlicensed moneychangers were transferred to the foreign remittance agents, either through hawala system or physically brought out from Malaysia; and
- Investigation discovered that monies from the foreign remittance agents were transferred to the investment scheme's bank account located in a tax haven jurisdiction. The returns paid to investors were paid out from the bank accounts controlled by person X in Malaysia, or from the investment scheme's foreign bank accounts.

213 *Actions taken to date:*

- Securities Commission of Malaysia (SC) had exercised civil powers under the securities law to obtain an international *mareva* injunction against person X and his associates, ordering them to cease all activities and freeze the monies collected from the investment scheme;
- SC had also obtained a further court order directing that RM35 million (~USD8.68 million) held in one of person X's foreign bank accounts to be transferred back to Malaysia;
- In addition, SC filed a civil suit against person X and his associates for the following breaches:
    - holding out as fund managers without a capital market license;
    - holding out as investment advisers without a capital market license; and
    - making false statements on the website inducing the public to invest.
- SC successfully obtained a consent judgment against person X and his associates. Following the judgment, SC entered into a settlement agreement with the defendants whereby a settlement sum of approximately RM31 million (~USD7.68 million) would be disgorged from them;
- In addition, a civil forfeiture has been filed on a further RM5.5 million (~USD1.36 million) of ill-gotten gains seized from local bank accounts under the AMLA (civil forfeiture); and
- An independent administrator was appointed by the SC to manage the restitution process to investors who suffered losses as a result of the illegal investment scheme. A total of RM30.53 million (~USD7.57 million) disbursements were made to 19,625 eligible claimants.



PAKISTAN

214 *Case 1: Suspect was involved in defrauding the general public through internet scams.* An STR was reported on person A by Bank X. This individual maintained a personal account and a business account at the same bank. The account title was 'paypayonline' which was a sole proprietor concern. The profession of the customer was stated as Software Developers. Another STR on the same individual was reported by Bank Y. A complaint was received from another customer of the bank and it was brought to their notice that the person A lures the general public by offering them a debit card after charging a fee through his website. Further, analysis of statement of account showed multiple cash deposits of small fixed amounts of Rs.3,000 (~USD28.00) in the account of person A. The funds deposited into the account were mostly withdrawn through ATM by person A. Because of the suspected fraudulent activities, the financial intelligence was reported to LEA.

215 *Case 2: Individuals suspected to have links with individuals running an International Cyber Crime Racket.* The accounts of individuals suspected to have links with individuals running an international cyber-crime racket were reported. Moreover, upon further investigation, one of the culprits was also listed with Interpol. The suspects were involved in cybercrime and earned revenue by generating traffic on various Premium Rate Services (PRS). The suspects used a complex method to defraud the telecom service providers. The suspects hacked into a vulnerable enterprise's PBX (telephone system) and placed multiple calls to his own PRS numbers. The hacked enterprises were technically responsible for paying the fraudulent charges but in reality they rarely paid for them. The enterprise service provider then routed the call to the provided premium rate numbers and got the call terminated by a hosted IVR system. The service provider payed the premium rate number provider the extra fee that it should be receiving from the hacked enterprises, who then shared a portion of the revenue from the calls with the number's owner.

216 These activities resulted Rs. 32 million (~USD300,000) in losses by one of the telecom company in Pakistan. Various accounts were opened by the suspects and their associates in different banks under different titles of account. The common observation in all these accounts were receipt of remittances from different telecom companies operating in different parts of the world. The matter was referred to LEA for investigation.

SAMOA

217 *Case 1.* Bank A reported a suspicious transaction involving a local company. Accordingly, the bank received instructions from the company to remit funds overseas as payment for construction supplies. An invoice and an authorisation letter (signed by the authorised signatories of the company) were provided to support payment. However, it was later discovered that the supporting documents were faked. Unfortunately, the bank had already processed the payment and the company lost thousands of Tala.

218 *Case 2.* Bank A also reported another suspicious activity involving a local company. This company sells lubricant oil and tyres and all their products are imported. The Director of the company received an instruction (via email) from his supplier to place an advanced order because oil and tyres will be running out very soon. The supplier demanded payment ASAP and the payment must be made/credited to a different bank account (and not the usual bank account that has been used for ages). The Director instructed the bank to process payment. It was later discovered that the real supplier did not send any instructions. His personal email was hacked and it was the hacker who sent those instructions. The company lost thousands of Tala.

219 *Case 3.* Another scam was reported to the FIU by one of the government ministries regarding an online job offer. The victim applied for a job on a cruise ship. He was notified that he got the job then he was instructed to pay upfront fees and charges such as employment visa, legal fees, etc. The victim later realised that it was a scam.

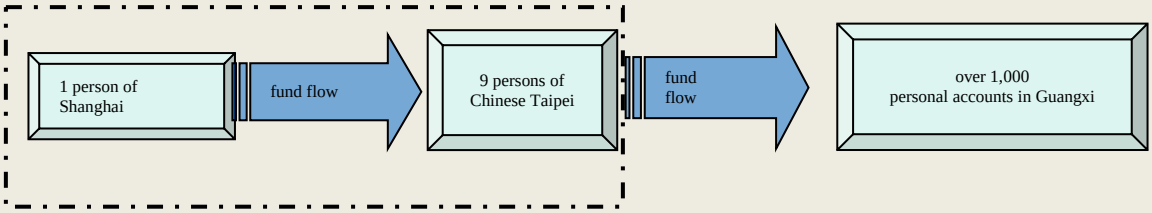
220 *Case 4.* Two different internet banking scam cases were reported by bank X. One case was related to a company while the other one was an individual. In the company case, the bank received an instruction to remit funds to pay for goods supplied. The bank actioned the transaction. Later on, the company confirmed that they did not authorise the transfer. In the individual case, the hacker transferred funds from the victim's account to another local's account. The hacker then instructed the local (via Facebook) to send funds to a given destination though a money transfer order and to keep a 10% commission.

4.10 Use of new payment methods / systems

CHINA

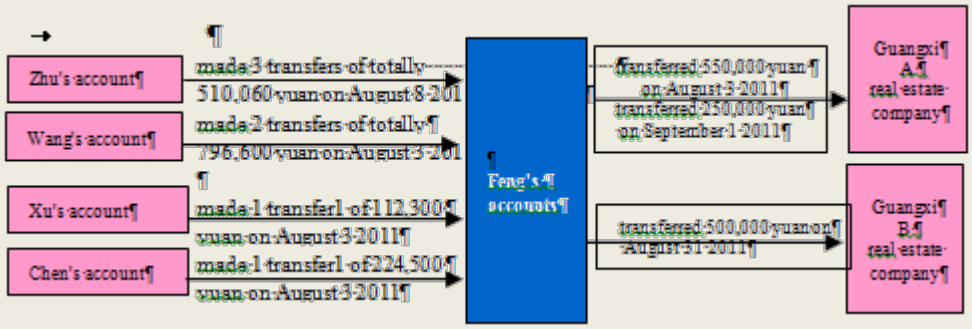
221 In 2013, the public security authority set up a team to investigate a serious pyramid selling case in China's Guangxi Zhuang Autonomous Region (Case 3.28). At the same time the China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) proactively found out that person X and 14 other people (who were the major suspects of the Case 3.28) were involved in pyramid selling. After analysis and research, this information was disseminated to the public security authority, thus providing important support to the case. The public security authority arrested 35 major suspects involved in the case and seized more than RMB 5 million (~USD770,500).

222 *Case details.* The fund transfers among person X and the others were intricate and complicated. The whole transaction amount reached RMB 0.56 billion (~USD86 million) and the transactions took place in Guangxi region. The following diagram shows the fund flow of their transactions.

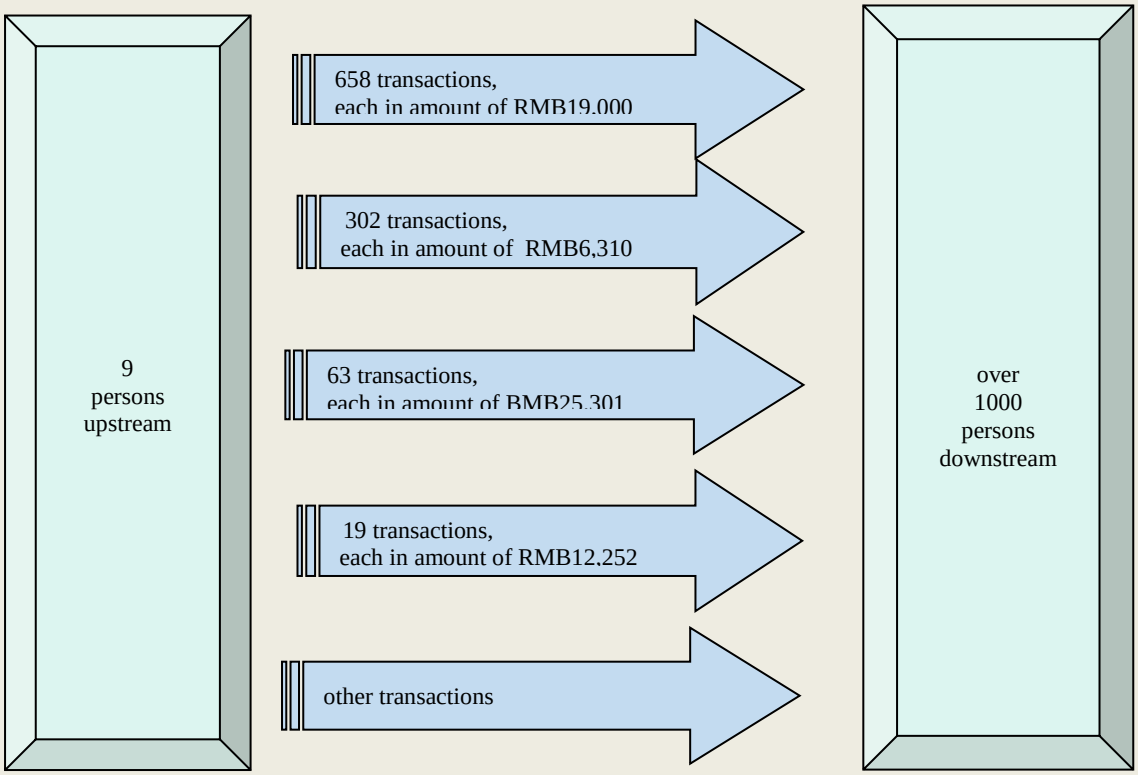


223 Taking person X as an example, she opened 40 personal accounts of which the accumulated RMB transaction amount reached 97.68 million and the accumulated foreign-currency transaction amount was equivalent to about USD 590,000.

224 It was suspected that person X committed money laundering by taking advantage of real estate. Person X and her followers made 60 transfers with the total amount of RMB 9.2913 million (~USD1.42 million) to 4 real estate companies. It was suspected that person X and her followers together transferred large funds to X's accounts that then transferred the funds to two real estate companies. The following diagram shows the transactions among them.



225 It was also found that person X posted messages of selling 48 houses in a second-hand housing trading website. The transactions took on the characteristics of funds related to an illegal pyramid selling scheme. The transactions were typical and comprised regular amounts, as illustrated in the following diagram:



226 These transactions were mostly within certain amounts and had no obvious multiple relationships, which was in line with the characteristics of a pyramid selling "rebate". Moreover, these outward transactions mostly took place on the dates of 5, 6 and 7 of each month and online banking and third-party payment methods were mostly taken advantage of in those transactions.

227 After analysis and research conducted by CAMLMAC together with the public security authority, Laibin Municipal Public Security Bureau and Nanning Municipal Public Security Bureau concluded the investigation of the case in 2013, arresting 35 primary criminal suspects and seizing more than RMB 5 million (~USD770,500) involved in the case.

228 CAMLMAC conducted detailed intelligence analysis that provided accurate and important leads for investigation by the public security authority.

CHINESE TAIPEI

229 Suspect A engaged in running a fraud syndicate with an unknown suspect B. The syndicate was involved in fraud schemes as follows: after a victim's confidence was gained, the victim was then instructed to transfer money to a designated account. Suspect A withdrew criminal proceeds, with counterfeited China Union Pay cards and cell phones provided by suspect B, through ATMs in convenience stores and financial institutions. Suspect A was then instructed to carry criminal proceeds to a designated location and delivered to suspect B. Through the initial investigation performed by Criminal Investigation Bureau, suspect A and three other accomplices were arrested at the scene, capturing 68 counterfeited China Union Pay cards, NTD 510,000 (~USD15,700) of criminal proceeds in cash, cell phones and other related evidence. The case was transferred to the Changhua District Prosecutors Office in 2015 for further investigation.

FRANCE

230 Payment sector companies are attractive to investors and also appeal to criminal organisations. The interest shown by organised crime groups may be greater than expected because some companies in this sector are not or will not be regulated, and they can sometimes be run by a limited number of staff – making the company easier to control. The search for channels through

which to launder the proceeds of cybercrime can only increase the sector's overall exposure to the risks of criminal interference.

231 Some payment sector companies are appealing to criminal organisations as they allow the layering of financial flows and the mixing of funds from legal sources with sums of illegal origin, as well as expanding the scope of the collection account technique, as the following case illustrates. When it comes to these fund collection schemes that may bring in various individuals or legal entities resident abroad, information exchanges with FIUs make a big contribution to the detection and investigation process.

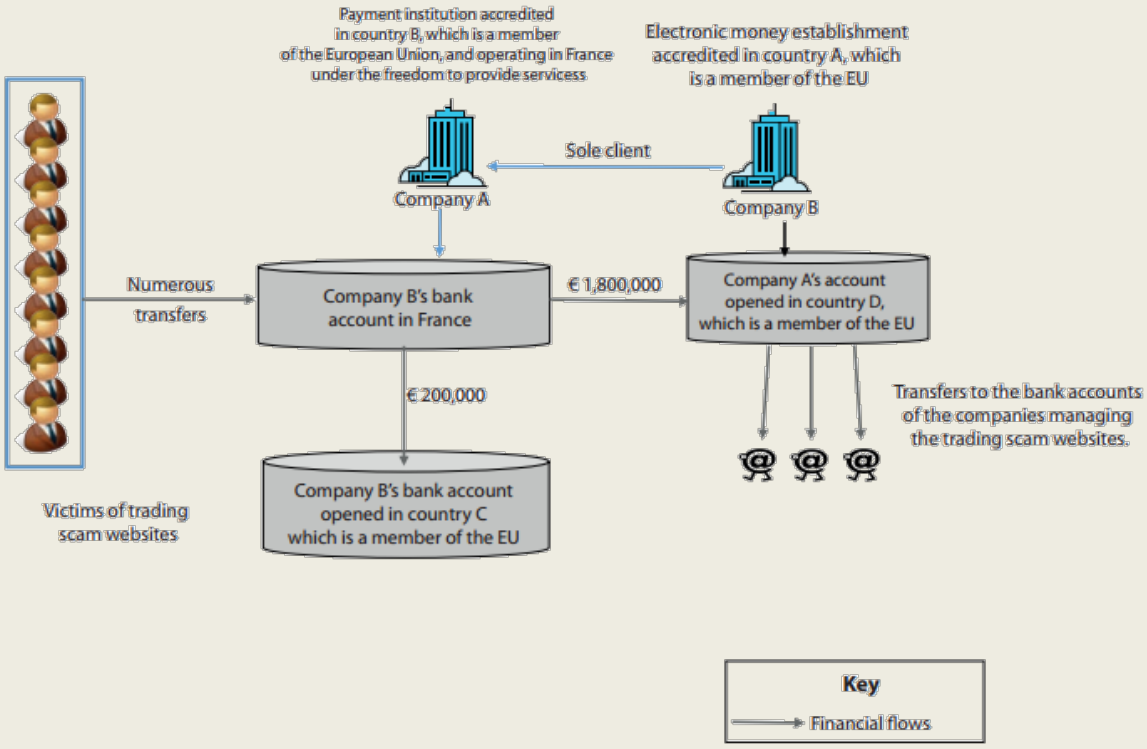
232 *Case of flows leading to the suspicion of wrongdoing*. The victims of the scam were canvassed by telephone and invited by a call centre agent to place a first, often small, bet on websites offering binary option trading, for which no authorised investment service provider could be clearly identified. The legal information on these websites referred to registered companies in countries lacking an effective AML system. The professional appearance of the websites and the fact that bets could be placed by bank transfer to a bank account opened in France inspired confidence in the victims, to gradually increase their bets. The deception continued until they requested the collection of their winnings.

233 Company A, a payment institution accredited in country B, which is a member of the European Union, used as its main selling point on its website its ability to collect bank transfers from banks in many countries on behalf of its e-merchant clients. The amounts collected were then transferred to their final beneficial owner (the e-merchant) in exchange for a fee. Company A had opened bank accounts in various countries, including country C, in order to provide this service.

234 The bank account opened in France by company A therefore received numerous transfers from individuals. When the account was opened, company A's representative explained that this account would receive payments for purchases, with an average shopping basket of around €300 (~USD335.00) from various merchants using company A for their payments initiated by French customers. This explanation did not match the actual flows received, as the bank account was soon credited with transfers ranging from a few hundred euros to several tens of thousands of euros, whose instructing parties were individuals located in France and in other European countries.

235 The funds collected in company A's French bank account, amounting to nearly €2 million (~USD2.2 million) in the space of two years, were then transferred to two accounts abroad. Nearly €1.8 million (~USD2 million) was paid into the account opened in country D by company B, an electronic money establishment accredited in country A, which is a member of the European Union. These funds were subsequently transferred to the foreign accounts of the companies linked to the trading scam websites. The remaining €200,000 (~USD200,000) was transferred to the foreign account of company B in country C.

236 The contrasting of an electronic money establishment (company B), as the sole, long-standing client of the payment institution (company A), therefore represents a double layering of financial flows that might reasonably be thought to come from internet trading scams and was therefore intended to obscure the financial network in order to limit its traceability, see below figure.



4.11 Laundering of proceeds from tax offences

CHINA

237 In China, when goods are exported abroad, the value-added tax (VAT) will be rebated. Some people use that policy for making illegal profits. In 2013, the police in Fujian province cracked a big case, which involved eight suspects who produced false VAT invoices. It was revealed that these suspects had used two shell companies to make false VAT invoices for about 750 companies. These suspects helped companies make false trade, so that those companies could get a tax rebate, and they got money from the companies. According to the police statistics, the sum of the false VAT invoices reached to RMB 5 billion (~USD 0.77 billion), and suspects had earned about RMB 10 million (~USD 1.5 million) from their illegal activities.

FIJI

238 *Case 1.* Fiji FIU received three STRs on transactions occurring in the personal bank account of person X. Analysis of these STRs found that person X, who is also the director of company X, received large inward remittance transactions from a foreign jurisdiction for the purchase of property in exclusive tourism locations in Fiji. Fiji FIU investigation established that person X did not purchase any property at the intended location. The amount involved in the case was FJD0.4 million (~USD193,000). Further analysis established possible tax offences involving company X, where business proceeds were deposited into person X's personal bank accounts. Furthermore, company X was not fully declaring its income to tax authorities. A report was disseminated to the Police and Tax authority for possible money laundering and tax offences. Investigations are currently underway.

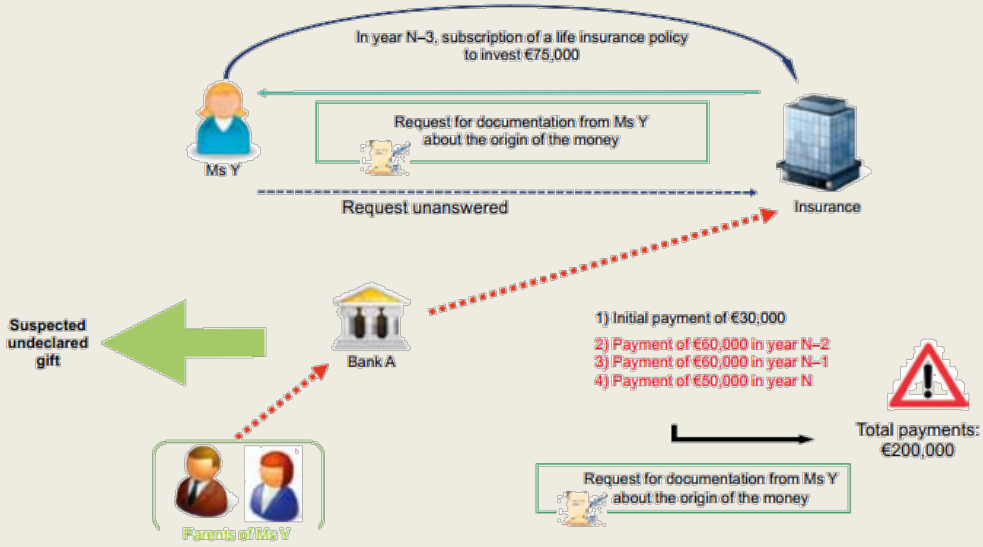
239 *Case 2.* Fiji FIU received a STR on person X. person X was reported for paying a one-time premium of FJD140,000 (~USD67,500) for a life insurance policy for his son who resides in another country. Fiji FIU established that person X is the director of 3 business entities. Analysis of person X's bank accounts revealed that person X was receiving deposits in excess of the amount he was declaring as income for tax purpose. A report was disseminated to the tax authority for possible tax offences.

240 *Case 3.* The Fiji FIU received a STR on a large number of cheque deposits made into person X's personal bank account. Analysis revealed that person X's personal bank account was used to conduct 'business like transactions'. The amount involved was approximately FJD0.7 million (~USD337,000). A report was disseminated to the tax authority for possible tax offences.

241 *Case 4.* In 2011, Fiji Revenue and Customs Authority (FRCA) noticed an anomaly in their database. It was found that 27 tax payers were using the same postal address. FRCA conducted an investigation into the anomalies and discovered that fraudulent transactions had occurred. It was discovered that between 1 February and 31 March 2007, person X negotiated a cheque for FJD2,400 (~USD1,155) that was obtained using a fraudulent tax return. Person X was not registered as a tax payer and therefore not entitled to receive a tax return. On 23 September 2015, person X was convicted of money laundering and in 2015 the High Court of Fiji sentenced her to 5 years imprisonment.

FRANCE

242 *Case involving life insurance, tax fraud and suspected undeclared gifts.* In year N–3, Ms Y took out a life insurance policy with an initial payment of €30,000 (~USD34,000). Additional payments of €60,000 (~USD68,000) were made in year N–2 and N–1, and €50,000 (~USD56,500) was paid in year N. The following year, Ms Y fully redeemed the policy. She stated that she needed money for a real estate purchase. Additional enquiries and requests for documentation by the insurance firm revealed that the payments had not been made by Ms Y but rather by her parents. Actions such as these may be used to circumvent gift taxes.



KOREA

243 Due to frequent money transfers and cash withdrawals in large amounts from person L's accounts, who was the employee of XX Steel Co., Ltd, and family members of the CEO of XX Steel, an STR was filed on the grounds that borrowed accounts may be used to evade corporate tax.

244 Analysis was performed on transactions of accounts titled to person K (CEO of XX Steel Co., Ltd), person S (wife of person K) and five other persons (including the sister and brother-in-law of person K). Analysis showed that large amounts of funds were deposited into these accounts from potential trading partners of XX Steel Co., Ltd and subsequently funds were withdrawn in cash and deposited back to trading partner's accounts. Out of KRW 5,124,000,000 (approximately USD 4,300,000) deposited into accounts person L account, KRW 3,609,000,000 (approximately USD 3,000,000) was withdrawn in cash in order to avoid tracing the source of funds. Thus, it is believed

that accounts of 6 persons mentioned above were borrowed in order to manage of sales generated by XX Steel.

245 The information was disseminated to the National Tax Service of Republic of Korea on suspicion of tax evasion.

PAKISTAN

246 The proprietorship accounts of IK and SA were opened in a tax exempted region and transactions in their accounts were conducted online in order to evade withholding tax on cash withdrawals. Furthermore, from the transactional activity and the region where the accounts were maintained, it was likely that IK and SA were involved in hawala/smuggling.

247 Case details. The bank reported two proprietorship accounts maintained by IK and SA. The accounts were maintained at XYZ Bank's branch located in tax exempted area. The accounts were reported by the bank due to large turnover and inconsistent patterns of transactions – transactions were conducted with unrelated counterparties and the transactions in the accounts were conducted online from different regions.

248 Upon analysis, the accounts of IK and SA were found to be linked due to same office contact number provided in the account opening forms. Further, it was revealed that the accounts were operated by a third party under a mandate, which raised concerns regarding the beneficial ownership of the accounts. Furthermore, besides large turnover reported in the accounts, many transactions in cash mode were conducted in the accounts and a majority of the transactions in the accounts were conducted online from XYZ Bank's branch located in tax exempted area.

249 Many CTRs were reported on IK and SA and from these reports various other banking relationships maintained by IK and SA in different banks were identified. For an account maintained by IK, an STR was reported when he tried to remit USD 900,000 – the request to transfer the funds was, however, declined by the bank. The said activity was also conducted in ABC Bank's branch located in tax exempted area.

250 It was apparent from the transactional activities that the accounts of IK and SA were maintained in tax exempted area to evade withholding tax on cash withdrawals. Due to large turnover in the accounts being maintained in the tax exempted area which is prone to misuse of tax exemptions, trade of smuggled goods and hawala / hundi, the financial intelligence was shared with relevant LEAs for investigation . Furthermore, the matter was also referred to the regulator to look in to the matter to discourage such practices.

NEW ZEALAND

251 *Case study Operation Starlifter – transnational tax evasion.* This operation involved an investigation into New Zealand registered shell companies that were being utilised to legitimise false expenses for companies in jurisdiction X, in order to reduce their income tax. The fraud involved an accountant based in jurisdiction Y who registered shell companies in countries including New Zealand. The accountant used the certificates of incorporation of these shell companies to set up 150 foreign currency accounts in New Zealand. Over a period of 10 years the accounts were used to evade an estimated NZD100 million (~USD68 million) of tax by jurisdiction X citizens. Approximately NZD30 million dollars (~USD20 million) was seized by New Zealand Police in bank accounts held for the shell companies.

252 This case is published in Typology Report Q2 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014-2015.pdf

THAILAND

253 *Tax fraud case.* Offenders set up several entities to act as sellers and value added tax (VAT) claimant entities. All entities were set up during the same period of time with the same shareholders and business addresses. The entities remained open for only six to eight months. These entities were divided into two groups, trading in scrap metal and exporting scrap metal. Trading documents were created to mock the transactions with goods being overpriced, the exporters bought at 11 Baht (~USD0.3) per Kilogram and sold at 600 Baht (~USD17.00) per Kilogram. These documents were then submitted to Revenue Department for tax refund. Proceeds from fraud were used to buy real estates, cars, land, and the opening of gold bullion trading accounts.

4.12 Real Estate, including roles of real estate agents

CHINESE TAIPEI

254 Person C worked in company T (a company listed in 1964), and was in charge of the components purchasing business. Between September 2010 and February 2014, person C conspired with person W, the chairman of company S, and person CH, the chairman of company L, to engage in simulated/sham/fraudulent purchases. Based on the scheme, person C operated the purchasing system of company T to reduce the enquiring date from 18 days to several days or even 1 day to impede manufacturers to submit prices. He also forged quotation forms to create a false appearance that companies S or L quoted the lowest price for purchasing. Therefore, the two companies could win the bids with C's illegal behaviour. As a matter of fact, the price that S and L companies quoted was multiple or hundreds of times of market price. Company S won 244 purchasing cases and falsely quoted with about NTD 49 million (~USD1.5 million), and company L won 271 purchasing cases and falsely quoted approximately NTD 54 million (~USD1.6 million). For the reward, person. W gave person C NTD 9.51 million (~USD0.29 million) in cash; person CH gave person C NTD 5 million (~USD0.15 million) in cash and remitted about HKD 1 million (~USD30,000) to person C's wife's account in jurisdiction X. In order to conceal the proceeds of crime, person C on behalf of his wife transmitted NTD 7.43 million (~USD0.22 million) to company Y as the fund for purchasing real estate. The authorities initiated a criminal investigation and then referred this case to the District Prosecutors Office in 2015 for prosecution.

JAPAN

255 An executive of company X provided a building owned by a subsidiary of company X to a man managing a massage parlour and received as rent payments around JPY 11.4 million (~USD0.1 million) into an account opened in the name of the subsidiary company. Rent payments were made out of profits earned through prostitution. As a result, the executive of company X was arrested for violating the Act on Punishment of Organized Crimes (receiving of criminal proceeds).

NEW ZEALAND

256 *Case study - Purchase Using Proceeds Outside Of Banking System.* Exchange of high value goods and cash for property may allow criminals to integrate proceeds while avoiding the financial system, as indicated in this case reported in a suspicious transaction report by a vendor's lawyer. The vendor indicated to his lawyer that a NZD50,000 (~USD34,000) deposit for a rural property had been paid to him in cash by the purchaser. He then confirmed in writing to the lawyers that the purchaser had paid the NZD130,000 (~USD88,400) balance by way of an unknown amount of cash, the transfer of a boat, caravan and car and offsetting debts owed by the vendor to the purchaser for building work completed by the purchaser (amount unknown). The vendor was unable to provide conclusive evidence to his lawyers that any money had been received from the purchaser, or that the money had been banked into his account.

257 Conducting the sale and purchase of property in this manner is highly unusual and the vendor's unwillingness to provide full information and evidence to his lawyers regarding the

settlement suggests that he was attempting to conceal the true nature of intentions of the property transaction.

258 Subsequent investigation by Police established that the cash and the assets were the proceeds of methamphetamine dealing.

259 *Case study - Purchase Using Rent to Own Scheme to Hide Offender's Interest in the Property.* The rural home of the respondent in a drug supply case was the scene of the predicate offending and the subject of forfeiture order.

260 The property was listed in the sole ownership of an unrelated third party. Police investigation discovered that the effective control of the offender was hidden by a 'Rent to Own' contract between the offender and the owner of the property. This contract details the purchase of the property for the consideration of NZD118,000 (~USD80,240). The contract further stated that as consideration for this option to purchase, the buyer (the offender) shall pay the seller a fee of NZD60,000 (~USD40,800) which was remitted by the transfer of a motor home/bus. The contract then detailed the outstanding balance at the time of signing as being NZD58,000 (~USD39,440). This was to be satisfied by a lump sum payment of no less than NZD5,000 (~USD3,400) with a further NZD200 (~USD136) per week, to be paid by automatic deduction from the buyer's bank account.

261 The rent to own agreement included a residential tenancy agreement which provided for ongoing weekly rental payments of NZD200 per week along with other tenancy obligations. The initial deposit on the house was NZD50,000 (~USD34,000).

262 This deposit was paid in cash in a mixture of denominations including NZD100s and NZD50s. The seller also received a house bus valued at NZD60,000 (~USD40,800). The effect of this arrangement was to allow the property to remain in the name of the vendor and attempt to hide the true ownership of the property from any interested parties. There is no evidence that the vendor is part of the offending or the agents acting on her behalf.

263 *Case study - Trusts and Accountant Used to Hide Ownership and Facilitate Tax Evasion.* In this case, the beneficial ownership was hidden using a trust and the services of an accountant. The respondents borrowed significant funds to purchase their house. These funds were borrowed in the name of a trust and the ownership of the property was also put into the name of the trust. The first respondent then received about NZD1.5 million (~USD 1 million) as a commission for consultancy work completed through a company she controlled. The funds were transferred through a number of accounts to finally be used to part pay for the asset the trust owned. Again the funds were transferred to an accountant with a view to minimise the tax that would be required to be paid on the funds. They were then returned immediately less the commission taken by the accountant and was then again deposited into the mortgage account of the trust.

264 *Case study - Use of Proceeds to Repay Mortgages.* Use of a mortgage to be repaid in cash appears to be a common method that allows structured cash placement. In one case, a family-based crime syndicate used multiple real estate investments to place the cash proceeds of drug dealing. An initial flat was put into the name of the family trust. This property appeared to be purchased from legitimate sources in that it came from the estate of the deceased husband. Further flats were put in the name of a family trust and what appears to be legitimate finance was used to purchase them. The loans were paid back via the payments in the normal manner from bank accounts that were receiving large amounts of cash, which proved to be from the proceeds of drug dealing. But for the cash payments the respondents could not have funded their lifestyle and the repayments of the finance.

265 There were also two sections belonging to the son and business partner of the principal offender. These sections were transferred into the name of the mother for a nominal amount. It is suspected that these properties were transferred for an amount significantly lower than the market values to either satisfy a debt owed or to provide an asset base where the acquisition of assets can be justified given the low cost of the assets. These assets could be sold a later date for a premium which

would then instantly provide the respondents with what appears to be legitimate funds to reinvest or use as equity for further property investment at a later date.

266 *Case Study - Cash Paid Directly To Lawyer.* In this case, a lawyer played a direct role in hiding the ownership of a property and the use of proceeds of crime to pay for the property. An offender met with the lawyer to discuss purchasing a section with a view to building a house on the section. The offender was bankrupt and owed the official assignee NZD1.2 million (~USD.81 million). The lawyer suggested establishing a trust where the offender would be a beneficiary of the trust and the lawyer and the offender's girlfriend would be trustees. This was an attempt hide assets from the official assignee.

267 Within a couple of weeks of this first meeting, the offender took NZD300,000 (~USD204,000) in cash and gave it to the lawyer who subsequently deposited it into the lawyer's trust account in four separate deposits. The lawyer filed a suspicious transaction report in relation to this cash transaction. However, the lawyer lied when completing the STR by writing that it was the offender's girlfriend who bought the cash in when in fact it was the offender himself.

268 The lawyer then transferred the funds electronically to the vendor's lawyer on settlement day. A year later the offender took NZD129,000 (~USD87,700) in cash and gave it to the lawyer who subsequently deposited it in two separate deposits into the lawyer's trust account. Two progress payments were then made from the lawyer's trust account to the company building the offender's house. Further cash was deposited to the bank account of the offender's trust that the lawyer set up enabling the remaining payments totalling NZD300,000 to be made to the company building the offender's house. The offender took a further NZD122,000(~USD82,000) in cash and gave it to the lawyer who subsequently deposited it in two separate deposits into the lawyer's trust account. This money was to pay the offender's former girlfriend when the offender and the girlfriend separated. In total, the offender gave the lawyer NZD578,000 (~USD393,000) in cash which was transacted on behalf of the offender.

269 The above five real estate case studies are all published in FIU Quarterly Typology Report Q4 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q4-2014-2015.pdf

4.13 Association with human trafficking and people smuggling

FIJI

270 A STR was received on a foreigner, person X, who was allegedly receiving remittances totalling FJD31,523 (~USD15,000) from different individuals overseas. The purpose given for these remittances was "student allowance and fees". Fiji FIU established that person X was supposedly directed by person Y, a local travel agent, to receive the remittances on his behalf. The remittances were alleged to be fees for foreign students to study at Fijian tertiary institutions. Fiji FIU investigations established that person Y obtained the funds for his personal use and he also seized these foreign students' travel documents. A report was disseminated to the Police and investigations are currently underway for possible human trafficking.

MACAO, CHINA

271 In mid-2015, local LEA was informed that a human smuggling syndicate was raided by Chinese authorities and found that the leader of the syndicate was a Macao citizen. The syndicate had been operating since 2008. There was indication that the members within the syndicate hid their criminal proceeds in Macao, China. In order to trace and seize the criminal funds flowing within Macao, an ML investigation was initiated against the syndicate leader and his relatives. Further investigation revealed that their bank accounts had irregular large amounts of cash deposits since 2000, and the funds had been aggregated for a long period of time. These deposited funds were under the control of the leader and his wife. Local LEA effectively seized all the related illegal funds

discovered in the bank accounts of the leader and his relatives, totalling approximately HKD10 million (~USD1.28 million).

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

CANADA

272 In 2015, two individuals (husband and wife of foreign decent from jurisdiction X) were convicted and sentenced to eight years in prison by a Quebec Court judge for laundering more than CAD100 million (~USD77 million) in illicit drug-related proceeds on behalf of a prolific cocaine smuggler. From 2000 to 2004, one of the two individuals transported millions of dollars of cash to jurisdiction X that was subsequently deposited into bank accounts for laundering purposes. The initial cash seizure, which initiated the investigation, was made at the Montréal-Trudeau International Airport. In addition to the eight-year sentence, each individual were ordered to pay a fine of CAD2.4 million (~USD1.85 million) or face an additional five years imprisonment. The Crown confiscated a range of assets from the two individuals, including bank shares worth $5 million (~USD3.85 million), two pieces of real estate, CAD600,000 (~USD460,000) in cash, and jewellery worth CAD1 million (~USD.77 million).

CHINA

273 *Case 1*. In 2014, the People's Court of Guangan, Sichuan Province pronounced judgment on person X's money laundering case after a public trial. Person X was found guilty of: (i) collusive tendering and fined RMB 4 million (~USD0.6 million), and (ii) money laundering sentenced to 3 years imprisonment with a 3-year reprieve and a fine of RMB 2 million (~USD0.3 million). The court decided to execute the penalty of 3 years imprisonment with a 3-year reprieve and a fine of RMB 6 million (~USD.92 million).

274 *Case details.* During the investigation of the corruption case of person Y, the general manager of Sichuan branch of China Mobile Communications Group Co., LTD, who fled to jurisdiction X. Person X, the legal representative and president of a technology company in Chengdu, opened two bank accounts of offshore companies in jurisdiction Z under the instructions of person Y, which was provided to person Y for misuse from 2007 to 2008. Person Y took advantage of the bank accounts of the two offshore companies to take and transfer the bribes of over HKD 22 million (~USD2.8 million). After person Y fled to jurisdiction X in 2010, person X sent somebody to inquire the above two accounts and found there were a balance of HKD 22 million (~USD2.8 million) in them, and then reported the loss of the two accounts to the bank. Person X instructed somebody to go to jurisdiction Z and transfer the illicit money to China through the underground money shops but then the illicit money was frozen by a competent authority on suspicion of money laundering. The Public Security Bureau of Deyang, Sichun province commenced investigation in 2010.

275 *Case 2*. In 2014, the People's Procuratorate of Lucheng District, Wenzhou, Zhejiang Province instituted a public prosecution of person X for money laundering. The Intermediate People's Court of Wenzhou convicted person X of money laundering and person X was sentenced to 4 years imprisonment and a fine of RMB 1 million yuan (~USD.15 million).

276 *Case details.* From 2007 to 2009, person Y fished more than 60 investors and defrauded them of over RMB 200 million (~USD30 million) under the cover of investing in businesses including mines and hotels, and a promise of higher profits. On suspicion of committing fund-raising fraud crime, person Y was arrested on August in 2013. During the investigation, the police found that person Y had financial problems since 2011. Person Y and his brother person X conspired to transfer person Y 14.12% share of a mine company to person X in the way of false equity transfer. Clearly knowing that the shares were purchased with the funds illegally raised by person Y, person X still colluded with him to disguise and conceal the proceeds of crime by purchasing those shares and changing the registration to the name of person Y with the false payment of RMB 9.6 million

(~USD1.4 million) through a telephone transfer service opened by a food company limited in Wenzhou whose legal representative was person X.

277 *Case 3.* In 2014, the Intermediate People's Court of Zhangzhou, Fujian province convicted person A, B and C of fund-raising fraud crime. Person A was sentenced to life imprisonment, deprival of political rights for life and confiscation of all personal property. Person B was sentenced to 12 years' imprisonment and a fine of RMB 100,000 (~USD15,500). Person C was sentenced to 8 years' imprisonment and a fine of RMB 60,000 (~USD9,200).

278 *Case details.* Since 2002, person C had been in a debt from illegal gambling. From 2009 to November 2012, person A, alone or conspired with person B and person C, fished and defrauded 55 investors of large sums of money with a promise of higher profits and various excuses for financial needs such as repaying the loan on behalf of others or opening farms. The funds were used to gamble in illegal "sports lottery" and "mark six lottery" or repay the original investment and higher profits of the former investors. The loss of RMB 130 million (~USD 20 million) of the victims had not been returned until the case was discovered. When person A illegally raised the fund from person C and four other victims between 2010 and 2012, person B passed himself off as the employee of a rural credit cooperative or industrial and commercial administration to participate as a co-partner or a guarantee, finally leading to the loss of RMB 60 million (~USD9.2 million), which had not been returned until the case was discovered. Clearly knowing that person A intended to avoid the detection of competent authorities, person B provided his bank accounts to person A for the transfer the criminal proceeds from his fund-raising fraud. Clearly knowing that person A and person B committed the crime of fund-raising fraud, person C still participated and defrauded illicit money to the total of RMB 7.36 million (~USD 1 million) in 2012.

FIJI

279 *Case 1.* A STR was received on person X for misuse of pre-signed cheques of company Y. Person X was employed by company Y and was issued with pre-signed company Y cheques to facilitate daily business payments required for company operations. Person X cashed these pre-signed company cheques at various retail outlets of company Z. The funds cashed from the pre-signed cheques were used to conduct a money lending business. The pre-signed cheques cashed totalled over FJD4 million (~USD1.9 million). Person X profited from the interest she charged for lending money and deposited the principal sum back into her employer's bank account. Person X was able to cash company Y's cheques through company Z as her spouse was a Manager at company Z. The case is currently under investigation.

280 *Case 2.* From May 2012 to October 2013, person X, while an employee of Bank Z, stole funds from the Bank Z suspense accounts and convinced Bank Z account holders as third parties to allow him to transfer the stolen funds to their accounts and conduct withdrawals for himself. Internal audit checks revealed discrepancies in the accounts and after investigations it was revealed that person X stole and laundered approximately FJD350,000 (~USD168,000). In April 2015, person X was sentenced to 8 years imprisonment after being convicted of 8 counts of money laundering. In December 2015, person X was sentenced to 5 and a half years imprisonment.

HONG KONG, CHINA

281 Between 2008 and 2012, a financial investigation by the Hong Kong Police Force (HKPF) revealed that an ex-senior accounting officer (person A) of a local insurance company, by fraudulent insurance claim, issued 75 cheques amounting to HK$73.8 million (~USD9.5 million) to nine non-clients of the insurance company. These nine people who assisted person A in receiving crime proceeds were his wife and friends. In 2015, person A pleaded guilty to two counts of money laundering and two counts of fraud with seven years and six months imprisonment. Five other syndicate members were also convicted of money laundering with imprisonment ranging from 28 to 53 months.

JAPAN

282 *Case 1.* Associates of Boryokudan (Japanese crime syndicate) arranged for an acquaintance to obtain the position of an originator by making payments for shares issued at the time of the establishment of a stock company using JPY 9 million (~USD80.000) out of some JPY 16 million (~USD140,000) defrauded on the pretext of a loan for fictitious purchase of equipment of a company managed by himself. The man also arranged for the acquaintance to be appointed as a director of the stock company at the time of foundation and to make the foundation registration of the company at a regional legal affairs bureau, thereby making the foundation effective, and to be appointed as the representative director of the company. As a result, the man was arrested for violating the Act on Punishment of Organized Crimes (management control through illicit proceeds).

283 *Case 2.* A male dentist, in an attempt to defraud a company selling dental treatment materials of metal and to gain profits by selling it, falsely stated to the company that he needed the metal for treatment and defrauded it of the metal. The dentist arranged for an acquaintance unaware of the situation to sell the metal for around JPY 9.3 million (~USD85,000). As a result, the dentist was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

284 *Case 3.* A man illicitly retailing methamphetamine sent it his customer by postal delivery. He had his customer transfer purchase payment to the bank account opened under the name of third party. As a result, around JPY 13.5 million (~USD124,000 million) was transferred to the account. He was arrested for violating the Anti-Drug Special Provisions Law (concealment of drug-related criminal proceeds).

MACAO, CHINA

285 *Suspicious money laundering of fraud proceeds with the use of third party individual bank account.* Person A from Country X opened a bank account with a local bank in Country Y. He claimed to work in a local restaurant and the account was opened for receiving his monthly salary. After a few months without any transactions, the account of person A suddenly received a large sum of inward remittances from a company in Country Z. Shortly afterwards, Bank Y received a refund request from the remitting bank because the funds were related to a fraud case in Country Z. The fund was then returned to the remitting bank as requested.

286 Further analysis revealed that the company in Country Z was a technology company and there was no apparent business relationship between the company and person A. There was no reasonable ground to support the purpose of the remittances and it was believed that the account was used for receiving funds from fraud victims overseas. The case was submitted to the Public Prosecutions Office for further investigation.

NEW ZEALAND

287 *Case Study - Operation Keyboard.* Police conducted a financial investigation into a large drug importation and supply ring centred in jurisdiction X and New Zealand that culminated in multiple convictions for money laundering and drug offences along with restraint of almost NZD 3 million (~USD2.04 million) worth of property, vehicles, cash and other assets.

288 Concurrent with its drug offending, including multiple importations of ecstasy and LSD, the syndicate involved in the case laundered millions of dollars using intermediaries. The use of intermediaries allowed the central New Zealand-based figure of the drug supply ring, person RB, to maintain a front of being an unemployment and later sickness beneficiary. The vast majority of transactions identified during the financial investigation involved intermediaries for RB rather than RB himself to deflect any possible scrutiny of RB's finances.

289 However, even excluding money laundering transactions, RB's lifestyle would have appeared suspicious given his declared source of income as being a long term benefit. While on the unemployment benefit, RB's owned several high value vehicles, acquired a bar and later established a company with no identifiable business purpose. RB's business practices were also unusual, for example business expenses for the bar were paid in cash. RB was able to use intermediaries in interactions with the financial institutions and dealers which may have otherwise aroused suspicions about his unusual financial profile.

290 RB used intermediaries to conduct transactions to place the cash proceeds of his drug supply so as to integrate the funds in the form of high value assets. RB would give cash to one or more intermediaries who would purchase the vehicle from a dealer either using RB's cash or banking that cash and using a bank cheque. In some instances RB's company was used as a front by the intermediary. When the vehicle was purchased, it was registered either in a RB family member's name or in RB's company's name.

291 RB also used intermediaries to send proceeds to multiple countries overseas. This was accomplished by intermediaries banking cash and wiring funds or by cash deposits to remitters. In one instance this involved the same individual remitting hundreds of thousands of dollars in multiple transactions over a few months with little explanation. Cash was also carried internationally by Lithuanian cash couriers using false passports.

292 In February 2011, RB was sentenced to 11 years six months imprisonment after admitting importing ecstasy, LSD and methamphetamine, and using a passport in a false name. A number of other individuals involved have also been convicted of drugs and money laundering offences while others are still before the court. The jurisdiction X-based 'mastermind' of the syndicate, RK, was also convicted and sentenced to six years three months imprisonment.

293 Typologies: use of third party intermediaries, use of front companies, wire transfers, cash couriers, cash deposits, purchase of assets (vehicles).

294 Money laundering indicators:

- unexplained activity that does not fit the profile of the customer;
- customers who do not know the origin of funds;
- customers who do not know the receiver of funds (i.e. in cases where money is being remitted overseas);
- another individual accompanying the person making the transaction and instructing them;
- purchases of valuable assets made in a third party's name; and
- large cash transactions to purchase assets (vehicles).

295 This case is published in FIU Quarterly Typology Report Q2 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014.pdf

296 *Case Study - Forfeiture of Drug King-Pin's Farm.* In February 2014, the farm of methamphetamine cook and dealer, person TC, was forfeited to the Crown following a long term operation conducted by Police in the Waikato. The forfeiture was part of Operation Cape, which smashed a NZD1 million (~USD.68 million) a year methamphetamine manufacturing and dealing ring. This ring also involved person SG, who was sentenced to 12 years in prison and from whom more than NZD5 million (~USD 3.4 million) worth of assets were forfeited in March 2013. The 2,720 acre farm at Waitetuna had been purchased by TC with funds laundered through a firm of accountants. Analysis of TC's financial accounts showed that he had received an income of around NZD4.1 million (~USD2.78 million) between June 1999 and May 2003 from drug offending. The farm was used to manufacture methamphetamine and to store the chemical precursors. A large number of firearms were also recovered from the property including two fully automatic assault rifles.

297 TC used an accountant to receive cash from his drug dealing and convert it into various purchases of farm land over a number of years. He used two of his farm employees to collect and take cash from drug sales to the accountant's office. The accountant had 12 accounts held at different banks in which he would deposit the cash. The accounts were held for his accountancy practice, a gift shop he and his wife owned, his personal accounts and a company account he was nominee director and shareholder of on behalf of the drug offender. The accountant went to different branches across the Waikato region and banked the cash into the various accounts. Some excuses he gave about the source of the cash were 'it was cash takings from a client who owned a bar' or 'it was his cash takings from a stall he operated at a market'. The deposited cash would then be electronically transferred to his accountancy practice to be held on behalf of TC. With his accumulated wealth, TC purchased farm land in the name of his family trust. The trustee of his trust was a corporate trustee company that the accountant was the director and shareholder of. This trust arrangement enabled TC to hide the fact he owned the farm land. It was estimated that, over ten years, the TC had accumulated NZD4.8 million (~USD3.26 million) from his drug offending. He was sentenced to 12 years prison and his farm land (valued at approximately NZD5 million; ~USD 3.4 million) was forfeited to the crown.

298 Whilst it was clear the accountant had engaged in money laundering, he was used as a witness against TC in exchange for immunity from prosecution.

299 Money laundering indicators:

- large cash deposits;
- use of third parties;
- use of a professional;
- comingling of criminal proceeds with legitimate business;
- use of nominee directors/shareholders to hide the ownership of business;
- purchase of real estate; and
- use of trust to hide the ownership of real estate.

300 This case is published in FIU Quarterly Typology Report Q3 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2013-2014.pdf

301 *Case study - Operation Ark.* 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 to hide the beneficial control of companies controlling assets;
- use of a professional service provider to access complex structures and act as an intermediary; and
- use of trust to hide criminal involvement in transactions.

302 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.

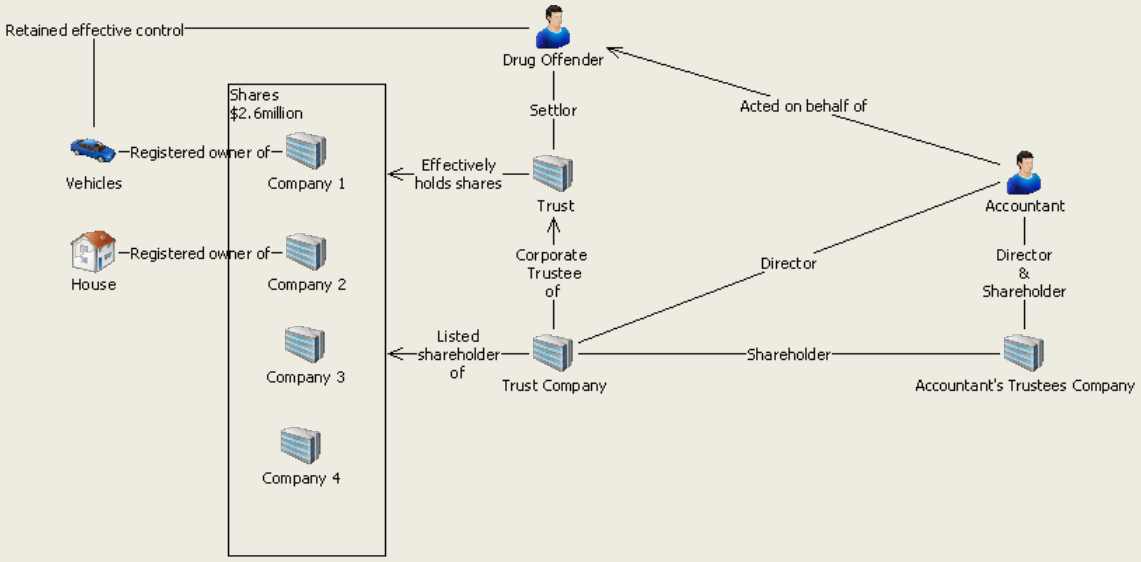
303 The offender also used his accountant as an intermediary and additional layer in the legal structure of his finances. Ultimately, as was the case in his layering of entities to hide ownership of the magazine and vehicles, the offender used the accountant and the trust to hide his own beneficial ownership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

304 Possible indicators:

- complex legal arrangements;

- property owned by a company which is in turned owned by a professional intermediary; and
- ownership of property cannot be traced to a natural person.

305 This case study is published in FIU Quarterly Typology Report Q1 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2014-15.pdf



PAKISTAN

306 *Background of the Case:* Person A was killed in May, 2015 in an encounter with law enforcement agencies on account of his alleged involvement in different criminal activities and most notably he was alleged to be a facilitator of a gang of target killers.

307 *On analysis of the transactions in A's and Z's (A's mother) bank accounts and counterparts'* details, it was suspected that the accounts maintained by persons A and Z may have been used for routing funds related to different criminal activities.

308 *Modus Operandi: Some connected accounts were reported by XYZ Bank* owing to huge amount of funds routed through these accounts. Person A was allegedly involved in different criminal activities and most notable he was alleged to be a facilitator of a gang of target killers. Out of the different accounts reported by XYZ Bank, it was observed that one of the reported accounts was of person A's mother Z, in which huge amount of funds were placed over a long time period. Person Z's account was opened as a photo account by the bank which requires personal presence of account holder for transactions in the account. Upon analysis of the statement of her account, it was revealed that huge amount of funds were credited in her account via 104 clearing cheques deposited in a single day raising substantially the available balance in the account. Interestingly, the cheques deposited in the account were of different amounts and drawn on various banks. No transaction in the account was subsequently noticed in the account for a long time. However, most of the funds were withdrawn from her account in the months of May and June, 2015. The withdrawals from her account were made via transfers of huge amounts and pay orders. From analysis of counterparts' details, it was revealed that most of the withdrawals from her account were made on account of investments in different properties.

309 Various links were identified (by using both open and closed sources) during the analysis of the accounts and the counterparty details acquired from different banks. Due to huge amount of suspicious funds routed from the accounts of A and Z, it was suspected that the funds routed from their accounts may have some connection to the alleged criminal activities of person A and other members of his gang. Further, it was believed that the linking information identified during the

analysis of accounts maintained by person A and his mother person Z, the law enforcement agencies will be able to identify the people associated with person A in his alleged criminal activities. Therefore, the matter was referred to LEA for investigation in the matter.

SRI LANKA

310 *Case of collecting third party deposits using lottery scams.* According to a licensed bank an individual had received an e-mail stating that he had won a prize of GBP 500,000 (~USD708,000) from the United Nations Organization. This individual had been requested to deposit money to an account number of a third party. Total deposits to the said account for a period of two weeks amounted to LKR 474,000 (~USD3,200).This case was referred to LEAs for further investigation.

311 *Case of collecting third party deposits using employment fraud.* A licensed bank had received complaints regarding receiving telephone calls from an individual claiming to be from the Department of Health, requesting money to be credited to an account number for offering jobs in a bank and giving a fax number to which the bio data of the applications could be sent. During a period of one month, twenty seven cash deposits totalling approximately LKR 500,000 (~USD3,450) were made to the account and the money was withdrawn immediately. The bank has tried to contact the customer but he had not responded to the branch inquiries. The case was referred to LEAs for further investigation.

CHINESE TAIPEI

312 Ponzi scheme case. In March 2014, the Anti-Money Laundering Division (AMLD) received an STR from Bank U indicating that Company J opened an account in December 2013 and then conducted several transactions to transfer about NTD 80 million (~USD 2.5 million) to foreign bank accounts for the purpose of real estate investment. After investigation by AMLD, it was revealed that Company J and person L were suspected to be engaged in Ponzi scheme made by M Group and person C who was the regional chairperson in Chinese Taipei of M Group. Person L and others (see below) were indicted on the charge of violating the Banking Act, the Multi-Level Marketing Supervision Act, and the Money Laundering Control Act in September 2015. Additional details of the case are as follows:

- In December 2014, person L wanted to withdraw NTD 4 million (~USD124,000) cash and deposit the money into her account. After the requirement was rejected by staff of Bank U, person L withdrew NTD 4 million (~USD124,000) cash and left the bank. Person L came back after a short period of time to deposit NTD 4 million (~USD124,000) cash into her account;
- Bank U has assigned staff to visit company J and found the registry address of company J was a general residential house. Bank U doubted whether company J had any actual business activities. Bank U considered the transactions conducted by company J and person L to be suspicious and filed the STR to the AMLD;
- From February 2013, person C held several seminars to attract investors to invest M fund. Person C promised investors monthly returns ranging from 3% to 8% depending on the amount of investment with opportunity to retrieve the capital after 18 months. Person C also used high rewarding system to allure person L et al., to help her canvass the investment. Since March 2013, the number of investors have quickly amassed to over 1,000 and the amount of investment has reached to NTD 13.9 billion (~USD 0.4 billion);
- In the beginning, investors remitted the investment to M Group's account in Jurisdiction X. Person C earned the difference of currency exchange by helping investors to withdraw capital and monthly returns. In order to seek more profit, person C et al. asked investors to give cash directly to person C, L or T or remit funds to personal or legal persons' accounts owned or controlled by person L; and
- The total amount of funds that persons C, L and T received directly was about NTD 3.2 billion (~USD0.09 billion). Person L remitted about NTD 2.3 billion (~USD.07 billion) to overseas accounts and then transferred to M Group as the investment. NTD 300 million

(~USD9.2 million) and NTD 600 million (~USD18.5 million) were hidden by persons L and T separately. In order to conceal the proceeds of crime, person C et al. used them to buy real estates, luxurious jewels, racing cars, motorcycles, and other precious properties.

THAILAND

313 *Case of fraud in financial institution (cooperative)*. Offenders had duties in overseeing a cooperative's money derived from members' deposits and repayments. The offenders undertook the follow activities:

- Took principal and interest received from members and documented them as advance expenses, to a total of THB1.9 billion (~USD54 million);
- Cashed cooperative's cheques from banks and documented them as advance expenses, to a total of THB10 billion (~USD280 million).
- Granted loans to companies with them being directors, shareholders or stakeholders, without board approval and collateral assets, including forgery of documents.

314 Proceeds were then laundered by buying real estates and cars using nominees. Some of the money was also donated to religious organizations.

315 *Case of illegal oil trading.* Illegal oil trading networks exist because petrol prices in neighbouring countries are cheaper. Smugglers modified their fishing boats or freight vessels to be able to transport petrol. High capacity vessels buy petrol from neighbouring countries and stay afloat in international waters while smaller boats take this petrol to sell to other fishing boats or other sea vessels. This is customs evasion. Offenders used nominees to launder proceeds by using their names to conduct transactions, buy real estate and precious items, and invested in restaurants, bars and currency exchange businesses. Proceeds are also used for establishment of front businesses to launder proceeds.

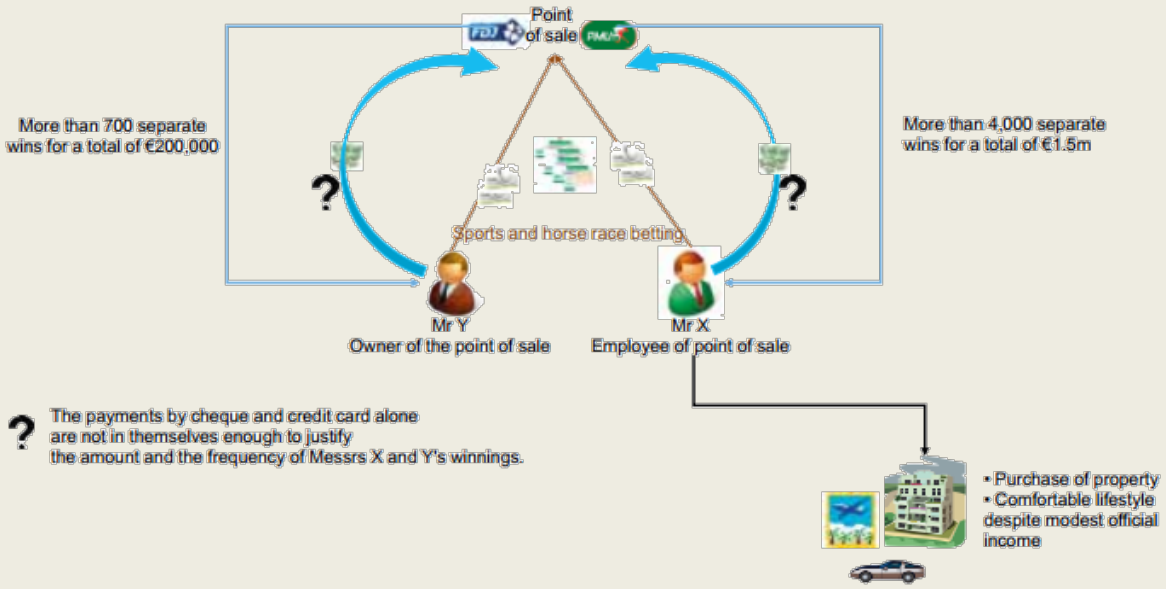
316 *Case of proceeds management*. A woman was charged for a narcotic offence, which she denied. During the investigation and prosecution, she declared that her salary was THB3,000 (~USD85.00) per month while her account turnover was hundreds of million Baht. She also claimed, without proof that her Chinese employer asked her to open accounts for convenience because customers are in Thailand and the factory is in Tachileik, Myanmar. The money deposited was immediately withdrawn. There is other evidence showing that she withdrew money on her employer's behalf because he signed as the person given authorization in withdrawal slips, attached with his ID document. Transactions involved many other drugs offenders. It is believed that she was involved in drug smuggling group. But without proof that the money derived from drugs trade, the Court cleared her of the drugs offense. However, money seized during the process is subject to a civil forfeiture case, which is with the public prosecutor.

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

FRANCE

317 *Case of laundering through gaming of the proceeds of criminal acts and offences.* Mr X is an employee of a point of sale business for two casinos (FDJ and PMU) located in the greater Paris region and run by Mr Y. Tracfin (France FIU) was alerted to an unusually large number of cheques and wire transfers of winnings credited to the bank accounts of these two individuals. Over a 15-month period, Mr X deposited more than 4,000 separate winnings totalling about €1.5million (~USD1.69 million). Mr Y deposited nearly 700 separate winnings for more than €200,000 (~USD225,600). The winning tickets, nearly all of them sports and horseracing betting products, were validated in Mr Y's outlet, whose turnover in gaming products increased exponentially over the same period. However, the origin of the money bet by Mr X and Y was not clear. Upon investigation it was determined that although payments by cheque, wire transfer or credit card were registered with their bank accounts, they did not sufficiently account for the recurrence and the extremely high amount of the winnings. Mr X and Y must have been injecting additional money into gaming, whose origin was

unknown and therefore raised red flags. Finally, it should be pointed out that Mr X, whose official sources of income were quite modest, lived a quite comfortable lifestyle and also acquired real estate.



JAPAN

318 There are no casinos in Japans. In Japan, gambling is illegal except for some kinds permitted by the law such as betting on horse racing. However, the Japanese police actively detect illegal gambling activities and related money laundering.

319 *Case 1.* A man who manages a teashop obtained money from customers by using an illegal gambling video game machine and put the funds into the different person's bank account. He was arrested for habitual gambling and violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

320 *Case 2.* Male senior members of Boryokudan (Japanese crime syndicate) received a total of JPY 200,000 (~USD1,850) in cash from a man managing a gaming store as protection money while knowing the payment was made out of profits earned through habitual gambling using slot machines. As a result, the male senior members were arrested for violating the Act on Punishment of Organized Crimes (receiving of criminal proceeds).

PHILIPPINES

321 *Case of casino gambling debt payment used to conceal laundering of proceeds from drug trafficking.* In 2013, operatives of the jurisdiction X's National Police arrested person AC and five other individuals in the Philippines and confiscated/seized 433.236 kilograms methamphetamine hydrochloride estimated to be worth USD43.3 million. In October 2013, the AMLC (Philippines FIU) received a letter requesting a financial investigation on the arrested persons together with a list of bank accounts that were allegedly used in the drug transactions of the group.

322 A STR was also filed by Universal Bank against one of the accounts of person AC. The narrative portion of the STR cited AC's arrest for drug trafficking as the cause for reporting, adding that AC is also known to be actively engaged in casino gambling. Verification with the Department of Trade & Industry (DTI) showed that person AC had two registered businesses, namely: A Trading and G Center. Certifications from the Business Permit and License Office showed that A Trading had gross receipts of only ~USD3,800 and that it had been closed since January 2011 while G Center was registered as a new business only in March 2013 with a capital of only ~USD1,085 and only one

employee. Further verification w showed that person AC did not appear as stockholder, incorporator or board member of any corporation registered in the Philippines.

323 In spite of the small capitalization and meagre declared income of person AC's businesses, the AMLC Secretariat's financial investigation revealed that AC's bank transactions involved more than USD8.6 million. One bank account was found to have made more than 200 fund transfers amounting to more than USD2.16 million to several individuals. The fund transfers were all made under the guise that they were AC's payment for gambling debts owed to the recipients of the transfer. However, no documents were presented to prove that person AC owed large sums of money by virtue of his gambling activities.

324 Financial investigations also showed that AC's bank accounts received funds from persons MST and CW who have also been charged with drug trafficking. Apart from his bank accounts, person AC also owned several prime real estate properties, a foreign currency trust account and money placement worth a significant amount. In August 2014, the Court of Appeals granted the Petition filed by the AMLC for the Issuance of a Freeze Order against the bank accounts, investments, real properties and motor vehicles of Mr. AC and his cohorts.

HONG KONG, CHINA

325 *Illegal bookmaking case*. Financial investigation by the Hong Kong Police Force (HKPF) against a local triad leader (person B) and his associates revealed that they had been engaging in cross-boundary illegal bookmaking activities and using their bank accounts to launder HK$357 million (~USD46 million) between 2006 and 2011. The bookmaking syndicate was neutralized in July 2012 with 11 persons arrested. Over HK$1 million (~USD129,000) cash was seized at the residence of two syndicate members. Three of the arrested persons were convicted of money laundering in March 2015 and sentenced to 18 to 38 months' imprisonment, while the other four arrestees were charged pending trial. A confiscation order was granted in August 2015 to confiscate the realizable assets amounting to HK$583,678 (~USD75,000) of person B and one of his close associates.

4.16 Mingling (business investment)

MONGOLIA

326 An organized crime group, from jurisdiction X was suspected of laundering criminal proceeds in Mongolia through investing in real estate (hotel). The group was also suspected of organizing trafficking of persons for sexual exploitation purposes.

327 According to the Police, another growing trend seems to be investing in the extractive industry in Mongolia by using illegal proceeds of crime derived overseas.

NEW ZEALAND

328 *Case study - Operation Ark*. Person CC and person LV, New Zealand citizens resident in jurisdiction X, 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 LV's mother's home for temporary storage. The cash was packed into boxes, generally in the form of bundles of NZD20 and NZD50 notes. The boxes were then picked up by couriers, who transported the cash to jurisdiction Y where it was deposited in the bank accounts of three companies beneficially owned by LV. Bank statements for these jurisdiction Y accounts were sent to LV's mother's address in New Zealand. The money laundering process was completed by loans made by one of the jurisdiction Y companies to another New Zealand company. Person CC controlled a trust that was a 50 per cent shareholder in the New Zealand company. A small portion of the cash, around NZD184,000 (~USD125,000), was retained by LV's mother for her own purposes.

329 Typologies: comingling, denomination conversion, cash couriering, shell companies, use of loans

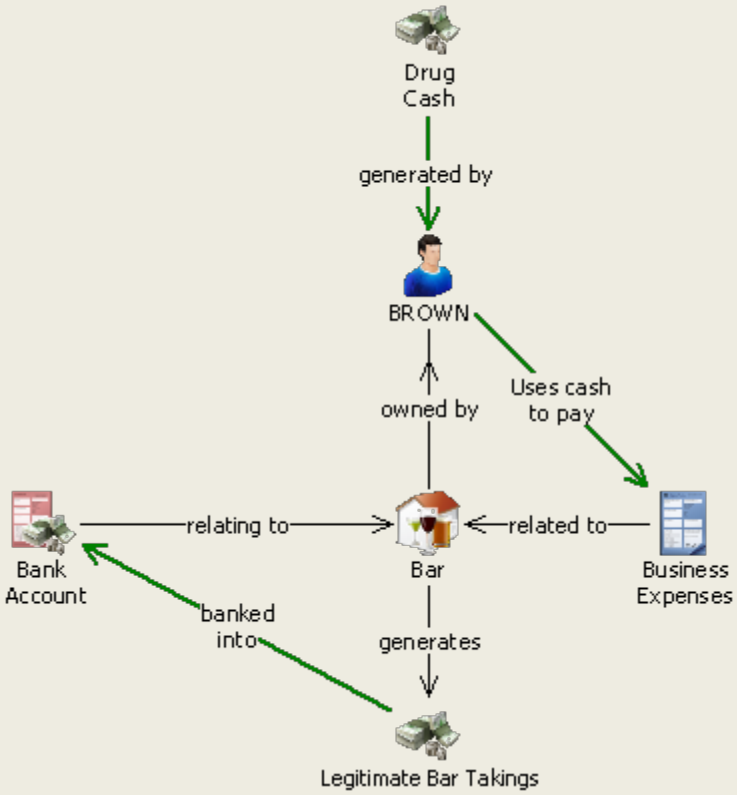
330 This case is published in FIU Quarterly Typology Report Q2 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014.pdf

331 *Case Study - Operation Keyboard.* Bars are a classic business through which to launder cash proceeds as:

- 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.

332 In Operation Keyboard, a central figure of a drug supply ring used a central Auckland bar to comingle the proceeds of drug sales. Person RB's declared source of income was an unemployment and later sickness benefit. However, in 2007, RB was able to purchase a bar.

333 While the business was run at a loss, the bar was an effective mechanism for RB 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 RB maintained beneficial ownership of. This relatively simple mechanism allowed RB to effectively swap the drug cash for the ostensibly clean bar takings.



334 This case is published in FIU Quarterly Typology Report Q4 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q4-2013-2014.pdf

335 *Case Study - Operation Acacia.* A methamphetamine manufacturer operated a business buying and selling building materials supplied from demolitions. Police financial analysis of the business accounts showed that approximately NZD150,000 (~USD102,000) 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.

336 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.

337 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.

338 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 NZD1.6 million (~USD1.08 million) that he earned from selling methamphetamine.

339 This case is published in FIU Quarterly Typology Report Q4 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q4-2013-2014.pdf

PAKISTAN

340 Bank A reported that large volumes of credits were observed in the PKR account xxx of person X. The funds were then debited from the account on same day/next day. It was also observed that most of transactions were related to Foreign Currency Encashment: person X made encashment from his foreign US Dollar account into PKR and the same were then credited in his PKR account. After that he made cash withdrawal from his PKR account on same day or next day. The purpose of these transactions was not provided to the bank.

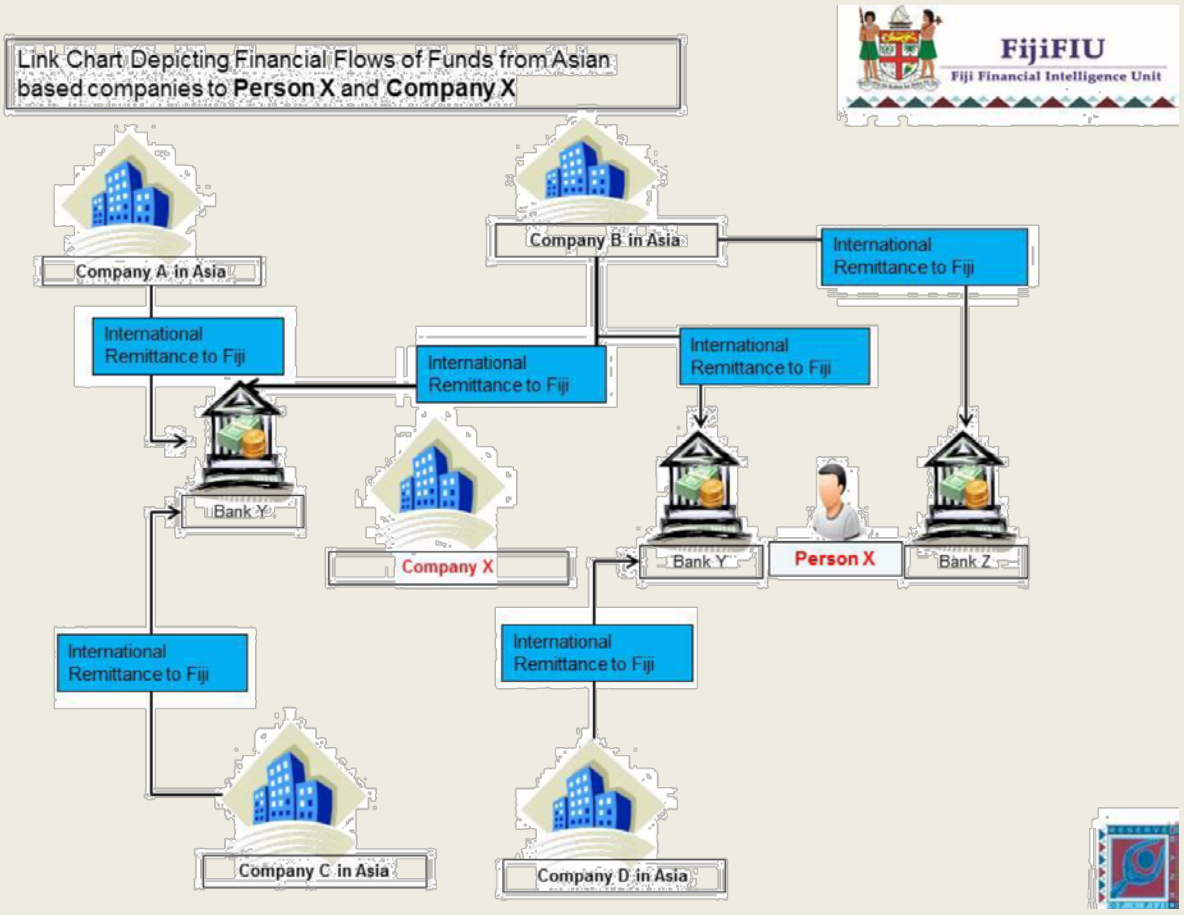
341 During analysis, it was observed that no significant activity was observed in his account no. xxx since inception of account on 13-10-2009 till an online credit transfer of relatively higher value from account no. yyy was made on 19-July-2012. After that, significantly high value transactions were noted in the account no. xxx during the months of September and December 2012. The account number yyy was searched in FMU's internal database and found several CTRs reported from that account under the title of Exchange Company. Large amount of funds were transferred in account no. xxx from person X's US Dollar Account. These funds were mostly withdrawn from the account no. xxx through cash transactions below CTR threshold on same day or next few days. The account holder was probably trying to mingle the suspected business income with his savings in the personal account. Financial information was, therefore, disseminated to central bank citing possible attempt to circumvent the rules involving money exchange business, structuring of transactions and intermingling the suspected business proceeds.

4.17 Use of shell companies/corporations

FIJI

342 Fiji FIU received three STRs on Company X and one of the directors, person X for receiving large inward remittances totalling FJ$15.3 million (~USD7.3 million). Analysis of the bank accounts of Company X and person X revealed that an additional FJ$6.7 million (~USD3.2 million) was

deposited either by cheque or cash. Fiji FIU was able to trace the funds to four foreign based companies that are believed to be shell companies. The funds were withdrawn and invested in real estate property in Fiji and transferred to an offshore lawyers trust account. A report was disseminated to Fiji Police Force for further profiling.



FRANCE

343 The identification and monitoring of the methods employed by organised crime groups to infiltrate the legal economy and launder funds of illegal origin are vital tasks that go hand-in-hand with risk assessment.

344 Two of the most common ways in which organised crime groups operate is by infiltrating the legal economy by means of companies specifically created for criminal purposes, or taking control of legitimate companies experiencing financial difficulties. Mid-sized establishments are prime targets in such cases, along with small- and medium-sized enterprises, and takeover methods used are designed to conceal the identity of the true beneficial owner through the interposing of foreign legal structures. A criminal group may also create and invest in one or more companies managed by one of its members. There are two options in this case: either the company or companies is, or are, created in order to legally generate profits, or they use illegal practices to fraudulently generate profits that can then be transferred abroad to members of the criminal group.

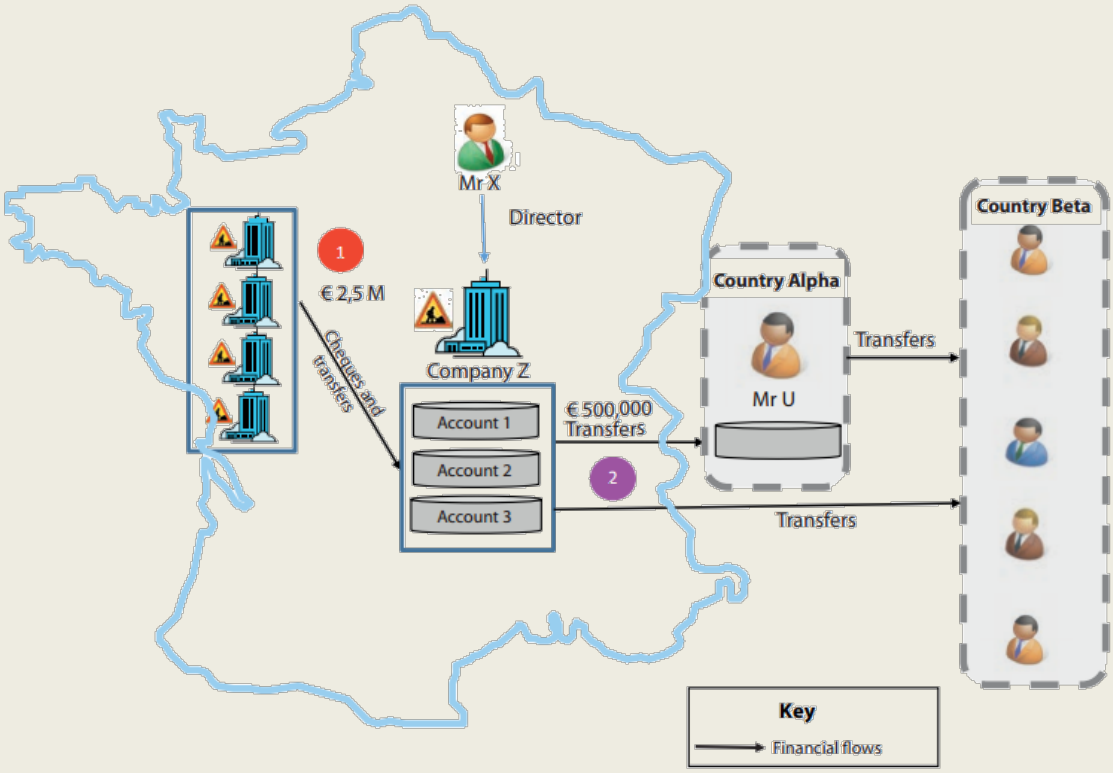
345 Some schemes reported by reporting entities are based on the use of short-lived companies and several tiers of subcontracting, so as to avoid controls and organise large-scale tax and social security fraud, the illegal revenue from which is a possible means of financing organised crime.

346 *Case of control of a network of building companies by individuals linked to an organised crime group.* Company Z, which was recently created and operated in the contracting sector, was fully owned by Mr X (Mr X had links to a criminal group in country Beta). This company had filed more

than fifty pre-employment declarations (DPAE) since it was created. On the other hand, the amount of the social security contributions that it had paid seemed extremely low considering the turnover of nearly €3 million (~USD3.3 million) recorded by the company in its bank accounts in less than one year of operation. The company did not appear to be meeting its tax and social security obligations and, in view of the turnover recorded in its accounts, it might be assumed that it was using undeclared labour and committing tax and social security fraud.

347 Company Z signed several subcontracting agreements with other contracting companies. The bank accounts of company Z operated like transit accounts, as the funds collected were either immediately transferred a Mr U's bank account opened in country Alpha, or redistributed to individuals living in country Beta. According to the FIU's investigations, Mr X, Mr U and certain contracting company directors and beneficiaries of company Z's funds, might have belonged to an organised crime group operating from country Beta that had dealings with people located throughout Europe. Mr U's account, opened in country Alpha, collected nearly 20% of the flows from company Z's accounts. The funds received by Mr U were also transferred to individuals living in country Beta.

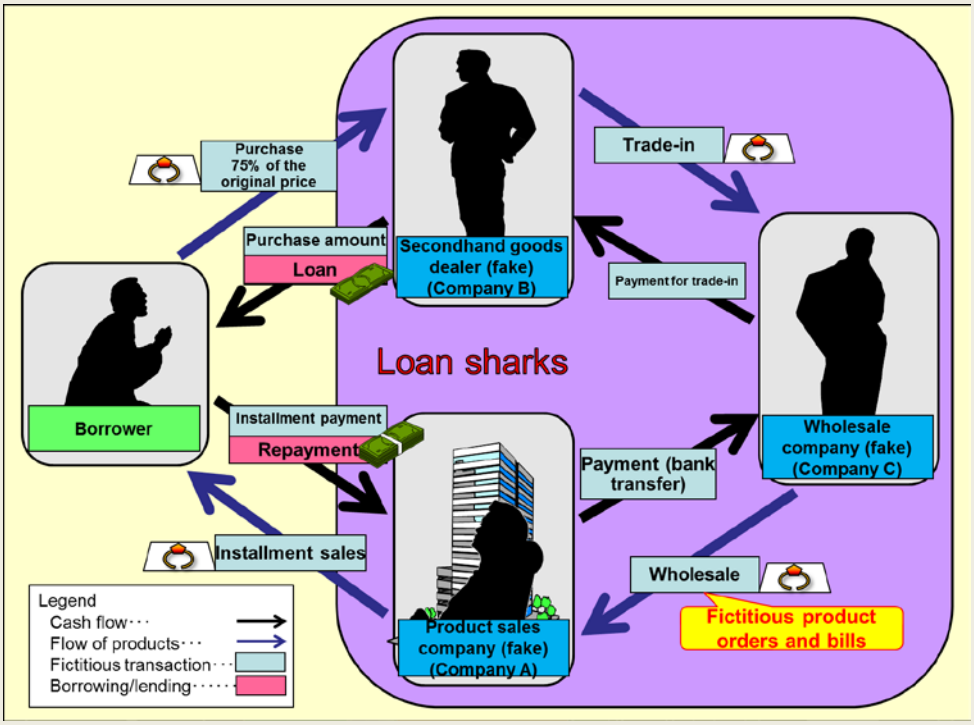
348 A large proportion of the debit flows from company Z's accounts did not appear to be economically justified, while the links between company Z and some of the funds' beneficiaries might have arisen from organised criminal activity. Company Z's operations might therefore be qualified as possible undeclared work or tax and social security offences, or any crimes or offences connected to organised crime activity.



JAPAN

349 A man engaging in loan sharking sold products to persons applying for loans through a disguised instalment sale by a product sales company (Company A) effectively managed by himself. Later, the man arranged for a company disguised as a second hand goods dealer (Company B) to purchase the products at prices lower than the sale prices by Company A and remitted funds equivalent to the purchase prices from the second hand goods dealer's account to the borrowers' accounts as loans. In addition, the man arranged for repayment funds to be remitted from the borrowers to an account opened in the name of Company A through disguised instalment payment and received the difference between the amount of the sale prices of Company A and the amount of

the purchase prices by Company B as interest. Fictitious product orders and bills were compiled jointly by a company disguised as a product wholesale company (Company C) which the man founded with a third-party man as its representative. Ultimately, a total of around ￥49.4 million (~USD.400,000) in repayment funds was remitted into the account managed by the man. As a result, the man was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).



PHILIPPINES

350 *Case of use of the internet and dummy corporations for swindling.* The scheme involves the use of call centres operating in the Country Y for large-scale investment fraud with operations in Country X and the Country Y under various names, such as B Brokers, AA Incorporated and LB Corporation (collectively referred to as "B Brokers").

351 Sales calls, to elderly victims residing in Country X, relating to sale of fraudulent certificates of deposits (CDs). The CD's were described as investment vehicles insured by the government of Country X and victims were convinced to invest and make payments through the issuance of personal checks. Thereafter, the victims would receive fraudulent monthly account statements concerning their investments by mail. None of the invested funds nor any of the promised interest has been returned or paid to the victims.

352 The operators of the call centres allegedly used false names and business addresses in brochures, business cards and marketing materials sent to the victims. The operators also disguised their true location and names when making telephone calls to the victims by using Enchanted Drive devices. These devices are plugged into a USB port of a personal computer and enable the user to place calls over the internet. The devices are assigned a specific area code and telephone number in Country X, which will be displayed as the calling number to the person receiving the phone call, no matter where the Enchanted Drive device and the caller are actually located. Based on the investigation, the Enchanted Drive devices used in this particular scam were assigned area codes corresponding to major cities in Country X but the logs of the "Internet Protocol" (IP) addresses used by the said devices showed that the calls were actually made from the Country Y.

353 After the victims had been convinced to invest in the fraudulent CDs, they were advised to write a personal check in the amount of the investment, and B Brokers would arrange for a courier to

collect the checks at the victims' residences. These checks were then sent to four separate virtual offices and subsequently forwarded to an address in Country Y.

354 It was noted that sometime in December 2011, B Brokers opened a new front company known as AA Incorporated with a new virtual office in Country X to receive the victims' checks. All mails for AA Incorporated was forwarded to an address in Country Y.

355 Based on the examination of the victims' cancelled checks, prior to September 2011, the vast majority of the funds collected by B Brokers were deposited into an account in Universal Bank A in the Country Y. It was also revealed that between approximately September 2011 and January 2012, cancelled checks issued by the victims to AA Incorporated, totalling approximately US$615,000 were deposited into two accounts in Universal Bank B in Country Y.

356 Using the front company named LB Corporation, B Brokers allegedly collected more than US$1.2 million from elderly victims between May to June 2012. These funds were deposited by B Brokers to Bank Z in Country X, and subsequently wire transferred to two accounts in Universal Bank C in Country Y.

357 The AMLC filed an Ex Parte Application for Bank Inquiry into the accounts used by B Brokers in Universal Banks A, B and C. The said Application was granted by the Court of Appeals. Examination and inquiry into the subject bank accounts were conducted and the bank documents obtained were transmitted to the Embassy of Country X through the Philippine Department of Justice.

NEW ZEALAND

358 *Case study - New Zealand shell company implicated in suspected attempted sanctions violation.* A New Zealand registered company approached the client of an overseas-based law firm seeking to buy a hotel in a third country. The law firm became suspicions about the transaction when it discovered that the owners of the New Zealand company did not have legal representation for the sale despite the size of the transaction which was in the tens of millions of dollars.

359 Know your customer and customer due diligence processes raised a number of additional concerns relating to individuals involved in the transactions. Firstly, the Iranian owners of the New Zealand company had passports issued by a jurisdiction known to sell passports. In addition, the law firm could not find any indication that the owners had any real connection to New Zealand or the country where their passports were issued.

360 The transaction was to involve two New Zealand companies – the company making the purchase and a second company that was to loan money to the first. However, the law firm could not establish the relationship between the two companies. In addition, the law firm could not establish what either company actually did or how the capital involved in the loan had been made.

361 The transaction for the New Zealand company to purchase of the hotel also raised the law firm's suspicions as the purchase was to be funded through an unusually complicated transaction structure which the law firm could not account for. The New Zealand company was proposing to raise funding by selling shares and through a loan from the second New Zealand company. Finally, a bank cheque drawing on Bank Melli (the Iranian national bank) was presented to pay for the purchase.

362 Based on these red flags, the law firm and the client became suspicious that the transaction was an attempt to circumvent sanctions against Iran. Based on the evaluation of the high risk of sanctions evasion, the client decided not to proceed with the transaction.

363 It seems likely that the Iranian nationals obtained passports from the offshore jurisdiction and set up a New Zealand shell company and structured the complicated transaction to obscure the Iranian origin of funds that they were attempting to move from Iran.

364 Typologies: use of false identity, use of shell companies, real estate, use of shares

365 Indicators:

- nationals of a State subject to sanctions using a company from a third country;
- individuals involved had newly issued passports from a country known to sell passports;
- unusually complex transaction; and
- obscure origin of funds and business of companies involved in transaction.

366 This case is published in FIU Quarterly Typology Report Q1 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2013-2014.pdf

367 *Case study - T Limited.* The T Limited case which was publically reported overseas and in New Zealand demonstrates the layers of people and entities that may be used in shell company formation. In this case foreign bank accounts in the shell company's name were used to move criminal proceeds under the guise of trade transactions with the shell company.

368 T Limited was a New Zealand shell company set up by a New Zealand trust and company provider, GT Group, based in Vanuatu. T Limited was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The address listed on the companies register for T Limited was the same virtual office in Auckland listed for GT Group. The nominee director resided in Seychelles, and the nominee shareholder, V (Auckland) Ltd, was a nominee shareholding company owned by, GT Group. V Ltd was itself substantially a shell company and had also been used as the nominee shareholder for hundreds of other shell companies registered by GT Group. For instance, one of the other shell companies V Ltd was used to facilitate was SP Trading Limited, which was used to charter an aircraft that was intercepted in December 2009 attempting to smuggle arms from North Korea.

369 The actual business of T Limited was not apparent and was not indicated by the company name. Unusual names that do not indicate the activity of the company is a common indicator of shell companies used to facilitate criminal activity.

370 The Organized Crime and Corruption Reporting Project (OCCRP), a network of Eastern European journalists, reported that, once T Limited was registered on the New Zealand companies register, a power of attorney document was used to transfer the directorship to a Russian national. A bank account was then opened at the Baltic International Bank in Latvia. Journalist enquiries with the man revealed he was unaware of either T Limited or its bank account. His identity had been used without his knowledge as he had sold his passport details.

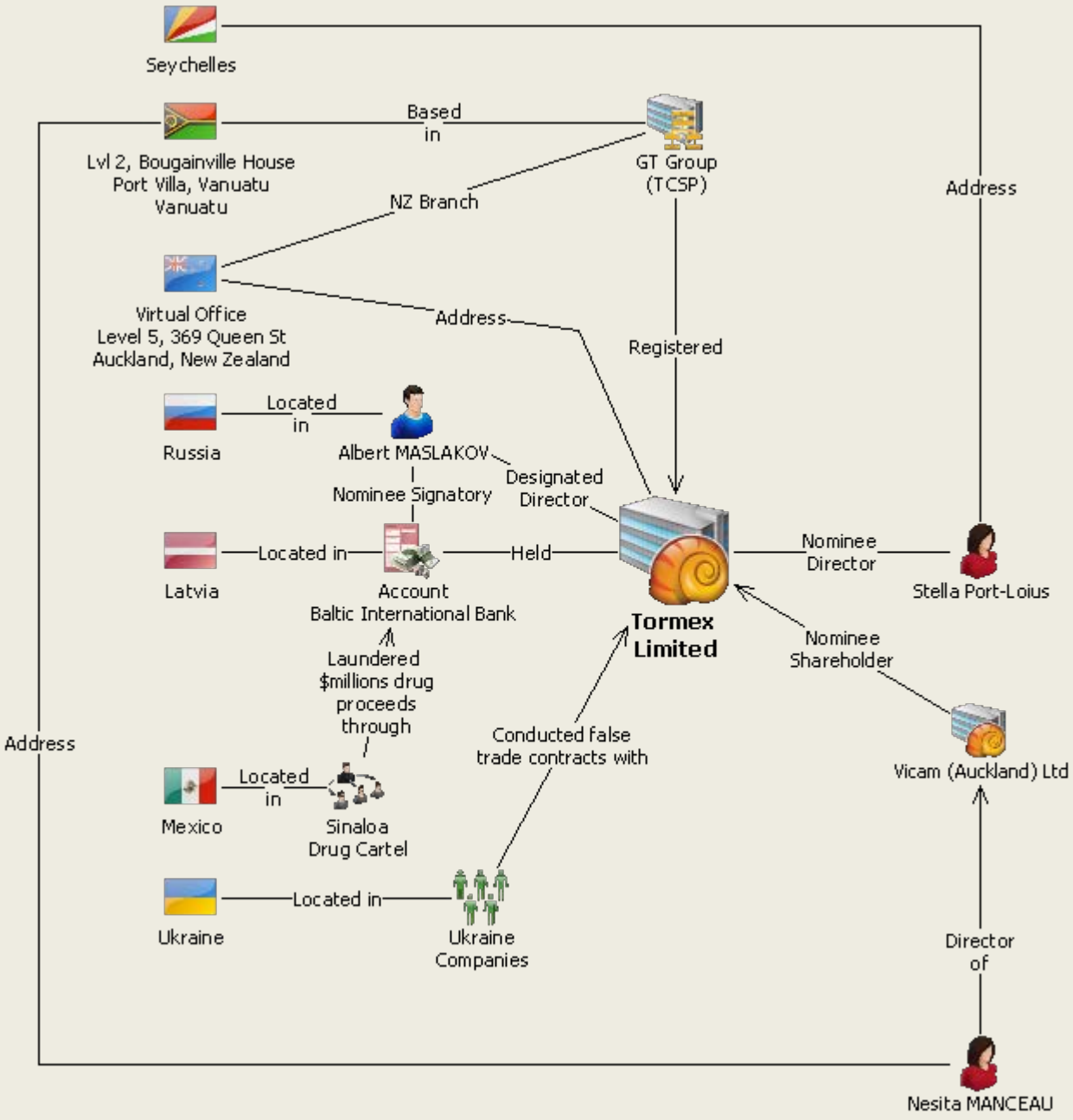
371 A former officer of the Russian tax police told journalists "There are hundreds of law firms in Moscow, which specialise in setting up ready-made shell companies for their clients, who want to remain in the shadows. Usually law firms use poor people, who sell them passport details. The sum for one passport may vary from USD100-300".

372 When the journalists examined bank statements for the Latvian account held by T Limited obtained by lawyers in a Moldova court case they discovered that during 2007 and 2008 USD680 million was transacted through the account. Analysis indicated the transactions were money laundering transactions carried out under the guise of trading contracts between T Limited and several companies. Trade transactions were conducted with several Ukrainian companies including a state owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third party offshore companies. The OCCRP journalists report that using transactions related to cancel trade orders with legitimate companies is a common money laundering method amongst Russian organised crime.

373 Transactions were also made with three other New Zealand shell companies, K Limited, M Limited and D Limited, which had also been registered by GT Group using the same nominee director, nominee shareholder and virtual office address as T Limited.

374 The UK's Guardian newspaper reported that T Limited, K Limited, M Limited and D Limited had been involved in laundering USD40 million for the Sinaloa drug cartel based in Mexico. Part of the money laundering process involved the New Zealand shell companies transferring funds to an account held at Wachovia Bank in London linked to the Sinaloa Cartel.

375



376 Possible indicators:

- use of nominated shareholders and directors;
- use of virtual offices;
- unclear whether the company is actually operating and providing goods or services;
- large number of international transactions transiting through the account;
- same person and/or address used in registration of multiple companies;

- companies with unusually complex or unexplained ownership structures;
- unclear who the natural person with ultimate beneficial ownership is; and
- company based in, or director/shareholder based in, jurisdiction associated with shell companies.

377 This case is published in FIU Quarterly Typology Report Q2 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q2-2014-2015.pdf

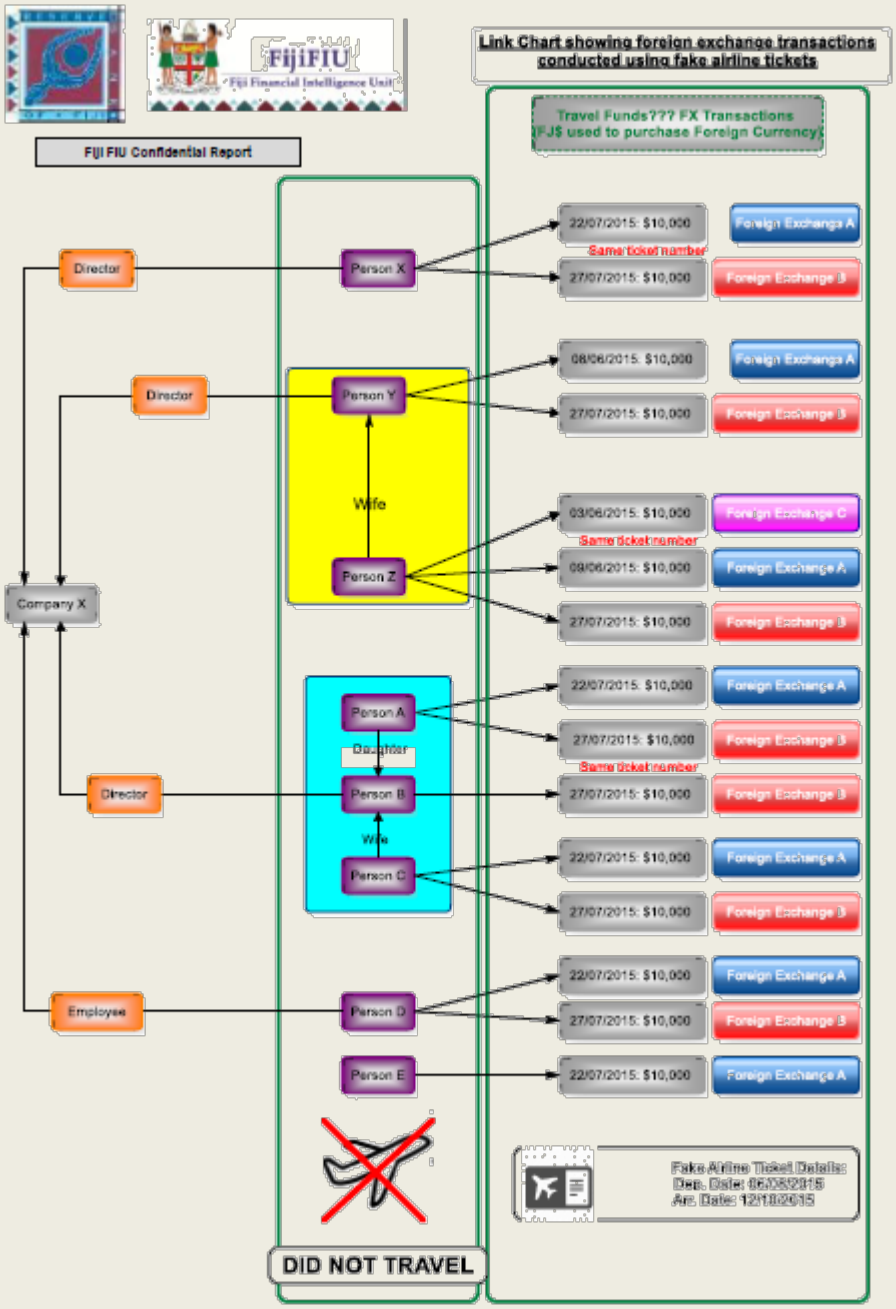
CHINESE TAIPEI

378 Mr. L established company X in July 2011. With the assistance from Mr. C, Mr. L borrowed money from private lender to complete a falsified capital increase from NTD 2 million (~USD61,500), the initial amount of the establishment, to NTD 100 million (~USD3 million) in 2013. The money was remitted back to the private lender right after auditing and not used for the company operation. Between October 2013 and January 2014, Mr. L continuously sold 3,830,000 shares of company X owned by himself and his wife to Mr. H with price of NTD 8.5 per share and consequently gained about NTD 32.55 million (~USD1 million) as profit. In order to conceal the origin of shares, Mr. H sold them to M. Y with price of NTD 23 per share and then sold to Ms H and other 4 persons. As a result, Mr. H gained NTD 24.7 million (~USD 700,999) as profit, and Mr. Y gained NTD 30.4 million (~USD00,000) as profit. Company X's shares derived from falsely capital increasing scheme were then sold to general investors with price between NTD 23 to 69 per share by Ms H and her staff. Ms H gained millions of dollars. Mr. L, Mr. C, Mr. H and Ms H used counterfeit financial reports, falsely stated that Company X received lots purchase orders and signed contracts with foreign companies to deceive investors to buy shares. Over 100 investors misunderstood the information to buy Company X's shares and lost lots of funds. The authorities initiated a criminal investigation and then referred this case to the Taipei District Prosecutors Office in October 2015 for prosecution.

4.18 Currency exchanges/cash conversion

FIJI

379 Fiji FIU received seven STRs on seven individuals suspected of using fake airline tickets to conduct foreign exchange transactions totalling FJD120,000.00 (~USD57,500). Analysis of the foreign exchange transactions conducted by these individuals revealed that two individuals used the same airline ticket number at two different foreign exchange dealers and two other individuals used the same airline ticket number at one foreign exchange dealer. Fiji FIU verified that the seven individuals did not travel on the dates specified on the airline tickets. A report was disseminated to the Fiji Police Force. While investigations were proceeding, Fiji FIU received intelligence that one of the seven individuals, person X, was suspected to be conducting similar transactions at a financial institution. Fiji FIU liaised with the Fiji Police Force and person X was arrested and charged with general dishonesty. Person X is currently awaiting trial.



4.19 Currency smuggling (including issues of concealment and security)

BRUNEI DARUSSALAM

380 Two foreign nationals and a foreign money changer were charged for money laundering under section 3(1), Criminal Asset Recovery Order, 2012 (CARO). This is in addition to a charge under section 27, CARO for failure to declare the movement of cash amounting to BND 1.2 million (~USD880.000) and various other foreign currencies from a foreign country into Brunei.

381 The two foreign nationals were initially stopped at a border while crossing into the country. It was found that they had attempted to move in large amounts of cash without declaration to the authorised officers at the border and so the money was seized by the Royal Customs and Excise Department under the Customs Order, 2006.

382 In their initial investigation, the Royal Customs and Excise Department obtained conflicting claims as to the source of the money. As the source money could not be ascertained, it raised the suspicion of money laundering and the matter was transferred to the Royal Brunei Police Force to pursue a money laundering investigation.

383 Further investigation by the Royal Brunei Police Force revealed the money was "Tainted Property" (property used in or in connection with the commission of a serious offence / property for which the income of that person from sources unrelated to criminal activity cannot reasonably account for the acquisition of that property). As a result the two foreign nationals and a foreign money changer found to be involved were charged with money laundering.

CANADA

384 In June 2015, border services officers at the Montréal-Trudeau International Airport seized €160,000 euros (~USD181,000) hidden in the suitcase of a Canadian traveller. The traveller was referred for a secondary exam. The inspection of the suitcase made by the officer and the ensuing X-ray exam revealed discrepancies. The opening of the suitcase showed that a total of €160,000 euros were hidden in its walls and its handle.

FIJI

385 Fiji FIU received intelligence that person X purchased Fijian currency with AUD51,120 (~USD39,500) at a foreign exchange dealer. Fiji FIU conducted further checks and established that person X later deposited FJD60,000 (~USD29,000) into his loan account and FJD15,000 (~USD7,200) into his savings account. It was established that person X frequently travels to Fiji. It was suspected that person X has been bringing foreign currency into the country without making any declaration at the border. Person X is under profiling and watch list by the respective law enforcement agency.

INDIA

386 The accused were found to be involved in cross border smuggling of narcotics, fake Indian currency note (FICN) and illegal arms & ammunitions. These cross border smugglers entered into India through the border in Punjab to circulate FICN, narcotics and weapons. Further investigation is ongoing about the role of smuggler who used to supply the contraband goods to the accused persons. However, in this case, the two accused were convicted for 20 years rigorous imprisonment and one for 10 years along with fines ranging from USD 1,034 to 29,551 respectively.

SAMOA

387 Person SS was reported by several financial institutions due to significant amount of foreign currencies he converted (into our local currency) without a proper explanation on where the funds were sourced from. Information obtained from one of the government ministries revealed that person SS was a regular traveller. It was noted that person SS exchanged large foreign currencies after every arrival. The FIU obtained his 'arrival cards' which he declared 'not' carrying any foreign currencies. Person SS is suspected of currency smuggling and the matter has been referred to the Police for investigation.

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

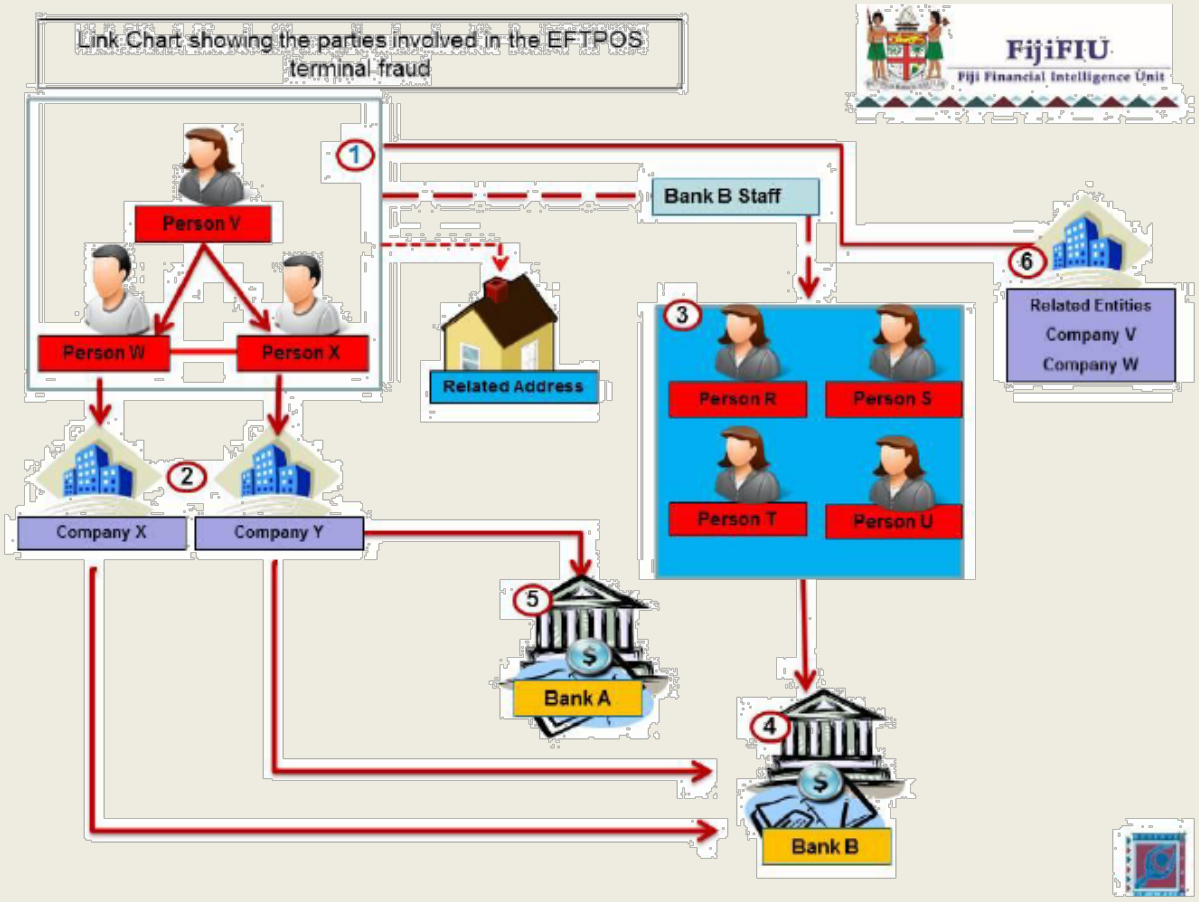
CANADA

388 In July 2015, an individual pleaded guilty to fraud and money laundering in connection with her bookkeeping responsibilities at a medical waste treatment company. The individual created fake invoices (addressed for payment to the company) and then transferred the company's payments to her

personal credit cards. The scheme allowed her to defraud the company of close to CAD650,000 (~USD508,000) over five years.

FIJI

389 Fiji FIU received three STRs on Companies X and Y for conducting fraudulent transactions at an EFTPOS terminal. The owners of the Companies opened business accounts and EFTPOS terminal accounts using fake foreign passports. Companies X and Y received deposits totalling FJD0.7 million (~USD.33 million) from merchant sales over a period of two weeks. Fiji FIU analysis of the company records revealed that the Companies X and Y were shell companies. Further analysis of the bank statements revealed that the transactions were being conducted with what is suspected to be stolen credit cards identity from foreign jurisdictions. The case was disseminated to the relevant law enforcement agency.



JAPAN

390 A senior member of Boryokudan (Japanese crime syndicate) and others were managing a hostess club without permission. They arranged for a credit card company to remit around JPY 4.8 million (~USD40,000) as proceeds which was paid by customers via credit cards. The credit card company remitted the money to the account opened in the name of another person. As a result, they were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

MACAO, CHINA

391 Bank A was alerted of a business dispute between a local Retailer B and its client. Bank A conducted enhanced due diligence and found out that the bank account of Retailer B was solely used for receiving funds for card clearing settlements, and that Retailer B's bank card receipts were

extraordinarily high for the current month and the trend was abnormal. As such, Bank A reported the case to the local law enforcement agency, as well as filed an STR with the local FIU.

392 After further investigation carried out by the local LEA and the FIU, the owner of Retailer B admitted that he was recruited by a crime syndicate to carry out fictitious Point-Of-Sale (POS) transactions by using forged bank cards. He would then transfer the cash to the crime syndicate and received a reward in terms of a fixed percentage in return.

MONGOLIA

393 In 2014, cases were uncovered in which foreign citizens used stolen credit card information to withdraw money from those cards. In 2015, Police report that Mongolian citizens in the service sector appear to cooperate with foreign citizens bringing in stolen cards or stolen card information to illegally withdraw money from those cards or pay for services. The local service providers include hotel, restaurant, bar and pub, and stores providing retail service.

SRI LANKA

394 One of the Licensed Commercial Banks raised an STR on a NGO for collecting donations through cloned credit cards. The president of NGO had received an offer from a Sri Lankan living in Jurisdiction X through person B stating that he would facilitate donations to the NGO on the condition that 45% of such donations must be given back to him, 5% to person B with the balance for the NGO. These donations were executed through cloned credit cards and funds were credited to an account maintained by the NGO at a licensed bank. When tracing the credit card details, original owners of these cloned credit cards had confirmed to their respective banks that they had not made any donations to the NGO.

395 The bank had credited approximately a sum of LKR 152,000,000 (~USD1.04 million) to the account of the NGO assuming the receipts were obvious. Money had been distributed through cheques to the people who were engaged in this chain of illegal activity as agreed.

THAILAND

396 *Pyramid scheme case.* Offenders registered their business as trading in herbal drinks and cosmetics but advertised to the public to invest in virtual currency. Investors were promised high returns. They also received commission for recruiting new investors. Money received (proceeds) was transferred to associates' accounts in southern provinces of Thailand and subsequently withdrawn and carried across the border to Jurisdiction X. Some of it was used to buy cars in the offenders' names and companies' names.

4.21 Structuring (smurfing)

AUSTRALIA

397 *Structuring and firearms offence case*. A suspicious matter report (SMR) was the catalyst for a law enforcement investigation, which led to the arrest of an offender for structuring cash deposits to avoid threshold transaction reporting requirements. The offender structured cash deposits totalling more than AUD2.5 million (~USD3.46 million) over a five-year period. The offender was charged with offences relating to structuring of transactions and firearms offences. The offender pleaded guilty to all offences and was ordered to pay a pecuniary penalty order of over AUD1 million (~USD1.38million). The full version of the case study is available on the AUSTRAC case studies hub http://www.austrac.gov.au/case-studies/offender-convicted-structuring-funds-launder-money-1-million-recovered.

PAKISTAN

398 Bank A reported several accounts maintained by individuals who were connected by ways of employment in company B. Company B attracted people by offering attractive profits as a return on their investment and secondly also offered jobs. Around 525 individuals filed applications against the company for depriving them of their hard-earned money. It was suspected that the scam involved a fraud of PKR1.88 billion (~USD 18 million).

399 It was noted in company B's account that large amounts of funds came through online transfers and cash from different individuals. The accumulated funds flowed from the company's account in a structured manner through online cash/ATM transfers to the personal accounts run by individuals who were either employees of the company or were involved in other businesses. The funds were then taken out from the personal accounts through online cash withdrawal. The matter was referred for investigation.

4.22 Wire transfers/Use of foreign bank accounts

AUSTRALIA

400 *Drug trafficking case*. Australian law enforcement worked together with jurisdiction X counterparts to dismantle an international drug syndicate with links to a number of other jurisdictions. AUSTRAC provided financial intelligence which showed the flow of funds between entities and enabled law enforcement to identify and link individuals not previously known to be associated with the drug syndicate. AML reporting by two banks, a remitter and foreign exchange dealer assisted with the investigation. AUSTRAC received an SMR from a currency exchange service. This SMR assisted authorities identify a drug courier recruited by the syndicate. The suspects were charged and convicted of aiding and abetting the importation of a marketable quantity of drugs. They received sentences ranging from two and a half years to eight and a half years imprisonment. The full version of the case study is available on the AUSTRAC case studies hub http://www.austrac.gov.au/case-studies/australia-and-colombia-join-forces-bring-down-international-drug-syndicate.

CANADA

401 In October 2015, three Toronto residents and six individuals in the jurisdiction X were charged for fraud and money laundering in connection with perpetrating romance scams that defrauded victims of CAD5 million (~USD3.9 million). The perpetrators established romantic relationships through dating sites and then convinced the victims to transfer funds to them based on a fictitious story about being in an emergency situation. The proceeds are alleged to have been wired through accounts in several countries to facilitate the layering and integration phases of the money laundering.

CHINESE TAIPEI

402 Person K was the president of S private school, and his wife, person H, was the director and adjunct vice-president of S private school. From 2011, each student had to pay about NTD 20,000 (~USD617.00) as regular fee and about NTD 40,000 (~USD1,200) as bilingual education fee. Person K instructed his staff to record false information in S private school's financial reports with receiving NTD 3,000 to 5,000 (~USD92.00 to ~USD154.00) regular fee and NTD 30,000 to 35,000 (~USD925.00 to ~USD1,000) bilingual education fee. After deducting the necessary expenses, the rest of the funds should be used for operating the school based on relevant regulations. Contrary to this, persons K and H instructed staff to transfer the rest of the funds to personal or legal persons' accounts of themselves or controlled by them in Chinese Taipei, Jurisdiction X, Jurisdiction Y, and the Jurisdiction Z. The funds were used for paying both the principal and interest of the mortgage loan, investing in securities, buying insurance policies, foreign bank's time deposits, and personal usage. Between 2011 and 2014, persons K and H have embezzled about NTD 144 million (~USD4.46

million) of S private school's property. Authorities initiated a criminal investigation and then referred this case to the New Taipei District Prosecutors Office in July 2015 for prosecution.

FIJI

403 *Case 1.* A STR was received on person X, a foreigner who arrived in Fiji with USD$28,700. person X declared the funds to border control authorities on his arrival. Profiling of person X established that he shared a common address in Fiji with other individuals originating from the same jurisdiction and was sending money to common beneficiaries in this jurisdiction. Person X had remitted FJD7,950.00 (~USD3,850) to beneficiaries in the jurisdiction. Fiji FIU also established that person X was granted a permit to commence business in Fiji which did not eventuate.

404 *Case 2.* An STR was received on persons X and Y who are the directors of 3 companies. Fiji FIU analysis found significant financial transactions being conducted through the personal bank accounts of persons X and Y amounting to over FJD1 million (~USD.48 million).

405 Analysis of financial transaction revealed the following:

- Numerous Telegraphic Transfers were made into the personal bank accounts of persons X and Y.
- Large cash withdrawals totalling more than FJD1 million (~USD.48 million) were made from 2013 to 2015.
- Person X continues to operate and trade and is non-compliant with requirement of the Tax Authority.

406 The case was disseminated to the local Tax authority and investigations are currently underway.

MACAO, CHINA

407 *Suspicious money laundering case involving criminal proceeds from overseas:* Person A and Person B from Country X had opened a joint account with a local bank, and received an inward remittance from person B's bank account in Country Y. The funds were then converted to a fixed term deposit. Through intelligence exchanged as part of the analysis process, the local FIU received information that person A and person B were being charged with forgery of documents, drug trafficking and money laundering. During the investigation, it was found that person A and person B had transferred all the drug proceeds to different bank accounts in several countries, in an attempt to hide the true destination of funds. The case was subsequently passed to the LEAs for further investigation.

MONGOLIA

408 A case related to embezzlement of funds of a state-owned aviation company involved multiple transactions to banks and companies located in Mongolia and overseas. Deposits were made to an international insurance company registered in Jurisdiction X and in Jurisdiction X from an official account of the company, and then transfers were made back to Mongolia from banks in jurisdictions X and Y to multiple account holders, one of which was opened under a false identity (identity theft).

NEW ZEALAND

409 *Case study - the love struck mule.* Person X became ensnared in two related scams that are unfortunately all too common. In the first scam, person X was victimised in a romance scam after meeting a man living in Nigeria on an online dating site. After a period of online chatting, the scammer convinced the person X to make several wire transactions over a few days to Nigeria, supposedly to pay for airline tickets for the scammer to come to New Zealand.

410 When the scammer did not arrive in New Zealand person X became suspicious and made a statement to Police that she was the victim of a scam. Contact from the scammer ended for several months leaving person X several thousand dollars out of pocket as a result of the scam.

411 Months later, the scammer resumed contact the person X to initiate a second scam that would see person X became an unwitting accomplice in money laundering. The scammer told person X that a friend would transfer money from a New Zealand account to the person X's bank account. Person X was to withdraw the money in cash and wire the money to several bank accounts in different South East Asian countries minus the money that person X had 'loaned' the scammer for the flight tickets.

412 Unbeknown to person X, the email address of the other New Zealand account holder had been hacked and fraudulent instructions had been send to the New Zealand bank. The person X's bank became suspicious when its account monitoring detected the money transfers being quickly followed by withdrawals and identified that she was being used as a mule.

413 Person X's bank reported the matter to Police. The subsequent Police enquiry resulted in a formal warning of person X for the money laundering offence under the Crimes Act 1961.

414 STRs were received in relation to the transactions where the person X was used as a money mule. However, no STRs were received in relation to the initial wire transfers to Nigeria relating to the original scam despite the indicators (below).

415 Typologies: wire transfers, cash deposits, electronic transfers, use of third parties

416 Money laundering indicators:

- deposits quickly followed by cash withdrawal;
- multiple international wire transfers over a short time period; and
- multiple transactions to structure transaction.

417 Scam indicators:

- multiple wire transfers over a matter of days; and
- wire transfers to high risk scam jurisdiction.

This case is published in FIU Quarterly Typology Report Q1 2013-14 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2013-2014.pdf

SRI LANKA

418 *Laundering proceeds from drug trade case.* One of the licensed commercial banks raised an STR on person U stating that his account turnover was unusual. He had been requested to provide an updated KYC form, however, despite several reminders he had ignored requests to provide the form and visit the branch. His account had been credited with multiple daily deposits from many outside branches. At the time of opening the account, he had stated that he is engaged in business activities. The deposits varied between LKR 100,000 (~USD700.00) to LKR 1.0 million (~USD7,000.00), with a total value of approximately LKR 31.0 million (~USD212,000.00) credited to the said account over a period of seven months. When his other banking facilities were investigated, a similar pattern of deposits was observed in another account of a commercial bank. His employment was declared in this instance as a labourer. The case involving person U was immediately referred to the LEAs for further investigations. The investigations revealed that Mr. U was one of the subordinates of a large scale drug dealer in Sri Lanka.

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

THAILAND

419 Criminal rings in the north and north eastern regions pursue cross-border illegal activities. These groups simultaneously engage in wildlife trade and drug trade, when selling wildlife to criminals in neighbouring countries, they sometimes get paid in drugs.

4.24 Use of false identification

FIJI

420 From 9 September to 29 September 2005, person C obtained a fake Fijian Land Transport Authority (LTA) driver's license under the pretence name of person M. He used this fake ID to open a bank account and deposit a fraudulently altered income tax refund cheque of approximately FJD47,000 (~USD22,750) into this bank account. Person C obtained a legitimate income tax refund cheque which he altered to show the pretence name of person M and an altered inflated amount of approximately FJD47,000 (~USD22,750). On 28 October 2015 person C was convicted of money laundering and on 12 November 2015 he was sentenced to four years imprisonment.

JAPAN

421 A man used a false identity card when purchasing a laptop from a second-hand shop. As the man had obtained the computer through committing fraud, he was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

PAKISTAN

422 A complaint was lodged against the suspect who was believed to be involved in fraud. The suspect 'JKL' opened an account at the branch of Bank X. At the time of account opening the information provided by the suspect stated that he was working as an Associate and dealing in property business. The account was opened for saving purpose. Two officials of the government department lodged a complaint against the individual and stated that their two cheques were stolen and issued with forged signature amounting to PKR3,000,000 (~USD28,600) and Rs.2,500,000 (~USD23,800). The proceeds of both the cheques were credited to JKL account through clearing. Some of the funds were immediately withdrawn in cash while the remaining funds were returned to the issuing bank after receipt of complaint.

423 The suspect admitted using a different signature. Both signatures were very different and therefore, a possibility of an unknown beneficial owner was suspected. From the trail of transactions it was observed that the account was primarily used to conduct transactions related to the stolen cheques and that no other significant transactions took place in the account. The case was forwarded to LEA for necessary action.

4.25 Gems and Precious Metals

MALAYSIA

424 *Method used:* gold buy back guarantee based on purchase price and not on the market price; substantial increase of deposits either through cash, cheque or inter-bank transfers to the suspect's bank accounts; reoccurrence of lump sum payments from the suspect's bank accounts to several individuals or businesses without apparent business cause.

425 *Background of subjects & modus operandi:*

- Company G conducted business activities in buying and selling gold bar which had grown to a multimillion ringgit company in short period of time with several branches in Malaysia as well as in foreign countries i.e. Country W, X, Y, and Z.
- Company G solicited funds from public through its gold investment scheme that offered a monthly profit return (or "hibah" – an Arabic term that means a "gift") to its customers for every gold investment made.

- Profit returns vary from 1% to 6% of the gold purchased price and the investment maturity was between 2 to 6 months contract period.
- Modus operandi of the gold investment scheme operated by Company G:
    - Investor purchased a gold bar/wafer from Company G at a premium price (slightly higher than the market price). Investor signed a Sale and Purchase Agreement (S&P) and collected the gold bar/wafer from Company G or through its agents. Company G issued a Certificate of Ownership and Letter of Profit, stating a monthly profit return (varies from 1% to 6%) and the contract period (maturity period) to the investor. Before the end of the contract period, the investor has an option to sell back the gold bar/wafer to Company G at the purchased price. The investor surrenders the gold bar/wafer together with S&P, Certificate of Ownership and Letter of Profit to Company G. Company G would buy back the gold bar/wafer by issuing cheques or funds transfer to the investor's bank account.

426 *Source of information:*

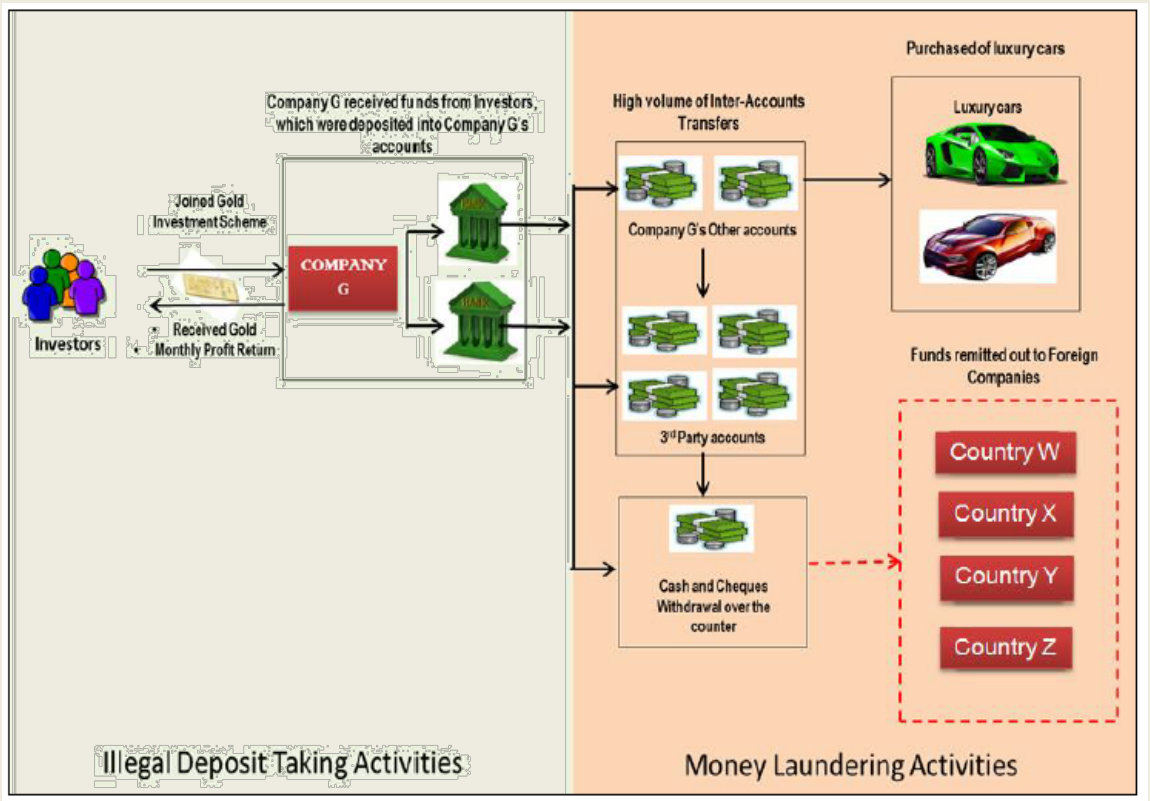
- STR and CTR records;
- Initial surveillance; and
- Exchange of information with foreign FIUs.

427 *Facts of the case:*

- It was reported that Company G had collected illegal deposits from public between year 2011 to 2012, without a valid approval from Bank Negara Malaysia, which was an offence under section 25(1) of Banking and Financial Institutions Act 1989 (BAFIA);
- Company G had also made several fund transfers to numerous associate companies and individuals in Malaysia, as well as other foreign entities abroad, and thus Company G had committed money laundering offence under section 4(1) of AMLA 2001; and
- Money trails showed that Company G had maintained several bank accounts with the local banks for the purposes of receiving funds from public and also for the repayment of profit return to investors.

428 *Actions taken to date:*

- Company G and its directors were charged under the offences of conducting illegal deposit taking activities, an offence under Section 25(1) of BAFIA 1989 and section 4(1) of AMLA 2001 for their involvement in money laundering activities by the company;
- All charges against Company G and its directors currently being heard in court; and
- Seized assets worth of RM100 millions are subjected to a forfeiture proceeding under AMLA, upon conclusion of prosecution against all the suspects.



INDIA

429 *Case:* The accused hatched a criminal conspiracy to cheat Indian Banks. The accused were running a company which was engaged in the business of trading gems and precious metals. They imported gold and thereafter exported diamond studded jewellery to Jurisdiction X based companies. Though the export bills could not be realized, the payments against the imports were realized by the overseas parties by encashing the Indian Banks' Letters of Credit. As a result the Indian Banks which had extended Letters of Credit were cheated.

4.26 Purchase of valuable assets (art works, antiquities, race horses, etc)

NEW ZEALAND

430 *Case Study - Operation Morph.* Police operation Morph related to supply of methamphetamine in the Wellington region. Three of the offenders involved, including the principal offender used purchases of high value goods to launder the cash proceeds of their drug offending.

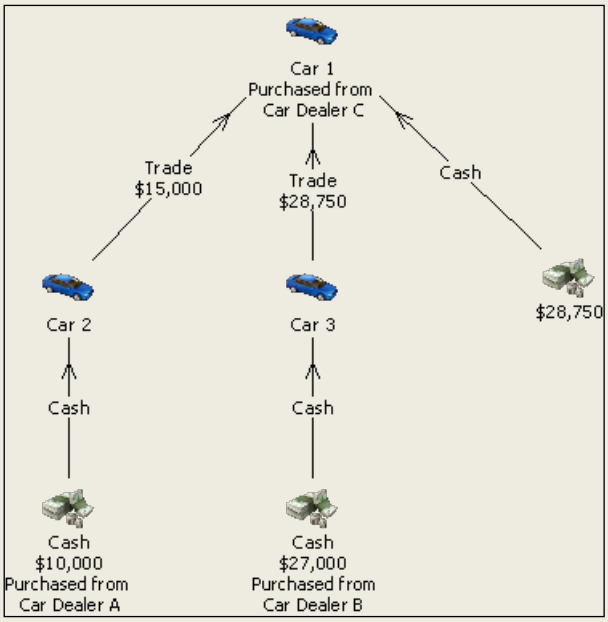
431 Person PR was the captain of the Wellington chapter of the Nomads gang and was the principal offender in an enterprise. During 2009-2011 person PR and his two associates, person C and person L, were receiving benefits, which where their only sources of income. However, their financial activity did not match their legitimate income. RP's legitimate benefit income, for example, amounted to NZD10,000 (~USD6,800) per annum. However, during the period July 2009 to February 2011 NZD129,000 (~USD87,700) in cash could be traced through RP's accounts and cash spending. NZD16,000 (~USD10,800) was also traced through PR's online gambling account although he only made one NZD40 bet.

432 PR, C and L all made several significant cash purchases between 2009 and 2011 to dispose of cash proceeds of crime. In particular, vehicles were purchased and placed in third parties' names to disguise the true ownership. Placement was also achieved by purchasing the vehicle with a credit card that would then be paid off in structured cash payments.

433 This case is published in FIU Quarterly Typology Report Q3 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2014-2015.pdf

434 *Case study - Operation Wigram*. High value goods such as vehicles are also an effective means of layering. In Operation Wigram buying and selling vehicles was used in a simple scheme to affect all three stages of money laundering.

In the placement stage, the offenders used the proceeds of commercial burglaries and methamphetamine dealing to purchase less expensive vehicles in cash. Layering and integration were achieved when these less expensive vehicles were soon after traded in for a single more expensive vehicle. Although simple, this structure allowed the offenders to structure the effective cash purchase of the final high value vehicle and establishes an origin of funds for the final transaction (the trade-ins).



435 This case is published in FIU Quarterly Typology Report Q3 2014-15 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2014-2015.pdf

4.27 Investment in capital markets, use of brokers

NEW ZEALAND

436 *Case 1.*The FIU has received several reports from New Zealand banks about a potential movement of layered funds by two foreign nationals residing in New Zealand as Category 1 investors. Under this category, a foreign national can apply for New Zealand residence if they can invest a minimum of NZD10 million (~USD6.8 million) in New Zealand for at least three years.

437 In 2012, on the same day but separately, both investors opened accounts to set up portfolios of New Zealand Immigration acceptable investments for the three year period in order to secure New Zealand residency. Shortly thereafter, investor 1 had funds of NZD10.5 million arrive into his newly opened account, originating from several international transfers. Less than two years later after the initial investment, NZD10 million were remitted to his own account held in his home jurisdiction. Meanwhile, investor 2 had about half of the required amount of NZD10 million wired into his Immigration New Zealand bond portfolio account, which 18 months later were moved out to a New Zealand corporate bank account and then subsequently transferred out further to another New Zealand

bank account the following day. When questioned, investor 2 was unwilling to provide details about the large account withdrawal, and soon after he closed his portfolio account.

438 The banks were unable to determine the purpose of the international transfers, there are serious questions and concerns that both individuals have breached New Zealand immigration rules and potentially laundered illicit funds through New Zealand.

439 *Case 2*. Several New Zealand banks have reported some unusual share trading patterns. Certain individuals would deposit cash of tens of thousands of New Zealand dollars into their newly opened accounts, and immediately start buying various high value stocks and selling them off in a few days, always for a loss. The banks became suspicious when they repeatedly tried to explain the customers that their sale trade would result in losses but the clients had expressed no concerns about the large loss and continued with the pattern.

440 One customer had small deposits of NZD1,000 (~USD680) coming into his account every couple of days. The source of the incoming funds was unknown as they were either cash or wire transfers. His trading pattern was not in line with common trading activity, for example, he would buy a few number of shares relating to one company and within a month sell the same number of shares on that company at an excessive loss.

441 Although no evidence of market manipulation has been proved at this stage, the banks have red-flagged these transactions as a potential money laundering tactic.

442 These two case studies are published in FIU Quarterly Typology Report Q1 2015-16 on New Zealand Police website http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q1-2015-16-capital-markets.pdf

4.28 TF and Foreign fighter

CANADA

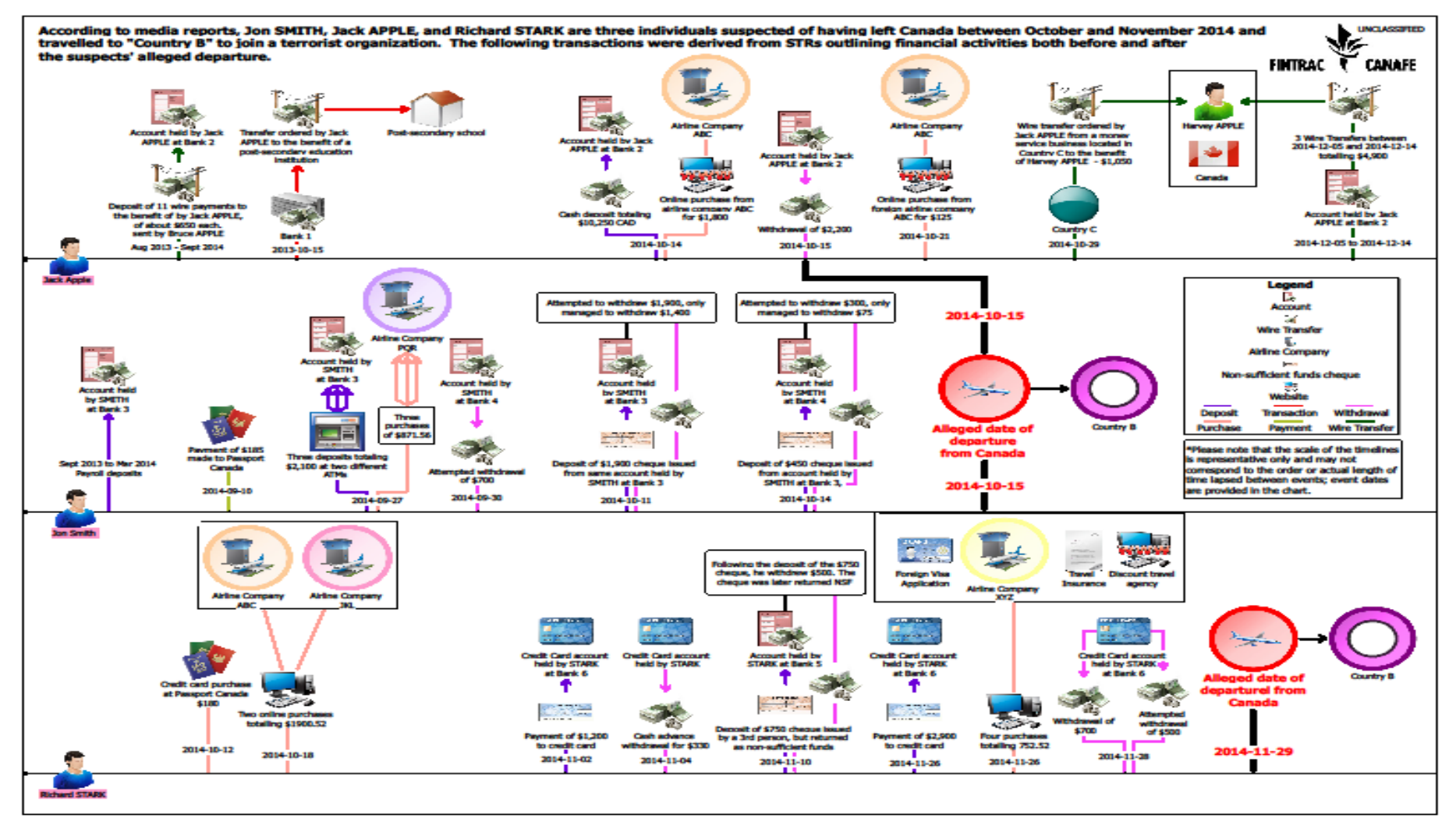
443 *Crowdfunding case*. FINTRAC (FIU Canada) has seen instances where individuals under investigation for terrorism related offences, including attempts to leave the country for terrorist purposes, have used crowdfunding websites prior to leaving and/or attempting to leave Canada. In one example, a reporting entity received information from law enforcement that an individual left Canada which prompted an account review and a STR being sent to FIU Canada. It contained details in regard to a crowdfunding website. Specifically, the reporting entity stated: “This account was used for four transactions, totalling CAD61.56 [~USD47.00] with a known crowdfunding website [web address provided]. This merchant is categorized by its merchant bank as “Professional Services”. The company’s website describes itself as an International Crowdfunding site, allowing people to easily set up a fundraising webpage and collect donations. Most of the donation options are related to conflict relief in Country A, Country B and Country C”.

444 *Foreign fighter case*. The FIU developed a case that shows the types of transactions related to individuals who have been reported to have travelled to foreign countries to join terrorist organizations (see explanatory diagram below). The transactions conducted by the suspected high risk travellers in the periods before, or after their reported departures from Canada, include purchases from airlines, a passport agency, as well as funds transfers, multiple cash deposits and withdrawals. Multiple reporting entities identified these transactions as suspicious because they provided the means for the individuals to travel to their destinations to join terrorist organizations. The transactions are all valued, at most, in the two to three thousand dollars range. In the case of cash deposits and international funds transfers, these are well below the CAD10,000 (~USD7,777) reporting threshold to in Canada. Therefore, due to the nature of these transactions, FIU Canada relied on STRs from reporting entities. The transaction information allowed Canada’s CFT regime to better understand the

financing aspect of this type of terrorist activity and helped FIU Canada develop the following terrorist financing indicators:

- Client identified by media or law enforcement as having travelled, attempted/intended to travel to high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations;
- Client accesses accounts, and/or uses debit or credit cards in high risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations;
- Client conducted travel-related purchases (e.g. purchase of airline tickets, travel visa, passport, etc.) linked to high-risk jurisdictions (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations; and
- The client mentions that they will be travelling to, are currently in, or have returned from, a high risk jurisdiction (including cities or districts of concern), specifically countries (and adjacent countries) under conflict and/or political instability or known to support terrorist activities and organizations.

FINTRAC Case on Transactions related to High Risk Travellers



5. INTERNATIONAL COOPERATION & INFORMATION SHARING

5.1 Cases of Cooperation between jurisdictions

445 In addition to the case studies above that include information sharing and other forms of cooperation, the below case studies demonstrate recent cases of AML/CFT international cooperation and information.

INDIA

446 Pursuant to Home Secretary level talks between India and Bangladesh held in October, 2012 in Dhaka, a Joint Task Force (JTF) on the Indian side was formed to combat the circulation of fake currency notes (FCN). A similar Joint Task Force was also formed on the Bangladesh side. The first and second meeting of the JTF between India and Bangladesh was held in New Delhi, India and Dhaka, Bangladesh respectively.

447 A MoU on FCN between India and Bangladesh was signed on 6 June 2015. As per the proceedings of the second meeting of the Joint Task Force, agreed by both the countries, a draft SOP was prepared and shared with Bangladesh Authorities through Ministry of External Affairs.

448 India has cooperated at the regional level (BIMSTEC) by providing assistance to countries on the CFT issues. During the period July 2014 – June 2015, FIU-India received 67 requests including 43 spontaneous disclosures from member jurisdictions. During the same period a total of 14 requests were sent to member jurisdictions by FIU-India. In addition, Indian Investigation Agencies have regularly sent requests under MLAT/letters rogatory and extradition to foreign countries in various terror funding/counterfeit currency cases being investigated by them. For example, on the basis of leads provided by Enforcement Directorate, USD 27.2 million was identified in two foreign jurisdictions.

CHINESE TAIPEI

449 Jurisdiction X law enforcement authorities conducted an investigation into a Latin American drug cartel in November of 2011, and found that a Chinese Taipei national known as Ms. Y had been laundering money from drug trafficking income under the cover of importing, exporting and selling garments in the jurisdiction X. Other than depositing part of the money in an account in the jurisdiction X, more than USD27 million was remitted into several bank accounts in Chinese Taipei. Chinese Taipei authorities have started to trace the funds and conducted intelligence exchange, in response to the request from the jurisdiction X. In September 2014, the Jurisdiction X requested Chinese Taipei authorities assistance in seizing Ms. Y's properties related to money laundering, pursuant to the Legal Assistance Agreement. The Taipei District Prosecutors Office successfully froze accounts involved in money laundering in Chinese Taipei and seized more than USD15 million in illicit money.

MACAO, CHINA

450 *Case of Third party money laundering.* Company A from Country X opened a local bank account mainly for the purposes of trading. Company A then received several remittances from Company B in Country Y, and transferred the funds to Company C in Country X shortly after the funds were received. As the bank account of Company A was apparently used as a channel for overseas fund transfer, the local FIU sent a request to the FIU in Country X for the background information of Company A and Company C.

451 Through intelligence exchanged as part of the analysis process, the information from the FIU of Country X revealed that both Company A and Company C were registered companies in Country

X, and the shareholders of Company C were being prosecuted for money laundering. As the funds that Company A received, could be criminal proceeds of a predicate offence committed overseas, the case was submitted to the Public Prosecutions Office for further investigation.

NEW ZEALAND

452 The Organised and Financial Crime Agency of New Zealand (OFCANZ) has restrained assets valued at an estimated NZD8.5 million (~USD5.78 million) as part of Operation Roller. Operation Roller was established as part of a wider strategy to target the supply of methamphetamine in New Zealand, and focused on three individuals, all of whom were arrested when methamphetamine to the value of NZD4.5 million (~USD3.6 million) was found in their possession. The investigations were undertaken as part of wider cooperation between New Zealand Police and Jurisdiction X authorities, which has resulted in several successful operations targeting the transnational methamphetamine trade. The assets restrained in this operation include a high end Audi R8, a Mercedes Benz E500, 17 bank accounts and cash sums totalling NZD3.3 million (~USD2.24 million), and eight residential properties in Auckland that are valued at an estimated NZD4.9 million (~USD3.33 million).

PHILIPPINES

453 *Execution of a request for documents via MLA in relation to human trafficking.* In January 2014, the Philippine Department of Justice (DOJ) endorsed to the AMLC Secretariat the request of Country U, pursuant to a Mutual Legal Assistance Treaty (MLAT), to obtain information/documents from several banks in the Philippines in connection with the investigation being conducted by jurisdiction U law enforcement agencies against company FN, and its owner, person X , for alleged trafficking of persons for exploitation, slavery, servitude and forced or compulsory labour, employment of an adult subject to immigration control, and money laundering.

454 Company FN employed a number of foreign nationals for its fishing vessels by bringing them to jurisdiction U. Between April 2012 and November 2012, eight seamen escaped from company FN vessels while six seamen were repatriated by jurisdiction U immigration officials. Some of these seamen appeared to be suffering from malnourishment and exhaustion. Information revealed that other seamen risked their lives by jumping overboard to evade the conditions aboard the vessels of company FN.

455 In December 2012, a number of search warrants were implemented on the business premises occupied by company FN and its associated companies, the premises occupied by the subjects and fishing vessels docked in Country U. 17 Asian nationals were rescued, some of whom were Filipino recruits who claimed that they were debt-bonded through a recruitment agency in the Philippines. They allegedly signed a contract with the Philippine Overseas Employment Agency (POEA) that was used to support their visa application with Country U. They were then issued a secondary contract, either upon arrival in Country U or shortly before their departure from the Philippines. These new contracts were often referred to as “adjustment of position and salary” documents and provide less favourable conditions and remuneration. The timing of the presentation of this secondary contract and prior debt bonding provided an element of duress to encourage compliance.

456 The seamen claimed that upon arrival in Country U, their passports and seaman’s books were taken from them. They also narrated how they were poorly treated prior to being taken on board the vessels of company FN- they were housed in cramped and dirty conditions; had limited access to water and sanitation facilities; fed inadequately with expired food; and locked within the compound of warehouse overnight.

457 The witnesses also collectively described appalling living conditions while at sea as they were subjected to repeated threats of violence, inadequate health and safety regime, physical injuries, denial of medical treatment and forced to operate machinery they were not qualified to handle. They were also forced to work in excess of 20 hours every day, denied adequate rest and undernourished. Their salaries were also not paid.

458 Company FN directly transferred the salaries of the seamen to the bank accounts of three Philippine recruitment agencies that would then deduct a certain sum before transferring the remaining amount into the seamen's accounts.

459 The AMLC filed an Ex Parte Application for Bank Inquiry into the bank accounts of the three Philippine recruitment agencies. The said Application was granted by the Court of Appeals and the AMLC conducted an examination and inquiry into the bank accounts. With the assistance of the Philippine Department of Justice, the bank documents obtained were delivered to Country U authorities, who personally travelled to the Philippines for the authentication of the documents in order to make sure that the said documents would be admissible in evidence in the trial courts in Country U.

460 *Execution of a request for documents via MLA in relation to an international boiler room operation.* In March 2014, the AMLC Secretariat received a request for information from the FIU of Country S in relation to person RSF and his companies that are under investigation for soliciting investors in Country S by means of false or fraudulent representations and promises. Funds from which were wired to his account in the Philippines. The AMLC Secretariat provided the FIU of Country S with the results of its initial investigation and database search, for intelligence purposes only. In May 2014, the AMLC Secretariat sent additional information on entities founded by person RSF.

5 Investigations revealed that person RSF employed telemarketers in several locations in the Philippines and Country S to conduct "cold calls" on potential investors and solicit funds for his companies in the Philippines, including SBS Corporation (SBSC), TGE Group (TGEG), and TB Electric (TBE) (collectively referred to as the Companies below). Person RSF and his telemarketers told investors that the companies would go public, the shares would be traded on a stock exchange and investors would make a lot of money. There were also promotional materials that indicated that TGEG "owns the global patent rights" for an invention that will turn garbage into electricity and touted TGEG as a "forever stock" like Coca-Cola, Apple, FedEx and Wal-Mart.

461 Person Y, who worked with person RSF in 2009-2010 and oversaw a branch of TGEG in Country S, opened a TGEG bank account with a universal bank in Country S in May 2009. Believing the representation and promises, funds from investors were wired and deposited into this TGEG account and were then wired to several accounts of person RSF in the Philippines.

462 Due to the unfulfilled promises, numerous investors complained to law enforcement authorities in Country S. Sources estimate that person RSF raised as much as USD50 million from investors. In July 2014, the Philippine Department of Justice (DOJ) endorsed the AMLC Secretariat request for assistance made by Country S, pursuant to an MLAT. In particular, Country S authorities requested assistance in seeking bank records from the Philippines to identify all the perpetrators of the scheme and to trace the proceeds of the fraudulent activity.

463 In October 2014, the AMLC issued a Resolution authorizing, among others, the AMLC Secretariat, through the Office of the Solicitor General, to file an Ex Parte Application for the issuance of an order allowing inquiry into certain bank accounts of person RSF and the entities founded by him. In November 2014, the Court of Appeals issued a Resolution granting the AMLC the authority to conduct an inquiry into and/or examination of the various bank accounts. Inquiry into the subject bank accounts was conducted and the bank documents obtained were transmitted to the Embassy of Country S through the Philippine Department of Justice in January 2015.

6. USEFUL LINKS

Anti-Corruption Research Network

464 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

465 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/

Global Center on Cooperative Security (GCCS)

466 The Global Center on Cooperative Security (GCCS) formerly known as the Center on Global Counterterrorism Cooperation (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; and
- survivors of terrorism around the world.

467 The GCCS builds these partnerships through collaborative research and policy analysis and by providing practical advice. GCCS develops innovative counterterrorism programming and training and assists key stakeholders to develop sustainable solutions to preventing terrorism. GCCS 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, GCCS 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.globalcenter.org

The Egmont Group

468 For FIU information and links to FIUs with websites.

http://www.egmontgroup.org/

Global Financial Integrity

469 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

7. ACRONYMS

ACA – Australian Central Authority
ACC – Australian Crime Commission
ADB - Asian Development Bank
AFP – Australian Federal Police
AGD – Attorney General's Department
AGO – Attorney General's Office
AML – Anti-Money Laundering
AMLA – Anti-Money Laundering Act
AMLC – Anti- Money Laundering Council (Philippines)
AMLD – Anti-Money Laundering Division (Chinese Taipei)
AMLO – Anti-Money Laundering Office (Thailand)
APG – Asia/Pacific Group on Money Laundering
ARS – Alternative Remittance Sector
ATM – Automatic Teller Machine
ATO – Australian Taxation Office
AUSTRAC – Australian Transaction Reports and Analysis Centre
BCR – Border Currency Report
BED – Business Express Deposit
CAMLMAC – China Anti-Money Laundering Monitoring and Analysis Center
C&ED – Customs and Excise Department (Hong Kong, China)
CARO – Criminal Asset Recovery Order (Brunei Darussalam)
CD – Certificates of Deposit
CDD – Customer Due Diligence
CDR – Cash Dissemination Report
CFT – Countering the Financing of Terrorism
CTR – Cash/ Currency Transaction Report
DIBP – Department of Immigration and Border Protection (Australia)
DMLI – Department of Money Laundering Investigation (Nepal)
DNFBP – Designated Non-Financial Businesses and Professions
DOJ – Department of Justice
EAG – Eurasian Group
EDD – Enhanced Due Diligence
EFT – Electronic Funds Transfer
ESAAMLG – Eastern and South African Anti Money Laundering Group
FATF – Financial Action Task Force
FIA – Federal Investigation Agency (Pakistan)
FinCEN - Financial Crimes Enforcement Network (US)
FINTRAC - Financial Transactions Reports Analysis Centre (Canada)
FITS – Fiji Integrated Tax System
FIU - Financial Intelligence Unit
FMU – Financial Monitoring Unit (Pakistan)
FRCA – Fiji Revenue and Customs Authority
FSRB – FATF-Style Regional Bodies
FTF – Foreign Terrorist Fighters
FTRA – Financial Transactions Reporting Act
GIF – Financial Intelligence Office (Macao, China)
HKC – Hong Kong, China
HKPF – Hong Kong Police Force
ICE – Immigration and Customs Enforcement (US)
ICRG – International Cooperation Review Group

IFTI – International Funds Transaction Instruction
INTERPOL –International Criminal Police Organisation
IP – Internet Protocol
JAFIC – Japan Financial Intelligence Center
KYC – Know Your Customer
LEA – Law Enforcement Agency
LTA – Land Transit Authority (Fuji)
MA Act – Mutual Assistance Act
MJIB – Ministry of Justice Investigation Bureau (Chinese Taipei)
ML – Money Laundering
MLA – Mutual Legal Assistance
MLAA – Mutual Legal Assistance Agreement
MLAT – Mutual Legal Assistance Treaty
MOU – Memorandum of Understanding
MTO – Money Transfer Operators
NAB – National Accountability Bureau (Pakistan)
NBI – National Bureau of Investigation (Philippines)
NGO – Non-Government Organisation
NPO – Non-Profit Organisations
NRA – National Risk Assessment
OCG – Organised Crime Groups
PDAF – Priority Development Assistance Fund
PEP – Politically Exposed Person
PNP – Philippine National Police
RBA – Risk Benefit Analysis
RMP – Royal Malaysia Police
RNP – Remittance Network Provider
RTC – Regional Trial Court (Philippines)
SEC – Securities and Exchange Commission (Philippines)
SMR – Suspicious Matter Reports
SOC – Serious and Organised Crime
SOCG – Serious and Organised Crime Groups
STR – Suspicious Transactions Report
TDRs – Term Deposit Receipts
TF – Terrorist Financing
Tracfin – Traitement du renseignement et action contre les circuits financiers clandestins (France FIU)
TT – Telegraphic Transfer
TTR – Threshold Transaction Reports
UNODC – United Nations Office on Drugs and Crime
VAT – Value Added Tax