APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2017

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

July 2017

APG Yearly Typologies Report 2017

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

Tel: +61 2 9277 0600
Email: 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 2016-2017

5 The Typologies Working Group continued its work in 2015-16, initially under the leadership of Mongolia and India as Co-Chairs. In January 2017, Mongolia stepped down as Co-Chair. The APG would like to express its gratitude to Mongolia for its support of the APG's typologies work.

6 In September 2017 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 was held in November-December 2016 hosted by Saudi Arabia.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2016 - 2017

7 This section of the report provides a brief overview of typologies related work undertaken by the APG between July 2016 and June 2017.

1.1 2016 MENAFATF 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 2016 MENAFATF APG Typologies Workshop was held in Jeddah, Kingdom of Saudi Arabia from 28 November to 1st December 2016 and hosted by the Anti-Money Laundering Permanent Committee (AMLPC). The workshop involved approximately 300 delegates from 55 jurisdictions and 15 international and regional organisations. The workshop was co-chaired by the MENAFATF and APG Typologies Working Group Co-Chairs from India and Tunisia.

11 The workshop included a plenary session (first and last day) and four two-day concurrent sessions on; (i) terrorist financing and social media, (ii) the challenges of pursuing the proceeds of corruption in foreign countries, (ii) money laundering through electronic means, and (iv) identifying operational best practices and barriers to domestic inter-agency information sharing.

12 The plenary included presentations on a new FATF project on the financing of recruitment for terrorist purposes; an update by UNODC on two projects titled APG Typologies project on ML and Wildlife, and Typologies and Their Use in the Automatic Detection of ML/TF Schemes; a MENAFATF project on ML and corruption; an update on FATF RTMG projects and a presentation by the United Nations on the financing of ISIL affiliates. The final day included report back presentations to the plenary on all four break-out sessions. The MENAFATF and APG secretariats presented on a new joint MENAFATF/APG project on Terrorist Financing and Social Media.

13 Across the four breakout sessions, the following common themes, needs and recommendations were identified:

- Risk assessments at both a national and regional level which involve both government and the private sector will greatly assist jurisdictions' understand the risk, scope and requirements to mitigate the risks posed by technology and emerging terrorism threats and will allow for a common understanding of risk and coordinated mitigating strategies.

- Public – private partnerships will greatly enhance efforts to counter the challenges of technology particularly those associated with social media, virtual currencies, payment systems and the development of IT to counter ML and TF.

- Improved domestic and international collaboration is critical.

- Jurisdictions need to actively engage in awareness raising with partner agencies and the private sector to ensure an enhanced understanding of the risks and the role each party has in ML and TF mitigation. These engagements should include discussion of research opportunities, respective roles, the sharing of information, emerging risks, new typologies and red flags, all of which will further strengthen global, regional and national efforts to mitigate ML/TF.

- Capacity and capabilities of authorities in regulating, monitoring, investigating and prosecuting ML and TF is variable and in many cases limited. Improved training both within jurisdictions and regionally is critical.

- Legislation needs constant review and updating to enable jurisdictions to operate in an evolving, global and technology driven world. Enhanced supervision and engagement with the private sector is essential.

1.2 Status of current and possible new typologies projects

14 In 2016–17, the APG had three on-going typologies projects, as follows:

- *Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime* project is being managed by UNODC supported by the APG secretariat. The project was initiated at the 2015 APG typologies workshop hosted in Nepal. Noting that wildlife crime poses a serious threat to thousands of species and is a global issue affecting almost every jurisdiction, either as a source, transit or destination for illegal wildlife products, this project aims to support APG jurisdictions in combating wildlife crime and detecting, investigating and disrupting illicit financial flows. Based on open source information and questionnaire responses from 45 jurisdictions (12 from Asia/Pacific; nine from Africa; 21 from Europe and three from the Americas), the report includes recommendations and a good practices guideline on how to make better use of financial investigation, financial intelligence, and anti-money laundering techniques to combat wildlife crimes. The report was finalised in July 2017;

- The *APG/MENAFATF Joint Project on Terrorist Financing and Social Media.* This project is being co-chaired by Malaysia and Egypt. In recent years it has become clear that social media provides new opportunities for terrorist organisations and individuals to promote their cause, recruit followers and raise funds for their activities. To better understand this phenomenon, a questionnaire seeking case studies abuse of social media for TF and measures to counter it was circulated to APG and MENAFATF members and observers in April 2017. The project is scheduled to conclude in November 2017; and

- *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 in late 2017.

15 In 2017-18 there is one new typologies project being undertaken:

- *Money Laundering and Terrorism Financing Risks Arising from Trafficking in and Smuggling of Human Beings*. Human trafficking is a crime which is second only to drug trafficking in the amount of proceeds it generates for criminal groups. People smuggling continues to be a global and regional challenge with, for example, the ongoing civil war in Syria leading to

massive displacement and reliance on people smugglers to gain entry into Europe. The APG project has two-phases, as below:

- *Phase 1* – a joint FATF/APG project focused on human trafficking; and
- *Phase 2* - an APG regional project that builds on the FATF/APG human trafficking project and includes consideration of people smuggling, which is out of scope in Phase 1, and implementation support for measures to manage both human trafficking and people smuggling.

- Overall the project aims to develop an updated understanding of ML and TF risks related to human trafficking and people smuggling; improved indicators of ML and TF, guidance on good practices and to provide implementation support where practical.

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

16 This section of the report provides a brief overview of typology reports published by FATF and other FSRBs between July 2016 and June 2017.

2.1 FATF typology projects

FATF TF Risk Indicators Report

17 The TF Risk Indicators report was a confidential report that developed risks indicators for the private and public sectors to identify TF activity. This report was circulated to FATF and FSRB Member States, who subsequently disseminated the report to financial institutions located within their respective jurisdictions. Outcomes of the report were assessed over a one year timeframe as part of an ongoing follow-up process.

FATF ISIL Updates

18 FATF released a report on ISIL financing in February 2015 and instituted an internal follow-up process to collect new information in advance of each Plenary. The first updates included information from multiple FATF and FSRB delegations. The updates emphasise the various actions taken by jurisdictions to combat ISIL, which include targeted financial sanctions, law enforcement and customs operations, as well as military operations. These updates are part of an internal procedure and are not published.

FATF/GIABA/GABAC Terrorist Financing in West and Central Africa

19 This joint FATF-GIABA-GABAC report reveals a number of terrorist financing threats and vulnerabilities that are specific to the West and Central Africa region, and highlights the role of cash, including foreign currency. The report looks at the contextual factors and the challenges that the region faces to regulate financial products and sectors. The report highlights the need for countries in the region to work closer together as well as with the broader international community to identify and disrupt terrorist financing. 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

20 In 2016 EAG continued working on several Typologies projects, as follows:

- The Republic of Tajikistan led the project *Laundering of proceeds from financial pyramid schemes*. This project was completed May 2016;
- The Russian Federation led the project *Typology: illegal expatriation of assets of the credit institutions and money laundering.* This project was completed November 2016;
- The Russian Federation led the project: *Typology of corruption offenses and money laundering*. This was completed November 2016; and
- The Republic of Kazakhstan, leader of the project *Structural analysis of financial flows related to cash-in with a purpose of committing offenses and money laundering*. This project will be completed November 2017.

21 In 2017 EAG started working on several projects, as follows:

- Money Laundering through the insurance companies – co-leads: China and Russia;
- Identifying persons facilitating terrorist organizations by purchasing tickets for FTFs – lead: Russia.

2.3 ESAAMLG – The Eastern and Southern Africa AML Group

A special typologies project report on poaching, illegal trade in wildlife and wildlife products and associated money laundering in the ESAAMLG region

22 This report highlighted the problem of poaching and illegal trade in wildlife and wildlife products and associated money laundering in the ESAAMLG Region. The key finding of the report is wildlife crimes are escalating at an alarming rate and could result in extinction of some species in the near future. The report discusses the ML risks in the ESAAMLG region due to the significant proceeds associated with wildlife crime. The report highlights that a lack of financial intelligence use and limited knowledge and information of the financial flows of illicit proceeds hampers wildlife crime investigations and prosecutions. This report also highlights the challenges faced by authorities in combatting wildlife crime, namely lack of resources, poor international cooperation and vulnerabilities in legal frameworks.

23 This report aims to provide awareness on the seriousness and repercussions of the wildlife trade and urges ESAAMLG member countries to reconsider their anti-wildlife crime policies and introduce tighter legal frameworks. 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

24 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. 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

25 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 organisation, and MMF proceeds are often remitted via different jurisdictions to conceal the source. Criminal organisations involved in MMF recruit “employees” and place them in countries around the world to perpetrate schemes and move the illicit proceeds.

26 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.

27 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.

28 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

29 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

Regional Risk Assessment on Terrorism Financing 2016 - South- East Asia & Australia

30 Australia's financial intelligence agency (AUSTRAC) and its Indonesian counterpart financial intelligence unit (FIU), Pusat Pelaporan dan Analisis Transaksi Keuangan (PPATK), co-led the research and development of the regional risk assessment, with contributions from the FIUs of Malaysia, the Philippines, Singapore and Thailand.

31 The risk assessment aims to inform responses to wider global terrorism financing issues under consideration by international anti-money laundering and counter-terrorism financing (AML/CTF) bodies, and contribute to the refinement of analytical tools to better assess terrorism financing risk. The assessment focuses on the terrorism financing methods and channels currently presenting the highest risks, as well as those forecast to pose increasing risks over the medium term (three to five years). These include channels that present joint country or intra-regional risks. The assessment also identifies priority areas where regional efforts could be focused to strengthen CTF capability and better mitigate terrorism financing risk. The report is available from http://www.austrac.gov.au

ML/TF risk assessments

32 Recently AUSTRAC published the below ML/TF risk assessments to assist industry and government understand and disrupt criminal financial activity. Each report provides an overall risk rating, based on an assessment of the criminal threat environment, the vulnerabilities in the sector, and the associated consequences.

- *Stored value cards* - AUSTRAC concluded the overall ML/TF risk associated with the use of stored value cards (SVCs) to be medium, and their vulnerability to criminal misuse to be high. The report found that the risk level of individual SVCs varies significantly depending on the features of the specific product. Travel cards that can be reloaded and redeemed offshore in cash carry significantly higher levels of risk than low value retail gift cards. The most common crime-types in which SVCs are implicated are money laundering and cyber-enabled fraud. Of particular concern is the use of SVCs for terrorism financing purposes. The report is available from http://www.austrac.gov.au/publications/mltf-risk-assessments.
- *Australia's financial planning sector* - AUSTRAC assessed the overall risk of ML/TF activity as medium. The report found that as financial planners facilitate access to financial services for their customers, this can make them susceptible to exploitation for criminal purposes. It also means planners are well-placed to detect suspicious behaviour by their customers. The report encourages the financial planning sector as a whole to ensure that AML/CTF compliance is a greater part of the organisational culture. The report is available from http://www.austrac.gov.au/publications/mltf-risk-assessments.
- *Australia's superannuation sector* - AUSTRAC identified higher than anticipated risks of fraud, cybercrime and terrorism financing in the superannuation sector, and has assessed the overall risk of ML/TF activity as medium. This report aims to develop awareness in the sector of these risks and help harden APRA-regulated superannuation funds against criminal activity. The report is available from http://www.austrac.gov.au/publications/mltf-risk-assessments.

33 In addition, in April 2016, AUSTRAC initiated a nation-wide campaign in response to persistent misconceptions about money laundering risk and methodologies it had observed in the pubs and clubs sector. In particular, AUSTRAC was concerned that there was a strong pattern of the pubs and clubs engaged opining that: (i) electronic gaming machines were low risk for money laundering, (ii) regular customers were unlikely to be money launderers, and (iii) customers that lose as much (or even slightly more) than they win cannot be laundering money.

34 AUSTRAC collected information from over 150 pubs and clubs and launched a broad-based education campaign, which substantially increased suspicious matter reporting by the sector. For example, since the commencement of the campaign in April 2016 the number of suspicious matter reports per month is approximately 40% higher than the number for 2015. In addition, the number of unique pubs/clubs reporting per month has increased by 75%. This is a more important indicator as it controls for the possibility of a particular pub or club skewing the results by submitting a significant number of SMRs in a month, and it also better demonstrates the extent to which awareness of AMLCTF obligations throughout the industry has increased.

NEW ZEALAND

35 The NZ-FIU has published Quarterly Typology Reports, which are available from http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents. The latest reports are as follows:

- *Quarterly Typology Report Q3 2015-2016 – Predicate Offence,* which includes an in-depth examination of ML predicate offences.
- *Quarterly Typology Report Q4 2015-2016 - Alternative Banking Platforms,* which includes an in-depth examination of ML methods, vulnerabilities and indicators associated with the alternative banking platforms
- *Quarterly Typology Report Q1 2016-2017 – Cryptocurrency,* which includes an in-depth examination of ML methods, vulnerabilities and indicators associated with the cryptocurrency
- *Quarterly Typology Report Q2 2016-2017 - Human Trafficking and People Smuggling,* which includes an in-depth examination of ML methods, vulnerabilities and indicators associated with the human trafficking and people smuggling

36 In addition the NZ-FIU has developed unpublished reports on: (i) New Zealand Casinos and Organised Crime, and (ii) Prepaid Cards in New Zealand. Please contact the NZ-FIU in relation to these reports.

3.2 Association of types of ML or TF with predicate activities

AUSTRALIA

37 AUSTRAC publishes real-life cases that present a snapshot of how criminals are seeking to misuse Australia's financial system and how AUSTRAC intelligence and analysis is instrumental in combating these criminals. These case studies are a valuable resource for industry and AUSTRAC's partner agencies. These reports are available from http://www.austrac.gov.au/case-studies, and recently AUSTRAC has published the following four reports on the association of different types of ML or TF with particular predicate activities:

- *Guns, Drugs, Pistons* – details of AUSTRAC role in supporting an investigation into a criminal syndicate suspected of importing firearms and illicit drugs into Australia from the United States via sea cargo
- *False Passports, Counterfeit Euros, 10 Years' Imprisonment* – details of law enforcements investigation into a person exchanging counterfeit currency after receiving information from banks across WA, SA and Victoria.

- *Car Park Drug Deal Leads To Arrest Of Organised Crime Members* - AUSTRAC support for law enforcement investigation into a drug trafficking syndicate suspected of having long-term involvement in the supply and distribution of narcotics in Australia.
- *AUSTRAC Helps Stop Illegal Tobacco Importation Syndicate* – details of a joint law enforcement investigation identified members of an Australian syndicate involved in the importation of illegal tobacco and cigarettes from South East Asia and the Middle East.

MALAYSIA

38 The ML investigations focus on the high risk crimes identified from NRA namely drugs, corruption, frauds, smuggling and tax evasion. Priority is given where there is an element of organized/syndicated crimes. Investigations on terrorism have also been extended for any TF element.

3.3 Emerging trends; declining trends; continuing trends

AUSTRALIA

Emerging Trend: Money mules

39 Money mules from an Eastern European country open Australian bank accounts and receive fraudulently obtained funds from Australian victims via cybercrime. Typically, they withdraw the funds as cash or make electronic transfers to offshore beneficiaries. They may also purchase high value items such as watches.

40 Money mules from a second Eastern European country typically open multiple bank accounts to receive stolen funds from Australian victims. They often register businesses and open associated bank accounts to avoid detection by banks and law enforcement agencies. The stolen funds are typically washed through their accounts via cash withdrawals, electronic transfers and purchases of foreign currency.

41 Money mules from a third Eastern European country register an Australian business and open bank accounts with that business name, within two weeks of arriving in Australia. In some cases, they open multiple bank accounts at various financial institutions. They also open personal banking accounts. They use their business and personal bank accounts to transfer funds between each and to make large cash deposits and withdrawals. Some mules are sending funds to the same Hong Kong based companies. The funds appear to be derived from internet banking fraud, malware activity and fraudulent refunds from Australian government departments. Fraud victims include Australian citizens and businesses.

FIJI

Emerging Trend: ATM Skimming

42 Cases were brought to the attention of the FIU involving foreign nationals who obtained customers bank card details by fraudulent means using ATM and EFTPOS skimming devices. The Director of the FIU stated in a press release that there was an increase in the number of skimming cases since June 2015. A major incident occurred in December 2015 that affected more than 500 credit and debit cardholders. An attempt to conduct ATM skimming in January 2016 was successfully foiled.

43 In August 2016, the Fiji FIU received information that three Asian nationals were using stolen and counterfeit Visa and MasterCard cards at BSP ATMs in Tonga and Samoa. Two of the Asian nationals were in custody in Samoa whilst the third national reportedly left for Fiji. The trend of ATM skimming appears to have emerged not only in Fiji but across the Pacific.

Continuing Trend: Advance Fee Fraud and Tax Evasion

44 The Fiji FIU issued 6 alert notices to commercial banks and money remittance service providers to conduct enhanced due diligence procedures for suspected possible advance fee fraud, lottery scam related remittances and email spoofing activities. The Fiji FIU continued to receive cases related to unsolicited emails promising attractive job opportunities, payment of lottery awards, inheritance of large amounts of funds, lucrative investment opportunities and other "get-rich-quick" schemes.

45 The Fiji FIU continues to note STR cases for possible tax evasion, such as the use of family members (including minors) personal bank accounts to hide business proceeds.

MALAYSIA

STR Analysis

46 A substantial increase in STRs submissions is attributable to heightened transaction monitoring by reporting institutions; and increased awareness of money services operators. The main offences reported by reporting institutions were fraud/scam, tax evasion and bribery/corruption.

Some ongoing trends

47 Cash transactions remain the preferred methods for movement of illegal proceeds (receiving, transferring and spending).

48 Usage of 3rd parties' account including mules account holders, for receiving and transferring the illegal proceeds of criminal activities.

49 The collection of funds for terrorism activities mostly for the financing of foreign terrorist fighters (FTF) rather than financing of the terrorist groups themselves.

50 The funds for FTFs are solicited via social media.

51 Usage of 3rd parties' account including mules account holder, to receive on behalf or to transfers to FTFs.

SINGAPORE

Emerging and ongoing trend – Money mules and international wire transfer fraud

52 In early 2012, the Commercial Affairs Department (CAD) detected a crime trend where illicit funds were being transferred to bank accounts in Singapore. In many of the cases, the criminals hacked into the email accounts of their victims to send instructions to the victims' banks for the transfer of funds to bank accounts in Singapore. On discovery of the fraudulent transfers, victims informed their banks which then attempted to recall the funds from the banks in Singapore. In other cases, victims fell for the scams perpetrated by the criminals and made the transfer of funds at the criminals' instruction. Some of these cases were detected when STRs were filed by Singapore financial institutions when they were asked to return funds deposited into their customers' bank accounts. In other cases, the victims of fraud lodged police reports online.

53 These cases, known as "international wire transfer fraud" rose from 93 reported cases in 2012 to 212 cases in 2013. The CAD investigations revealed that criminal syndicates operating overseas were behind the movement of stolen funds derived from criminal activities committed overseas. The bank accounts in Singapore are held by locals who befriended members of the criminal syndicates, mainly through social networking websites on the internet. These local bank account holders also known as 'money mules', wittingly or unwittingly, at the request of the criminal syndicate, agreed to

receive funds into their account and thereafter transfer the funds elsewhere, usually to bank accounts overseas. The money mules usually receive a commission for their role in the transfer of the funds.

54 In order to tackle the money mule problem, the CAD employed a multi-pronged approach. Firstly, the CAD promptly shared information with relevant agencies – for example, the Suspicious Transaction Reporting Office (STRO) worked closely with STR-filers and shared information by making spontaneous referrals to its foreign counterparts. In addition, STRO's findings on its assessment of this crime problem were shared with the affected banks as well as the Association of Banks in Singapore (ABS) so that the information could be further disseminated to other members.

55 Secondly, the CAD worked closely with law enforcement authorities of various jurisdictions to identify the victims whose monies may have been fraudulently transferred into Singapore. This enabled the CAD to conduct further investigations into money laundering and at the same time, take the necessary action to recover the victim's monies. The following table details the number of foreign victim bank accounts identified through the close collaboration between the CAD and its foreign counterparts, the amounts transferred from the victim's account and the amounts of criminal proceeds successfully seized by the CAD.

56 Table: Number of bank accounts identified and criminal proceeds seized by the CAD

	2012	2013	2014	2015	2016
No. of foreign victim bank accounts identified	129	264	148	64	37
Total amount identified to have been fraudulently transferred from the victims' account to Singapore accounts (million)	24.6	31.5	14.9	6.67	3.92
Percentage of criminal proceeds seized	11	18	15	15.6	25.2

57 In addition, the CAD worked with the Attorney-General's Chambers (AGC) to ensure that strong enforcement action is taken against money mules.

58 Thirdly, the CAD intensified its efforts in the area of crime prevention and public education. In November 2014, the CAD launched a campaign to increase public awareness of the new crime typologies. As part of the crime awareness campaign, police utilised several forms of out-of-home publicity such as billboards, advertisements on public transport, office buildings and hawker centres so as to bring the crime awareness message to the masses. Besides conventional media platforms, the police also leveraged on digital platforms such as YouTube, Facebook, Twitter. In addition to public education, the police worked closely with local media to publicize successful "money mule" prosecutions in order to deter potential criminals.

59 The above has been successful, resulting in a substantial fall in the number of reports of international wire transfer fraud proceeds being laundered through Singapore 'money mules'. The number of reports received fell by 83.5%, from 212 cases at the peak in 2013 to 35 cases in 2016.

4. A FOCUS ON MONEY LAUNDERING AND CORRUPTION

60 Corruption is a significant issue in the global economic system and can lead to increased poverty, destabilisation of governments, diminished economic performance and social inequality. Furthermore, corruption and ML are intrinsically linked - by successfully laundering the proceeds of a corruption offence, such as bribery or theft of public funds, the illicit gains may be enjoyed for private gain without fear of being confiscated. For these reasons, this the APG 2017 Typologies Report includes a focus on understanding emerging risks, trends and contextual issues associated with laundering the proceeds of corruption.

4.1 Scope of corruption in the Asia/Pacific region

61 A recent survey by Transparency International[1] found that one in four persons surveyed have paid a bribe to access public services. When extrapolated to the population, over 900 million people across the Asia Pacific region had paid a bribe in the past year in order to access basic services such as education or healthcare. Furthermore, results of the 2016 Corruption Perceptions Index show that the majority of Asia Pacific jurisdictions sit in the bottom half of the index with 19 out of 30 jurisdictions in the region scored 40 or less out of 100.[2]

62 These findings are reflected in APG members' national ML/TF risk assessments with a number of members highlighting corruption as a higher-risk ML threat and mutual evaluation (ME) teams paying particular attention to corruption issues in APG 3rd round ME reports.

4.2 International standards on combating money laundering and the financing of terrorism & proliferation

63 While the international standards are designed to combat ML, TF and PF because of the intrinsic link between corruption and ML, when the international standards are effectively implemented, they creates an environment where it is more difficult for corruption to thrive undetected and unpunished[3].

64 *The FATF Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight against Corruption*[4] provides an in-depth discussion on how effective implementation of FATF Recommendations can combat corruption. Very briefly, the FATF Recommendations can combat corruption by:

65 *Safeguarding the Integrity of the Public Sector* – the FATF Recommendations require that key government agencies have:

- sufficient operational independence and autonomy to ensure freedom from undue political influence and interference;
- adequate resources effectively performing their functions; and
- staff have appropriate skills, receive adequate training, and maintain high professional standards.

66 These measures facilitate a culture of honesty, integrity and professionalism, which makes it more difficult for corruption to thrive.

[1] *People and Corruption: Asia Pacific*, (2017), Transparency International, Retrieved from: https://www.transparency.org/whatwedo/publication/people_and_corruption_asia_pacific_global_corruption_barometer
[2] https://www.transparency.org/news/feature/asia_pacific_fighting_corruption_is_side_lined
[3] http://www.fatf-gafi.org/media/fatf/documents/reports/Corruption%20Reference%20Guide%20and%20Information%20Note%202012.pdf

67 *Protecting Private Sector Institutions from Abuse* - the FATF Recommendations require that;

- persons with significant controlling interest or management function in financial institutions, such as banks, must be vetted using "fit and proper" criteria, which helps to prevent corrupt persons from gaining control over private sector institutions;
- financial institutions must screen employees to ensure high standards, which helps to prevent corrupt persons from infiltrating or otherwise criminally abusing these institutions;
- financial institutions must implement internal controls and audit functions to ensure compliance with AML/CFT measures, which facilitates detection of abuse by corrupt persons; and
- financial institutions must be subject to adequate supervision and monitoring for AML/CFT compliance, which facilitates the detections of corruption activities.

68 *Increasing Transparency of the Financial System* - the FATF Recommendations require that;

- when establishing business relationships or conducting transactions on behalf of customers, financial institutions must verify the identity of the customer, any natural person on whose behalf a customer is acting, and any individuals who ultimately own or control customers that are legal persons (such as companies) or legal arrangements (such as trusts). These measures increase financial transparency by making it difficult for corrupt persons to conduct business anonymously;
- financial institutions must put in place risk management systems to determine whether a customer or the beneficial owner is a politically exposed person (PEP) or a family member or close associate of a PEP, which facilitates detection of where public officials are abusing their position for private grain;
- financial institutions must have timely access to adequate and accurate information, which identifies the individual(s) who own or control legal persons and legal arrangements this increases ownership transparency making it more difficult for public officials to hide the proceeds of corruption within these legal structures; and
- wire transfers must be accompanied by accurate and all required information that identifies the person who sent the transaction and to whom the transaction is being sent. This facilitates transparency and tracing of the movement of corruption proceeds.

69 *Facilitating the detection, investigation and prosecution of corruption and money laundering, and the recovery of stolen assets* - the FATF Recommendations require that:

- financial institutions are required to examine the background and purpose of all complex, unusually large transactions, which have no apparent economic or lawful purpose with scrutiny given to high risk customers, jurisdictions, business relationships and transactions. This facilitates the detection of suspicious activity, such as corruption, which must be reported to the authorities for further analysis and investigation;
- jurisdictions must establish a FIU, with adequate resources and powers, to receive and analyse suspicious transaction reports and other relevant information, and disseminate their analysis to law enforcement for further investigation;
- laundering of proceeds from a sufficiently broad range of corruption and bribery offences, by natural and legal persons must be criminalised;
- authorities must have sufficient powers to; (i) access financial records and obtain evidence for the purpose of ensuring proper investigation and prosecution of money laundering offences and underlying corruption related predicate offences, and (ii) trace, freeze and confiscate corruption related property. This facilitates the protection and compensation of the victims of corruption and bribery, and the recovery of stolen assets; and
- countries must have laws and mechanisms which enable them to provide a wide range of mutual legal assistance, execute extradition requests and otherwise facilitate international cooperation, which facilitate combating cross-border corruption.

70 In combination FATF's, APG's and other FSRB's efforts to combat corruption through implementation of the FATF standards, other regional initiatives to address corruption include The Anti-Corruption and Transparency Experts' Working Group which is linked to Asia-Pacific Economic

Cooperation (APEC). This initiative aims to implement the UNCAC and establish a cross-border network consisting of anti-corruption and law enforcement officers. The working group encourages collaboration with other multi-lateral organisations such as the World Bank and Transparency International, and delivers anti-corruption projects and workshops. Another initiative is the Asian Development Bank (ADB) and the OECD Anti-Corruption Initiative which consists of 31 governments in the Asia-Pacific Region committing to the fight against corruption.

71 The use of FATF standards and other mechanisms to combat corruption is outlined in the following typologies case studies.

4.3 Laundering the proceeds of corruption - cases studies of methods and trends

Use of third parties

72 Corrupt officials often use close relatives and associates to launder illicit funds and conceal ownership of funds and assets. Relatives and associates may launder illicit funds by undertaking transactions and purchasing assets on behalf of the corrupt official. Their names are often recorded on properties, trusts and accounts controlled by the corrupt official in order to distance themselves from illicit funds and avoid detection from authorities.[4] Both the FATF standards and UNCAC recognises the risk of family members and close associates to a person entrusted with prominent public functions.

73 The following case studies illustrate the use of third parties to launder proceeds of corruption.

Example 1 - Case originally provided by China for 2016 APG Yearly Typologies Report

74 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).

75 *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.

Example 2 - Case originally provided by Chinese Taipei for 2013 APG Yearly Typologies Report

76 Mr A was the owner of Company W. Mr B was the nominal owner of Company X which was controlled by Mr A. Mr C, a friend of Mr A's, was the owner of Company Y. Mr D was the division chief of the information management division of state owned Hospital Z. Mr E was a computer engineer under the direction of Mr D.

77 Mr D and Mr E were responsible for the procurement of Hospital Z's medical computerized system and maintenance contract from 2007 to 2010. Mr D demanded Mr A, who intended to win the bidding, to pay bribes for giving favour in the procurements, and abetted Mr E to set up some unnecessary qualification requirements to drive out other potential competitors.

[4] *Politically exposed persons, corruption and foreign bribery*, (2015), AUSTRAC for the Commonwealth of Australia, Retrieved from: http://www.austrac.gov.au/sites/default/files/sa-brief-peps.pdf

78 Mr A used Company A as a tender, and borrowed the names of Mr B's Company X and Mr C's Company Y to participate in the bidding. In this way, Company A usually won the bids. After winning the bids each time, Mr A would pay Mr D by cash or remit the bribe to the designated bank accounts of Mr F (one of Mr A's friends) or Company G and then withdrew cash or issued bearer cheques to Mr D.

79 During the abovementioned period, Mr D accepted bribes worth more than NTD 6 million (about USD200,000) in total. This anti-corruption case was successfully investigated by the Taipei Field Division of the Investigation Bureau and the abovementioned suspects were charged with violation of Government Procurement Act, bribery, corruption and money laundering by prosecutor of the Shi-Lin District Prosecutors Office in September 2011.

Use of professional facilitators

80 Corrupt officials often use professional facilitators such as lawyers, accountants, real estate agents and service providers to launder illicit funds. Professional facilitators provide specialist knowledge and advice to establish corporate structures and trusts, buy and sell real estate and manage a client's finances. This enables the corrupt officials to distannce themselves from illicit funds, evade tax, legitimise funds and evade detection by authorities. The professional facilitator may be an unwitting participant in the lawful activity or may be reckless to the suspicion of illegal activity. In some cases professional facilitators may derive financial benefit for providing knowledge and assistance.[5]

81 The following case studies illustrate the use of professional facilitators to launder proceeds of corruption.

Example 1 - Case provided by Hong Kong, China

82 In 2009, the executive director of a publicly listed company in Hong Kong conspired with the owner of a trustee company and the latter's financial consultant, who later became the listed company's vice-president ("the trio") to deceive the Stock Exchange of Hong Kong Limited ("SEHK") and the shareholders of the listed company. This deception included the acquisition of New Zealand dairy farms by providing false declarations that the ultimate beneficial owner of the trustee company was an independent third party to the listed company, failing to declare that the executive director had an interest in the acquisition, and that the executive director and the owner of trustee company had agreed to share the commission arising from the sale and purchase of the said New Zealand dairy farms.

83 False financial information of the New Zealand farm assets was also provided to the SEHK. The listed company made an announcement giving details of its plan to purchase the New Zealand farm assets but concealed the fact that the farm assets were suffering a substantial loss. The acquisition was approved by the shareholders of the listed company. HK$842 million was raised by the listed company through the issue of convertible notes. Part of the fund was paid to the trustee company in New Zealand which remitted back HK$73.7 million to a company owned by the executive director in Hong Kong. HK$68.95 million was then routed through the account of a solicitor's firm in Hong Kong to the wife of the executive director.

84 Following ICAC investigation, the wife of the executive director and the solicitor were convicted of ML in September 2014, and were sentenced to 78 and 72 months of imprisonment respectively. Following an appeal, the Court of Appeal ordered a retrial against them. In April 2016, the trio was convicted of conspiracy to defraud. In addition, the executive director was convicted of

[5] *Money laundering through legal practitioners*, (2015), AUSTRAC for the Commonwealth of Australia, Retrieved from: http://www.austrac.gov.au/sites/default/files/sa-brief-legal-practitioners.pdf

ML. They were sentenced to imprisonment ranging from 60 to 99 months. The trio have lodged appeals against their conviction.

Example 2 - Case originally provided by Indonesia for 2012 APG Yearly Typologies Report

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

Use of corporate vehicles and trusts

86 The Panama Papers and international case studies have highlighted the use of corporate vehicles to disguise illicit funds obtained by corrupt officials. Trusts, shell companies and corporate structures established either onshore or offshore are often held in the names of friends or relatives of the corrupt official. Some offshore jurisdictions lack sufficient AML/CTF regimes and can provide secrecy surrounding corporate structures and beneficial ownership, making it difficult for authorities to trace illicit funds and to determine the ownership and control of the companies.[6] The FATF recommendations surrounding beneficial ownership aim to put regulations in place to enhance detection and prevent the misuse of offshore companies.

87 The following case studies illustrate the use of corporate vehicles and trusts to launder proceeds of corruption.

Example - Case provided by Singapore

88 Singapore: On 28 May 2013, the Corrupt Practices Investigation Bureau (CPIB) received information that a foreign national, Person A, was laundering bribery proceeds on behalf of a foreign politically exposed person (PEP) and that the criminal proceeds of foreign origin were deposited into Singapore bank accounts. Person A was known to have absconded and an international warrant of arrest was issued against him.

89 Based on financial intelligence received, Person A was a beneficial owner of four offshore companies which maintained bank accounts in Singapore. The offshore companies were administered and managed by a Singapore corporate secretariat firm, which also offered "nominee" director and shareholder services to Person A.

90 The corporate secretariat firm was found to have assisted Person A to transfer significant funds of suspicious origins between the Singapore bank accounts of the offshore companies that were beneficially owned by Person A, as well as out of Singapore.

91 CPIB immediately initiated a domestic investigation and seized the funds in the Singapore accounts that were traced to be beneficially owned by Person A. A total of US$79million was seized pursuant to the exercise of domestic investigative powers.

92 Investigations by CPIB revealed that the corporate secretariat firm had moved funds on Person A's instructions, and had performed necessary due diligence and even questioned Person A when the transactions were found to be suspicious. However, as Person A was a successful fund manager by vocation, he was able to convincingly explain the source of the significant fund transfers

[6] *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers*, (2006), FATF, Retrieved from: http://www.fatf-gafi.org/media/fatf/documents/reports/Misuse%20of%20Corporate%20Vehicles%20including%20Trusts%20and%20Company%20Services%20Providers.pdf; *Behind the Corporate Veil, using corporate entities for illicit purposes*, (2001), OECD Publications, Retrieved from: https://www.oecd.org/corporate/ca/43703185.pdf

into Singapore (mostly originating from his personal accounts in foreign countries) as his investment proceeds and that the fund transfers between his offshore companies were settlement of inter-company loans. It was only later when Person A was featured in open sources as a subject of a foreign investigation, that the corporate secretariat firm filed a suspicious transaction report on Person A with Singapore's Financial Intelligence Unit.

93 In order to pursue the domestic money laundering investigation, CPIB proactively engaged the foreign authority overseeing the foreign predicate bribery investigation. From the foreign evidences obtained, only a small portion of the funds received in Singapore could be directly traced to the foreign predicate offences. According to the foreign authority, Person A had allegedly used a complex web of legal entities across multiple jurisdictions to launder the criminal proceeds, the global fund tracing effort was frustrated as certain foreign jurisdictions were either uncooperative or did not have complete bank information.

94 In 2015, the foreign authority secured a Court Order for preventive seizure of Person A's assets in Singapore. In late 2016, Singapore received a formal request to enforce the foreign Court Order to restrain the funds in the bank accounts that were beneficially owned by Person A. The request was acceded to and the bank accounts were restrained in April 2017 pursuant to the formal request.

Use of international funds transfers

95 Criminal groups and corrupt officials often use international funds transfers as a way of moving illicit funds offshore to foreign jurisdictions that do not have sufficient AML/CTF laws and provide a veil of secrecy around bank accounts and transactions.[7] Illicit funds are commonly transferred overseas in small amounts to avoid detection and transaction threshold reporting requirements. This method is referred to as structuring. Another trend in international funds transfers is cuckoo smurfing. This involves transferring illicit funds through the bank accounts of innocent third parties. Money remitters are often used to transfer legitimate funds as a cheaper alternative to using mainstream banks. The money remitter gives details of the transaction and the intended recipient to a criminal syndicate who then transfers illicit funds to the innocent third party. The money remitter then pays the legitimate funds to the criminal, successfully laundering the money.[8]

96 The following case studies illustrate the use of international funds transfers to launder proceeds of corruption.

Example 1 - Case provided by Macao, China

97 Mr. A was the chairman of a multi-national corporation (MNC) with its headquarters in Country P and subsidiaries in Country Q. The group concentrates on the manufacturing and trading of electrical appliances. Bank L is a multi-national financial institution with their headquarters in Country P and branches worldwide. In addition, Bank L is also the principal banker of MNC group.

98 In June 2016, MNC deposited cash into their bank account opened within the headquarters of Bank L. The purpose of the transaction was to use it as collateral for a subsidiary of MNC to apply a bank loan with a branch in Country Q. The application was acknowledged by the headquarters of Bank L, and a guarantee was issued by the headquarters of Bank L to its branch in Country Q in regard to the application of the bank loan. As such, a term loan was granted to MNC by the branch of Bank L in Country Q.

[7] *Money laundering in Australia 2011*, (2011), AUSTRAC for Commonwealth of Australia, Retrieved from: http://www.austrac.gov.au/sites/default/files/documents/money_laundering_in_australia_2011.pdf
[8] *Money laundering methodologies*, (2014), AUSTRAC for Commonwealth of Australia, Retrieved from: http://www.austrac.gov.au/typologies-2008-methodologies

99 Once the loan was granted to MNC group, the funds were immediately remitted to Company R with a registered office in a tax haven, claiming the purpose of transaction as repayment to suppliers, which was also in line with the purpose of loan application. However, MNC never repaid the loan when it was due and the headquarters of Bank L confiscated the amount deposited in Country P to offset the outstanding loan amount. The branch of Bank L found out that the subsidiary of MNC never intended to repay the loan, and filed an STR with the local FIU in Country Q based on this unusual aspect.

100 The local FIU performed the background check on Mr. A and MNC through local intelligence and international cooperation, and revealed that Mr. A was being investigated by the LEAs in Country P. The information showed that the major raw materials supplier of MNC wanted to extend their exclusive supplier contract with MNC for another 10 years. As such, the supplier secretly paid the kickbacks to Mr. A in return for his favourable influence in the negotiation process. In order to move the funds overseas without alerting the relevant authority, Mr. A used the funds as collateral to apply for a bank loan from an overseas branch. Even though the collateral was confiscated due to Mr. A's failure to repay the bank loan in Country Q, the funds have been successfully laundered and moved from Country P to Country Q. Mr. A has been discharged from the position of Chairman and was under investigation by the LEAs in both Country P and Country Q.

Example 2 - Case originally provided by Pakistan for 2012 APG Yearly Typologies Report

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

102 Stage 1: Mr A embezzled funds of Ms ABC Associates and sent them abroad to his family members and friends;

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

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

105 The overall pattern of activities suggests layering and integration of corruption money. The case was disseminated to LEAs.

Bribery through services payments

106 Foreign bribery payments can be concealed by trade in services payments to give the appearance of paying a legitimate company for services rendered. Companies linked to, or controlled by corrupt officials are often hired for services such as 'consulting' and paid through fraudulent invoices for non-existent services. A legitimate third party service company can also act as an intermediary for the bribe payments by inflating invoices for services rendered and then channelling the difference to accounts controlled by corrupt officials.

107 Another method of concealing bribery payments is to set up a false supplier for the purpose of issuing fraudulent invoices to receive payments. The payment is then refunded in cash which can be used to make the bribe. [9]

108 The following case studies illustrate the use of fictitious service payments to facilitate bribe payments.

Example 1 - Case provided by Malaysia

109 Mr A, as Secretary of the finance division in a government ministry, is responsible for financial matters related to the ministry and its related agencies under the ministry, including executing payments for all approved expenditure.

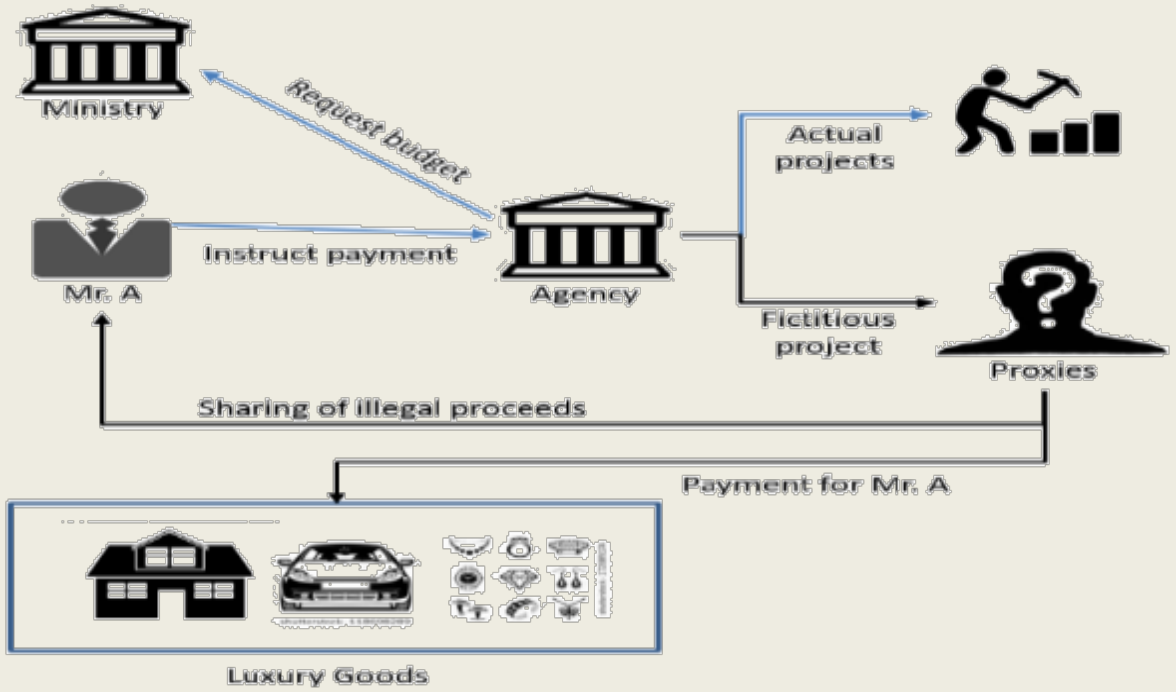
110 He took advantage of his position by instructing agencies to make payments to multiple vendors/companies for fictitious projects. The companies were set up by him and proxies were appointed as the company directors.

111 The proceeds, minus the commission to the proxies, were then transferred to his personal bank accounts and used to pay for cars, houses, jewellery and vacations.

112 Mr A received 32 corruption charges and 191 money laundering charges together with 3 other individuals.

113 The methods used in this case include:

- Laundering associated with corruption - using his position to instruct the payment;
- Use of nominees, trusts, family members or third parties etc; and
- Purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.).



[9] *How to Bribe, a typology of bribe-paying and how to stop it*, (2014), Transparency International UK, Retrieved from: https://www.transparency.org.uk/wp-content/plugins/download-attachments/includes/download.php%3Fid%3D1277&rct=j&frm=1&q=&esrc=s&sa=U&ved=0ahUKEwiUmOCd9uPTAhXCfbwKHQL9ALIQFggZMAE&usg=AFQjCNE3bP6rI4DCBSWk95orA8-Fi4cQrw

Example 2 - Case originally provided by the Philippines for 2016 APG Yearly Typologies Report

114 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).

115 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.

116 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.

117 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.

118 Financial investigations 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).

119 In relation to the funds received by person N from the scam, investigations 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.

120 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.

121 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.

Other case studies relating to corruption 2016-2017

FIJI

122 A former senior civil servant was charged in 2016 for engaging in a fraud amounting to over $4million. The Fiji FIU provided financial background assistance to the relevant law enforcement agency in relation to a request from the Fiji Independent Commission against Corruption (FICAC).

124 Viliame Katia, the ex-Acting Deputy Official Receiver for the Judicial Department was charged with 11 counts that included four counts each of forgery, three counts each of abuse of office, and a count each for embezzlement by servant, false information to public servant, unauthorised modification of data, and obtaining a financial advantage.

Count one – Abuse of office
125 It is alleged that between 1 July 2008 and 31 January 2010, at Suva, whilst being employed as Acting Deputy Official Receiver, Katia, in an abuse of authority, did an arbitrary act for the purpose of gain by causing payments amounting to $339,201.05 to be processed by the accounts section of the Official Receiver. The sum is alleged to have been drawn from the Official Receiver's bankruptcy account which was an act prejudicial to the rights of the creditors for whom the Official Receiver held the sum in trust and to the Government of Fiji.

Count two – Forgery
126 It is alleged that Katia colluded with an employee of the office of the Official Receiver in Lautoka and forged the signatures in order to facilitate the unlawful payment of monies from the official receiver's bankruptcy account to himself.

Count three – Forgery
127 It is alleged that emails were also sent from the same employee's account in Lautoka in order to state that purported creditors were willing to accept reduced payments from their bankrupt debtors in order to facilitate the unlawful payment of monies from the official receiver's bankruptcy account to himself.

Count four – Embezzlement by servant
128 It is alleged that Katia embezzled monies in the sum of $339,201.05 from the official receiver's bankruptcy account which had been entrusted to his office by virtue of his employment.

Count five – Abuse of office for gain
129 It is alleged that Katia, between 1 February 2010 and 31 July 2014, caused payments amounting to $2,472,161.18 to be processed by the accounts section of the office of the Official Receiver.

Count six – Abuse of office for gain
130 It is alleged that Katia between 1 July 2014 and 31 December 2015 caused payments amounting to $1,307,085.20 to be processed by the accounts section of the office of the Official Receiver. The sum is alleged to have been drawn from the Official Receiver's liquidation account.

Count seven – Forgery

131 It is alleged that between 1 February 2010 and 31 December 2015, Katia sent emails that were purported to have been sent by an employee of the office of the Official Receiver in Lautoka in order to dishonestly induce public officials employed within the office of the Official Receiver in Suva.

Count eight – False Information to public servant

132 It is alleged that Katia gave false information to the Acting Official Receiver which were the falsified emails and accompanying minutes written by him onto the printed emails knowing that it would cause approval of payments, which were made to the purported creditors which the Acting Official Receiver ought not to have done if the true state of facts were known to him.

Count nine – Unauthorised modification of data

133 It is alleged that Katia knowingly caused unauthorised modification of data held in a computer at the office of the Official Receiver in Suva which were editing of the official bankruptcy and liquidation records and addition of false debtor and creditor records into the FOX PRO System used by the official receiver.

Count 10 – Obtaining financial advantage

134 It is alleged that Katia obtained a financial advantage amounting to $3,779,246.38 from the office of the official receiver's bankruptcy and liquidation accounts knowing that he was not eligible to receive it.

Count 11 – Forgery

135 It is alleged that Katia on 14 January 2016 falsified a court order on winding up dated 28 May 1992, purported to have been made by the High Court of Fiji at Lautoka and proof of debt general forms, with the intention of dishonestly inducing public officials employed within the office of the official receiver in Suva, to accept them as genuine in order to influence the exercise of public duties and functions of the said public officials. A departure prohibition order had been imposed against him.

HONG KONG

136 A corruption investigation revealed that in April 2012, the former Chief Executive Officer (D1) of a Hong Kong company was entrusted to lease a building for refurbishing it into a hotel with around 50 serviced apartments.

137 D1 signed a lease agreement with the owner of a building. As stipulated in the lease agreement, the building could only be operated as a hotel or a guest house, including a restaurant inside the building.

138 In November 2012, D1 requested his associate (D2) to look for a caterer to operate a restaurant in the hotel. D1 and D2 conspired together to solicit HK$980,000 from a potential caterer for engaging the latter to operate and manage the restaurant. At a meeting on 16 April 2013, D1 and D2 received HK$250,000 cash as part of the bribe from the potential caterer.

139 D1 and D2 were convicted of corruption and ML offences and were sentenced to 30 months and 27 months imprisonment respectively.

INDONESIA

140 WI was a regent of district 'A' in Indonesia in the period from 20xx until 20xy. In 20xs, the local government planned the construction of a dock in district 'A' and in May, 20xs, the dock's construction site had been designated by WI and agreed to restitute the land at USD1,037 per acre. After approving the land value, WI purchased the land area of 8.400 m2 in the names of 'NMA' and 'IDA'. WI gained wealth by receiving compensation for the land bought at a specified location as the dock's building was valued at USD88,667. WI also received funds worth approximately USD3,165,518 and credit facilities in the form of money, worth USD1,480,370 exceeding the credit

limit, which is considered to be a bribe because it deals with the position of WI as Regent and contrary to WI's obligation or duty.

141 WI received this money gradually, either in cash or transfer into his private accounts and companies. WI sought to disguise or hide acquisition of land for the construction of the dock bought by WI, using another person's name. In addition, WI instructed his son to open a checking account and a deposit account on behalf of the company owned by his sons PT.BSA and PT.BPI and equipped with WI's signature aimed to withdraw money to include an authorised letter from the company's owner. He was charged with corruption, bribery and money laundering.

4.4 Open source materials on anti-corruption

AUSTRALIA

142 *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

143 *Money Laundering Through Legal Practitioners Brief*. This brief focusses on money laundering methods and vulnerabilities associated with money laundering through legal practitioners. This brief is available on AUSTRAC's website http://www.austrac.gov.au/publications.

FATF

144 The FATF has published publications focussing on corruption which are available from the FATF website http://www.fatf-gafi.org/publications/. Some useful publications are as follows:

- *The Misuse of Corporate Vehicles, Including Trust and Company Service Providers* - A FATF report which examines the various ways that corporate vehicles can be exploited for the purposes of money laundering and counter terrorist financing.
- *The FATF Reference Guide and Information Note on the Use of the FATF Recommendations to Support the Fight Against Corruption* – A FATF reference guide and information note to raise awareness of how the FATF Recommendations can help to combat corruption.
- *FATF Guidance: Politically Exposed Persons (Recommendations 12 and 22)* – This FATF report examines the risks associated with PEPs and how the FATF Recommendations can minimise and prevent these risks.
- *Best Practices Paper: The use of the FATF Recommendations to Combat Corruption* – This FATF Best Practises Paper raises awareness on the use of the FATF Recommendations to combat corruption.

APG

145 In 2016 APG has published the *Recovering the Proceeds of Corruption in the Pacific* – Joint Pacific Island Law Officers' Network (PILON) and APG project report co-led by Papua New Guinea and Vanuatu containing Pacific Island case studies and typologies focussing on corruption. This report is available from the APG website http://www.apgml.org/documents/.

Other FSRBs

146 Eastern and South African Anti Money Laundering Group (ESAAMLG) published the Report of the links between corruption and the implementation of anti-money laundering strategies and measures in the ESAAMLG region. This report is available from http://www.esaamlg.org/reports/typologies.php.

147 Groupe Inter-Gouvernemental d'Action Contre le Blanchiment de l'Argent en Afrique (GIABA) published a report on the nexus between corruption and money laundering in West Africa, which focuses on an analysis of risk and control measures. This report is available from http://www.giaba.org/reports/typologies/reports.html.

Asian Development Bank (ADB)

148 The Office of Anticorruption and Integrity (OAI) at the ADB manage ADB projects designed to fight fraud and corruption. Information and reports relating to these projects can be found on the ADB website https://www.adb.org/site/integrity/main

Organisation for Economic Co-operation and Development (OECD)

149 OECD has published publications focussing on corruption which are available from http://www.oecd.org/corruption/ Some useful publications are as follows:

- *Behind the Corporate Veil, Using corporate entities for illicit purposes* - This Report examines the misuse of a variety of "corporate vehicles", including corporations, trusts, foundations, and partnerships with limited liability features.
- *Does Technology Against Corruption Always Lead to Benefit? The Potential Risks and Challenges of the Blockchain Technology* - This paper examines how Blockchain technology could be used to curb corruption and the possible risk and challenges related to Blockchain technology.

Stolen Asset Recovery Initiative (StAR)

150 The Stolen Asset Recovery Initiative (StAR) by the World Bank and UNODC has published publications focussing on corruption which are available from http://star.worldbank.org/star/. Some recent publications are as follows:

- *Getting the Full Picture on Public Officials: A How-To Guide for Effective Financial Disclosure* - This guide features an unprecedented collection of data accompanied by an analysis of key implementation challenges to help countries develop more effective and robust financial disclosure systems.
- *Politically Exposed Persons: Preventive Measures for the Banking Sector* – This report combines policy recommendations and good practices aimed at making it harder for corrupt Politically Exposed Persons (PEPs) to launder their money, and make it easier to get stolen assets back.

Transparency International

151 Transparency International has published publications focussing on corruption which are available from www.transparency.org/ Some useful publications are as follows:

- *People and corruption: Asia Pacific – Global corruption barometer* – Extensive survey conducted by Transparency International across the Asia Pacific region on their perceptions and experiences of corruption.
- *How to Bribe: A Typology of Bribe Paying and How to Stop It* - This guide both identifies and categorises some of the different types of bribe, and the ways in which bribes are commonly demanded or paid.

Anti-Corruption Research Network

4 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/

5. CASE STUDIES OF ML AND TF

5.1 Terrorism Financing

INDONESIA

152 Mr. XY was convicted of terrorism offences for possessing illegal weapons and explosive materials and planning terror attacks. He had previously been arrested in relation to a conflict during local riots between an Indonesian ISIS Group and police. Based on information supplied on his bank account application, Mr. XY worked as a domestic entrepreneur in a clothing company. Intelligence revealed his wife had received money from a local religious foundation, which had been suspected of financing terrorism.

153 It was identified that Mr. XY had three local bank accounts namely as Bank A, Bank B and Bank C, which were suspected to be used as placement conduits to support terrorist groups in Indonesia. Total amount of incoming domestic funds in his accounts were up to ~USD81,147.

154 In terms of moving the funds, it was revealed that Mr. XY had conducted several transactions. Mr. XY frequently transferred funds to domestic bank accounts of several persons of interest including his wife. Mr. XY also sent funds to other persons of interest through money remittance services.

155 Mr. XY used to funds to purchase travel tickets and other products. In relation to international fund transfers, transfers were made to Philippine entities. Intelligence revealed that these funds were suspected to be used for purchasing illegal weapons in order to support terrorist operations in Indonesia.

156 INTRAC conducted intelligence analysis on financial database searches and liaised with local financial institutions in order to gather comprehensive information relating to the aforementioned transactions. The intelligence reports were disseminated to the required law enforcement agency.

157 Mr. XY was convicted under Article 15 vide 7 and 15 vide 9, Law of Republic of Indonesia Number 15 Year 2003 concerning the Combating of The Criminal Act of Terrorism and Article 4, Law of Republic of Indonesia Number 9 Year 2013 concerning The Prevention and Eradication of The Criminal Act of Terrorism Financing.

MALAYSIA

158 Two individuals were soliciting funds for the purpose of financing foreign terrorist fighters (FTF) who were travelling to Syria. The funds were solicited by using a blog and a Facebook account of the accused.

159 All funds were channelled into bank accounts of one of the accused before being transferred or given to FTFs and their family members for travelling expenses and stipends.

160 The methods used in this case included:

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

161 The individuals were charged and convicted of terrorism financing. Initially, the individuals were convicted and sentenced to 3 years imprisonment for soliciting funds and 2 years for disbursement of funds for a terrorist cause. On appeal of the sentence by the prosecutor, the sentence was increased to 15 years imprisonment for each of the charges.

NEW ZEALAND

162 In 2016 the NZ-FIU published a quarterly typology report focussing on terrorist financing. It is publicly available on the Police website: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents

SINGAPORE

163 In April 2016, the Commercial Affairs Department (CAD) received information on possible terrorism-related fund raising activities by several radicalised Bangladeshi nationals. The CAD immediately commenced a terrorism financing investigation.

164 Investigations revealed that these Bangladeshi nationals had formed a pro-ISIS group in Singapore called the Islamic State of Bangladesh ("ISB"). The ISB aimed to overthrow the Bangladeshi government through an armed struggle and establish an Islamic caliphate in Bangladesh with a view to eventually join ISIS. At the point of their arrest, the group managed to raise ~ USD 980 among themselves, to further their cause in Bangladesh.

165 On 27 May 2016, six ISB members were prosecuted for offences under the Terrorism (Suppression of Financing) Act (TSOFA). All six accused persons plead guilty and were convicted. Their sentences ranged from 24 to 60 months' imprisonment. This case was the first prosecution and conviction under the TSOFA in Singapore.

THAILAND

Case 1
166 Mr. A is a member of the terrorist or insurgency movement in the south. He collected funds from members of the movement staying in a neighbouring country and handed over the money to Mr. B who, in turn, gave it to Mr. C, another member, for use in launching attacks in Thailand.

Case 2
167 Mr. K was assigned the task of procuring vehicles for use in a bombing attack in Thailand. He purchased three vehicles from a used car dealer. The vehicles had been put up as security on loans from finance companies and were thus stolen cars. Mr. K drove the vehicles containing explosives to a department store.

Case 3
168 Mr. A and his associates had acquired a mobile phone and a motor bike. These items and money were given to Mr. B for use in launching the attack. The motor bike was fitted with explosives and detonated through the mobile phone.

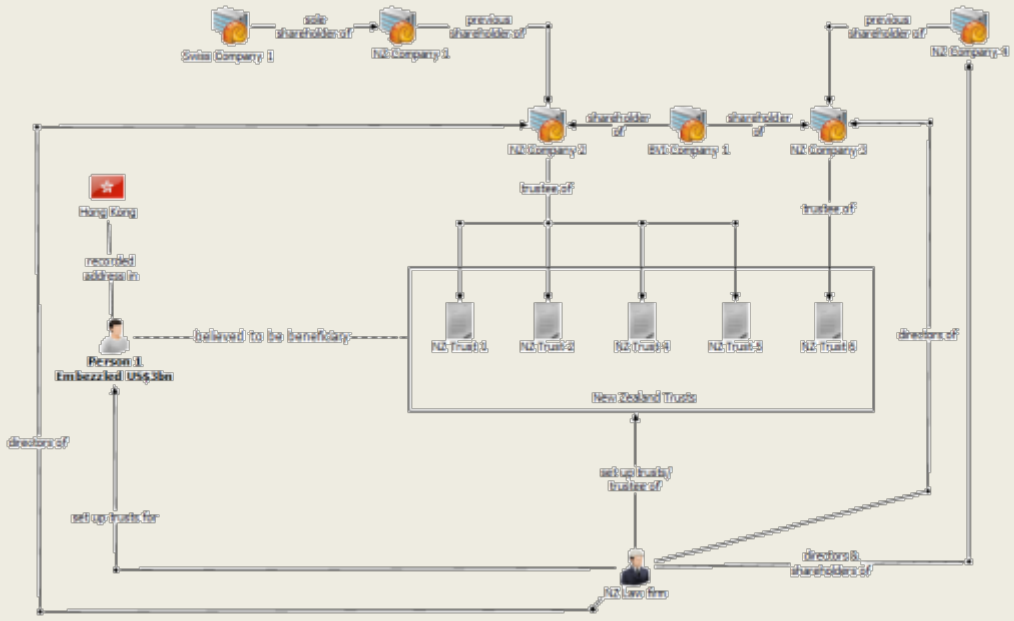
Case 4
169 Mr. A, a religious school executive, committed an offence related to aiding, abetting and providing financial aids to an insurgent group. He allowed the insurgency group to use his school as a place to promote violent ideology, provide training and to stockpile the arms.

Case 5
170 A school in Thailand had been used in support of insurgency activities and the propagation of ideas detrimental to security. It had also served as a training camp for operations.

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

NEW ZEALAND

171 Media reporting identified Person A had embezzled a large sum before purchasing high value assets with the proceeds. New Zealand trusts and companies were set up for Person A by a New Zealand based law firm specialising in setting up structures for offshore clients.



SAMOA

172 A trustee company filed an STR on Mr C, a former Director/Secretary of several offshore companies. Mr C was charged with offences relating to alleged embezzlement of significant amounts of money. He was convicted and sentenced to 1 year imprisonment, fined $1.5 million and suspended for 3 years from his post. Mr C was already sentenced before the trustee filed the STR for FIU information. Samoa FIU shared the information with other FIUs and relevant local authorities.

THAILAND

173 A human trafficking network conducted inward and outward transfers through commercial banks. Five bank accounts were opened under his name and also associates within the surrogacy company. Account types included savings, fixed, and foreign currency.

174 The network paid the salary for the manager in Thailand by transferring funds into a bank account located in Chinese Taipei. A cash payment was also provided for expenditure in Thailand.

175 Air fares for employees and doctor's fees relating to a pregnancy test were paid for by a credit card which was issued by the bank in Chinese Taipei.

176 Wages for surrogate women were transferred from overseas into employees' personal bank accounts and some were paid in cash to the company.

CHINESE TAIPEI

177 Mr. A is the director of N Company, registered in Samoa, which has no actual business activities. Mr. A opened an account for N Company with Offshore Banking Unit ("OBU") of Bank A in Chinese Taipei but provided it to an international fraud group through Mr. B. On 22 January 2015, the international fraud group pretended to be the executive director of U Company in Switzerland and

sent an email to Bank S in Switzerland requesting Bank S to conduct a remittance stated in an attached payment order. Bank S was deceived by the forged documents and transmitted ~ USD1,121,790 from U Company's account to N Company's account in Chinese Taipei.

178 In January 2015, Mr. B instructed Mr. A to transmit the partial funds in N Company's account to a specific account in Hong Kong, but Bank A refused to conduct the transaction since Bank A has received an overseas complaint letter indicated that the said funds were allegedly involved in a fraudulent scheme. In order to disguise the proceeds of crime, Mr. A transferred these funds to several personal and legal persons' foreign currency accounts controlled by Mr. A. Some funds were exchanged into $NTD and then transferred to NTD currency accounts. In February 2015, Mr. A instructed a friend of his to withdraw NT$3,000,000 in cash from one account.

179 Mr. A and Mr. B were indicted on the charge of violating the Criminal Code and the Money Laundering Control Act.

5.3 Use of virtual currencies

NEW ZEALAND

180 The following three cases studies were published in NZ-FIU quarterly typology report - Q1 2016-17 and are available online: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents

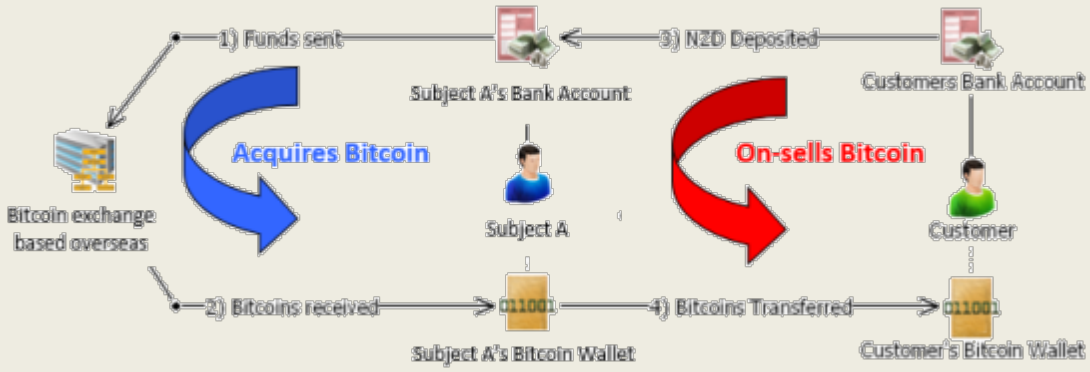
Case study 1

181 Bank monitoring detected that a New Zealand resident, Subject A, had been purchasing bitcoins in roughly NZD5,000 amounts six times during one month. Subject A also received numerous payments from third parties into their bank account indicating that Subject A was generating significant profits from selling bitcoins. However, no payments had been made to Inland Revenue.

182 The typology associated with these suspicious transactions has two phases. First, Subject A is acting as a "middleman", purchasing Bitcoin from an overseas marketplace. These bitcoins are then transferred to a Bitcoin wallet that is controlled by Subject A.

183 In the second phase, Subject A solicits and receives payments from customers into their bank account, and when these funds have cleared, Subject A transfers bitcoins from their own wallet to the customers' Bitcoin wallet (or wallets).

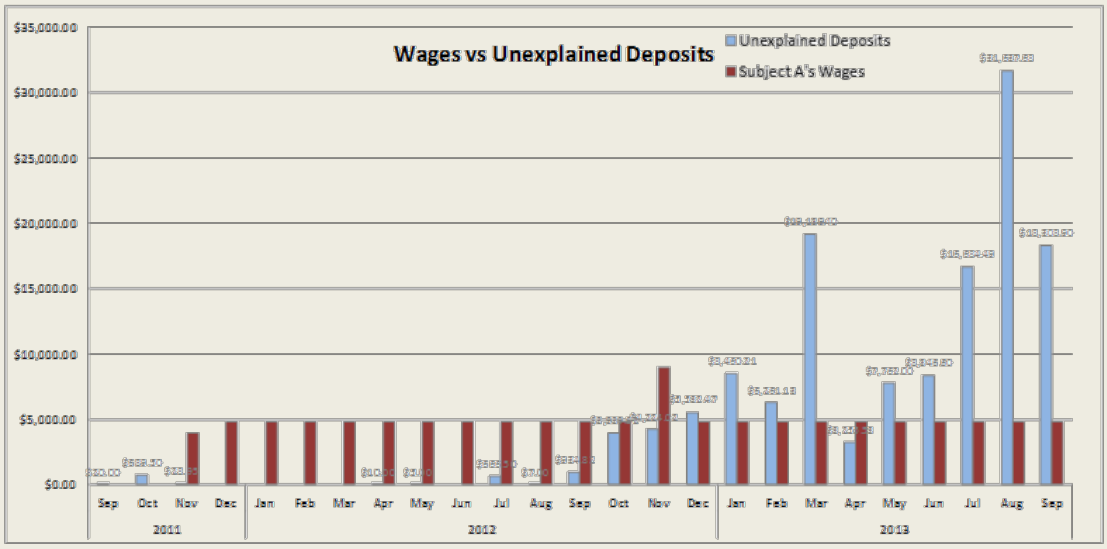
184 Central to Bitcoin's popularity with drug offending is that wallets are easily anonymised and hidden. However, by observing the NZD side, as shown in the top half of the below diagram, the New Zealand FIU was able to infer what Bitcoin transactions were taking place.



185 The financial analysis of Subject A's bank account records showed that since mid-2012 the account had received increasing amounts of ad hoc, unexplained deposits, throughout 2013. Subject A's income from their employer was dwarfed. A number of deposits contained reference numbers and noting's implying they were related to the purchase of bitcoins.

186 Further enquiry identified that a number of the people, depositing money to Subject A's bank account, had a drug dealing history and that the likely Bitcoin purchases were consistent with online drug purchases.

187 Enquiries also identified that victims of fraud or ransomware attacks were using Subject A to purchase bitcoins to pay to offenders.



188 While more Bitcoin dealers are coming to light, the total number operating in New Zealand is likely to be very small. This means there is a "choke-point" in terms of Bitcoin transactions, allowing for efficient monitoring and targeting of offenders.

189 The popularity of Bitcoin shows a growing trend towards high-value online offending, while much focus is rightly placed on drugs, other offending, from simple theft to Ponzi schemes is becoming more widely reported. The ability to observe Bitcoin purchases at point of sale will become a valuable investigative tool in the future.

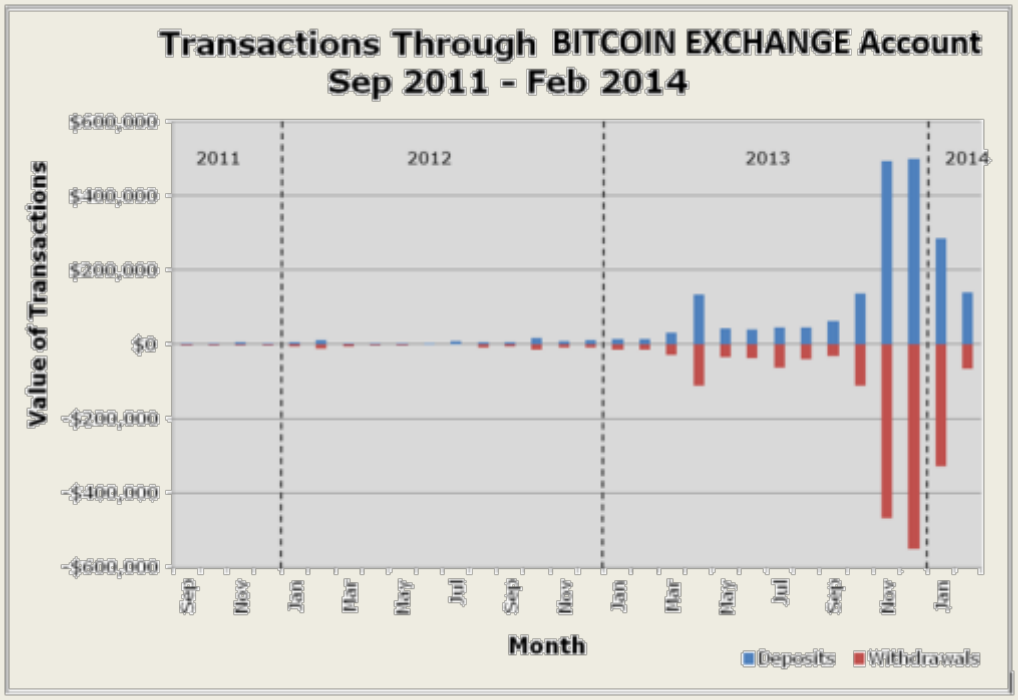
Case study 2

190 In 2014, New Zealand FIU identified an account associated with a Bitcoin exchange where bitcoins were traded for New Zealand dollars at the "point-of-purchase". Subject B has a history of hacking, and is currently under investigation for a "ransomware" computer program which locks down a computer and demands payment in Bitcoin.

191 Subject B was running a Bitcoin business through his personal accounts with one of New Zealand's largest banks. The subject had previously come to the bank's attention for involvement in phishing scams. The subject's transactional history clearly ascertained that a large number of cash deposits had gone through his account and then were paid to third parties which appeared to indicate the buying and selling of Bitcoin.

192 The cash deposits were made on three separate days and at different bank branches, they were placed into Subject B's account via bank cheques.

193 The transaction history of the account shows substantial growth in trades over the past year, peaking in December 2013. The pattern of transactions through the Bitcoin exchange account is graphed below. Incoming funds roughly mirror outgoing funds and rapidly increased in size, which is consistent with operating a Bitcoin exchange or as a conduit account to facilitate money laundering.



194 Analysis of the bank account identified 655 individual accounts transacting with the same Bitcoin exchange, as well as a large number of cash depositors. Of the 655 account holders, 13 per cent had some indication of involvement in illicit drug offending.

Case study 3

195 Bitcoin-enabled offenders tend to be young, opportunistic, and have little previous criminal history. These factors mean that such offenders may operate outside traditional criminal networks, and can offend for a significant amount of time, and at a high level, without detection.

196 In 2013, an investigation entitled Operation Racecourse was conducted by the Palmerston North Police in conjunction with the New Zealand Customs Service, originating from FIU analysis of four Bitcoin related STRs on a previously unknown 20-year old student – Subject C.

197 Operation Racecourse focussed on the drug dealing activities of Subject C who was believed to be involved in activities related to the importation and supply of Class A and B controlled drugs into New Zealand.

198 In April 2013, Operation Racecourse was terminated with the execution of Police search warrants and the arrest of the subject. Termination resulted in numerous charges for importation and distribution of cocaine, methamphetamine, ecstasy and LSD, as well as around NZD130,000 assets seized.

199 Subject C had been using other people's addresses, to which he had sent packages of drugs he had purchased from the Silk Road website. He also used other "dead" addresses where he had packages delivered to. The dead addresses were locations known to Subject C as being unoccupied at specified times, due to their occupants being either on holiday or at work. He would wait on the front porch at the "dead" address for drug courier packages to be delivered there.

200 Drug purchases were made by Subject C's bitcoin account on Silk Road. The subject also claimed he had another Bitcoin account with Japanese Bitcoin exchange MtGox, which he credited using USD and NZD currency from three of his numerous bank accounts he held in New Zealand.

201 Subject C had a number of accounts held at various New Zealand banks. None of these accounts showed legitimate income aside from student allowance payments and a small amount of seasonal wages. However, all accounts received significant cash deposits and electronic movement of funds between his bank accounts and/or to MtGox.

202 Subject C, whenever challenged by banks regarding the source of the cash deposits he was making, stated that he was engaged in the business of buying and selling computers for fellow students. There was no evidence of the trade of computers found on Subject C's TradeMe account, nor there were other business transactions that could explain the amount of income he had earned over the analysed period. The subject's TradeMe history did detail the purchase of a set of electronic scales, described as "digital 0.01g x 300g." The purchase date of the scales was consistent with Subject C's explanation to Police that his first purchase of controlled drugs was made in that same month.

203 The FIU received several suspicious transaction reports from New Zealand banks about irregularities in his financial activity, and they have contributed to Operation Racecourse.

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

FIJI

204 The Fijian FIU received an STR from a commercial bank relating to two individuals, Person K and Person L. Person K is an American national reported as one of the directors of Company J. Person K is reportedly a student. Person K arrived in Fiji on 1 February and departed Fiji on 5 February. Person L is an American national reported as one of the directors of Company J. Person L is reportedly retired. Person L arrived in Fiji at the same time as person K.

205 The Fijian FIU conducted checks and established that Company J was incorporated and is registered in the Republic of Seychelles. There was a mention of another entity, Company R which is reportedly based in Switzerland. Both Person K and Person L mentioned that they are expecting a transfer of 29 million EUROs from Company R to Company J's bank account in Fiji. Person K and Person L engaged a local accounting firm in Fiji to assist with the opening of the bank account of Company J with a local commercial bank in Fiji.

206 The local accounting firm requested that bank officers meet with Person K and Person L at the office to open a foreign currency euro bank account. The local bank was informed of the 29

million euros transfer from Company R. On 11 February, the local bank closed the bank account due to insufficient documentation provided to open the account.

207 On 19 February, Person K engaged another local bank through email to open a EURO account. The Fiji FIU issued a case report to the FINCEN FIU for possible attempted layering activities by the individuals and associated entities.

208 The possible offences in this case include money laundering and fraud.

209 The indicators that relate to this case include (1) Use of an accountant as a gatekeeper to facilitate alleged layering of funds and (2) Occupation of investors is dubious.

HONG KONG, CHINA

210 In 2009, the executive director of a publicly listed company in Hong Kong conspired with the owner of a trustee company and the latter's financial consultant, who later became the listed company's vice-president ("the trio") to deceive the Stock Exchange of Hong Kong Limited ("SEHK") and the shareholders of the listed company. This deception included the acquisition of New Zealand dairy farms by providing false declarations that the ultimate beneficial owner of the trustee company was an independent third party to the listed company, failing to declare that the executive director had an interest in the acquisition, and that the executive director and the owner of trustee company had agreed to share the commission arising from the sale & purchase of the said New Zealand dairy farms.

211 False financial information of the New Zealand farm assets was also provided to the SEHK. The listed company made an announcement giving details of its plan to purchase the New Zealand farm assets but concealed the fact that the farm assets were suffering a substantial loss. The acquisition was approved by the shareholders of the listed company. ~ USD107 million was raised by the listed company through the issue of convertible notes. Part of the fund was paid to the trustee company in New Zealand which remitted back ~ USD 9.37 million to a company owned by the executive director in Hong Kong. ~ USD 8.84 million was then routed through the account of a solicitor's firm in Hong Kong to the wife of the executive director.

212 Following ICAC investigation, the wife of the executive director and the solicitor were convicted of ML in September 2014, and were sentenced to 78 and 72 months of imprisonment respectively. Following an appeal, the Court of Appeal ordered a retrial against them. In April 2016, the trio was convicted of conspiracy to defraud. In addition, the executive director was convicted of ML. They were sentenced to imprisonment ranging from 60 to 99 months. The trio have lodged appeals against their conviction.

INDONESIA

213 A person known as AK, along with a notary, offered to sell land with an area of 4.165 m^2 to a property company known as PT.PP in district "Y" by using a Certificate of Property Rights, stating proprietorship of AK. PT.PP purchased the land for an amount of ~USD 4,118,700; however, the purchase remained unresolved. The legal counsel for PT.PP enquired with the National Land Office in district "Y" and was advised that AK was not the true owner of the land. The funds for purchase were paid into the personal accounts of AK and AK's relatives. AK was found to have committed a fraud as well dealing with the proceeds of crime. In such cases as the notary, is also subject to criminal fraud and money laundering charges.

CHINESE TAIPEI

214 In March 2014, the AMLD received an STR from Bank T indicating that Y Company opened an account in February 2014. After receiving transmittances, the accountant or staff from Y Company withdrew cash from this newly opened account and then separated the cash in to several envelopes.

There were over NT$10million of funds transferred into the abovementioned account and almost all of them were withdrawn in cash.

215 Bank T considered the transactions conducted by Y Company's employees in the company account to be suspicious and therefore filed the STR to the AMLD. After the preliminary investigation by the AMLD, it was revealed that Y Company was suspected to be involved in a Ponzi scheme. From June 2016, Mr. O et al. established several companies, including Y Company, and recruited investors by online advertisements, brochures, and seminars. After signing investment contracts with Y Company, the investors could transfer the investment funds to Y Company's account. Each unit of the investment was NT$500,000 and the duration of the investment was three months.

216 The investors could retrieve the original capital and 15% interest when the contract expired. In order to postpone the time of distribution of the capital and interest, Mr. O signed different types of contracts to make investors increase the amount of investment and extend the duration of investment. The more capital investors put in and/or the longer the investment duration chosen, the higher the interest the investors could get, up to 120% per year. Since June 2013, Mr. O et al. has recruited over 4,000 investors and the amount of investment has reached to NT$2.3 billion.

217 In addition to postponing the pay out of the capital and interest, Mr. O et al. further tried to reduce the amount of the interest that investors could retrieve. They claimed that Y Company intended to invest Exchange Trade Funds, Futures, and Foreign Exchange to canvass investors to transfer their investments into this project. Investors could retrieve the original capital and investment profits after 3 months. Even though the investment resulted in a loss, the origin capital was still returned to the investors. However, Mr. O et al. did not conduct the investment but forged performance reports with gaining profits to deceive investors in order to convince investors to contribute further funds into the project or attract more investors. From March 2014, the proceeds of crime obtained by Mr. O amounted to over NT$700 million. Approximately NT$30 million of the proceeds of crime was confiscated by the prosecutor during the investigation. The MJIB initiated a criminal investigation and then referred this case to the Chinese Taipei District Prosecutors Office in November 2016 for prosecution.

5.5 Trade based money laundering and transfer pricing

FIJI

Case Study 1

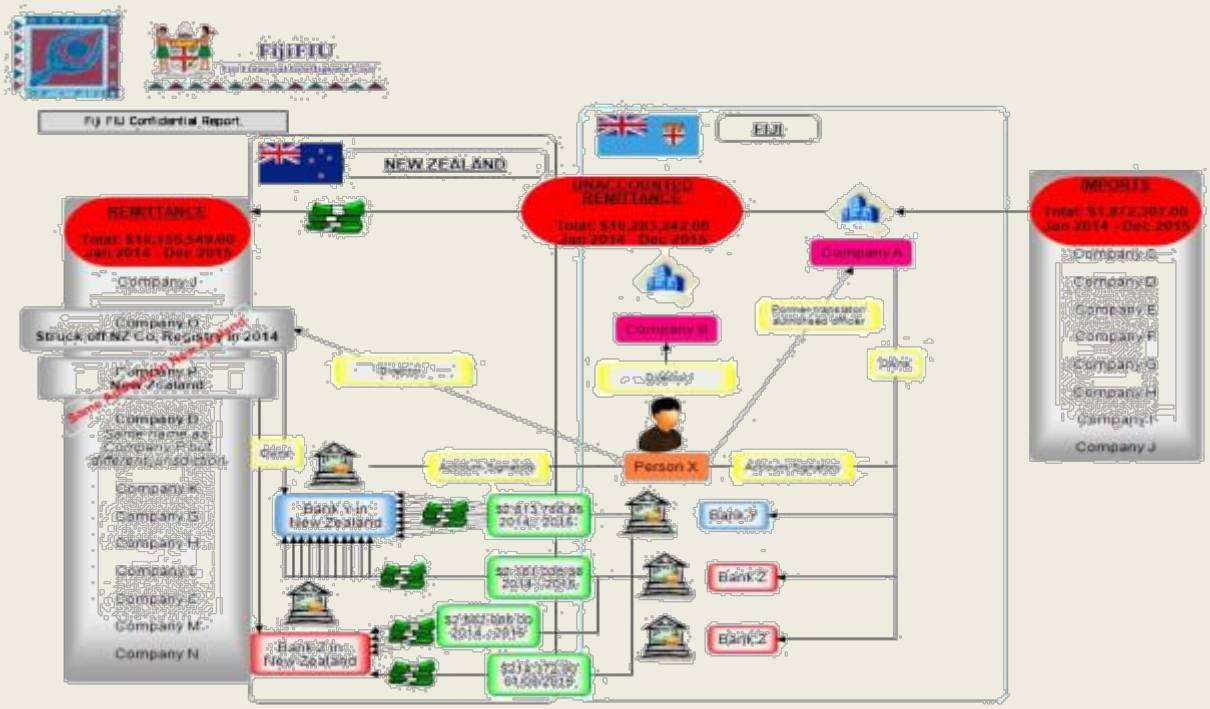
218 The Fijian FIU received a STR linked to an alleged trade based money laundering racket involving a 34 year old Chinese national, Person Q and 3 entities.

219 The Fijian FIU conducted financial checks and established that from January 2014 to December 2015, a local based entity, Company Z, remitted approximately ~ USD3.3 million to Company A which was registered in New Zealand and Company V which is reportedly registered in China but supposedly conducting business operations from the same address as Company A in New Zealand. Further enquiries revealed that Company A was reportedly struck off the New Zealand Company Registry in July 2014. Person Q was previously brought to the attention of the Fiji FIU in 2015 in relation to illegal cash smuggling and alleged money laundering. The Fiji FIU also established that Person Q has adverse travel records in New Zealand.

220 The Fijian FIU conducted checks with the Customs agency and established that there were no records of imports recorded from Company A to Company Z. There was approximately ~ USD1.93 million remitted from the bank account of Company Z to Company A. It is unusual for such a significant exchange of funds between two companies without any apparent trade relationships established. The FIU did establish that Person Q was the director of Company A in 2009.

221 A report was disseminated to the customs authority to investigate for alleged trade based money laundering. The possible offences included trade-based money laundering; Customs related offences and Tax Evasion.

222 The key indicators in the case included (1) Significant exchange of funds between local and overseas based entities without any apparent established trade relationships; and (2) remitting funds offshore to a company which was struck-off the Company Registry and was possibly operating illegally.



Case Study 2

223 The Fijian FIU received a STR from a member of the public in March on Company A.

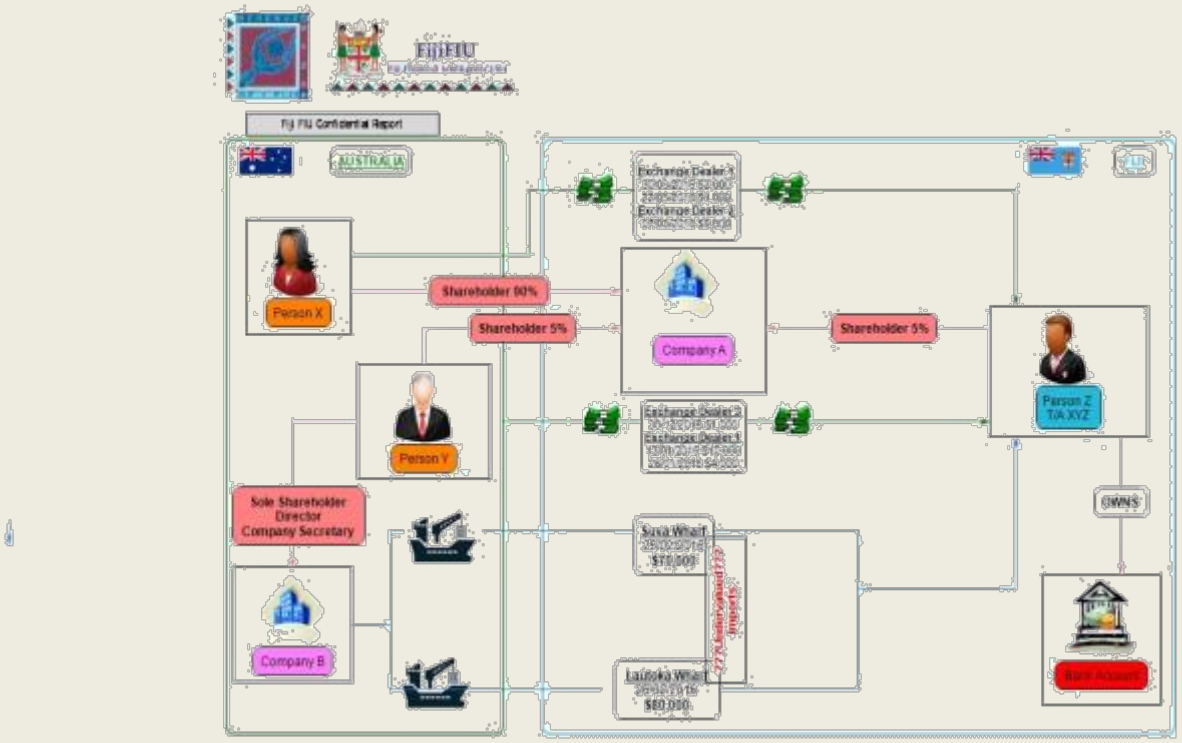
224 Person X & Y (foreigners) were reportedly using Person Z to set up a "construction company", Company A in Fiji. The name of the company Person Z was trading as (XYZ) was similar to Company A. The Fijian FIU conducted financial checks and established that Person X & Y were sending funds via three separate FX dealers to Person Z between Dec 2015 and March 2016 from Australia.

225 The Fijian FIU conducted checks with FRCA Customs and established that two excavators were sent from "Company B" in Australia to Person Z (T/A Company XYZ) in Fiji. The Fiji Revenue & Customs Authority (FRCA) Customs officials interviewed Person Z and established that there may have been possible undervaluation of invoices for the excavators. Moreover, the Fijian FIU established that the excavators were intended to be used for Company A's operations.

226 The Fijian FIU established that Company A was not yet registered with Investment Fiji & Registrar of Companies. It was only registered after the excavators came into the country and funds were exchanged between the parties.

227 The suspicion that authorities had was that the business transactions were conducted between the foreigners and Person Z without proper business registration. The possible offences were trade based money laundering and customs related offences.

228 The key indicators in the case included; (i) use of Person Z as a mule to facilitate alleged trade based ML, (ii) engaging in alleged tax/VAT evasion by Person Z and Company XYZ as funds sent from Australia to Person Z via FX Dealers could be business funds, which were not remitted to the bank account of Person Z, and (iii) possible manipulation of invoices by understating the value of the machinery.



THAILAND

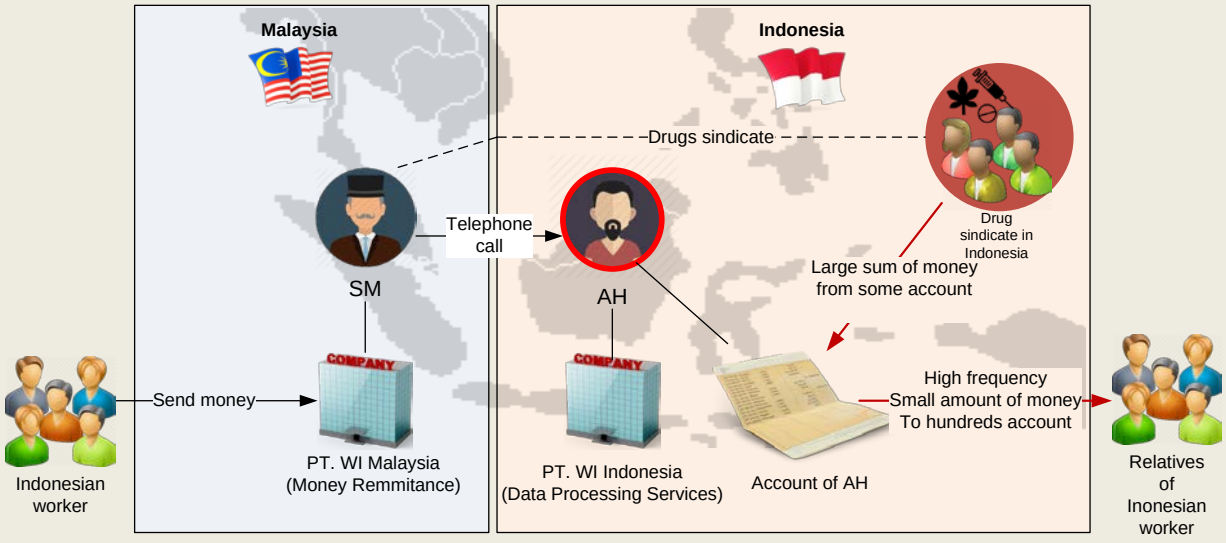
229 The Thai authorities examined false VAT refunds for more than 30 scrap export companies. The investigation found that 18 civil servants of the Revenue Department were involved in the case, including high-level civil servants involving ~ USD120 million. The investigation found that the offenders gathered copies of identification cards of poor people and used them to register the company with the Social Security Office with payment of ~ USD6.00 to ~14.00 to each of the poor people. Moreover, the offenders hired a workplace pretending to be a juristic company. The investigation of the workplace found an empty room, no employees or equipment. In addition, there are documents showing the cost of metal which the company will buy for ~ USD14.00 per kilogram which is higher than market price. The offence committed related to false claiming of payment for VAT refunds after export.

5.6 Underground banking/alternative remittance services/hawala

INDONESIA

230 Indonesian workers located in foreign jurisdiction X sent funds to relatives in Indonesia through a money remittance company known as PT.WI, which was owned by SM. However, these funds were not sent directly by the company in Indonesia. The owner of the company, SM, requested AH (located in Indonesia), via telephone to open an account to be used as the sender's account for the relatives of Indonesian workers. However, the funds were not transferred from the company's account in jurisdiction X, but instead came from a criminal syndicate in Indonesia. The funds were then transferred to the families or relatives of Indonesian workers in accordance with the instructions by SM to AH. This method caused mutations on AH accounts consisting of credit transactions of some parties, some of which were very large, while the debit transactions performed for a lot of parties was a smaller nominal amount. Such transactions are known as "Hawala Banking".

231 Based on mutation of AH's accounts, AH is known to have received funds from several parties, among others are AZ, NAS and TAR, drug criminals. The total amount transferred to AH from each of the parties is ~ USD1,296,296. While on debit transactions, there are flows of fund to hundreds of parties (relatives of Indonesian workers) with small nominal amounts. AH accounts were found to be used as an intermediary account of the proceeds from narcotics.



JAPAN

232 A foreign person, X, who was requested to transfer money by another foreign person, Y, located in the Kumamoto prefecture, illegally transferred approximately ~ USD1.79 million to the foreign person jurisdiction. Person X was arrested for violating the Banking Act (business without license). Person Y was arrested for violating the Act on Punishment of Organized Crimes (receipt of criminal proceeds) as receiving a part of trust money.

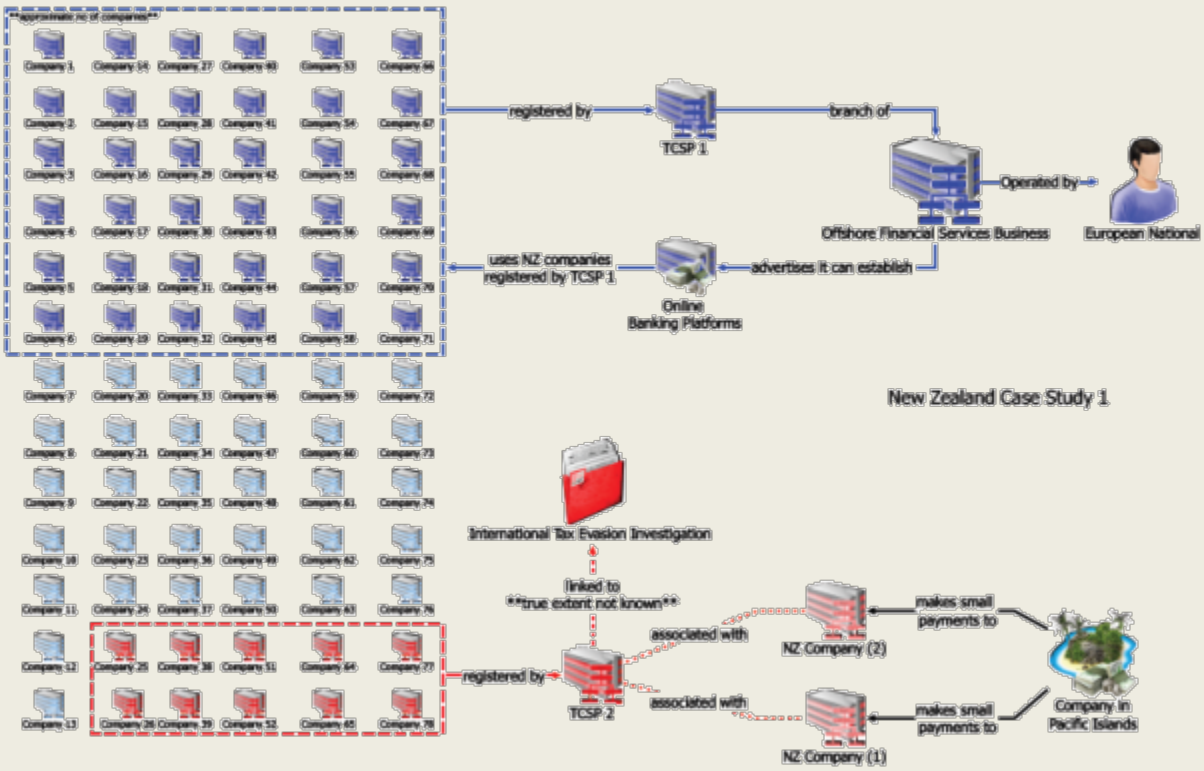
233 A man who was engaging in a 'loan-sharking' business arranged for borrowers to remit a total of ~ USD26,950.00 in loan repayments to multiple online bank accounts opened in the names of other persons. As a result, they were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

NEW ZEALAND

234 The following two cases studies were published in NZ-FIU quarterly typology report Q4 2015-16 and are available online: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents

Case study 1

235 Between 2010 and 2013 the NZ-FIU and Reserve Bank of New Zealand received queries from overseas questioning the legitimacy of 78 New Zealand registered companies that appeared to be operating overseas as alternative banking platforms. Nearly 60% of the questioned companies were registered by two TCSPs in New Zealand.



236 Intelligence gathered by the NZ-FIU indicated that TCSP1 was a company formation branch of an offshore financial services business, operated by a European national. This offshore financial services business advertised on its website that it could establish online banks for clients using a banking software application. The European national used companies registered in New Zealand by TCSP1 to establish alternative banking platforms.

237 TCSP2 had a link to an international tax evasion investigation. The true extent of the link was not known by the NZ-FIU; however, the New Zealand arm of the operation identified that TCSP2 was associated with two New Zealand registered companies that received small payments from a company in one of the Pacific islands. The NZ-FIU identified at least ten NZOFCs registered by TCSP2.

Case study 2

238 In March 2013, the Federal Bureau of Investigation of the United States (FBI) contacted the NZ-FIU requesting all information held on a New Zealand company A, its bona fides and the legitimacy of all recorded addresses. It was alleged by the FBI that company A was part of a fraudulent scheme operated in the United States in 2009 whereby fraudulent letters of credit were used.

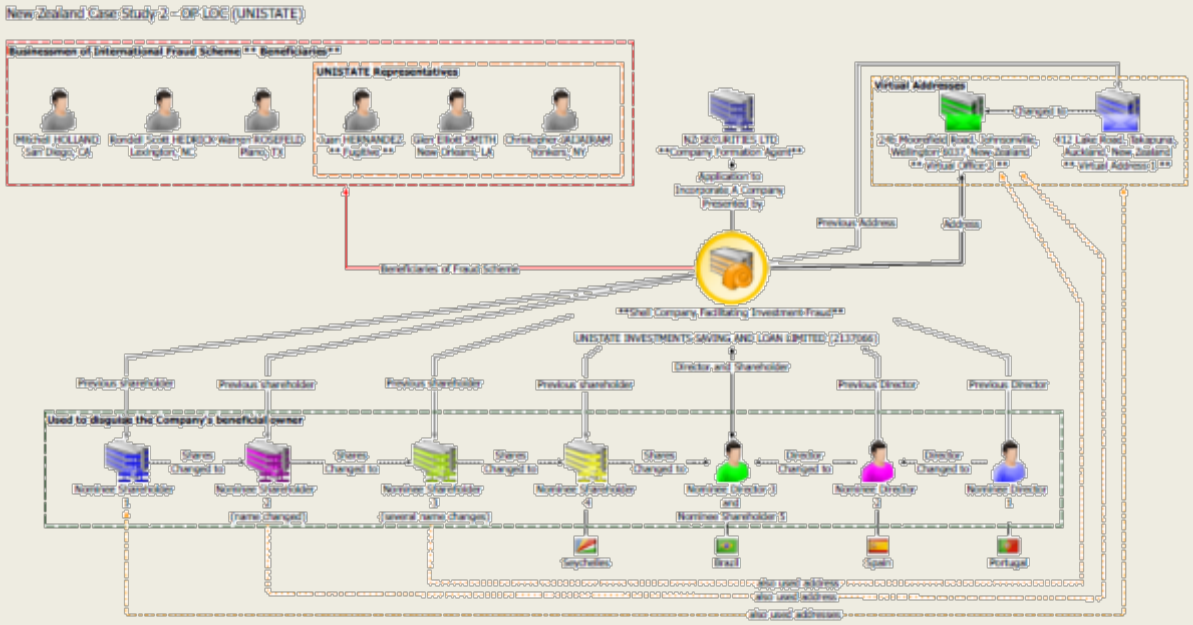
239 Background on company A

- Company A was a suspected shell company facilitating investment fraud by overseas persons.
- Company A was registered by a New Zealand company formation agent called NZ Securities Ltd.
- Nominee directors and shareholders were used in the formation. These directors acted purely as nominees. During the time company A was registered as a company (5 June 2008 to 29 February 2012) directorship changed three different times. In the same period, the shareholders of company A changed four times.
- The company structure used to form company A was similar to nine other New Zealand companies identified by overseas law enforcement agencies to have facilitated fraud in various foreign jurisdictions.

240 Main features of company A

- It was registered by a Company Formation Agent.
- Numerous nominee directors and nominee shareholders were used to disguise the company's beneficial owner.
- The company did not have a physical presence in New Zealand.
- The registered physical address for company A was 412 Lake Road, Takapuna, Auckland, the address for the registering NZ Securities Ltd – a company formation agent previously utilised by New Zealand registered shell companies controlled by overseas criminals.

241 Company A was registered on 5 June 2008 and struck off the New Zealand Companies Register on 29 February 2012.



242 The evidence (Brief of Evidence and Exhibits) provided to the FBI by the NZ-FIU, along with evidence given by the NZ-FIU Manager in April 2015 supported several successful convictions in a Florida law court.

CHINESE TAIPEI

243 J Company was an import and export trade company for clothing commodities. Ms C was the chairperson and Ms D was the finance manager of J Company. There is a high demand for correspondent banking services for clothing companies; however, the official remittance channel is time consuming and expensive due to high remittance fees. In order to earn a service fee and benefit from a difference in the exchange rate, from 2010, Ms C and Ms D operated an underground banking system for customers from Chinese Taipei and Mainland China to pay/receive Chinese Yen (CNY) or NTD and conduct transaction activities.

244 To avoid the detection of law enforcement agencies, Ms C requested several employees from her company to open bank accounts on her behalf to receive funds from customers via the underground banking system. After receiving funds, Ms D informed the contact points in China to remit CNY with equal value to appointed accounts.

245 Between 2010 and 2016, the accounts controlled by Ms C and Ms D have received approximately ~ USD831 million. Approximately ~ USD117,000.00 has been confiscated by the prosecutor. The MJIB initiated a criminal investigation and then referred this case to prosecutors in December 2016.

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

BHUTAN

246 A financial institution in Bhutan reported an incident in which an email account of a government officer was hacked and was fraudulently remitting funds offshore to three countries namely India, Malaysia and Thailand.

247 A total of three fund transfers were initiated amounting to INR 1,266,500.12 and USD 226,240.53. This included a transaction amount of USD 150,000 to jurisdiction X, which was rejected and returned due to an incorrect account number. Employees of the financial institution detected the suspicious transactions due to the failed transaction attempt.

248 The FIU noted that apart from the recklessness of the government officer for using a personal email address, there was some negligence from the bank employees who initiated the fund transfers. The employees of the financial institution should have exercised due diligence by confirming the transactions with the officer in charge of the government entity before carrying out the fund transfer. On this matter, all financial institutions were informed and directed not to initiate any fund transfers based on email requests without exercising appropriate checks.

FIJI

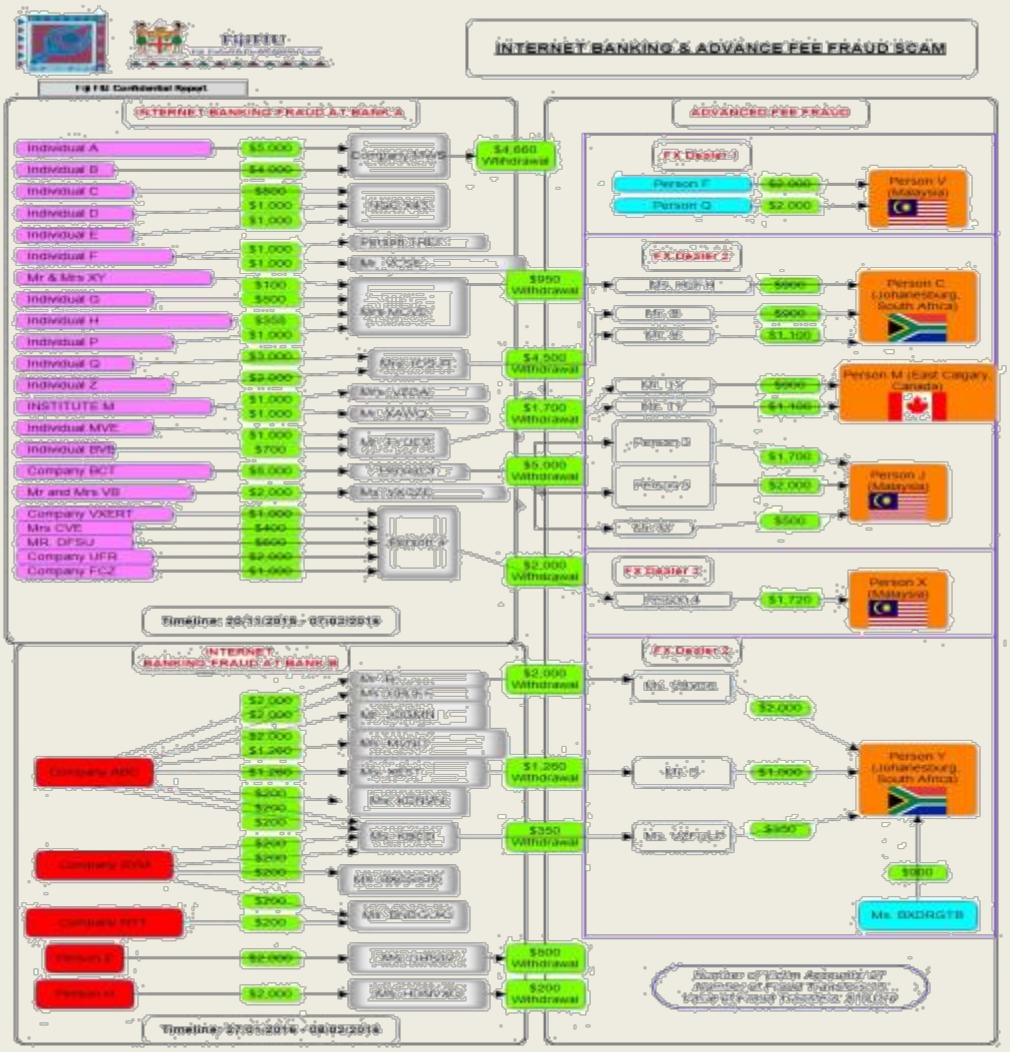
249 Between 2015 and 2016, the Fijian FIU received 8 suspicious transaction reports from two commercial banks whereby a total of 27 bank account holders accounts were affected by fraudulent fund transfers. The total amount of funds transferred via internet banking for both banks amounted to ~ USD26,000.

250 The FIU found that ~ USD9,000 of the fraudulent fund transfers were initially deposited into local bank accounts which were subsequently remitted via foreign exchange dealers to beneficiaries offshore who had no apparent relationships with the senders.

251 The nature of the fraud involved wire transfers and advance fee fraud (job scams, romance scams), utilising social media and other electronic communication mechanisms. The use of “money mules” to remit funds offshore is clearly evident in certain scenarios.

252 The possible offences committed included money laundering, possession of property suspected of being proceeds of crime and fraud.

253 Key indicators in this case include; (i) use of money mules to remit funds offshore, (ii) no apparent relationship established between sender and beneficiary, (ii) fraudulent internet banking transfers, and (iv) use of social media and electronic communications to facilitate fraudulent activity.



SAMOA

254 A local bank received payment instructions from a bogus email address (the email address is quite similar to the client's email address) demanding significant payment of imported goods. The payment was processed but it was later discovered that it was a scam. The bank cancelled the transaction and requested the return of funds. Only 59% of total funds were recovered.

255 A project accountant for one of the government authorities received a significant payment instruction from what appeared to be one of his project managers who was away at the time on a business trip. The accountant contacted his manager before the payment was processed. It was confirmed that the instruction was a scam and the payment was cancelled immediately.

5.8 Use of new payment methods/systems

CHINESE TAIPEI

256 In April 2016, the Criminal Investigation Bureau ("CIB") arrested eight suspects belonging to a criminal syndicate at a residence in northern Chinese Taipei. The residence was used by the syndicate for the purpose of money laundering. According to the CIB's investigation, the syndicate allegedly helped telecommunication fraud syndicates to launder illegal funds. Using a complex process and utilizing a Chinese based online trading platform for Bitcoin currency, a digital asset and payment system, the syndicate helped to secure illegal proceeds obtained by the fraud syndicate and evade detection by authorities. Since its establishment in April 2016, the syndicate had laundered millions of Renminbi to accounts controlled by the syndicate. Four of eight suspects were taken into

custody. The case was transferred to prosecutors for further investigation – the matter remains under investigation.

5.9 Laundering of proceeds from tax offences

AUSTRALIA

257 The following case study was published by AUSTRAC and is available online: http://www.austrac.gov.au/case-studies/austrac-helps-stop-illegal-tobacco-importation-syndicate

258 A joint law enforcement investigation identified members of an Australian syndicate involved in the importation of illegal tobacco and cigarettes from South East Asia and the Middle East. The tobacco products were imported from overseas using the services of complicit freight forwarders and a transport company operating domestically.

259 During this investigation, AUSTRAC provided financial analysis relating to the syndicate members and their associates. This analysis identified financial transactions used for the purchase of the tobacco and cigarettes, specifically involving funding flows to two foreign jurisdictions. Six Australian offenders were charged with possessing and importing tobacco products with intent to defraud the Commonwealth. The offenders received sentences ranging from fifteen months to six years and two months.

260 Law enforcement estimated that approximately ~ USD52 million in taxes would have been evaded, if it had not been seized. The potential profit for the sale of the illicit tobacco and cigarettes was estimated between AUD35 million to AUD45 million.

FIJI

Case Study 1

261 The Fijian FIU received a STR on a 27 year old, Person Y, who was receiving significant deposits into his personal bank account. Upon conducting further checks, the Fijian FIU established that Person Y is reportedly the managing director of a DVD shop. Mr. Y was in control of approximately five personal accounts across a number of financial institutions and was transferring funds between the accounts. The Fijian FIU also established that there were no bank accounts under the company's name.

262 A report was disseminated to the tax authority for possible tax offences (tax evasion).

263 Key indicators in the case include: (i) using personal bank account to conduct business like transactions, (ii) maintaining several bank accounts and conducting significant transactions, (iii) Transferring funds between his personal bank accounts, and (iv) no bank account established for the business for which Person Y is a managing director together with a business associate.

Case Study 2

264 Mr. M.S. between May 2005 and November 2009 derived ~ USD49,000 by creating fictitious records of 27 tax payers on the Fiji Revenue and Customs Authority FITS database. Each tax payer was allocated a tax identification number. The tax payers lodged tax returns under the salary and wage earner category. The 27 tax payers shared the same postal address. The same postal address of the tax payers triggered internal investigations by FRCA. The tax returns lodged showed that a certain amount was deducted as PAYE tax.

265 Mr. S.V. who was an auditor with FRCA had accessed the tax payer accounts and altered certain information. FRCA refunded the PAYE deductions which were processed as refund cheques

and posted to the address. The key to the postal box was collected by Mr. M.S. and 56 refund cheques were cashed by Mr. M.S. used the identities of his acquaintances to create the fictitious tax payers.

266 A significant degree of planning and execution was undertaken over a long period of time and the sum of ~ USD49,000 was not recovered by FRCA due to aggravating factors.

267 Mr. M.S. was sentenced to 7 years imprisonment and was not eligible for parole until he completed 5 years and 6 months of his imprisonment term.

268 Refer to FIU website for court judgment: http://www.fijifiu.gov.fj/getattachment/Pages/Case-Laws/ML-Case/2016/State-vs-Mukeshwar-Narayan-Singh-Sentence.pdf.aspx

INDONESIA

269 Person AM issues fictitious tax invoices (sales invoices that are not based on actual transactions) to the amount of USD9,141,481 with a profit of USD3,640,740. AM subsequently uses the funds obtained by the payment of the fictitious invoices to purchase assets such as land, apartments and vehicles. Assets in the name of AM with an estimated value of USD1,991,851 have been seized by authorities.

NEW ZEALAND

270 The following cases study was published in NZ-FIU quarterly typology report Q3 2015-16 and is available online: http://www.police.govt.nz/advice/businesses-and-organisations/fiu/news-and-documents

271 Person A was the Director and Shareholder of Company B. Person A made claims to Inland Revenue based on false invoices. Based on the same invoices they evaded taxation responsibilities estimated by Inland Revenue at approximately ~ USD181,900 and received approximately the same amount from Inland Revenue. Person A was charged with tax evasion offences having used nominees, trusts, family members and third parties to co-mingle funds. Person A then fled to jurisdiction X.

272 Person A was extradited from jurisdiction X and was returned to New Zealand. Person A was convicted on 18 charges of Evades Tax Payment and was sentenced to nine months home detention and 150 hours community work. Their assets, including two properties and cash, were also forfeited.

5.10 Real Estate, including roles of real estate agents

CHINA

273 Person A lead an illegal property organisation and used coercive tactics in trading to gain the rights to a piece of land covering 4500 square meters (worth more than ~ USD17.55 million). Person A then established the Changsheng Company and used the valuation of the land mentioned above as equity in the Changsheng Company. This combined the illegal asset with legitimate assets within the company. The 100% equity of the Changsheng Company was then transferred to others and the laundering of proceeds of crime was realized.

SINGAPORE

274 On 16 September 2013, the Corrupt Practices Investigation Bureau (CPIB) received information from a foreign authority that an owner of a Singapore resident company was involved in the bribery of foreign officials in return for classified information. One of the persons suspected to have been bribed was a Singaporean, Person B, who was under the employment of a foreign agency.

275 CPIB immediately conducted an investigation on Person B and arrested her the next day. Investigations revealed that Person B had been leaking classified information relating to her employer to the Singapore company owner since 2006 so that the Singapore company would have advantage over other prospective contractors of her employer. In return, Person B was rewarded with fully paid or subsidised hotel accommodation and monetary gratification of ~ USD 72,000.

276 The first ~ USD36,000 was received in cash in $1,000 denominations and was hidden in a hamper received during the 2008 Christmas celebrations. Person B then used the criminal proceeds, together with her own cash savings, to purchase an insurance policy. Although the insurance policy was a regular premium endowment plan, there was an option for the insurance premium to be paid-off over a shorter period. Thus, Person B made a lump sum payment of ~ USD72,000 (including ~ USD36,000 of criminal proceeds) towards the insurance plan.

277 The second ~ USD36,000 was also received in cash in $1,000 denominations. The cash was passed to Person B in an envelope in April 2009. Person B used the cash to pay for the 5% option fee for a condominium purchase in Singapore. Six months after the exercise of this option, Person B sold off the property to another buyer and earned a profit of ~ USD192,400 from the transaction.

278 For the above acts, Person B was charged with 7 counts of offences under section 6(a) of *Prevention of Corruption Act* for accepting corrupt gratifications and 2 counts of section 47 of *Corruption, Drug Trafficking and other Serious Crimes Act* for the laundering of the criminal proceeds.

THAILAND

279 The offender purchased 6 plots of land using the proceeds of crime, 2 plots in 2005 and 4 plots in 2007. In the following year, the offender gradually bought the Government Savings Bank lottery, to the value of several hundreds of thousand baht. When he became the suspect in intellectual property violation case, he sold all 6 plots of lands at the same time to his mother at very low price, lower than half of valuation price of the Land Office.

5.11 Association with human trafficking and people smuggling

THAILAND

280 A people smuggling syndicate was responsible for smuggling people from Myanmar to Thailand. The police searched and arrested 98 foreigners in 5 vehicles. Mr. P and Mrs. S were arrested and charged with people offences. The investigation found that Mrs. S was linked to the transnational labour smuggling network. A Malaysian national was in control of the network, and gave orders to a Myanmar dealer who would lure Rohingya Muslims to work. Mrs. S arranged boats on behalf of the Myanmar dealer to take the labourers from the pier. Mrs. S then transported the labourers by land to the destination. This transnational human trafficking gang divided duties among themselves at the originating and destination countries, persons who made fund transfer, arranged vehicles, etc. Traffickers also demanded that their families paid ransoms if they wanted to be free. When the victims reached Malaysia, they worked with the employers to repay the dealers. The proceeds of crime had been laundered through the purchase of boats and hotel businesses.

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

AUSTRALIA

281 The following case study was published by AUSTRAC and is available online: http://www.austrac.gov.au/case-studies/carpark-drug-deal-leads-arrest-organised-crime-members

282 AUSTRAC supported a law enforcement investigation into a drug trafficking syndicate that were suspected of having long-term involvement in the supply and distribution of narcotics in Australia.

283 AUSTRAC's analysis of transaction reports submitted by industry partners provided authorities with a snapshot of financial activities and identified additional persons linked to the syndicate for potential targeting by law enforcement.

284 The main suspect and two associates were arrested during a drug deal in which two kilograms of methamphetamine and ~ USD242,000 in cash was seized.

285 This investigation resulted in members of the syndicate being charged with attempted trafficking of a controlled drug; dealing in the proceeds of crime; and possessing a controlled drug. The main suspect was subsequently sentenced to 11 years imprisonment.

286 In this case, analysis of the syndicate's activities established that the primary syndicate members were not conducting transactions in their own right, rather their accounts were linked to account withdrawals/deposits carried out by family members and associates.

FIJI

287 Between April and May 2012, Indra, the mother of Natasha, befriended Steven on Facebook and commenced an online romantic relationship. Natasha managed Indra's Facebook account and communicated with Steven through this account as well as her own personal email and Facebook account. Steven had reportedly promised Indra and Natasha that he would marry Indra and settle the family in the United States.

288 After 8 months of online chatting, Natasha received ~ USD 35,000 into her bank account. Two transactions were received from a WHB Ltd from another jurisdiction. The second transaction was recalled by the bank and the funds were frozen. Natasha claimed that the funds were sent by her stepfather for the purchase of a house in Fiji.

289 The bank referred the matter to the Fiji Police Force and investigations revealed that the WHB Ltd had not sent the funds to Natasha.

290 Upon instructions from Steven, Natasha had transferred funds to Indra's bank account and withdrew cash to send to different beneficiaries in a second foreign jurisdiction X. Natasha also used Indra and her associates to send funds to these beneficiaries. Indra also used her boyfriend to seek approval to send funds.

291 Natasha claimed that she was blackmailed by Steven, and that the funds which she was sending overseas to different beneficiaries were for the treatment of his son who was dying. His son was reportedly residing in jurisdiction X. There were telephone conversations exchanged between Steven, his son and Natasha. Natasha also claimed that she was also asked to remit funds to beneficiaries in jurisdiction X to pay the employees of his business.

292 Natasha did utilise a portion of the funds to buy groceries. A reasonable person who is a university graduate ought to have known that the funds received into her account were reportedly sourced from some unlawful activity.

293 On 4 November 2016, Natasha was convicted for one count of the possession of property suspected of being proceeds of crime.

Refer to FIU website for court judgment: http://www.fijifiu.gov.fj/Pages/Money-Laundering-Conviction/State-vs-Natasha-Nilma-Singh.aspx

INDONESIA

294 Person A was a known businessman accused by the National Narcotics Agency (BNN) of buying and selling narcotics. Person A acted as the middle man of the narcotic transaction, receiving

payments into his bank account for narcotics and then transferring the funds person B after each transaction. Person A received a payment of USD3,703 for each transaction he coordinated. Person A then decided to purchase narcotics directly from person B and paid USD48,148 for one kilogram and on-sold the narcotics for USD59,259, resulting in a profit of USD11,111 for every kilogram sold. Person A used bank accounts in the name of his wife and other associates ("H", TP" and "ZD") for narcotics business purposes.

JAPAN

295 An unemployed man, aiming to found a stock company using a portion of illegal proceeds totalling billions of yen, collected through illegal means from members across Japan. He remitted funds equivalent to the portion of the illegal proceeds to an acquaintance's account and had the acquaintance and others pay for shares issued when the company was founded using the said funds. Through this means, the unemployed man, with the aim of obtaining the management control of the company himself, arranged for the acquaintance and others to obtain the position of an originator, to be appointed as board directors of the company at the time of foundation and to make foundation registration of the company at a regional legal affairs bureau by exercising their authority as the originator. As a result, the unemployed man was arrested for violating the Act on Punishment of Organized Crimes (management control through illicit proceeds).

SINGAPORE

296 A former bank officer requested various customers to sign blank funds transfer forms on the pretence that the said forms were a requirement for the customers' application for investment products. Thereafter, he completed the funds transfer forms with instructions to transfer funds from the customers' bank accounts into bank accounts belonging to his mother and friends.

297 Using this method, he made 15 unauthorised funds transfers amounting to ~ USD381,525 from the bank accounts of 10 customers. Additionally, he defrauded one of his customers of ~ USD57,677 cash handed to him for the purchase of a non-existent insurance policy. The misappropriated funds were used to finance his gambling habit. He was convicted of the offences and sentenced to 56 months' imprisonment in May 2016.

THAILAND

Corruption case

298 Person J accepted $1.8 million in bribe payments from a U.S. filmmaker in connection with contracts to run an entertainment event in Thailand. Person J then transferred the illegal funds to her daughter and her associate's foreign bank accounts. Person J was subsequently charged for bribery offences and malfeasance in office.

Online gambling case

299 Receive transfers from gamblers, through nominees' bank accounts, i.e. hired or deceived individuals who do not have direct knowledge of online gambling.

CHINESE TAIPEI

300 Mr. E was a senior public servant responsible for making the final decision on all procurements. Between January 2012 and January 2015, efforts to improve the information system were being undertaken. Mr. E received a bribe of ~ USD 1.2 million to ensure that W Company won the bid for the new information system. Following requests from Mr. F, the chairman of W Company, Mr. E asked his staff to set up conditions in favour of W Company, revealed information related to procurements to W Company, and proposed budget plans coordinating with W Company. W Company could therefore win the bid with a price that was higher than the general market price. As a

consequence, the purchase was of expensive goods and ultimately resulted in losses. Mr. F paid cash bribes to Mr. E. Mr.E then instructed Ms G, the section chief of the agency and Ms H, Mr. E's wife, to deposit the funds to Ms G's accounts, Ms H's account, other relatives' accounts and several legal persons' accounts controlled by Mr. E. In May 2016, prosecutors charged Mr. E and his associates of violating the *Anti-Corruption Act*, the *Criminal Code* and the *Money Laundering Control Act*.

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

AUSTRALIA

301 The following case study was published by AUSTRAC and is available online: http://www.austrac.gov.au/case-studies/austrac-helps-bust-money-laundering-syndicate

302 A law enforcement investigation identified a professional money laundering syndicate operating between Australia, Jurisdiction X and Jurisdiction Y.

303 The investigation revealed the offender flew to Australia from Jurisdiction Xand two days after arriving attended a casino. There she received ~ USD473,000 in cash in a backpack from an associate (suspect A) in the casino car park and deposited it into her casino account. After unsuccessfully attempting to transfer a portion of the funds from her casino account to the bank account of another associate (Ms X), the offender withdrew ~ USD227,000 in cash and attended a bank. There she attempted to deposit the cash with the intention of transferring it to Ms X who worked for an Australian money remittance business based in a different state. The offender was unable to provide satisfactory information when questioned by bank staff as to the origins of the cash and purpose of the transaction. As a result of the law enforcement investigation the offender was arrested at the bank attempting to deposit the cash.

304 The offender was charged with one count of dealing with more than AUD100,000 that it was reasonable to suspect was the proceeds of crime and was sentenced to 16 months imprisonment.

INDONESIA

305 Person M is a known entrepreneur, and is the suspect of money laundering and dealing with the proceeds of crime. Person M sells coupons used for gambling in District "T" supplied by person P who lives in district "B". Person M has two accounts used to carry out the gambling transactions, account "1" used for placement, transfer and receipt of proceeds from gambling and account "2" used to place profits from the sale of gambling coupons supplied by person P. The profit amounted up to 17% from all coupon transactions.

JAPAN

306 The owners of an online gambling establishment let customers engage in illegal online gambling by installing a computer in the café. Senior members of Boryokudan received a total of around JPY 90,000 in cash as protection money while knowing that the money was derived from illegal gambling. As a result, owners were arrested for habitual illegal gambling and members of B were arrested for violating the Act on Punishment of Organized Crime (receipt of criminal proceeds).

307 A male senior member Boryokudan who manages the illegal online casino made the staff remit around JPY ~ USD5,303 in revenue to an account opened in the name of another person. As a result, he was arrested for violating the Act on Punishment of Organized Crime (concealment of criminal).

SINGAPORE

308 Three casino patrons, all members of its loyalty programme, were found guilty and convicted in November 2016 of misappropriating ~ USD640,000 from a casino in Singapore.

309 Investigations revealed that the three patrons exploited a system error in one of the electronic gaming promotional activities offered by the casino. Thereafter, the accused persons laundered their criminal proceeds by placing bets through roulette machines and remitting monies to parties in the region.

310 Using a significant portion of their criminal proceeds, the accused persons gambled at casinos and accumulated more than ~ USD1.02 million. The police seized cash, gaming chips and bank accounts amounting to a total of ~ USD.977 million.

311 The three persons were convicted and sentenced to 21 months', 26 months' and 12 months' imprisonment respectively.

5.14 Mingling (business investment)

INDONESIA

312 Person I was a regent of district "A" in Indonesia. Person I instructed his son to open a chequing account and a deposit account on behalf of his son's company, PT.BSA and PT.BPI. Person I was made to be a signatory on both accounts in order for person I to withdraw funds from the accounts and combine both legal business transactions and proceeds from his criminal activity.

5.15 Use of shell companies/corporations

AUSTRALIA

313 Four days after arriving in Australia as the holder of a short term visitor type visa, Mr X registered as the sole director of an Australian company. Two weeks later, Mr X made three separate cash deposits - ~ USD12,111 into an Australian bank account; ~ USD15,100 into another Australian bank account; and ; ~ USD15,100 into a yet another Australian bank account. All accounts were opened using Mr X's newly registered business. On that same day, Mr X made an outgoing electronic transfer of ~ USD15,000 to an account in jurisdiction X. In the following two weeks, Mr X made six further cash withdrawals totalling over ~ USD64,350. This included four cash withdrawals on the same day from four separate branches of an Australian bank. The source of the funds is currently unknown.

5.16 Currency exchanges/cash conversion

AUSTRALIA

The following case study was published by AUSTRAC and is available online: http://www.austrac.gov.au/case-studies/false-passports-counterfeit-euros-10-years-imprisonment

314 Law enforcement commenced an investigation into a person exchanging counterfeit currency after receiving information from banks across Western Australia, South Australia and Victoria. After travelling to each state, the offender attended multiple branches of several banks and opened up bank accounts using aliases and false passports. The offender then exchanged counterfeit Euro for Australian dollars. The offender was arrested after exchanging a total of ~ USD263,100 over a four month period and sentenced to 10 and a half years imprisonment.

315 Within three weeks of opening a personal savings account with an Australian bank, Mr A received electronic transfers totalling ~ USD204,450 from two Australian businesses over two days. The majority of these funds were then washed through his account in the days following.

FIJI

316 Mr. A, a Fijian citizen with American residency is 60 years of age. The Fiji FIU received a STR from a foreign exchange dealer.

317 The Fiji FIU conducted checks on the immigration database and established that Mr. A had travelled to Fiji three times in 2016. He exchanged substantial amounts of USD into FJD during his visits.

318 A report was disseminated to the FRCA Customs Unit to examine possibility of non-declaration of BCR.

HONG KONG

319 A corruption investigation revealed that five persons (D1-D5) working in various industries were individually recruited by middlemen to act as sole directors-cum-shareholders of different shell companies in Hong Kong. D1-D5 opened bank accounts in the name of the shell companies with various banks in Hong Kong and allowed the middlemen to use the bank accounts to launder criminal proceeds. By doing so, D1-D3 had each received monetary rewards from the middlemen ranging between ~ USD250 and ~ US1,280.

320 Between August 2004 and June 2009, D1-D5 each conspired with another middleman to deal with sums of money ranging from over ~ USD1.025 million to over ~USD56.413 million through the said bank accounts held in the name of shell companies.

321 The total sum of the proceeds of crime dealt by the defendants and middlemen amounted to over HK$1 billion.

322 Upon conviction of ML offences, D1-D5 received custodial sentences ranging between 18 months and ~ USD128 million.

MACAO, CHINA

323 In May 2014, the economic crime division (ECD) of the LEA received a report, stating that the employees of a company in Country Y were involved in forging documents to embezzle funds from the company. After an initial investigation including cross checking with the central database of intelligence from all sources, the case was found to be a fraud case involving millions of criminal proceeds and wire transfer transactions in a number of bank accounts. The case met the criteria of the Parallel Financial Investigation Guideline, thus the AML division initiated a parallel financial investigation on the case and worked together with the ECD.

324 After the financial investigation, the mastermind was found to be a clerk of the company, who was responsible for the receipt of product transportation fees of the company, as well as receiving and managing the cheques. The involved party took advantage of his/her job, to set up a shell company and bank account(s) under his/her sister's name. The shell company's name was similar to the name of the involved party's working company. He/she changed the beneficiary's name on the cheques to his/her sister's company and deposited those cheques to the shell company's accounts. The investigator carried out an in-depth financial investigation on the shell company's bank accounts, interviewed the bank employees and monitored the suspect's activities and determined the shell company's ultimate beneficial owner was the suspect. When each cheque was deposited into the shell company account, the mastermind withdrew most of the funds in cash and transferred a small portion to another account which belonged to him/her and a third party.

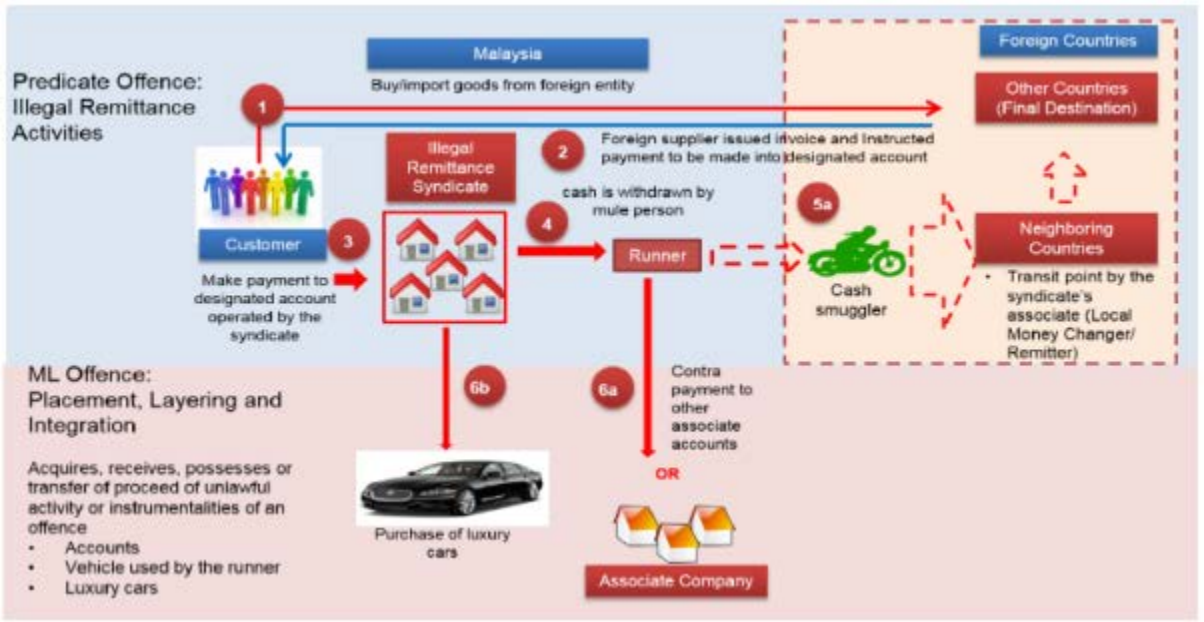
325 The case involved both fraud and forged documentation. The suspect was sentenced to four years and 9 months and ordered to pay back $ USD3.5 million to the company.

MALAYSIA

326 Malaysian Authorities recently disrupted the activities of a group of illegal remittance operators that were suspected to have illegally remitted more than USD3 billion from Malaysia to several foreign countries over the period of 5 years. It is believed that these illegal remittance activities were operated by a syndicate which had facilitated fund transfers out of Malaysia, either through informal fund transfer networks such as the hawala system or physical smuggling of cash into a neighbouring country.

327 The majority of these funds were used to facilitate trade mispricing activities between local traders and foreign suppliers, remittance activities for foreign workers to remit money to their home countries and also transferring illegal proceeds overseas.

328 Surveillance and financial intelligence analysis revealed that several companies and bank accounts were operated by the syndicate using their proxies. The syndicate actively recruited "mules" as their proxies by opening accounts in several financial institutions. Analysis of the transactions showed that significant amounts of cash were deposited into the accounts by a number of different people. Subsequently, the syndicate withdrew funds from the accounts on the same day or the following day, leaving a minimal balance in the accounts. It is believed that the funds were then remitted or smuggled out of Malaysia by the syndicate to the intended recipient in the foreign countries.



329 The money laundering methods used included:

- Use of nominees, trusts, family members or third parties etc
- Trade based money laundering and transfer pricing
- Underground banking / alternative remittance services / hawala
- Currency exchanges / cash conversion
- Currency smuggling (including issues of concealment & security)

SAMOA

330 A foreigner named Ms L exchanged approximately ~ USD22,400 at a money transfer business. She claimed to be a tourist and the money was to fund her travel expenses. She stayed in

Samoa for a period of less than two weeks before leaving the country. She was suspected of carrying undeclared currency of ~ USD22,400 with her when she arrived.

CHINESE TAIPEI

331 In 2015, Mr. I and Mr. J obtained 24,500 pieces of counterfeit bills from an unknown origin. These counterfeit bills with a denomination of US$100 could pass the examination of old money detectors. Between January and February 2016, they sold 23,490 pieces of counterfeit bills to Mr. K et al. with the price lower than the foreign exchange rate. Mr. K handed over these counterfeit bills to his friend, Mr. L who is the director of L Company and requested him to deposit them into bank accounts. Mr. L instructed Ms M, the accountant in L Company, to deposit these counterfeit bills into L Company's foreign currency account respectively. Ms M exchanged them into NTD using the foreign exchange rate on the same day of the transaction and then transferred them into L Company's NTD account. After deducting the cost of buying counterfeit bills and the profit to Mr. K, the rest of the proceeds of crime were transferred to Mr. L, Ms M, and other accomplices' accounts or delivered to them in cash. Mr. I et al. were indicted on the charge of violating the Criminal Code by prosecutors.

THAILAND

332 Mr. J and associates engaged in the drug trade as a transnational organised crime syndicate. They had opened a coffee store chain as a front business for their illegal activity earning a yearly income of ~ USD17.6 to 23.5 million.

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

AUSTRALIA

333 The following case study was published by AUSTRAC and is available online: http://www.austrac.gov.au/case-studies/guns-drugs-and-pistons

334 The investigation centred on a well-known Australian criminal syndicate, with an extensive criminal background in car re-birthing, card skimming and the lodgement of fraudulent skimming claims. The syndicate had links to foreign jurisdictions and was known for importation of commercial quantities of drugs, importation of firearms and exporting stolen vehicle components.

335 The investigation focused on funds transferred via a remittance service to the syndicate's associates in the foreign jurisdiction X for the legal purchase of the firearms. In jurisdiction X, the legally purchased weapons were hidden inside -hollowed-out car engine blocks along with illicit drugs, to be smuggled within these components to automotive industry facilities in Australia.

336 Further to this, records of the gun purchases and engine shipments closely matched the prime syndicate member's multiple visits to Nashville.

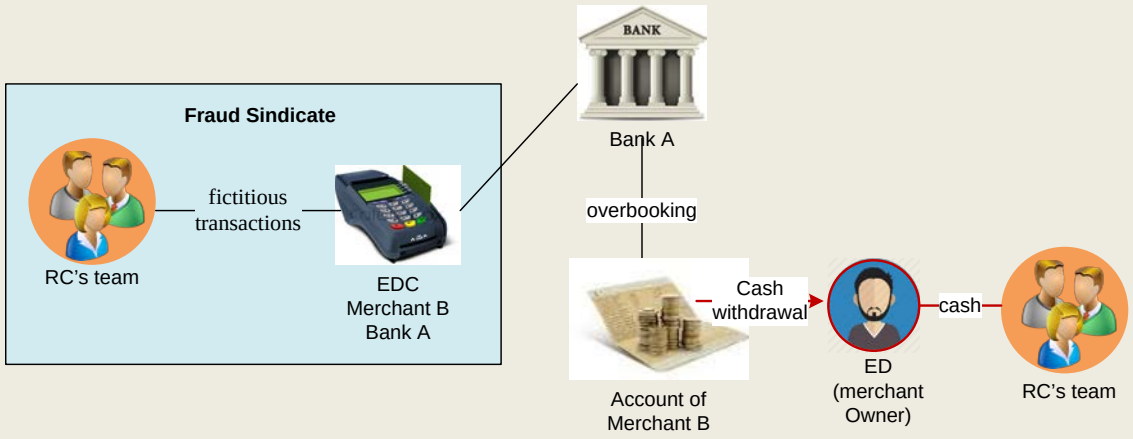
337 Jurisdiction X Customs and Border Protection intercepted one consignment and discovered cocaine hidden inside engine pistons. Jurisdiction X Customs confiscated the cocaine and arranged a controlled delivery and surveillance of the shipment to Australia.

338 Australian law enforcement reconstructed the consignment and delivered it to the prime suspect's associate. The associate's movements were kept under surveillance, resulting in the arrest and conviction of one Australian suspect.

339 The investigation also resulted in the detection and closing down of a supply route for illegal firearms and drugs between jurisdiction X and Sydney.

INDONESIA

340 Person D is an entrepreneur who helps RC conduct fraudulent transactions using debit/credit cards by providing a merchant account to accept the transaction. An EDC machine of Bank G was used in the transaction, however some criminals do not use EDC lent by the banks as additional information is modified to conform to the merchant's original EDC machine. The transactions appeared in the system as though they were conducted from a phone number in town A; however the transactions were actually conducted in town B. Whenever RC fraudulent transactions are entered into a merchant account owned by person D, the next day person D would make cash withdrawals with the same value minus a commission of 5% for each transaction with a total of USD50,074.



CHINESE TAIPEI

341 The CIB have received information from INTERPOL since 2015 regarding cases of money being stolen from accounts belonging to European customers using credit cards in Chinese Taipei. The information also revealed that the money was returned to Europe through Western Union and an international counterfeit bank card ring led by a foreign individual operating out of Chinese Taipei. In addition, police have received reports from domestic banks indicating that several fake ATM cards had been locked in their machines and the cards were used by foreign nationals.

342 According to the investigation, most of the suspects were from foreign jurisdiction X who led lavish lifestyles in Chinese Taipei, often hanging out in nightclubs and bars. In 2016, the police authorities conducted two separate waves of raids in March and April and arrested foreign nationals and Chinese Taipei citizens who were members of an international counterfeit bank card ring involved in bank card fraud. So far, a total of 15 domestic and foreign suspects have been arrested, including 12 foreign nationals, and around ~ USD1.976 million has been confiscated. Another member was arrested in foreign jurisdictions. This case was transferred to the Chinese Taipei prosecutors.

THAILAND

343 The offender withdrew cash with a value of ~ USD884,250 from a Bank in Mukdaharn province and concealed it in the pick-up truck in order to smuggle to jurisdiction X.

5.18 Structuring (smurfing)

INDONESIA

344 Person K along with a Notary CL has offered PT.PP (property company) to buy land with an area of 4,165 M2 in district "Y" with a Certificate of Property Rights, recognising the proprietorship of person K. Then PT.PP bought the land by handing over money for USD4,118,722, but the buying and selling process promised by person K and this notary is not resolved. The proceeds of these crimes by the defendant, person K were placed on personal accounts of his sister, wife and children.

345 Person K placed the proceeds of crime into five deposit accounts with ownership on behalf of his wife, children and families. Transactions conducted by structuring to 5 deposit accounts with the mechanism of payment transactions below USD37,037 (the threshold of reporting cash transaction) until the total funds placed around USD1,481,481.

5.19 Wire Transfers/Use of Foreign Bank Accounts

AUSTRALIA

346 Refer to the AUSTRAC case studies hub for the following three case studies:

- "Car park drug deal leads to arrest of organised crime members" recorded against category # 12;
- "AUSTRAC helps stop Illegal tobacco importation syndicate" recorded against category # 8; and
- "Guns, drugs, pistons" recorded against category # 27.

347 Mr B admitted to opening up multiple accounts across a variety of financial institutions, linking personal accounts to a business account, with the purpose of diverting these funds across accounts utilising wire transfer companies. The majority of his deposits abroad were to entities in Jurisdiction X. In his last six months of activity he estimated his involvement in the receipting and distribution of some ~ AUD68,100.

CHINA

348 A gang-related case involving principal criminals "B" and "C" (deceased) in Shanwei, Guangdong province shows a combination of several means of money laundering in one case, involving wire transfers (use of foreign bank accounts), real estate, use of family members and investment in capital markets.

349 Wire transfer (use of foreign bank accounts): The principal criminal "B" entered into a sham marriage with a Hong Kong person and applied to the Entry-Exit Administration Division of Guangxi Autonomous Region in October 1997 for residence in Hong Kong. In December she got the approval and has gained Hong Kong citizenship. Taking advantage of the citizenship, criminal "B" has set up a Hong Kong bank account to which criminal "B" succeeded in transferring the proceeds of crime. With these proceeds, criminal "B" purchased real estates and set up companies in Hong Kong.

350 Real estate: The principal criminal "C" also engaged in money laundering by the means of purchasing real estate in Hong Kong with the proceeds of crime.

351 Use of family member: To escape regulatory controls, criminal "C" deposited the proceeds of crime worth ~ USD938,000 into the bank account of his/her son.

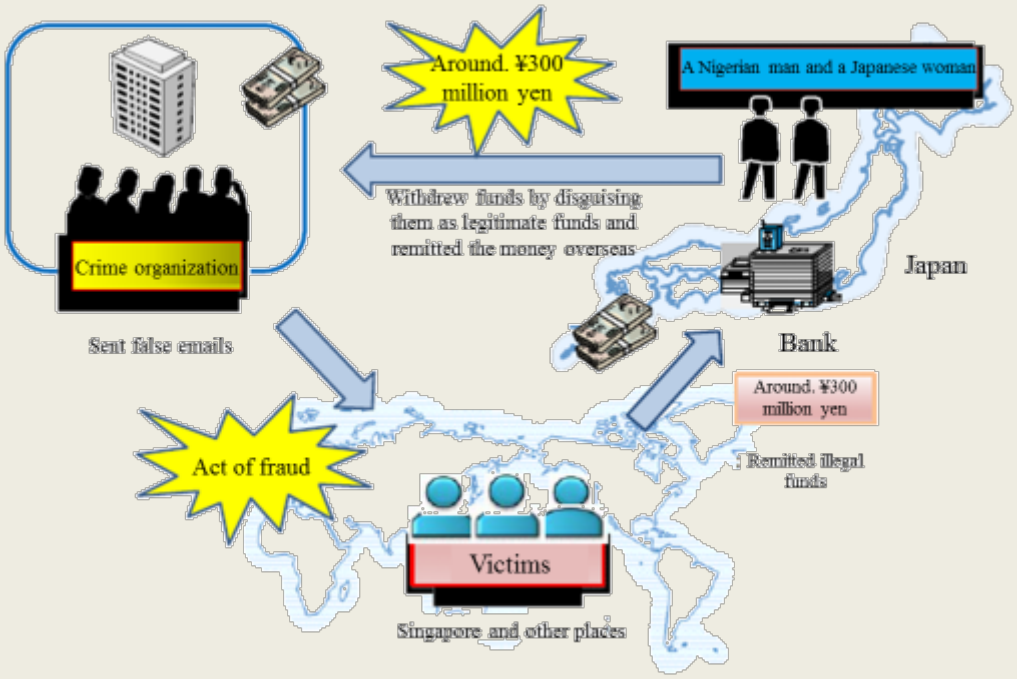
352 Real estate and investment in capital markets: The principal criminal "B", "C" and others invested the proceeds of crime into the rights of 26 pieces of lands, 26 real estate, stocks and securities, lots of jewellery and other precious items. Through reselling slots or cashing the stocks and securities, they gradually turned those assets into legal money and assets. For instance, a slot with 5000 square meters in Binhai residence area was evaluated and resold at ~ USD2.2 million in the year of 2009.

JAPAN

353 A foreign man from jurisdiction X and a Japanese woman withdrew funds from an account at a Japanese bank opened in the name of the foreign man. This account was used to transfer funds from victims of fraudulent transactions deceived by falsified emails. These funds were remitted from foeign jurisdiction A and other countries. When withdrawing the funds, the offenders explained to a bank employee that those funds were remittances relating to normal commercial transactions, thereby

disguising the money as legitimate business profit. As a result, they were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

354 A total of around ~ USD2.695 million was sent from foreign countries into the account held by the foreign man over a period of several years through a total of 51 remittances. The funds withdrawn by the offenders were transferred to accounts held by the Japanese woman and others or remitted to overseas accounts.



SAMOA

355 A foreigner named Mr W arrived in Samoa with his partner and they claimed to be tourists. Mr W was reported receiving several inward TTs from different senders in various countries. He stated that the monies were to finance their vacation. Mr W tried to remit these funds (he received) to another country but was unsuccessful because of lack information in the supporting documentation he provided.

CHINESE TAIPEI

356 A foreign national, Mr. N, is the director of T Company which was responsible for promoting business of the “M website” in Chinese Taipei. The “M website” sold virtual currency for online games. In order to attract investors, from March 2013, Mr. N and several Chinese Taipei citizens used online advertisements and held seminars to claim that their investment plans were properly secured. They used sophisticated calculating formula to mislead investors into profiting. After giving cash or transmitting the funds to T Company’s account and other appointed accounts, the investors could get electronic accounts to buy virtual currency sold by the “M website”. The investors also used their electronic accounts to redeem their investments.

357 However, the investors needed to pay 10% of the proceeds as the transaction fee, 30% of the proceeds to buy virtual currency forcibly, and 5% of the proceeds to exchange electronic points which could be used to purchase goods from physical stores. Investors could freely use the rest of the 55%.

358 In order to raise the price of virtual currency, Mr. N et al. designed various rewarding systems to encourage investors to recruit other investors to purchase the virtual currency. From August 2012

to August 2016, the total amount of the investment was over ~ USD98 million. In order to avoid detection by law enforcement, Mr. N et al. transferred around ~ USD9.880 million to other natural and legal persons' accounts controlled by Mr. N or disguised them in the removable ceiling of T Company's office. The investigation into Mr. N resulted in confiscated cash, real estate, vehicles and froze several accounts owned or controlled by Mr. N et al. The total value of confiscation was over ~ USD13.173 million. Mr. N et al. were indicted on the charge of violating the Banking Act and the Money Laundering Control Act by the Taichung District Prosecutors Office in November 2016.

THAILAND

359 A drug dealing network laundered illicit funds through numerous bank accounts. Buyers deposited funds using ATM's into bank accounts, some accounts were hired for use from genuine labourers. The funds were then transferred from the labourer's account to accounts controlled by the drug network. The head of network (Mr. A) owned dozens of accounts, with a fund flow over 1,000 million baht.

360 In an online gambling case, transfers were received from gamblers, through bank accounts within the criminals' network. They received transfers to several other accounts, opened in several areas, for layering and concealing the illicit source.

FIJI

361 A former Fijian citizen aged 53 (person M) was reported to the FIU for sending a substantial amount of funds via wire transfers from her bank account in Country P to her local bank account with Bank D in Fiji. Person M was reportedly engaged in domestic duties. Once the substantial amounts were transferred to bank account with Bank D, she withdrew ~ USD270,000 and deposited this into her bank account held at Bank E.

362 It appeared that Person M was layering funds originated from Country P. A report was disseminated to the relevant foreign FIU for further profiling. The possible offence included money laundering and layering.

363 The key indicators in the case include: (1) Client is engaged in domestic duties; (2) Fund transfers of substantial amounts not commensurate with occupation; (3) Movement of funds between local bank accounts as soon as large amount of funds received from offshore and (4)
Commodity exchanges (barter – e.g. reinvestment in illicit drugs).

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

NEW ZEALAND

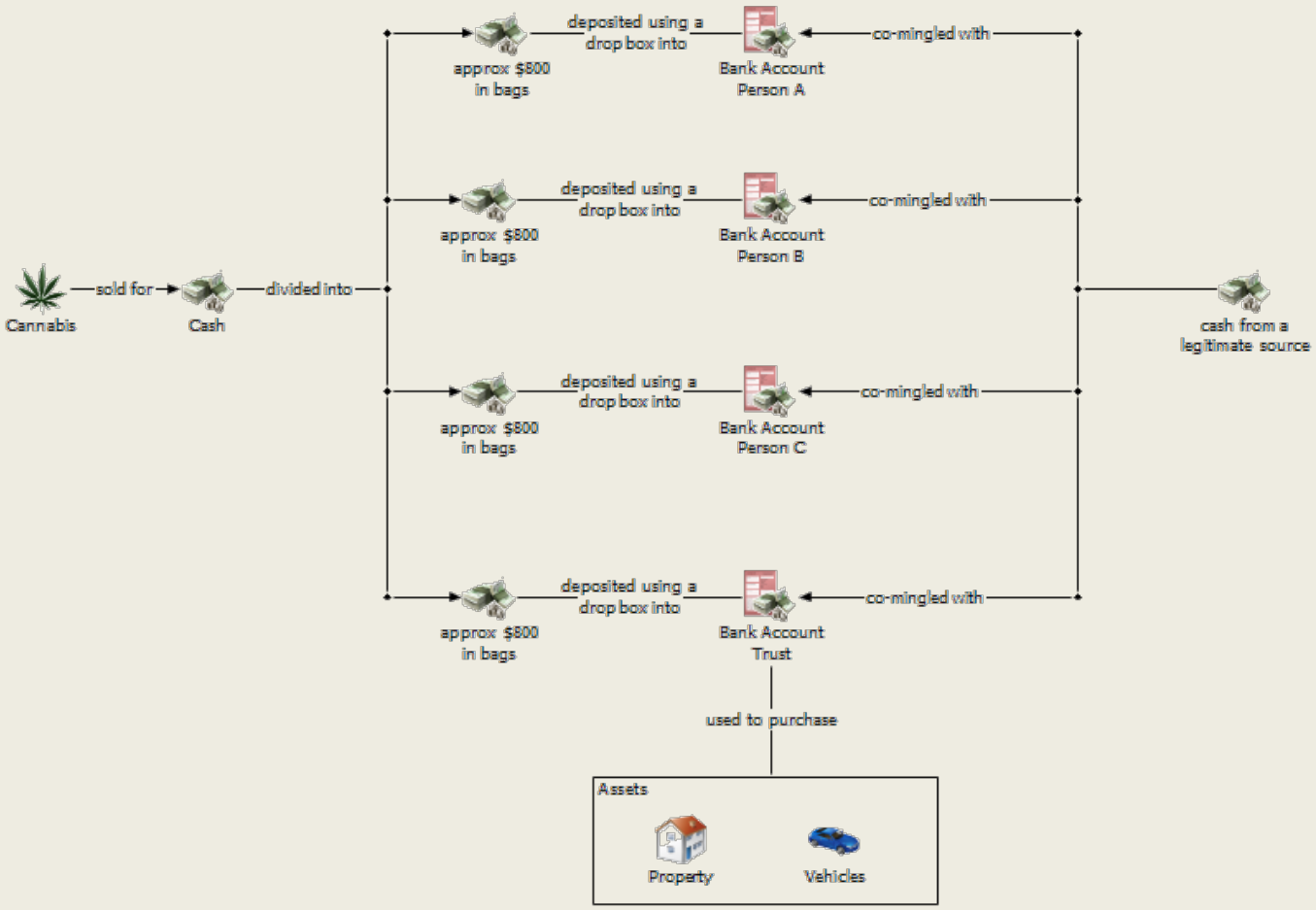
364 The following cases study was published in NZ-FIU quarterly typology report Q3 2015-16 and is available online: http://www.police.govt.nz/sites/default/files/publications/fiu-quarterly-typology-report-q3-2015-16-predicate-offending.pdf

Operation Foxy: drug offending

365 The Wellington Covert Operations Group and the Central Asset Recovery Unit started investigating a family syndicate for the commercial distribution of cannabis. The syndicate grew and sourced cannabis from other growers to sell. The syndicate earned a significant profit, and over a seven year period syndicate members made over ~ USD1.16 million in cash deposits into numerous bank accounts operated by family members. The head of the syndicate, Person A, would spend several hours each morning banking cash, then the afternoon selling cannabis, and the evening preparing for the next day's activities.

366 To attempt to hide the origin of funds, the head of the syndicate, Person A, smurfed cash into multiple accounts. Person A opened multiple bank accounts with several banks either in their name, the trust name, or a family member's name. Person A would then package cash earned from the sale of cannabis into drop box plastic bags. Generally the money was in ~ USD500 amounts. Person A would then visit multiple banks and bank the cash into various accounts via drop box. Person A did not interact with bank tellers, it was likely that this was an attempt to minimise the risk of detection. Person A then co-mingled the funds with legitimately sourced funds to purchase assets. Syndicate members purchased ten properties, many of which were owned by the trust the syndicate set up. Cash was also deposited into the trusts bank accounts.

367 ~USD2.25 million in assets were restrained under the Criminal Proceeds Recovery Act 2009. These assets included properties, vehicles, and cash. Person A, was subsequently charged with selling cannabis, possession of cannabis for supply and money laundering.



THAILAND

368 Buyers made payments to the head of a drug syndicate through various companies in an import-export business for goods such as agricultural produce, oil and construction equipment. These companies then sent the goods to the drug dealer.

5.21 Use of False Identification

FIJI

369 A 53 year old businessman, Person N and his associate Person V, allegedly falsified airline tickets with the intention of dishonestly obtaining USD3,500.00 from a local commercial bank in July 2016. It was suspected that Person N may have two passports issued under his name. A report was

disseminated to the Fiji Immigration Department. Person N and Person V were charged with one count each of general dishonesty and remanded by the Magistrates Court. The possible offences included obtaining financial advantage through deception and general dishonesty.

370 A possible indicator for this crime was intent to defraud authorities based on false documentation.

JAPAN

371 Men gained the use of a post-office box by using a forged health insurance card and sent obscene DVDs to customers. The customers paid funds to the post-office box. As a result, they were arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

INDONESIA

372 The defendants, known as Persons A, B, C, D and E committed the crime of theft of bank customers' funds. It is known that Person D worked for Bank X. Person D requested Person E to search a bank's customer database. Person D then used the customer data for Person WL to falsify a passbook and identity card used to steal Person WL's funds. The defendants used the fake identity cards to obtain an ATM card on the account belonging to WL. The defendants made multiple low value withdrawals at different branches and ATM's in various locations. To conceal the origin of money derived from criminal acts, the defendants transferred some money into multiple accounts and purchased some assets.

5.22 Gems and Precious Metals

JAPAN

373 A man used another person's credit card to take rings and necklaces away by deception. He sold them at around ~ USD8,785 by showing the other person's health insurance card to the pawnbroker. As a result, he was arrested for violating the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

5.23 Purchase of Valuable Assets (art works, antiquities, race horses, etc)

INDONESIA

374 Cases related to corruption of IW. He was a regent of district "A" in Indonesia. He purchased assets in the form of heavy equipment such as excavators and trucks to cover the mode of criminal offenses.

MALAYSIA

Case 1 – Drugs Trafficking Syndicate

375 The Royal Malaysia Police recently charged a drug trafficking syndicate operating in the northern area of the country which was linked to a drugs syndicate in a neighbouring country. The syndicate was also involved in the production of drugs where the drugs laboratory was set up by a shell company. The proceeds of drugs trafficking were managed by the proxy of the main suspect, who is also the girlfriend of the suspect. The proceeds were mainly used for purchasing of luxury cars, jewelleries, real estate properties and shares.

376 The financial analysis revealed that a portion of the proceeds were also used to finance other illegal activities including illegal gambling. The money laundering methods used included the use of

nominees, trusts, family members or third parties; purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.) and the use of shell companies/corporations.

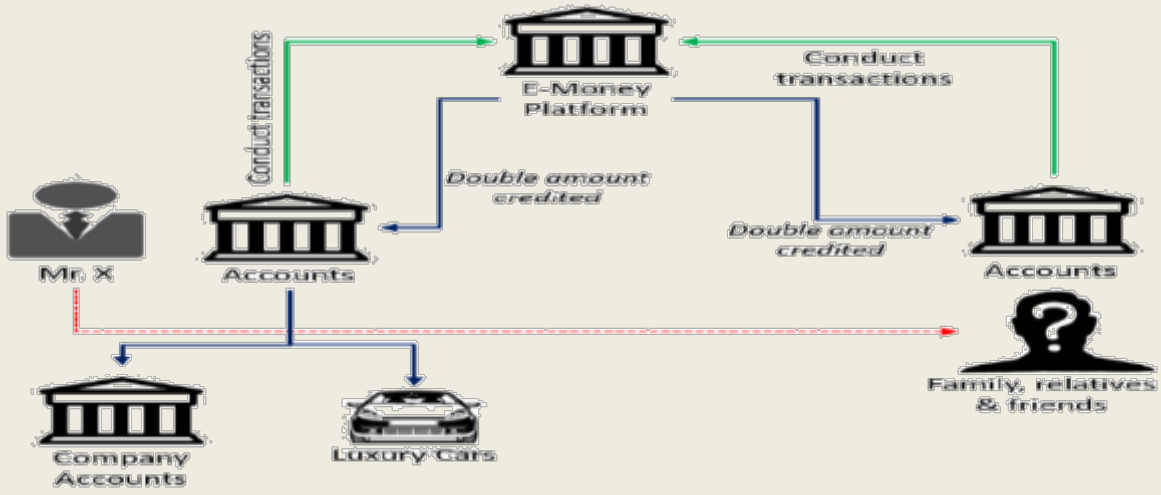
Case 2 – Fraud

377 Mr. X was subscribed to an international e-money company, which was linked to his savings account in a commercial bank. During a systems maintenance exercise conducted by the e-money company, a system glitch caused a payment error, whereby funds intended to be deducted from the account, were mistakenly doubled and credited into Mr. X's savings account. Mr. X took advantage of the system error which occurred at a specific time each day and repeatedly conducted transactions to fraudulently obtain funds. Mr. X induced his family, relatives and friends to do the same. Over a period of 5 months, more than 100 accounts involved in this fraudulent scheme amounted to more than USD10 million.

378 The illegal proceeds were placed in the personal accounts of the suspects for personal expenditures besides being layered for the purchase of luxury cars and placement into company accounts.

379 To date, 24 suspects have been charged for fraud and money laundering offences.

380 The money laundering methods used include use of nominees, trusts, family members or third parties etc. and purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.).



THAILAND

381 A high ranking police officer, C and his associates committed the following offences;

- Malfeasance in office by receiving a ~USD88,300 to ~147,300 bribe from police officers who wanted to buy positions. The officers also demanded he pay a sum of ~USD295 – ~58,900 a month.
- Bribery from oil smuggling gangs to the amount of ~ USD58,900 to ~147,290 a month.
- Illegal gambling business.

382 The assets connected with the commission of offences had been laundered through buying 111 items of land, cars, precious stones and gems, antiques, bank deposits, with an approximate value of ~ USD16.5 million.

5.24 Investment in Capital Markets, Use of Brokers

INDONESIA

383 Person A was the marketing manager of Bank X. He offered person D opportunity to invest/deposit in Bank XX. Later, the deposited funds invested by person D totalling ~ USD 5.5 million actually belonged to PT.PI (state-owned enterprises). Furthermore, person D looking for a company, namely PT. KK construction company which is an existing customer at Bank X. Then, these deposit guaranteed to get a finance working capital by using PT.HI as the applicant. In a very short time, person D dilute the deposited guarantee and placed in a bank account of person S amounting to USD3,703,703 and some transferred to account of PT.HI amounted USD56,944, the rest are withdrawals and integrated to capital market (shares) and purchase of assets such as property and motor vehicle.

THAILAND

384 The offender bought shares with the proceeds of crime using a securities company which he was a client. He deposited cash into the company's account on the same day of the shares purchase. The process was repeated several times, with about 3 to 5 days apart. The shares bought were of mining companies and medical companies, with a total value of millions of Baht. The payment was cleared through the Automatic Transfer System and the dividend was transferred to another account under his name, which he was also an ultimate beneficial owner.

5.25 Environmental Crimes

THAILAND

385 Mr. K, a Thai-foreign national at the centre of a major wildlife trafficking ring, was involved in smuggling protected Thai rosewood to foreign jurisdictions. K's networks utilised as many as 28 separate accounts and exploited his connections in Thailand, many neighbouring jurisdictions to move illicit funds. Payments related to rosewood shipments originated in a foreign jurisdiction and were sent via K's associates in southern Thailand to accounts in another foreign jurisdiction.

- K's network laundered as much as 1.18 billion Baht (~USD35 million) using his accounts, connections, and business interests.
- Jewellery – Police found 14 luxury women's watches at the home of K's wife.
- Cars – 29 cars were seized from the car dealership jointly owned by K and his wife.
- Cash – Police seized 6 million Thai baht (~USD$185,000) in cash from members of the network.
- Land – Members of K's ring owned as many as 24 plots of land.

5.26 Drug Related

THAILAND

386 AMLO received a STR detailing transactions conducted by Ms. S, mistress of Mr. P, involving numerous cash deposits and withdrawals amounting to 1-1.9 million Baht (~USD30,000 to ~47,000). Ms. S only took small denomination banknotes to avoid reporting to the AMLO. As a result of an investigation by the AMLO, it was found that the couple held 70 accounts at various banks. Mr. P had a record of drug involvement while Ms. S had no such record. AMLO disseminated the financial analysis report to the Narcotics Suppression Bureau (NSB) of the Royal Thai Police for further action.

387 The NSB conducted an investigation and found that the couple were involved in drug trafficking and had direct contact with the WA (a minority group in Thailand). The NSB organised a bait purchase of 74 kilograms of heroin and were able to arrest the couple together with 3 other

people. The NSB confiscated 74 kilograms of heroin, Thai currency worth ~ USD455,590 in Baht, a total of USD114,251 and bank accounts worth ~ USD360,175. AMLO officials, NSB officials and officials of ONCB searched 13 houses of people believed to have acted for the disposal of the couple's drug proceeds and found ~ USD215,835 worth of cash and 9 bank books worth USD1.15 million and a number of vehicles.

6. USEFUL LINKS

Basel Institute of Governance

388 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)

389 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 organisations, and states;
- communities, police, and governments;
- researchers, practitioners, and policymakers; and
- survivors of terrorism around the world.

390 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

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

Global Financial Integrity

392 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 Organisation (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

國際金融業務(OBU)

N 公司設立登記於薩摩亞，且無營業活動。A 君係 N 公司之經理人，並以該公司名義於台灣 A 銀行 OBU 開立帳戶。該帳戶經由 B 君轉介為國際詐騙集團所用。2015 年 1 月該國際詐騙集團人員偽裝為瑞士 U 公司經理人，並發送 EMAIL 至瑞士 S 銀行，指示 S 銀行自 U 公司帳戶匯出 1,121,790 美元至 N 公司台灣帳戶；惟該指示交易經 S 銀行辨識為假造文件。

2015 年 1 月，B 君指示 A 君自 N 公司台灣 A 銀行帳戶匯出部分款項至香港特定帳戶，惟 A 銀行因獲海外情資得知該筆資金涉嫌詐騙，爰拒絕交易。A 君為隱匿犯罪所得，遂將款項轉至其所控制之人頭外幣帳戶，其中部分款項轉換為新台幣並存入新台幣帳戶。2015 年 2 月，A 君指示友人自其上開新台幣帳戶提現三百萬元。B 君及 A 君皆被控告違反刑法及洗錢防制法。

虛擬貨幣(Virtual Currencies)

<u>案例 1</u>

銀行監控發現紐西蘭 A 君一個月內自海外購買 6 次比特幣，再出售予第 3 人，獲利頗佳，惟未申報所得稅。A 君係擔任比特幣交易之「中間人」，將所購比特幣轉入其電子錢包；出售時，係將比特幣電子錢包轉至第 3 人電子錢包，第 3 人再將款項匯入 A 君銀行帳戶。2012 年~2013 年間，A 君銀行帳戶存款大幅增加，多數款項係來自比特幣之相關交易。比特幣電子錢包具隱匿特性，常為毒品犯所用。將款項匯入 A 君帳戶及購買比特幣者多涉有毒品交易紀錄，或涉有刑事 (詐騙或勒索) 案。

<u>案例 2</u>

紐西蘭 B 君有從事駭客紀錄，且因涉駭侵他人電腦勒索案而受調查。B 君以其個人銀行帳戶經營比特幣買賣，且其帳戶曾涉詐騙案而受銀行關注。B 君以銀行支票方式將款項於不同時間分散存入不同銀行帳戶。過去一年內交易紀錄顯示，其比特幣交易有顯著成長，且存款存出入之金額與比特幣交易金額相當，顯示該帳戶被作為洗錢之管道。經查該銀行計有 655 個存款帳戶從事比特幣交

易，其中 13%涉有非法毒品案。

案例 3

運用比特幣犯罪者多屬年輕、鮮有犯罪紀錄，以非傳統犯罪方式作案，作案次數多且不易被偵測。紐西蘭 C 君係未滿 20 歲學生，C 君以其「絲路網站」比特幣帳戶購買管制藥品，另以日本比特幣交易所之比特幣帳戶從事紐西蘭幣與美金之換匯。C 君於紐西蘭多家銀行開有存款帳戶，渠等帳戶除獎助學金及少數季節性薪資外，其餘款項皆為非法款項，其中不乏鉅額現金存款及匯入款。當銀行質疑其存入款項來源時，C 君概以代同學買賣電腦為藉口，惟經查 C 君並無買賣電腦之事實。

專業服務(Professional services)

Y 公司於 2014 年 2 月於台北 T 銀行開立一存款帳戶，嗣有一千萬台幣匯入該帳戶，旋即 Y 公司派員工將款項全數以現金提領，爰 T 銀行向調查局申報可疑交易。嗣經調查局調查，Y 公司涉嫌投資詐騙案。Y 公司以每單位 50 萬台幣，期間 3 個月，利率 15%誆騙民眾投資。為延後投資人取回本利，該公司續以其他形式合約及更高利率誘使投資人展延投資本金到期日。迄 2013 年 6 月，該詐騙集團共騙 4,000 位投資人，吸金達 23 億台幣。

貿易洗錢

案例 1

斐濟調查局(FIU)由 STR 發現，當地 Z 公司於 2014 年 1 月~2015 年 12 月間匯 3.3 百萬美元予紐西蘭 A 公司及中國 V 公司。經查 A 公司已於 2014 年 7 月向紐西蘭主管機關註銷公司登記，FIU 發現中國人 Q 君於 2009 年任職 A 公司之經理人，並於 2015 年有走私現金及涉嫌洗錢等情形，另 Q 君於紐西蘭亦有不良旅遊紀錄。斐濟 FIU 發現 A 公司與 Z 公司之間並無明顯貿易關係或進出口紀錄，惟 Z 公司匯 1.93 百萬美元予 A 公司。

案例 2

斐濟 X 君及外國人 Y 君利用斐濟人頭 Z 君於斐濟設立 A 公司(建築公司)，X 君及 Y 君於 2015 年 12 月~2016 年 3 月間透過澳洲三家金融機構匯款予 Z 君。斐濟 FIU 及海關發現澳洲 B 公司出口 2 部挖土機予 Z 君，且挖土機之發票價格可能有低估情形；另 FIU 發現該 2 部挖士機事實上係為 A 公司所用。FIU 發現 A 公司之設立登記時點，係在挖土機進口及價金交付之後。

地下匯款

案例 1

印尼工人在 X 國工作，並透過 X 國之 PT 匯款公司將錢匯至印尼家人帳戶；惟 PT 匯款公司並非將款項直接匯至印尼工之家人，PT 匯款公司之負責人 SM 君，以電話指示印尼 AH 君於印尼開立一存款帳戶，作為轉匯小額款項予印尼工人之家人之用。惟查 AH 君之印尼帳戶匯入之款項並非來自 PT 匯款公司，而是印尼當地毒品犯罪集團帳戶，而 AH 君帳戶成為毒品犯罪集團之洗錢管道。

案例 2

台灣 J 公司係一服飾業貿易商，而台灣服飾業對跨境匯款有高度需求，惟銀行體系之跨境匯款不僅手續費昂貴且耗時。爰 J 公司負責人 C 君於 2010 年起開始經營兩岸地下匯款，可同時賺取匯差及手續費。為避人耳目，C 君要求其員工至銀行開立人頭帳戶供其辦理地下匯款。2010~2016 年間 J 公司共處理 831 百萬美元之地下匯款。

新式支付方法洗錢

2016 年 4 月台灣調查局於北台灣某民宅內逮捕 8 名犯罪集團成員，該民宅為犯罪集團之洗錢場所。經查，該集團為另一電信詐騙集團從事洗錢，過程複雜並運用一華人(比特幣、數位資產及支付系統等)線上交易平台。該犯罪集團為詐騙集團保管犯罪所得並規避政府之查緝，自 2016 年 4 月該洗錢據點設置以來，犯罪集團累計洗錢之金額已達數百萬人民幣。

運用家人或第三人帳戶洗錢

E 君係台灣高階公務員，負責採購案之最後決策。2012 年~2015 年間，E 君就某資訊系統採購案收賄 1.2 百萬美元，以確保 W 公司能順利得標。E 君應 W 公司之請求，指示其部屬為 W 公司設定有利之採購條件，並將採購之相關資訊洩漏予 W 公司，並配合 W 公司之要求編列採購預算，最後 W 公司以高於市價之價格得標。W 公司以現金行賄，最後款項流入 E 君之配偶、部屬 G 君及其控制之人頭帳戶。

偽外幣換匯洗錢

台灣 I 君於 2015 年自來源不明處取得 24,500 張百元美金偽鈔，該等偽鈔可通過舊款驗鈔機之檢驗。2016 年 1 月~2 月間，I 君將其中 23,490 張偽鈔以較低匯率價格售予 K 君。K 君再將該批偽鈔轉交 L 君，並要求將偽鈔存入 L 君之公司銀行帳戶。爰 L 君指示其公司會計 M 君將該批偽鈔存入公司外幣帳戶，同日 M 君又將該筆偽鈔美金存款轉換為新台幣，並存入 L 君公司台幣帳戶。最後該次偽鈔美金換匯獲利分別由 K 君、L 君及 M 君等人取得。

匯款至人頭帳戶洗錢

N 君係台灣 T 公司外籍經理人，負責 T 公司之「M 網站」行銷業務。「M 網站」主要以線上遊戲進行銷售虛擬貨幣。為吸引投資人，2013 年 3 月起 N 君與數位台灣同夥運用線上廣告或舉辦說明會宣傳其投資計畫。渠等以複雜計算公式誤導投資人可以獲利。投資人支付投資款項後，即可獲得電子帳戶，用以購買或贖回「M 網站」銷售之虛擬貨幣。惟投資之款項中，10%為交易手續費、30%為強制購買虛擬貨幣數額，5%為電子交換點數，餘 55%投資人始可自由運用。為提高虛擬貨幣價值，N 君設計各式酬勞辦法鼓勵投資人介紹新成員參加投資虛擬貨幣。2012 年 8 月~2016 年 8 月間，投資累計總額逾 98 百萬美元。為規避司法偵查，N 君將 9.88 百萬美元款項匯入其所控制之人頭帳戶，或藏匿於辦公室之活動式天花板內。