APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2018

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

July 2018

APG Yearly Typologies Report 2018

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 and trends 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 undertakes typologies work in coordination with the FATF and other partners in the global AML/CFT network. This includes joint projects and coordinating the sequencing of projects on regional and global priority areas.

3 Publication of an APG Yearly Typologies Report is provided for under the APG's Strategic Plan and the APG Operations Committee terms of reference and includes observations on ML and TF techniques and methods. APG typologies reports are intended to assist APG members to identify suspicious financial activity. Case studies and indicators in this report will assist financial institutions and non-financial businesses and professions (casinos, accountants, lawyers, trust and company service providers, real estate agents, etc) to detect and combat ML and TF.

4 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 a network of typology experts involved in APG typologies work.

5 The case studies featured in this report are only a small part of the work in 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/judicial processes. This report contains a selection of illustrative cases of various typologies gathered from APG members' reports as well as open sources. Some of the cases included in this report took place in previous years but the summary information has only been released this year.

Typologies in 2017-2018

6 The APG conducts its typologies work through the APG Operations Committee (previously the Typologies Working Group), which is currently co-chaired by India and New Zealand.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2017 - 2018

1 This section of the report provides a brief overview of typologies related work undertaken by the APG between July 2017 and June 2018.

1.1 APG's current and possible upcoming typologies projects

APG/MENAFATF Joint Project on Terrorist Financing and Social Media

2 The APG / Middle East & North Africa Financial Action Task Force (MENAFATF) joint project on TF and Social Media is co-chaired by Malaysia and Egypt. The project has arisen due to recent observations that social media provides TF vulnerabilities, including 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. A report has now been drafted and the project is scheduled to conclude in July 2018.

Money Laundering and Terrorism Financing Risks Arising from Trafficking in and Smuggling of Human Beings

3 Human trafficking is estimated to generate approximately US$150 billion in proceeds for criminal groups. People smuggling also generates very large proceeds of crime and continues to be a global and regional challenge. The APG project has two-phases, as below:

a) *Phase 1* – a joint FATF/APG project focused on human trafficking which concludes in June 2018; and
b) *Phase 2* – an APG regional project that builds on the FATF/APG human trafficking project and considers implementation support for measures to manage both human trafficking and people smuggling.

Risks and Vulnerabilities of Trans-Pacific Drug Routes

4 This is an on-going project co-led by Tonga and Vanuatu. The project is due for completion in December 2018.

APG/EAG Terrorism Financing & Proceeds of Crime (including Organised Crime)

5 The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) and the APG will undertake a joint project on *Terrorism Financing & Proceeds of Crime (including Organised Crime)* which will focus on the techniques and trends associated with the use of proceeds of crime, including from organised crime, for TF.

6 The project will include contributions and comments from EAG and APG members and interested observers, with a jurisdiction from each regional group co-leading the project. The Russian Federation will lead the project from EAG, with an APG co-lead yet to be determined. The EAG and APG secretariats will coordinate the project.

7 The project will include:

a) An information collection phase that will involve questionnaires to obtain case studies, typologies and best practices; and sessions at the joint EAG/APG Typologies Workshop (December 2018) to share case studies;

b) a report to be developed which includes case studies, typologies, guidelines and recommendations on the project for further consideration.

1.2 2017 APG/FATF TREIN Joint Typologies and Capacity Building 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 agencies 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. These events:

- Bring together the APG community of practitioners to share experiences and foster networks of cooperation;
- Support research being undertaken by the APG Operations Committee;
- Facilitate APG members to contribute to typologies projects led by FATF and FSRBs;
- Share best practices and strategies for practical application of AML/CFT measures;
- Expand partnerships between the public and private sectors and the academic research sector 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.

9 The 2017 APG/FATF TREIN Joint Typologies and Capacity Building Workshop was held in Busan, Republic of Korea from 13 and 16 November 2017 and hosted by the FATF Training and Research Institute (FATF TREIN). The workshop involved over 200 delegates including members from the private sector, non-government organisations and civil society. The workshop was co-chaired by India and FATF TREIN.

10 The workshop included a plenary session and three two-day sessions on; (i) ML associated with human trafficking and people smuggling; (ii) proliferation financing; and (iii) investigating and prosecuting internet facilitated ML and TF.

11 The typologies workshop included presentations on social media and TF; and on the recently published APG/UNODC report on: "*Continuing to enhance the detection, investigation and disruption of illicit financial flows from wildlife crime in the APG region"*.

12 The following common themes, needs and recommendations were identified through the course of the workshop:

- Human trafficking generates enormous proceeds of crime, but receives few fewer AML enforcement responses than many other crimes generating comparable proceeds of crime;
- Development of effective and useful red flag indicators will assist both government and the private sector;
- Partnerships between governments, the private and civil society sectors, research institutes and non-government organisations are critical to better target enforcement of financial aspects of human trafficking;
- Many jurisdictions face challenges in identifying and assessing the risks in their jurisdiction from human trafficking and related ML;
- ML risk mitigation needs to better reflect and respond to the identified human trafficking and ML context.

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

13 This section of the report provides a brief overview of typology reports published by FATF and other FSRBs between July 2017 and June 2018.

2.1 FATF typology projects

Inter-agency CT/CFT Information Sharing: Good Practices & Practical Tools (non-public)

14 The effective sharing of information and intelligence between agencies at a domestic level is critical to the fight against terrorism and TF. Enhancing the appropriate inter-agency sharing of counter terrorism (CT) and CFT information and related intelligence products is a priority for FATF and FSRB (including APG) Members.

15 This report seeks to:

- inform both policy makers and operational experts on the key operational authorities involved in the domestic CT/CFT framework, as well as the relevant information collected by such authorities;
- set out the challenges that these authorities often face when sharing this information; and
- highlight examples of practical tools and good practices implemented on a domestic level to overcome identified challenges for the purposes of combating terrorism and TF.

16 This report highlights that effective, timely inter-agency information sharing is essential to cut the financial flows to and from terrorist(s), terrorist organisations, terrorist financiers and sympathisers and facilitation networks. Furthermore, it also points out that effective inter-agency information sharing of CT/CFT information has positive spill-over effects for effective international information sharing, given that information sharing at an international level is predicated on the availability and access of relevant information at a domestic level.

17 While the domestic information sharing framework may vary from one jurisdiction to another, identifying challenges, practical tools and good practices has the added value of identifying how agencies have effectively adapted their domestic legal and administrative frameworks to facilitate inter-agency information sharing for CT/CFT purposes.

18 APG members interested in obtaining this report should contact the APG Secretariat.

ISIL and Al-Qaeda and Affiliates Financing Updates (October 2017) – non-public

19 In February 2015, the FATF published a comprehensive report on the Financing of the Islamic State in Iraq and the Levant (ISIL). Since that time, the FATF has been producing regular, non-public updates three times per year, based on voluntary contributions. These updates also cover Al-Qaeda, and ISIL and Al-Qaeda affiliates. APG members interested in obtaining these updates should contact the APG Secretariat.

Financing of Recruitment for Terrorist Purposes

20 Recruiting members and supporters is crucial to a terrorist organisation's survival. Each terrorist organisation has different recruitment techniques, depending on whether it is a large or small organisation, or a dispersed network of individuals.

21 Using input collected from authorities within the FATF Global Network, this report increases understanding of terrorist organisations' funding needs to recruit members and supporters. In some

cases, these funding needs are minimal. In other cases, where recruitment networks are involved and connected to facilitation networks, the value of financial intelligence and investigations could be significant.

22 This report identifies the most common methods of recruitment used by terrorist organisations and terrorist cells, and the costs associated with these different methods and techniques of terrorist recruitment:

- Personal needs of the recruiter and the maintenance of basic infrastructure for the recruitment/ facilitation network
- Production and dissemination of recruitment materials
- Payment for goods and services to facilitate the new recruits' early participation in the terrorist organisation, and
- Financial incentives provided directly to recruits or for the hiring of mercenaries or civil experts.

23 This report sheds a light on how terrorist organisations fund the recruitment of new members and supporters. It will also provide LEAs, FIUs, and other operational and security agencies with the opportunity to disrupt terrorist recruitment from the onset and prevent additional individuals from joining terrorist groups.

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

Unified financial profile of FTFs in the EAG region

24 The purpose of this project is to summarize the EAG members' experiences in identifying typologies of financing foreign terrorist fighters (FTFs), in order to highlight the specific characteristics of persons and their accomplices who may be supporters of international terrorist organizations, including ISIL, or be FTFs themselves. The study's focus on the financial behaviour of potential FTFs is designed to aid reporting entities in identifying such behaviour and minimizing threats to EAG member states.

25 The report is intended to support FIUs of the EAG member–states, jointly with the private sector, and includes special indicators that will allow credit institutions and other national AML/CFT stakeholders to detect suspicious transactions related to terrorism.

Money Laundering through Insurance Companies

26 The project is co-led by China and Russia and looks at various measures to combat ML in the insurance sector, including risk characteristics and red flag indicators of suspicious transactions, common challenges and obstacles, as well as typical case studies. The report would consist of the information from many public and private sector bodies, including supervisory authorities, FIUs, LEAs and others. The report is to be adopted in November 2018.

Identification of Individuals Assisting Terrorist Organizations

27 The practice of the financial intelligence units shows that one of the typologies of assistance to terrorists is the purchase of air tickets in the interests of third parties.

28 Information on the facts of the acquisition of air tickets can be obtained from credit organizations, information on passengers is contained in databases of government agencies, but these registers are not being synchronised.

29 The objective of this research is to accumulate the experience of countries in building the systems of control over the purchase of air tickets for the benefit of third parties, as well as determine the most effective mechanisms allowing the accumulation of information about buyers of air tickets, passengers using these tickets, and the comparison of these registers.

Cross-border drug trafficking & legalization of drug proceeds - electronic payment tools & cryptocurrency

30 Experience of drug enforcement agencies has identified that drug traffickers closely monitor and make use of a broad range of continuously upgraded electronic financial services. Modern online asset management technologies are exploited by criminals to disguise their illegal activities and also enable them to convert and keep criminal proceeds by separating such proceeds from their criminal origin in order to avoid prosecution and punishment.

31 Practice shows that the wide availability and accessibility of electronic means of payment and imperfection of the regulation pertaining to identification of customers of international electronic payment systems impede detection of drug-related crimes and identification of the entire chain of offenders, which, in turn, prevents execution of justice and allows organized drug trafficking groups to build up their "criminal" capacities.

32 The research team will summarize and analyse information available to the LEAs and FIUs on the criminal methods used and the national models utilized for regulation of the electronic payment sector and crypto-currencies.

33 The results of the proposed research project may become the information platform for the development of initiatives aimed at harmonization of the relevant legislation of the EAG member jurisdictions for improving the illegal financial transactions curbing mechanisms as well as for potential development of the action plan for LEAs and FIUs.

3. TRENDS IN MONEY LAUNDERING AND TERRORISM FINANCING

34 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

BRUNEI DARUSSALAM

35 Brunei Darussalam's recent research on ML/TF methods and trends found trends in STRs received in 2017. The FIU noted the following re basis for suspicion:

- Involves personal or joint accounts (individuals, not companies).
- Account turnover (debit/credit) is more than the expected income of the individual(s).
- Multiple inward/outward fund transfers with no clear purpose.
- Transactions of similar amounts or a similar range of amounts.
- Involvement of online purchases or wire transfers.

JAPAN

36 JAFIC published a risk assessment which indicated the extent of risk in each category of transactions carried out by a business operator was published on the Japan Financial Intelligence Centre (JAFIC) website (Japan's FIU). The JAFIC Annual Report includes AML/CFT statistics, case studies and trends. The trends reflected in the report include:

- Unregistered money lending business and loan-sharking.
- Concealment and receiving of criminal proceeds obtained through fraud crimes.
- Possession, assignment and/or receipt, or sale or purchase of illegal drugs by use of internet for delivery services.
- Passbook smuggling, fraudulent receipt of welfare benefits and other benefits, and fraud in relation to sale of concert tickets and contracts for cell phones.
- Fraudulent cash withdrawal from ATMs using other persons' cash cards obtained through illegal means and extortion arising out of money loans.
- Sale or purchase of share certificates which change the stock price on the market in violation of the legal framework.

MACAO, CHINA

37 Macao, China's Financial Intelligence Office (GIF) received a total of 1,527 STRs from January to June 2017, with 1,074 STRs from the gaming sector, 414 STRs from the financial sector (including banking, insurance and financial intermediaries) and 39 STRs from other sectors.

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

- Casino chips conversion without / with minimal gambling activities;
- Casino chips conversion / marker redemption on behalf of third parties;
- Irregular large cash withdrawals;
- Attempted but unsuccessful transactions;
- Use of ATM, phone banking, cash deposit machines;

- Suspected underground banking/alternative remittance services;
- Suspicious wire transfers;
- Significant cash deposits with non-verifiable source of funds;
- Currency exchange/cash conversion;
- Unable to provide identification/important personal information.

MALAYSIA

39 Malaysia has prepared its 3rd National Risk Assessment (NRA 2017) which is to be issued by the National Coordination Committee (NCC) to Counter ML in mid-2018. The 3rd NRA focuses on threat and sectoral risk assessments and is based on enhanced and revised data points namely; (a) case studies analysis (b) independent reports produced domestically and internationally (c) statistical data and reports (d) perception survey (e) experts' view and (f) moderation process. The NRA 2017 process also considered overriding macro factors (such as economic, financial, political and sociocultural system, governance level and informal economy) and the inter-connectedness between crimes and sectors. Besides threats and sectoral risk assessments, the revised NRA would also incorporate other risk assessments, conducted independently, namely, Domestic Review and National Risk Assessment (DRRA) on the NPO Sector and Labuan Offshore Risk Assessment (LRA). The NRA 2017 has been concluded by the NCC, and is expected to be tabled for deliberation and endorsement by high level NCC in Q2 2018. Communication to stakeholders including the public will be initiated after sign-off by the high level NCC.

NEW ZEALAND

40 New Zealand published its latest National Risk Assessment (NRA) in March 2018 which is publicly available on New Zealand Police website. The NRA examines key ML threats generated both domestically and internationally and the risk they pose to New Zealand's financial, legal, property and retail sectors:

- *Domestic ML threats*. The major groups of crimes known to generate ML domestically are drugs offending, fraud offending and tax offending.
- *Offshore ML threats.* Three key areas of known threat from offshore to New Zealand are in: (1) transnational organised crime groups linked to New Zealand, such as transnational drug distribution networks; (2) overseas criminal organisations not generally connected to New Zealand who may seek to move funds through New Zealand and/or New Zealand's legal structures; and (3) dedicated ML networks, which may also seek to move funds through the New Zealand's financial system or New Zealand's legal structures.

41 The NRA 2018 assesses the key vulnerabilities to ML in New Zealand. The channels that offer ML opportunities in New Zealand are those financial, legal, accounting, real estate, and dealers of high value commodities that:

- offer anonymity to the offenders;
- are available for moving large values and volumes of legitimate funds and which provide a screen for illicit transactions;
- are widely available internationally and also have poor AML/CFT controls internationally; &
- are cash intensive, which are particularly used to disguise drug proceeds.

42 The NRA 2018 highlights the highest priority observed vulnerabilities for New Zealand:

- International wire transfers, which are electronic transactions to and from other jurisdictions.
- Alternative payment methods: Alternative payment methods for moving value and funds are highly vulnerable to displacement of illicit activity away from regulated sectors. Alternative money remittance, international trade-based transfers, and alternative banking platforms

have each emerged as vulnerabilities. These methods of moving value are also vulnerable to displacement of illicit activity from AML/CFT-supervised sectors.

- New Technology: Misuse via new technology is closely related to the vulnerability to alternative methods of moving value and funds. New Zealand's exposure to new payment technologies, including digital currencies, may not yet be as high as other jurisdictions. Nonetheless, the rapid development of payment technology creates a highly dynamic environment in which vulnerabilities may emerge quickly.
- Gatekeeper professional services: Currently there are low levels of AML/CFT controls of, and reporting by, New Zealand professional services providers (lawyers, accountants, real estate agents). These vulnerabilities are compounded by difficulties in identifying the beneficial owners of New Zealand companies, charities and trusts. The vulnerability also opens ML channels in which professionals may facilitate criminal transactions such as in the real estate sector.
- Cash proceeds: remain the dominant means of transacting for domestic drug crimes. Dealers in high value commodities remain vulnerable to illicit cash proceeds, as is casino gambling.
- Businesses industries: Many business industries are vulnerable to use as fronts for ML. In particular, cash intensive businesses are a common method of establishing an ostensive origin of cash proceeds. This type of ML can have anti-competitive effects with negative consequence for legitimate competitors.
- High value goods: Non-financial assets are also abused at all stages of ML. In particular, high value transportable goods can be used to store wealth or to move value between criminals. Similarly real estate assets are vulnerable to abuse involving large ML transactions.

43 In addition to ML risk, the NRA 2018 assesses terrorism risks. The threat of terrorism in New Zealand is lower than many of our partners. Consequently, there have been no prosecutions or convictions for TF in New Zealand. However, overseas terrorism financers may seek to abuse New Zealand's reputation for low-corruption and high integrity. Further, the consequences for New Zealand's reputation are considerable should overseas terrorist groups:

- Use New Zealand's businesses, companies, payment platforms and charities to support TF, or
- Find local supporters to assist in TF.

44 The NZ-FIU has completed the following other strategic research products:

- Typology Report on Human Trafficking and People Smuggling.
- Typology Report on Virtual Currencies which examined how virtual currency exchanges can facilitate crime, emerging risks associated with virtual currencies, the challenges that come with addressing those risks and the implications for New Zealand Police and reporting entities. It aims to assist with the development and improvement of strategies to detect, prevent and disrupt financial crime.
- Typology Report on The Risk of Gang Members Travelling to Secrecy Jurisdictions: a risk assessment assessing the risks of gang members travelling to secrecy jurisdictions in the Pacific, and the implications for New Zealand from a ML perspective.
- Typology Report on Misuse of Stored Value Cards: a report summarising STR information involving stored value cards received between January 2016 and January 2017. The report describes the various ways in which stored value cards were misused by New Zealand-based criminal entities identifies key vulnerabilities of stored value cards and the risks of permitting the activity to continue.
- Typology Report on Alternative Money Remittance: a strategic report on a complex ML typology being used by organised crime groups to transfer value offshore. The report

identifies gaps in AMLCFT legislation that render it vulnerable to criminal misuse, and identify the risks of permitting the activity to continue.

- Typology Report on Online Gambling: a strategic report on offshore online gambling websites bring used by local drug suppliers/ distributors to launder funds. The report identifies indicators of ML via online gambling, and assesses whether any regulations exist to prevent laundering through online gambling sites.
- Paper on Preventing Organised Crime in New Zealand. The specific focus of this paper is on preventing organised crime at the strategic level, while the emphasis being on proactively addressing emerging organised crime issues and the conditions that facilitate organised criminal activity, rather than the activity itself.

3.2 Association of types of ML or TF with predicate activities

AFGHANISTAN

45 Afghanistan has highlighted the association of types of ML or TF with particular predicate activities related to terrorist organisations and the smuggling of drugs. Cases reflecting this association are set out below:

Supporting a Terrorism Organisation

46 Subject A, a resident of Konar Province, was accused of being a member of the Taliban (UNSCR 1267/1998) and of TF and was arrested in May 2016 in Pacheer Agaam district of Nangarhar Province, Afghanistan. During the investigation, it was revealed that the suspect was carrying the payroll sheet and distribution sheets for Taliban fighters. He was also carrying two bank cheques valued at PKR 10.3 million (US$88,000). After completion of the prosecution, the case was referred to the Primary Court and the suspect was convicted and received:

- Five and half year's imprisonment and monetary fine of AFN 400,000 (US$ 5,600) for terrorist financing pursuant to the CFT Law;
- 18 months imprisonment for being a member of the Taliban pursuant to the Counter-Terrorism Crimes Law; and
- Confiscation of the assets and instruments.

Drugs Smuggling

47 According to the request for information by the Counter Narcotics Justice Centre (CNJC), subject X was accused of smuggling drugs to jurisdiction A.

48 The subject X was caught and arrested by law enforcement officials at Kabul International Airport while carrying drugs inside his abdomen. Also, two bank account cards related to two commercial banks were found during the physical body search of the subject. The drug smuggling case was forwarded to CNJC for prosecution.

BANGLADESH

49 BFIU received a complaint from Ministry of Finance (MoF) against Mr. X who was suspected to be involved in TF and anti-government activities. After receiving the complaint, BFIU collected his account information from the concerned bank. It was found that Mr. X received funds from seven different persons of a foreign jurisdiction (ABC) during 2012-2013 amounting to USD 58,672.

50 In order to further analyse the case, BFIU took the initiative to establish a relationship between remittance senders and receivers. For this reason and analytical purposes, BFIU collected information from the FIU of the concerned foreign jurisdiction. ABC FIU informed that it received an

STR on one of the seven different persons named Mr. Y who was mentioned in the STR as a sender of money to Mr. X several times via Western Union. According to an open source, the ABC FIU also found that Mr. Y is a member of a humanitarian foundation based in the capital of the ABC. The mentioned foundation carries out humanitarian relief activities and cooperates with 45 national and 32 international non-governmental organizations (NGOs). Money was observed to be deposited in the account of Mr. X from different areas of the jurisdiction and withdrawn in cash via ATMs.

51 Based on the finding BFIU prepared an analysis report and sent it to LEA of Bangladesh Police. Based on the report LEA arrested Mr. X for being involved in TF and anti-government activities and a case has been lodged against Mr. X under the ATA 2009, 7(a).

HONG KONG, CHINA

Case Study 1

52 Upon investigating a smuggling syndicate, Hong Kong Customs found that the syndicate had employed general merchandise operators ("GMOs") to carry large quantities of cash, which were suspected to be generated from the smuggling offence, from Mainland China into Hong Kong, China and subsequently deposited into a local bank account. After an in-depth investigation, Hong Kong Customs identified eight local residents and mounted arrest operations in 2015. Investigation findings revealed that, between 2011 and 2012, these eight persons had carried into Hong Kong, China significant amounts of cash from Mainland China. They then either deposited them, in HK$100,000 (US$12,800) to HK$400,000 (US$51,000) each time, at different bank branches; or arranged transfers, in HK$5,000 (US$641) to HK$500,000 (US$64,105) each time, through their personal bank accounts to the same bank account controlled by the syndicate, to earn a reward ranging from HK$20 to HK$100 for each transaction. During this period, the total amount laundered was HK$54 million (US$6.9 mill).

53 Eventually, they were all convicted for conspiracy of ML in 2017 and sentenced to 12 - 48 months' imprisonment.

Case Study 2

54 In early 2013, Hong Kong Customs conducted a joint investigation with the Customs authority of Mainland China against a syndicate involved in exporting luxury left-hand drive vehicles from Hong Kong, China to Vietnam and then smuggling them into Mainland China, as well as laundering the criminal proceeds from Mainland China into Hong Kong, China in circuitous ways.

55 The buyers made the payments for the vehicles into bank accounts in Mainland China held by the mastermind who then arranged the transfer the funds to bank accounts in Mainland China held by a Hong Kong, China money service operator (MSO). The mastermind ultimately arranged to collect the monies from the MSO, mainly in cash, in Hong Kong, China (i.e. the criminal proceeds generated from the smuggling activities). The total amount laundered was HK$59 million (US$7.5 million).

56 In September 2013, Hong Kong Customs arrested the mastermind, who was eventually convicted of ML in 2018 and sentenced to five years' imprisonment.

JAPAN

57 Japan has highlighted the association of types of ML or TF with particular predicate activities such as drugs and fraud reflected in the following cases:

Money Laundering and fraud Cases related to 'Japanese violent groups'

58 A number of ML and fraud cases have been conducted by Japanese violent groups a.k.a. *Boryokudan* (including Boryokudan members, associates, and other related parties). Criminals were

obtaining criminal proceeds (proceeds derived from selling stolen items under false names) by lending money in exchange for its repayment at an interest rate that exceeds the percentage approved by law, and using intimidating methods or threats of force in order to obtain repayment (loan-sharking). The proceeds of loan-sharking were concealed in a bank account opened in another party's name.

Concealment of drug-related criminal proceeds related to trafficking of stimulants

59 A man, who was engaging in the trafficking of stimulants, sold stimulants by using a home delivery service and arranged for customers to remit a total of approximately 1.2 million yen (US$11,000) in payment to an account opened in the name of another person. He was arrested for violation of the Anti-Drug Special Provisions Act (concealment of drug-related criminal proceeds).

Fraud and Money Laundering Cases

60 Recently, specialized fraud cases are often reported in Japan. For example, some people sell their own bank accounts to cover amusement expenses or cost of living, while others establish bank accounts in the name of fictitious persons or another party by using a falsified ID card and then on selling them to criminals who will use those accounts to facilitate ML activities.

MACAO, CHINA

61 From January to June 2017, 79 STRs were disseminated to the Public Prosecutions Office. These cases were mainly related to fraud. The Judiciary Police processed 74 cases as investigations.

MALAYSIA

62 ML investigations focused on high risk crimes identified in the NRA, namely drugs, corruption, fraud, smuggling and tax evasion. Priority was given in cases where there is an element of organized/syndicated crimes. Investigations into terrorism have also been extended for any TF element.

PAKISTAN

Corruption

63 The individual had purchased a high volume of foreign currency from ABC Exchange Company without disclosing his true occupation/source of funds. During the analysis it was found that he was retired from a senior level position in a government organization, and as per media news he was involved in corruption during his service. He maintained multiple joint accounts with family members at Alpha Bank, whereby a high value of funds were credited in all accounts during a specific period.

64 The statement of accounts revealed that these funds were invested in term deposits for a period of one year. On realization of term deposits, the funds were withdrawn from the account through cash/ clearing and were followed by the purchase of foreign currency from the open market. The suspect deliberately structured the currency exchange transactions to purchase foreign currency through cash in order to break the trail of funds.

65 Keeping in view the pattern of transactions and adverse media news on suspect, it was probable that he remained involved in corruption/bribery and the source of funds involved in bank accounts and subsequent currency exchange transactions was suspected. Therefore, the intelligence was shared with LEAs.

Smuggling

66 Two individuals Mr. X and his father Mr. Y opened individual and joint accounts in different branches of different banks. They were engaged in the business of cloth and carpets. These accounts were reported by A, B and C banks to FMU as high volumes of funds and unusual patterns of transactions were observed in the accounts by the reporting banks.

67 During analysis, it was noted that a high volume of funds were deposited in suspects' accounts through cheques and the same amount were then withdrawn immediately through cash transactions not exceeding the CTR threshold to avoid the transactions being reported to the FIU.

68 Mr. X and Mr. Y were making transactions through online transfers to each other and to/from individuals engaged in the business of cloth and related fields. Few of the accounts of suspects were also identified through search in FMU's internal database wherein a similar pattern of transactions was noticed in these accounts. Interestingly, the suspects were not found registered for national tax numbers despite the fact that they were making high value transactions in their respective accounts as they wanted to keep the nature of business undisclosed to tax authorities and also evade taxation.

69 The financial intelligence was disseminated to LEAs under the suspected offences of smuggling and tax evasion.

THAILAND

70 Thailand has reflected the association of types of ML or TF with particular predicate activities including corruption, drugs, fraud and cash smuggling highlighted in the following cases:

Drugs trafficking

71 Mr. J, a Netherlands national, and associates, engaged in drug trafficking, a transnational organized crime. The Office of Attorney General (OAG) received a request from the Netherlands and referred it to the Anti-Money Laundering Office (AMLO) for urgent asset seizure/freezing action against Mr. J and his associates without a willingness to reclaim the assets and with consent for the assets to be forfeited to the state. A joint task force was formed between OAG, Department of Special Investigation (DSI), the drug police and AMLO. The competent officer took swift action to seize/freeze more than 100 million THB (approx. USD 3 million) worth of assets under section 48 of Anti-Money Laundering Act. Evidence was found for probable grounds to believe that the assets had been obtained by Mr. J and associates during engagement in an activity constituting a drug offence.

Corruption

72 The Crime Suppression Bureau and the Royal Thai Police (RTP), requested AMLO to examine and conduct financial analysis as well as to restrain the financial transactions of Mr. T, Ms. U, and their associates (ex- government officials). The criminals misappropriated money of a state education institution and were charged with theft, falsifying and using forged documents and malfeasance in office. The Transaction Committee ordered seizure and restraint of the assets of Mr. T and his associates. The Transaction Committee also requested the AMLO to submit the case to the public prosecutor for filing a petition to the court for a court order that stated that the asset connected with the commission of the offence return or compensate the damaged person in amount of 271.08 million THB (US$8.5 mill). The case is under civil court process.

Companies in public fraud and cash smuggling

73 AMLO along with RTP initiated legal proceedings against a group of companies and its executives including its secondary parties on charges of public fraud. The company was registered as a multi-level marketing company with three products. These products had never been produced or

sold but the company offered payments and rewards at a much higher interest rate than the rate prescribed by the Bank of Thailand for the members who recruited others to join their network.

74 One of the major shareholders, a Malaysian national, had fled to Thailand after being wanted in Malaysia. He had undergone plastic surgery to change his appearance and had illegally obtained a dead Thai man's identity in order to run businesses in Thailand.

75 There are more than 120,000 members found in one record with the estimated cash flow of approximately 38 billion THB (USD 1.073 billion). However, the number of its Thai members can be as high as 300,000 members with an estimated loss of 100 billion THB (USD 2.824 billion). The funds received from the members were shared directly with the major shareholders' bank account (except the nominees).

76 Each of the arrested shareholders have been found to keep their cash at home instead of depositing into a bank account, and had used cash to purchase luxury vehicles, mansions and expensive items.

77 Four couriers, who were accused of bulk cash smuggling from Thailand to Malaysia, were arrested. Each of the couriers confessed that they were hired to open a bank account in Padang Besar, a border district on Thai-Malaysian border, in order to withdraw and carry the cash across the border to Malaysia for a person in the fraud company. One courier confessed that he carried more than 300 million THB (USD 10 million) in cash for the company.

3.3 Emerging and continuing trends

BRUNEI DARUSSALAM

78 Brunei Darussalam observed that fraud (scams) is a continuing trend among predicate offences in 2017. Types of scams identified feature investment scams prominently and to a lesser extent, romance scams and other forms of get-rich-quick schemes.

79 The FIU has observed a growth in activity involving unregulated online gaming sites since 2016. The combination of ease in transferring funds and the uninhibited access to such sites have allowed these activities to continue.

FIJI

80 Fiji notes an emerging trend of fake bank statements and employment letters. The Fiji FIU noticed an increase in the number of cases involving the use of fake bank statements and employment letters to obtain loans at various financial institutions. The Fiji FIU received 15 reports from various financial institutions claiming that more than 30 individuals applied for unsecured personal loans using falsified bank statements and fake employment letters.

81 The Fiji FIU also received reports that individuals had falsified bank telegraphic transfer forms to fraudulently obtain goods from overseas suppliers and clients.

Emerging Trend: Cheque Washing

82 Fiji notes an emerging trend of 'cheque washing'. The Fiji FIU has seen an increase in the number of cases of "cheque-washing" to purchase items at various retailers. Individuals have purchased bank cheques for small amounts and have 'washed' the bank cheques to amend the amount and payee field to purchase alcohol and meat in bulk amounts.

83 The retailers were not aware that the bank cheques were fraudulently altered until they deposited them into their bank accounts. In some cases, the items were sold to other retailers at a discount to obtain cash.

84 Fiji notes a continuing trend of ATM skimming. The Fiji FIU continues to see foreign nationals entering Fiji and withdrawing funds using stolen credit cards. These individuals have been observed to enter Fiji with skimming devices and use blank cards (that contain stolen credit card information) to make multiple withdrawals at various ATMs across the jurisdiction. On 8 December 2017, three Bulgarian nationals were sentenced to one year imprisonment for possession of a skimming device and unauthorized access to restricted data. On 8 January 2018, two Cyprus nationals were charged with 293 counts of ML and attempt to obtain property by deception in Fiji. The case is still before the Fijian courts.

85 Fiji notes a continuing trend of business email interceptions. The Fiji FIU received STRs on six entities who were victims of business payment intercept scams in 2017. The total value of funds lost amounted to approx. FJ$639,106. The funds were sent to Australia, U.S, Canada and Korea. The Fiji FIU issued case dissemination reports to its overseas counterparts to trace the ultimate beneficiary and explore avenues to recover the funds. In most cases, it was too difficult to do so.

86 The Fiji FIU continues to increase awareness of email-related scams. See this link

JAPAN

87 Instances of concealment of criminal proceeds in 2016 consisted largely of cases in which offenders attempted to transfer funds to bank accounts under the name of other persons. This is a common method used in ML crimes in Japan.

88 In addition, criminals use various methods to frustrate investigative authorities from following money trails, including selling stolen items using a false name, disguising reasons with respect to acquiring criminal proceeds, and more.

LAO PDR

89 Drug trafficking is continuing to be a ML/TF trend, particularly when considering the increase in conducting this predict offence each year, freezing, seizing and confiscating related assets, as well as the increase in sanctioning drug dealers in Lao PDR.

MACAO, CHINA

90 Macao, China notes an emerging trend of frauds in remittance. Analysis of STRs received shows rising frauds in remittance, which have been warranted the banking industry's specific attention in the past few months. Typically, a local bank account receives overseas remittances which are then immediately remitted to other jurisdictions. The beneficiary bank later receives a telegraph from the ordering bank, or an email from the victim claiming the relevant remittances are related to fraudulent acts.

MALAYSIA

91 A substantial increase in STR 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.

92 Malaysia notes the following continuing trends:

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

- Using third party accounts including mule account holders, to receive and transfer illegal proceeds of criminal activities.
- Collection of funds for terrorism activities mostly for the financing of foreign terrorist fighters (FTF) rather than financing of the terrorist groups themselves.
- The funds for FTFs are solicited via social media.
- Using third party accounts (including mule accounts) to receive or transfer to FTFs.

PAKISTAN

93 Pakistan notes the following:

- *Emerging Trend:* virtual currency related STRs.
- *Continuing Trend:* Hawala/Hundi related STRs received in the year of 2017.

THAILAND

94 Thailand notes an emerging trend with Fintech and crypto currencies are used as a channel for the commission of crimes. TBML is increasing particularly related to drugs trade gangs.

95 Thailand notes the continuing use of offshore banks, third party ML/ nominees and underground banking.

4. A FOCUS ON INTERNET FACILITATED MONEY LAUNDERING AND TERRORISM FINANCING: CYBER-LAUNDERING

96 The use of technology to enable financial crime has grown steadily over the past 10 years. This is in line with advancements in the variety and accessibility of available Information and communications technologies (ICT) such as the internet and social media technology and related financial platforms.

97 Internet-facilitated ML/TF can be broadly understood as two issues: the use of the internet to conduct predicate offences (Cybercrime) and the use of the internet to launder proceeds of crime or fund terrorist acts (Cyber-laundering).

98 Cybercrime is an evolving area of crime. Criminals in the field of cybercrime are utilising the anonymity, speed, and convenience of the internet to commit a variety of illicit activities that do not recognize physical or virtual borders, pose real threats to victims globally and cause severe harm, such as conducting unauthorised removal of funds from bank accounts, payments card fraud and others.

99 The APG 2018 Typologies Report includes a focus on understanding emerging risks, trends and contextual issues associated with cybercrimes and laundering the illegal proceeds cyber-laundering.

4.1 Scope of cybercrime in the Asia/Pacific region

100 Cyber fraud is a particularly prevalent threat in the region. A recent survey published in 2017[1] found that the Asia Pacific Region is increasingly targeted by fraud with a 35 percent growth in cybercrime year-on-year, focusing on account takeovers and payment fraud.

101 The report also indicated that cybercrime has increased across the globe nearly 100 percent since late 2015. The main driver is the increase of new account origination fraud, which has risen 30 percent since late 2017.

4.2 FATF initiatives on combating ML, TF & PF and cybercrime

102 The FATF standards include a wide range of tools relevant to combating cybercrime. In particular the criminalisation of ML and TF covers many of the categories of offences which may be applied to various aspects of combating cybercrime.

- Terrorism financing (including terrorism): TF may take place over the internet and social media as supporters seek to provide funds to terrorists and terrorist organisations located overseas. Please refer to the Joint APG/MENFATF typologies report on social media and terrorism financing.
- Sexual exploitation (including sexual exploitation of children): The sexual exploitation of children may include the production, dissemination and distribution of child exploitation material online which generate proceeds of crime, worth billions of dollars each year. The use of ICT for this commercial sexual exploitation of children can increase potential profits for offenders as they have a lower cost to producing and distributing the material, as well as

[1] ThreatMetrix – a LexisNexis Risk Solutions Company, *Asia Pacific Cyberattacks up 35% Year on Year, As Global Organized Fraud Rings Turn Their Attention to Emerging Financial Services*, (2017).

access to a larger potential customer base online.[2] Improvements in internet speeds and access to mobile devices has also resulted in an increase in child sexual abuse that is live streamed to viewers at a fee, and may also then be recorded and sold to others.[3]

- Illicit trafficking: The FATF Standards refer to illicit trafficking in narcotic drugs and psychotropic substances, illicit arms trafficking and illicit trafficking in stolen and other goods. Drugs, weapons and stolen goods might also be sold through online marketplaces on the World Wide Web, or more anonymously through the 'dark web'.[4]
- Fraud, identity theft and scams: those have been present on the internet for quite some time and remain a commonly noted issue faced by member jurisdictions.
- Robbery or theft: ICT have also facilitated new forms of robbery and theft.
- Extortion: Extortion may also take place through ICT in a similar fashion to how criminals might extort money from victims offline. ICT have also led to some new methods of extortion, for example, ransomware. Ransomware is a form of malicious software that either locks the device or uses encryption to prevent access to data until a ransom is paid.[5] Ransomware attacks often seek payment in the form of cryptocurrencies[6], such as Bitcoin, to a specific address in order to have their accounts unlocked.[7]

103 Recommendation 36 (of the FATF recommendations) regarding international instruments encourages ratification and implementation of the Convention on Cybercrime, July 2004 (also known as the Budapest Convention on Cybercrime or the Budapest Convention). This Convention is the first international treaty seeking to address internet and computer crime by harmonizing national laws, improving investigative techniques, and increasing cooperation among nations to combat cybercrimes.[8]

104 The FATF also issued a report on the *Money Laundering & Terrorist Financing Vulnerabilities of Commercial Websites and Internet Payment System* (2008). This report highlighted the following:

- Vulnerabilities of commercial websites and internet payment systems are: possible anonymity of the users, limited human intervention, speed of transactions, high number of transactions, non-face-to-face registration, international presence, limited jurisdictional competences, difficulties for traditional financial institutions to monitor and detect suspicious financial transactions with the consequence that their abilities in the detection of suspicious financial transactions, when an Internet payment service provider is used, could be affected.
- A number of the ML/TF risks associated with non-face-to-face business and financial transactions and trade-based ML, apply as well to internet payment systems and commercial websites. The majority of online payments come from financial transactions that are initiated from a bank account or a credit card; those already involve a process for customer

[2] United Nations Office on Drugs and Crime (UNODC) (2014) Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children, Vienna pp.18-19
[3] UNODC (2014), p. 23
[4] Dark Web is the World Wide Web content that exists on darknets, overlay networks that use the Internet but require specific software, configurations or authorization to access.
[5] Richardson R & North M (2017). Ransomware: Evolution, mitigation and prevention. International Management Review, 13(1), p. 10.
[6] It is noted that ML networks may require relatively high level of tech skills to use cryptocurrencies for laundering schemes, however they are still considered to be of great risk because of a lack of AML/CFT regulation. Anonymity of many cryptocurrencies attracts criminals.
[7] van Wegberg, R, Oerlemans, J and van Deventer O, (2018) "Bitcoin money laundering: mixed results?: An explorative study on money laundering of cybercrime proceeds using bitcoin", Journal of Financial Crime, 25:2, p. 419.
[8] Banks J (2011) European regulation of cross-border hate speech in cyberspace: the limits of legislation, European Journal of Crime, Criminal Law and Criminal Justice 19:1-13

identification, reporting obligations and transaction record keeping. As low value transactions do not necessarily associate with low risk, it remains subject to the regulatory controls already applicable to the financial sector.

- There is a need for online identity verification solutions such as electronic identity cards used in certain jurisdictions for instance, to help commercial websites and internet payment service providers mitigate the risk of criminal activity, when it comes to the risks related to non-face-to-face registration and the possible anonymity of the users.
- If internet payment service providers adequately monitor the financial transactions of their customers, monitoring for and acting on deviations from the customer transaction profile, the lack of face-to-face contact at the beginning of the relationship with the commercial website and the internet payment service provider may not constitute a problem.
- The availability of comparable AML/CFT obligations is crucial for online and offline retail merchants and payment services.
- The efforts to fight ML/TF by internet payment service providers and commercial websites in diverse jurisdictions not to be hampered by different privacy legislation, potentially interfering with the amount of customer information that service providers could exchange regarding suspected ML/TF.

105 In 2013, the FATF issued a report on *Guidance for a Risk Based Approach: Prepaid Cards, Mobile Payments and Internet-Based Payment Services*. The increased functionality, swift growth, and growing use of new payment products and services (NPPS) worldwide has created obstacles for jurisdictions and private sector institutions in ensuring that these products and services are not exploited for ML and TF purposes. Jurisdictions are seeking to develop and implement AML/CFT regulation for NPPS, by:

- Explaining how new payment systems work, who the entities involved in the provision of NPPS are, and their roles/activities.
- Examining which entities involved in the provision of NPPS are already covered by the FATF Recommendations (i.e., because they fall within the FATF definition of a financial institution).
- Determining the risks involved in the provision of NPPS, including through consideration of any relevant risk factors and risk mitigation measures.
- Considering the impact of regulation on the NPPS market, including whether such regulation would impact financial inclusion and the positive implications of money deposits moving to regulated financial institutions.

106 Based on the NPPs Guidance, the FATF issued in 2014 a report on *Virtual Currencies: Key Definitions and Potential AML/CFT Risks*. This report is suggesting a conceptual framework for understanding and addressing the AML/CFT risks associated with one kind of internet-based payment system: virtual currencies. Specifically, the paper proposes a common definitional vocabulary that clarifies what virtual currency is and classifies the various types of virtual currency, based on their different business models and methods of operation and identifies the participants in typical virtual currency systems. It also applies risk factors set forth in Section IV (A) of the 2013 NPPS Guidance to specific types of virtual currencies to identify potential risks; describes some recent investigations and enforcement efforts involving virtual currency; and presents a sample of jurisdictions' current regulatory approaches to virtual currency.

107 In 2015, the FATF issued *Guidance for a Risk-Based Approach to Virtual Currencies*. The Guidance is part of a staged approach taken by the FATF, which has built on the 2014 Virtual Currencies report and on the risk matrix and the best practices of the Guidance for a Risk-Based Approach to Prepaid Cards, Mobile Payments and Internet Based Payment Services report (2013 NPPS report). In fact, the development of VC payment products and services (VCPPS) and interactions of VCPPS with other New Payment Products and Services (NPPS) and even with

traditional banking services, give rise to the need for this Guidance to protect the integrity of the global financial system from criminality and cybercrimes including cyber-laundering.

108 The focus of this Guidance is on the points of intersection that provide gateways to the regulated financial system, in particular convertible virtual currency exchangers.

4.3 Existing efforts and challenges to combat cybercrime

109 Internet-facilitated ML/TF, and cybercrime more generally, have been the focus of much international attention in recent years. There are a number of activities at the jurisdiction, regional, and international level which seek to better understand the nature of cybercrime, strategies for its prevention, and tools to investigate and prosecute offenders.

Regulation of crypto-currencies

110 In addition to the *Budapest Convention* that seeks to establish consistent legal frameworks and investigatory powers amongst its signatories, jurisdictions have also sought to address one of the key concerns regarding crypto currencies by subjecting this sector to AML/CFT regulation and supervision.

111 Malaysia has imposed AML/CFT requirements on digital currency exchangers by including these entities as 'reporting institutions' under Schedule 1 of the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.[9] This requires digital currency exchangers to ensure they have effective measures in place against ML/TF risks associated with crypto currencies and to increase the transparency of digital currency activities in Malaysia. In addition, these digital currency exchangers must also provide further information on their business profile and activities as well as submit monthly reports on digital currency transactions.

112 Australia has also imposed AML/CFT requirements on digital currency exchangers via the AML/CTF Digital Currency Exchange Register Policy Principles 2018 issued under the Anti-Money Laundering and Counter-Terrorism Financing Act 2006. Digital currency exchangers are required to, among other things, register with AUSTRAC, have an AML/CFT program in place, report suspicious transactions and maintain sufficient records.[10]

Challenges for jurisdictions

113 Internet-facilitated ML/TF poses a number of challenges including:

- A lack of LEA expertise in investigating cybercrime. This can be further complicated by poor domestic coordination between LEAs responsible for investigating cybercrime and ML/TF.
- There may also be a lack of legislation to combat cybercrime or elements of related technology changes. The nature of the cyber threat is constantly evolving as technologies change, the tradecraft of attackers develops and the attackers themselves change.[11]
- The transnational nature of many cybercrimes. A crime may be committed by an individual in one jurisdiction, using an internet platform hosted in another jurisdiction, to commit an offence against a victim in a third jurisdiction. Investigating cybercrime and related ML/TF requires strong international cooperation between jurisdiction linked by geography and those

[9] Further details at: http://www.bnm.gov.my/index.php?ch=en_press&pg=en_press&ac=4628&lang=en
[10] Further details at: http://www.austrac.gov.au/digital-currency-exchange-providers
[11] Emerson R G (2016) Limits to a cyber-threat, Contemporary Politics, 22:2, p. 178

with close ICT links. Given the porous nature of jurisdictional border when interacting in cyberspace, international collaboration and cooperation are vital in combatting cybercrime.[12]

- Cybercrime and internet-facilitated ML/TF investigations also require strong cooperation with the private sector. The online infrastructure operated by the private sector is not often developed with security and cooperation with law enforcement agencies as a priority.[13] As noted above, the transnational nature of cybercrime inhibits the ability of jurisdictions to enforce their laws on foreign-based private companies. Instead, cooperative rather than punitive approaches to gaining assistance from private companies, such as social media and telecommunications companies, may reap more benefits.
- A lack of confidence in the security of online transactions and trading could limit the number of financial transactions occurring in a jurisdiction as customers may move to other markets which are perceived to be safer.

4.4 ML through Cyber-laundering (Internet facilitated ML/TF)

BANGLADESH

Case Study 1

114 Through regular monitoring work on social media, the Social Media Monitoring and Surveillance Team (SMMST) identified an account in the name of 'X'. The account was being used to propagate radical ideologies and to inspire other social media users to participate in on-going conflict. The account was also used to call for money to destroy secular Bangladesh and establish Khilafah. Later the account also published that a terrorist had come and was on the verge of strike.

115 At this backdrop SMMST had sought help from the concerned social media firm to identify the owner of the account. Following the information provided by the social media firm and mobile tracking, the SMMST team was able to arrest the person behind the account. During investigation SMMST learned that 'X' is a fictitious name and the actual individual 'Y' was running that account on the social media site. Investigators also learnt that 'Y' is an active member of Bangladesh Government designated entity Ansar Al Islam Bangla Team (ABT).

116 Having information from the investigating authority about 'Y', BFIU conducted searches of his accounts in the financial sector. The search resulted in three accounts with banks and multiple mobile financial services (MFS) accounts. All three bank accounts identified the customer as one who has online business and affiliate marketing. However, no online business entity, partner entity, account or page with which the business was being carried out was named either in the AOF or KYC profile form. The accounts had sporadic small cash deposits from different parts of the jurisdiction. The MFS accounts had frequent transactions mostly cash and the accounts used the full MFS transaction limits. All accounts were maintaining the bare minimum balance.

117 A case has been filed against the person under *Anti-Terrorism Act, 2009* and *Information Technology and Communication Act, 2006*. Currently the investigators are further investigating to identify his associates.

Case Study 2

118 A Facebook page was opened in the name of a high government official of Bangladesh. On that page some posts regarding extending financial aid by the government to unemployed people were published. To make the page trustworthy some slogans like "Leave terrorism and come to a normal

[12] Skopik F, Settanni G and Fiedler R (2016) A problem shared is a problem halved: a survey on the dimensions of collective cyber defense through security information sharing, Computers & Security, 60. P. 157
[13] Cavelty M D (2014) Breaking the syber-security dilemma: aligning security needs and removing vulnerabilities, Science and engineering ethics 20:3, p. 704

life: Government extends financial aid to the unemployed destitute people" was used. The page also used some pictures of cheque handing-over ceremonies by the government official. Mentioning a phone number and e-mail address, the page instructed the interested persons to contact them for financial aid.

119 Allured by posts on that Facebook page, interested persons contacted the phone number and e-mail address. Then they were informed through e-mail that they had been selected for government aid and the cheque of financial aid shall be handed over to them by the government official shortly. The mail also instructed them to deposit 25 percent of the sanctioned aid in advance, as security money, into the bank account of the Project Director of the aid program. The title of the bank account was "Ms. J". As per instruction some persons deposited money in the account but did not get any response from the so called government office.

120 The issue came to the notice of the concerned ministry and they reported the issue to the LEA, the concerned bank and the central bank. After being informed of the issue the bank lodged a STR and different departments of the central bank forwarded the matter to BFIU. The BFIU analysed the issue and found that a group of persons were committing fraud and had deceived people by using the said Facebook page and bank account. Tk. 6 lac was deposited in the account. The deposited money was withdrawn within a short period. Some portion of the withdrawn money was deposited in another account of the bank. Those two bank accounts along with one mobile financial services account of the fraudsters with Tk. 2 lac balance were frozen under MLPA 2012. An analysis report in this regard was prepared and disseminated to the law enforcement agency.

BRUNEI DARUSSALAM

Identity Theft

121 Offenders use a victim's name or identity to commit crime. Identification details including name, national identification number, financial information (account number and PIN) are obtained through various methods including social engineering (phishing through electronic media, voice telephone or instant text messaging platforms). Such information is used to commit fraud including credit or ATM card fraud and unauthorized online bank transfers.

Online Scams

122 Offenders use social media to gain the confidence of victims and eventually defraud them through the offers of products, services, business investments, romance etc. For instance, a romance scam (also known as a parcel scam) is that it is a type of advanced fee fraud where victims are asked to send funds to the offender for example, in order to secure their passage to the victim's jurisdiction.

Sexual Extortion

123 Victims (often young men) are tricked into carrying out sexual acts over video chat. Victims are then forced to pay in order to prevent the upload and distribution of these videos.

FIJI

Studying for Crime

124 Mr Manjeet Singh and Mr Rajneel Chaudary were two friends studying at the University of the South Pacific (USP) who conspired to steal funds by illegally accessing internet banking of their associates. Mr Manjeet Singh knew where his landlord kept all his bank account details and used the stolen details to register his landlord for internet banking. Mr Manjeet Singh then conducted three internet banking transfers amounting to FJ$22,000.00 from his landlords account to accounts held under his name, Mr Rajneel Chaudary and Ms Arti Darshana Reddy. Ms Arti Darshana Reddy was a friend that Mr Rajneel Chaudary approached to use her account to supposedly pay for his school fees.

After transferring the funds to Ms Arti Darshana Reddy, he used her ATM card and withdrew the funds.

125 Mr Rajneel Chaudary visited a bank branch and made enquiries on a bank account of another victim under the pretence of depositing funds into the account. Mr Rajneel Chaudary was able to obtain personal details to access the victim's account. Mr Manjeet Singh then conducted three internet banking transfers totaling FJ$4,340.00 from the victim's account.

126 In March 2017, Mr Manjeet Singh was convicted of three counts of money laundering and in April 2017, he was sentenced to nine years imprisonment. In April 2017, after pleading guilty to three counts of money laundering, Mr Rajneel Chaudary was sentenced to eight years imprisonment.

127 This case study was the first domestic cybercrime case that resulted in two ML convictions. The level of collusion and manipulation of banking systems was evident and resulted in wider implications on internet banking system in Fiji.

JAPAN

128 Japan FIU (JAFIC) found through its strategic analysis that a number of bank accounts have received criminal proceeds derived from internet gambling. Information regarding these criminal activities was disseminated to law enforcement authorities.

MACAO, CHINA

129 In August 2017, the Judiciary Police were informed of a fraud case, in which a female victim reported to have been defrauded of a huge sum of money and posted her story online in 2016. She then made friends with a suspect who claimed to be another victim in the same case. On 30 July 2017, the above suspect approached the victim via a mobile messaging app and claimed that he had been a senior police officer and was able to prioritize the retrieval of her lost money in a legal manner through his connections with the court. The victim later wired a total of MOP 630,000 (US$78,000) on over 20 occasions to a designated bank account as instructed by two fraudsters posing as staff of the court. Eventually she realized that she had been defrauded and reported the case to the police.

130 Another female victim of a similar case reported to the Judiciary Police on 8 November 2017, stating that she had lost contact with a local man after lending him HKD 550,000 (US$78,100) in 2015. A suspect alleging to be the lender, contacted the victim on a social networking platform on 31 October 2016. He claimed to be willing to repay her, but demanded her to pay processing fees first for unfreezing his bank account. The victim subsequently received messages sent with a mobile messaging app from three individuals posing as staff of the Public Prosecutions Office and the court, demanding her to settle the processing fees by bank transfers in person. She was eventually defrauded of HKD10,000,000 (US$1.3 mill).

131 The Judiciary Police confirmed and identified the involved individuals of the above cases were from the same fraud syndicate. Eight men and women were arrested in several apartments in the northern and central districts on 11 November 2017. HKD240,000 (US$31,000) of illicit money and evidence were also seized.

132 Investigation revealed that one of the arrested women was the mastermind of the case and the remaining involved individuals posed as staff of the judicial authority to commit fraud. Using the other involved individuals' or the mastermind's own bank accounts, the mastermind received and withdrew the illicit money and circuitously transferred the amount, which was eventually deposited into their overseas bank accounts.

133 The Judiciary Police transferred the 8 men and women to the Public Prosecutions Office for the charges of fraud and ML, while pursuing the other involved parties and the proceeds.

MALAYSIA

Business Email Compromise (BEC)

134 A senior accountant in his organization, Mr A received a hand-delivered instruction, in the form of email print-out supported by an invoice purportedly sent by his senior officer regarding the change of beneficiary bank details for a scheduled payment involving a sum of USD 1.2 million. The bank account of the intended recipient is supposed to be located in jurisdiction A, however it was changed to a different bank at jurisdiction B. The names of both account holders were exactly the same.

135 Convinced by the instructions in hand, a new telegraphic transfer (TT) form was completed to make changes to the new beneficiary account and it was approved and signed by relevant supervisors. The newly completed TT form was given to the banker to initiate transfer to the new beneficiary account number.

136 Later on that day, Mr A received a phone call from one of the supervisors who realised that the TT was fraudulent and was informed that the email correspondences between the senior officer and the intended recipient of the fund have been intercepted by an unknown perpetrator to make the change on beneficiary bank details. A police report was lodged and an instruction was immediately given to recall the funds.

137 In this case, the transfer was successfully blocked due to prompt action by the FIUs and relevant law enforcement agencies from both jurisdictions (the victim's jurisdiction and jurisdiction B) that leveraged on Egmont's BEC rapid response program.

138 In general, indicators involving BEC cases are as follows:

- The establishment/use of company names similar to the victim's, including renowned international companies.
- Amounts siphoned off were not too high/within company's normal range to avoid suspicion by the victims.
- Unusual transaction instruction methods.
- Use of forged documents.
- The funds are immediately withdrawn from the account, either in cash or via transfers to proxies.
- Inconsistent conduct of the account, including variation on the purpose of fund transfer.

NEW ZEALAND

139 New Zealand Police noted a case of the use of a Vietnamese Facebook community page that sought out unsuspecting participants to facilitate ML on behalf of a transnational crime network responsible for a substantial cocaine importation.

140 Police when investigating the importation of a large amount of cocaine, were monitoring an offender meeting with a known money launderer. The male offender passed a bag of cash to the to the woman, who later met with another person outside a bank – a smurf. NZD100K was then deposited into the smurf's bank account.

141 When the smurf was arrested, she explained that she had posted on the wall of a local Vietnamese Facebook page, saying that she wanted to get money from Vietnam into New Zealand without the Western Union or bank fees. A male responded and organised for her to meet with his mother who wanted to get money back to Vietnam. When the two females met at the bank, the smurf's mother was at a bank in Vietnam depositing the equivalent of NZD100K into a Vietnamese

bank account. She told police this was a completely normal practice in Vietnam, and people regularly post similar requests on Facebook.

142 Further enquiries showed that the initial male offender and his mother had done this with about eight other individuals with no questions asked as this was normal in the context.

143 The initial smurf was charged with ML, but this charge has been withdrawn when the extent of the use of smurfs became apparent. New Zealand Police's Asset Recovery Unit has restrained the NZD100K on the basis that it is still clearly the proceeds of criminal offending.

SINGAPORE

International Wire Transfer Fraud (Money Mules)

144 In early 2012, the Commercial Affairs Department (CAD) detected a crime trend where criminals hacked into the email accounts of their victims to send fraudulent instructions to the victims' banks to transfer funds to bank accounts in Singapore. In other cases, victims fell for scams, including internet love scams, and made the transfer of funds at the criminals' instruction.

145 CAD's investigations established that overseas criminal syndicates 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 remitted money in 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.

146 The following table details the number of foreign victim bank accounts identified through the close collaboration between CAD and its foreign counterparts, the amounts transferred from the victim's account and the amounts of criminal proceeds successfully seized by the CAD.

Number of bank accounts identified and criminal proceeds seized by CAD

	2012	2013	2014	2015	2016	2017
No. of foreign victim bank accounts identified	129	264	148	64	37	44
Total amount identified to have been fraudulently transferred out from the victims' account to Singapore accounts (million)	24.6	31.5	14.9	6.67	3.81	5.41
% of criminal proceeds seized	11	18	15	15.6	25.1	36

147 Singapore has made successful efforts to combat this trend, 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 foreign victim bank accounts fell by 83.3%, from 264 accounts at the peak in 2013 to 44 accounts in 2017. The figures have remained fairly constant in its decline since 2015. Singapore took a multi-pronged approach where CAD (i) promptly shared information with relevant stakeholders including foreign FIUs and industry partners, (ii) worked closely with LEAs of various jurisdictions to identify the victims whose monies may have been fraudulently transferred into Singapore to further ML investigations in Singapore, (iii) worked with the Attorney-General's Chambers (AGC) to ensure that strong enforcement action is taken against money mules and (iv) intensified its efforts in the area of crime prevention and public education.

THAILAND

Online Lottery Scam

148 Mr W from a country in the Middle East region contacted AMLO to release a cheque which was sent through Worldwide Express Courier Company immediately. He claimed that this cheque was from Yahoo winning lottery and AMLO had no rights to hold it. After talking with AMLO officer he realized that he had been deceived by someone who pretended to be a Yahoo Coordinator in a lottery program.

149 Mr W lost USD 650 by transferring the money via Western Union to a Mr S to release his winning lottery cheque before he contacted AMLO. The AMLO name had been used to add credibility to the scheme.

Fraudulent Act by Social Media

150 The victim had been in touch with Mr. P, a foreigner, through Facebook. She was deceived to make 11 money transfers to several bank accounts opened by the offender. The loss was more than one million THB (approx. USD 35,000).

151 The victim transferred 350,000 THB (approx. USD 10,000) to Ms Y's account (she was an associate of Mr. P) opened with Bank T. Prior to that, the bank system detected irregularities of the transactions and notified the bank branch to summon the account holder for more information in accordance with the EDD process. The branch however could not contact the person.

5. CASE STUDIES OF ML AND TF

5.01 Terrorism Financing

MALAYSIA

152 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.

153 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.

154 The methods used in this case included:

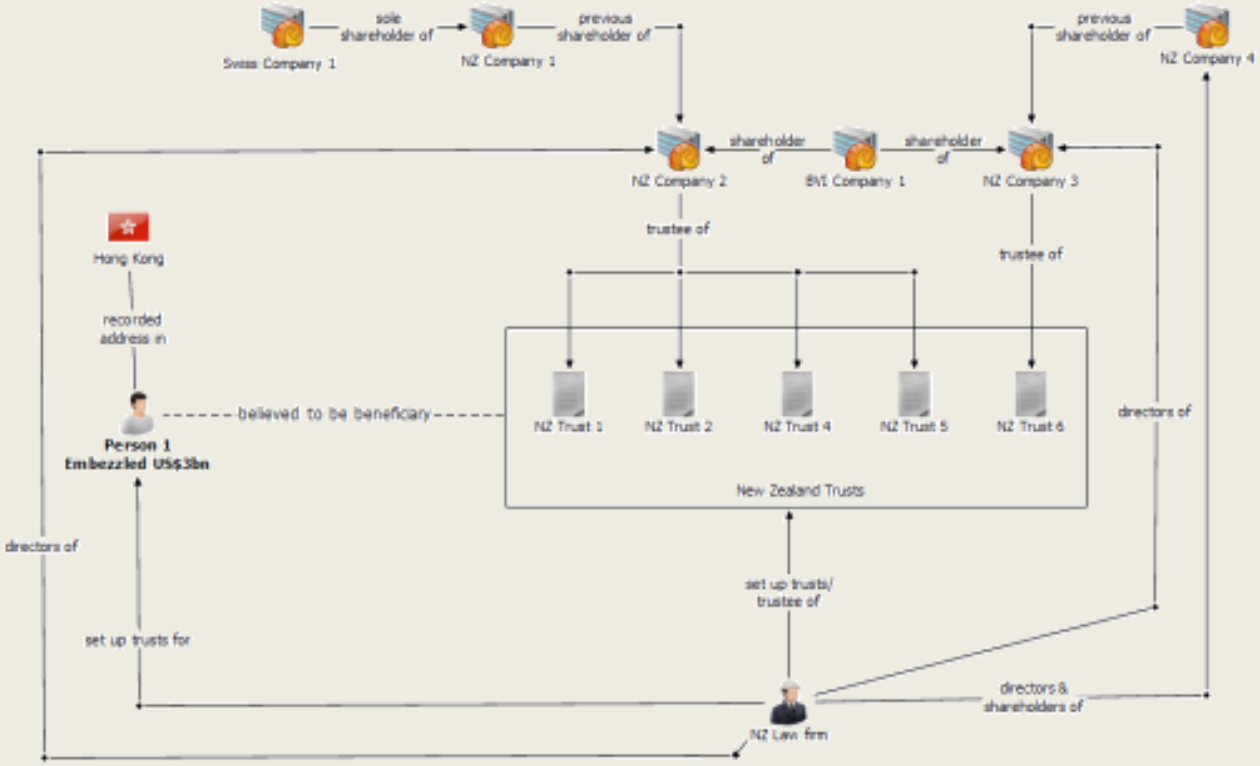
- Use of nominees, trusts, family members or third parties etc.
- Use of cash

155 The individuals were charged and convicted of TF. Initially, the individuals were convicted and sentenced to three years imprisonment for soliciting funds and two 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.

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

NEW ZEALAND

156 Media reporting identified Person A had embezzled a large sum before purchasing high value assets with the proceeds of crime. 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.



PAKISTAN

157 Multiple STRs were reported on an individual, Mr. Adam. Mr. Adam was the CEO of 'Alpha Company' which was a subsidiary of 'Beta Company', a Cayman Island based company. 'Gama Company' acquired 'Alpha Company' against a consideration of PKR 250 million. After the acquisition, the sale proceeds were transferred from the account of Gama Company being maintained at AA Bank, to the account of Beta Company being maintained at BB Bank. Mr. Adam was the only authorized person to operate the company account of Beta Company who then further transferred the funds to his personal account maintained at CC Bank, which was found to be unusual. The funds were withdrawn from his account in cash, followed by a purchase of foreign currency from exchange companies and deposited cash into his foreign currency account, maintained at CC Bank. The funds were then remitted out of the jurisdiction to his personal account maintained at DD Bank, in a foreign jurisdiction.

158 The financial activities of Mr. Adam seemed unusual and it appeared that he was the beneficial owner of companies Alpha and Beta, and had deliberately structured the transactions to avoid detection.

5.03 Use of virtual currencies

CHINESE TAIPEI

159 Person 'X' - a scam syndicate member - extensively studied Bitcoins over the Internet. He converted fraud proceeds into Bitcoins and transferred them in and out of e-wallets repeatedly, creating five barriers that stopped the police from tracing the money and successfully laundered NT$50 million in one month.

160 X first used forged identity documents to apply for a Bitcoin account, then converted fraud proceeds into Bitcoins and used cell phone apps to transfer Bitcoins to another account before directing them to the accounts of the scam syndicate. Due to the difficulties involved in tracing Bitcoins, X successfully laundered more than NT$50 million in one month. In a bust by the Criminal Investigation Bureau, X was charged with an offense against the law.

FIJI

161 The Fiji FIU received a STR on Mr and Mrs X for receiving more than US$80,000 in inward remittances in a period of 18 days. The Fiji FIU conducted checks and established that Mrs X was a local national who married Mr X, a foreign national. Travel details of the individuals revealed that both Mr and Mrs X reside in jurisdiction A.

162 Initial analysis of the inward remittances revealed that an over the counter (OTC) Bitcoin team in Asia had remitted funds to Mr. and Mrs X. A request was immediately sent to three foreign FIUs through Egmont Secure Web (ESW) to obtain more information on the other individuals that remitted funds to Mr and Mrs X. One of the foreign FIUs located in jurisdiction B identified one of the remitters of funds (Mr Y) as a person of interest in their jurisdiction.

163 Mr Y had been reported several times to the FIU in jurisdiction B for links to the purchase and sale of digital currencies. Mr Y was included in a report for tax evasion and was charged for various computer related offences in jurisdiction B. A report was disseminated to the Fiji Police Force and the FIU in jurisdiction A. The FIU in jurisdiction A later disseminated the contents of the Fiji FIU report to their relevant law enforcement agencies:

a) Possible Offences:

- Cyber related offences
- Tax Evasion

b) Indicators included:

- Unusually large remittances from unrelated foreign third parties in a period of 18 days.
- Account holders do not reside in the jurisdiction.
- Two of the remitters were involved with virtual currencies.

JAPAN

164 Japanese LEAs addressed a ML case involved in Bitcoin in which a suspect defrauded a Bitcoin exchange of a certain amount of Bitcoin and combined it with Bitcoin acquired from legitimate sources. Then, the suspect cashed the Bitcoin and concealed the funds by transferring it to a bank account under someone else's name.

165 The suspect was convicted of violating Article 246-2 of Penal Code (Computer fraud) and Article 10 of the Act on Punishment of Organized Crimes and Control of Crime Proceeds and Other Matters (Concealment of Criminal Proceeds).

PAKISTAN

166 Multiple STRs were reported from different banks wherein a similar nature of transactions was noticed in several accounts being maintained by different individuals. It was suspected that the individuals were involved in dealing with Bitcoins (virtual currency). The transactional pattern in their accounts revealed that funds were credited into the account through IBFT, INET, Mobile Banking and transfers through ATM, which were subsequently withdrawn in cash via ATM and transfers.

167 A public database search found that the individuals were active on social websites and were influencing people through internet marketing on buying and selling of E-Currency and providing a platform of potential customers of Bitcoins. The State Bank of Pakistan does not recognize crypto currencies such as Bitcoins.

168 As per information extracted from FMU's database of STRs, a few of the individuals involved in the crypto currency business, were maintaining other accounts and a similar pattern of transactions were observed. Based on analysis, the financial intelligence was shared with the regulator for considering appropriate measures/controls on emergent use of bank accounts for digital currencies such as Bitcoins.

PHILIPPINES

169 The AMLC received a request for information from a Philippine LEA on the bank accounts of JD Cruz who allegedly committed a networking scam. JD Cruz is the registered owner of XYZ Trading and Services in Cavite, which is purportedly engaged in exchange trading.

170 The reported transactions for the accounts of JD Cruz consisted mostly of withdrawals ranging from Php509,000 to Php4.2 million. This may indicate that there are credits to the accounts that are below reporting threshold amounts.

171 A virtual currency exchange (VCE) filed STRs on JD Cruz for two cash deposits totalling Php100,000 and domestic outward remittances totalling Php78,000 transacted in September 2017. The VCE considers the transactions as not commensurate with the business or financial capacity of the client.

172 The VCE also filed STRs on Brabo, an associate of JD Cruz, stating that there is a strong indication that Brabo's account is associated with swindling. The reported transactions consist of Php122,000 cash deposits and Php92,000 domestic outward remittances for September 2017. Another entity, a bank, filed several STRs on Brabo on various transactions (i.e. cash deposit, fund

transfer, cheque deposit/encashment) totalling Php27.02 million for the period August – September 2017. The bank deemed the transactions to have no underlying legal trade obligation, purpose and economic justification.

173 The results of this analysis were forwarded to the requesting LEA to be used for intelligence purposes and to aid in their investigation of the case.

THAILAND

Illicit drug trafficking on the dark web

174 Mr. C, a 25-year-old Canadian citizen, was arrested in Thailand at the request of the United States. Thai officers confirmed he was the administrator of Alphabay, a dark web devoted to the sale of illicit goods and used virtual currencies like Bitcoin to avoid detection. He appeared to be living a life of luxury in Thailand, where he owned three houses and four sports cars. Mr. C was charged related to narcotics distribution, identity theft and ML.

5.04 Trade-based money laundering and transfer pricing

AFGHANISTAN

Case Study 1

175 The Afghanistan FIU's analysis for 11 STRs related to a wire fraud, revealed the involvement of two money service providers (including a money exchange service provider) in a misappropriation of international transfers facilitating trade-based ML.

176 Group X was found to be transferring money overseas and providing inadequate documents to support the wire transfer. The commercial invoices for the purchase of textile and solar from jurisdiction A were flagged as fraudulent. Key red flags identified by the FIU are listed below:

- The email address provided on the commercial invoice was different from original supplier email address. All the verification emails sent to the fake email address placed on invoices, were replied confirming that the invoice is original.
- Type of business, address and contacts were picked up from the relevant businesses of jurisdiction A to make the fraudulent invoice appear legitimate.
- Original business transactions were also mixed up with fraudulent invoices to make it difficult to compliance officers for identification.
- Mobile numbers placed on the invoice were seemed to be prepared in collusion with the sale agents providing positive feedback to the bank officer.

The difference of more than 70 percent was identified between the amount transferred and goods imported. Under invoicing was demonstrated as a key red flag for the difference.

177 Afghanistan FIU disseminated the case to the Major Crime Task Force in 2016. During the investigation, two suspects (owner of money service provider) had tried to bribe the investigating officers. The Primary Court of the Anti-Corruption Justice Center convicted both suspects of providing kickbacks with 18 months imprisonment each and ML is under prosecution.

Case Study 2

178 The FIU made spontaneous disclosure on trade-based money laundering to the Investigation Agency, 11 businesses including money services providers (MSPs) and FXD suspected in transferring X amount of US dollars overseas, which were found to be using forged and inadequate supporting documents in order to purchase and import commercial goods back to the jurisdiction.

179 Based on STRs reported by the commercial banks, the subjects have transferred X amount of US dollars abroad in order to purchase and import commercial goods to Afghanistan. Some of the customs documents submitted by the businesses were not authenticated or acknowledged by the customs department. Also, according to the Bank A's STR, one of the subjects has proposed kickbacks to a bank official on a monthly basis for facilitating the transactions overseas.

180 The analysis findings have determined from account signatories and business activities that some of the businesses are interconnected with each other, via familial relations. The red flags and suspicious matters identified are as following:

- Providing foreign exchange services without legal authorization; money
- Providing fake invoices to conduct FTTs;
- Conducting several transactions in contradiction with the monthly turnover;
- Proposal of kickbacks;
- Having multiple corporate bank accounts.

181 The investigation of spontaneous disclosures was completed by a joint task force and was forwarded to the Attorney General's Office for the prosecution on the following charges:

- Money laundering;
- Tax evasion;
- Forgery;
- Concealment of the illicit origin of funds; and
- Proposal of kickbacks.

AUSTRALIA

Under-invoicing of goods

182 Company A is a domestic exporter of scrap metal and machinery with a customer base located in Asia. Irregularities in relation to the value of IFTIs and export values declared to border authorities indicate company A is possibly involved in TBML. Over a financial year, Company A received IFTIs from ordering customers in Asia likely related to scrap metal and machinery exports totalling AUD2.5 million compared to a total export declaration value of AUD3.1 million. The company's use of trade finance was also suspicious. Company A secured trade finance for the importation of machinery from Europe valued at USD137,500, without any corresponding IFTIs related to the purchase or records showing the product was received. Moreover, the company's physical export value declared to border authorities is less than the export sales value declared to the Australian Taxation Office (ATO) indicating a deliberate effort to inflate the amount of GST credits claimed.

Over-invoicing of goods

183 An Australian exporter network consisting of three companies (A, B and C) exports telecommunications devices and other electronic products to Hong Kong, Singapore and the United Arab Emirates. Export and transaction records indicate the value of exports declared by Companies B and C broadly corresponded with IFTIs received from overseas buyers. Conversely, Company A's records showed evidence of over-invoicing. Company A declared exports valued at just over AUD11 million but received funds amounted to approximately AUD33.6 million. The approximate AUD23 million surplus funds, which do not relate to equivalent export trade, were remitted overseas to the original ordering customer.

FIJI

184 The Fiji FIU received a STR linked to alleged drug trafficking involving a dual citizen (Fiji and New Zealand), Person X. Between November 2016 and November 2017, Person X was reported six times in STRs from local foreign exchange dealers and banks. Person X was first brought to the attention of the Fiji FIU for conducting a significant currency exchange in NZ dollars.

185 The Fiji FIU conducted financial checks and established that Person X had not declared the NZ currency at the border upon arrival. The foreign currency exchange was equivalent to FJ$91,640 and the Fiji FIU was unable to establish its ultimate use. Prior to the currency exchange, Person X had opened a bank account at Bank A. Person X also opened bank accounts at another local bank, Bank B.

186 Person X remitted significant funds from NZ to an individual in Fiji, Person Z. Person Z had received remittances from both Person X and his spouse person Y in New Zealand. Person X and Person Y are also directors of Company A, B and C in New Zealand. Person Z also received remittances from Company A in New Zealand. Person Z has no apparent relationship with either Person X or Y.

187 Person X stated that the reason for the large currency exchange was to set up a business in Fiji. Company D was later set up in Fiji and Person X used various other individuals to conduct currency exchange on his behalf.

188 The Fiji FIU also established that Person X has adverse travel records in New Zealand. A case dissemination report was first disseminated to the NZFIU to investigate alleged tax evasion and ML in NZ and the same report was later requested by the Transitional Crime Unit (TCU) Fiji for drug related offences. Dissemination of the STRs that followed was disseminated to TCU thereafter. The Fiji Revenue and Customs Service were also issued the same report for profiling at the border:

a) Possible offence included:

- Trade based money laundering
- Customs related offences
- Tax Evasion

b) Indicators included:

- Significant exchange of funds between local and overseas based entities without any apparent established trade relationships.
- Remitting funds to various individuals in Fiji
- Large currency exchange without declaring at the border.

PAKISTAN

189 A STR was reported by Alpha Bank on individual Mr. A, who was running a sole proprietorship concern "M/S ZXY". Adverse media news found that the suspect was involved in a scam. The analysis of STRs indicated that the individual was involved in an importation business of medicines and was maintaining multiple banks accounts. The activities in his accounts were found to be abnormal as they had high liquidity turnover, cash withdrawals and foreign remittances in last few months. However, the tax status of individual was not in line with the level of financial activities in the accounts.

190 It was found that the suspect was suppressing the actual transactional value of imported goods by submitting fake import invoices and other documents before customs for clandestine clearance, while the funds were being remitted abroad through Hawala/Hundi. On the basis of abnormal account activities and adverse media news, the intelligence was initially shared with LEA for necessary action.

THAILAND

191 The Ministry of Finance and Office of the Auditor General cooperated to examine the false VAT refund for more than 30 scrap metal export companies. The investigation found that 18 civil servants of the Revenue Department were involved in the case, including high-level civil servants involving an amount of 4.1 billion THB (approx. 150 million USD). Office of the Auditor General cooperated with Department of Special Investigation, NACC, and AMLO to expand the investigation.

192 The investigation by DSI found that the offenders paid 200-500 THB (7-15 USD) to poor people to use copies of their identification cards to register the company with the Social Security Office. Moreover, the offenders hired a workplace posing as 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 of 600 THB per kilogram which is higher than the market price. The offence committed related to a false claim of payment for a VAT refund after export.

5.05 Underground banking/alternative remittance services/hawala

AUSTRALIA

193 An AUSTRAC referral was the catalyst for a law enforcement investigation into two unregistered remittance businesses operated by two offenders. The offenders were arrested after search warrants were executed by law enforcement. Following an internal investigation, AUSTRAC referred the companies and directors to law enforcement for criminal investigation. AUSTRAC

provided law enforcement with financial intelligence reports prior to and during the investigation, focusing on the reporting and transaction activities of the companies and related entities.

194 In October 2016, the offenders pleaded guilty to operating an unregistered remittance service and money laundering offences, and received suspended sentences between 24 to 26 months each. Additionally, over $2 million of funds were seized and forfeited as a result of the law enforcement investigation.

195 See: "AUSTRAC referral helps catch unregistered remitters" (http://www.austrac.gov.au/case-studies/austrac-referral-helps-catch-unregistered-remitters) published 22 September 2017.

CHINESE TAIPEI

Case Study 1

196 From March 2013, Person 'Y', a Malaysian national, used many accounts in Chinese Taipei and overseas to operate an underground banking system, providing correspondence services for customers from Indonesia, Thailand, Vietnam, and Philippines who work in Chinese Taipei. Y used accounts of local companies to receive funds and then transferred funds into US dollars to an overseas banking unit (OBU) account of a foreign company. The funds were then transferred to contact points' accounts in different jurisdictions. After confirming the amount, the contact points then transferred funds into appointed accounts with different currencies in line with customers' demands. Y collected service fees which depended on the amount of the remittances.

197 Between March 2013 and December 2016, the total amount that Y dealt with was about NT$56.6 billion. The transactions fees they earned was about NT$700 million. In April 2017, the Taichung District Prosecutors Office indicted Y for violating the Banking Act and the Money Laundering Control Act and applied to the court for the declaration of confiscation of the proceeds of crime which was about NT$700 million.

Case Study 2

198 Person 'X' ran an illegal underground banking syndicate that used clothes to hide and transport large sums of cash (NT$15 million each run) in luggage cases. According to investigations, X had Indonesian nationality and operated a store selling Indonesian goods in Chinese Taipei. She ran the store with her husband, and her mother-in-law. In addition to selling Indonesian food and supplies, the store also took private requests to help Indonesian workers remit cash to Indonesia; in return, she earned commissions and exchange rate differences without a proper license. The syndicate has earned NT$8 million to date.

199 LEAs initiated a search that culminated in 8 suspects being arrested. The police found NT$14,545,000 of cash in the 3 pieces of luggage carried by X, along with evidence including criminal correspondence, records of transactions and a residential permit. X was charged with offenses against the Money Laundering Control Act and the Banking Act.

HONG KONG, CHINA

Case Study 1

200 Between September 2013 and March 2014, unidentified culprits purportedly offered three Chinese Taipei victims highly lucrative returns on an investment in Hong Kong stocks, and lured them into remitting a total of US$80,000 into the local bank accounts of a licensed money service operator (MSO). The victims subsequently lost contact with the culprits and reported the case to an

authority in Chinese Taipei, which referred the case to the Hong Kong Police (HKP) for investigation in August 2014.

201 The HKP's enquiry with the person-in-charge of the MSO revealed that his client (later known as defendant) arranged the proceeds to be transferred from Chinese Taipei to the MSO. The defendant visited the MSO in person, and requested the remit of the proceeds totalling US$0.91M (including the US$80,000 from victims) to three accounts in China for the construction business of her friend in China on 39 occasions between January and April 2014. The defendant also withdrew US$7,200 cash from the MSO for herself as a reward.

202 The defendant was later arrested and was charged with ML. In September 2017, the defendant was convicted as charged. In October 2017, the Judge ruled that the offence committed by the defendant was serious, and involved an international element. The defendant was subsequently sentenced to three years and nine months' imprisonment.

Case Study 2

203 Between November and December 2013, unidentified culprits purportedly offered two Chinese Taipei victims highly lucrative returns on an investment in Hong Kong stocks, and lured them into remitting US$14,103 in total into a local bank account. Victims subsequently lost contact with the culprits, so they reported the case to an authority in Chinese Taipei, which later referred the case to the HKP for investigation in August 2014.

204 The HKP's investigation revealed that a total of US$74,359 (including US$14,103 from the victims) was remitted from Chinese Taipei to the local bank account. Immediately after the deposits, US$69,231 was transferred via ATM to a licensed MSO. The Person-in-Charge of the MSO stated that his client (later known as defendant) claimed to have deposited US$69,231. The defendant visited the MSO in person, and requested the MSO to remit the money into three accounts in Mainland China for his trading business on 10 occasions between November and December 2013.

205 The defendant, who laundered crime proceeds of US$69,231 arising from an investment scam in Chinese Taipei, was convicted of ML after a trial in 2017. He was sentenced to one year and three months' imprisonment.

MALAYSIA

206 Malaysian Authorities had disrupted the activities of a group of illegal remittance operators that were suspected to have illegally remitted more than USD 3 billion from Malaysia to neighbouring jurisdictions over the period of five years. It is believed that these illegal remittance activities were operated by a syndicated group who had facilitated money transfers out of Malaysia, through informal money transfer networks and physical smuggling of cash into a neighbouring jurisdiction.

207 The larger part of the monies was transferred abroad to facilitate trade payment between local traders and foreign suppliers, remittance activities for foreign workers to remit money back to their home jurisdictions and also transferring of illegal proceeds overseas.

208 The modus operandi of this case involved the following:

- Foreign workers/local companies transacted with the illegal remittance operators.
- Illegal remittance operators transferred funds to recipients in jurisdiction C using internet banking facility of jurisdiction C. This was made possible via prefunding arrangement between the illegal remittance operators and the head of syndicate.
- Funds collected from customers were then transferred into bank accounts controlled by the syndicate. Surveillance and financial intelligence analysis revealed that several companies and banking accounts were operated by the syndicate using their proxies. Analysis on the

transactions showed that significant amounts of cash were deposited into the accounts from various depositors. Subsequently, the monies were withdrawn in cash from the accounts by the syndicate, either on the same day or the next day, leaving a minimal balance in the accounts.

- The monies were then remitted or smuggled out of Malaysia by the syndicate to neighbouring jurisdiction S which act as transit for the monies.
- Runners from jurisdiction C collected the monies in jurisdiction S and the physical monies smuggled to jurisdiction C.
- Jurisdiction C syndicate deposited the monies and topped up the balance of accounts held in jurisdiction C used for illegal remittance from Malaysia to jurisdiction C.

209 The ML and predicate offence investigation on the syndicate is on-going, including seeking mutual legal assistance from the concerned jurisdictions. The money laundering methods used includes:

- Trade based money laundering.
- Underground banking/alternative remittance services / hawala.
- Use of the internet (internet banking).
- Use of nominees, family members or third parties.
- Currency smuggling (including issues of concealment & security).
- Currency exchanges/cash conversion.
- Structuring (smurfing).

PAKISTAN

Case Study 1

210 Two STRs were filled on Mr. AB by two different banks for maintaining approximately ten accounts with different branches of Bank A Ltd. & Bank B Ltd., in different cities with diverse businesses namely general order suppliers, auto parts, commission agent, dry fruit, flour and oil, coal and chromites, steel works etc.

211 Searches across FMU's internal database identified more linked suspicious and currency transaction reports which were found to be linked by a common cell number and common business addresses. A few of those linked STRs included suspicious reports on another individual "Mr. CD", which was earlier disseminated to LEA on the suspicion predicate offence of Hawala.

212 The reporting banks requested details of Mr. AB's counterparties for further analysis, which identified two STRs on two of his counterparts namely Mr. EF and Mr. GH. Suspicion on these two individuals was raised on the basis of having very high turnover in the account along with transactions with unrelated counterparties. The bank also gathered market information on these suspects, which confirmed that these suspects were involved in Hawala business.

213 The information was shared with LEA and Regulator for necessary action.

Case Study 2

214 Mr. Z was maintaining a sole proprietorship business account having title "XYZ Enterprises" at ABC Bank Ltd. The suspect was conducting transactions of large amount and of inconsistent nature in M/s. XYZ Enterprises' account. High value funds had been credited through cash and transfers, which were mostly transferred to unrelated counterparties in different cities across Pakistan.

215 The suspect was also maintaining multiple accounts with different banks and was conducting high value transactions with unrelated counterparties in these accounts. These counterparties of the

suspect's accounts were engaged in different businesses such as fruit business, grain dealers, spare parts dealers, property dealers, computer and hardware traders, construction business and general traders. While checking the tax status of the Mr. Z, it was observed that the suspect was not registered for NTN. Keeping in view the disparity in the suspect and his counterparties businesses there was a probability that he might be engaged in Hawala/Hundi business. Therefore, the matter was referred to LEAs for the suspected offence of Hawala/Hundi.

THAILAND

216 China made a request to AMLO (Thailand Financial Intelligence Unit) to investigate and gather evidence on Mr. Z, a 38-year-old Chinese national and his associates who lured 30,000 Chinese people to invest in a scheme and promised to give a return at a high rate with an approximate value of 1 billion THB. Mr. Z intended to launder the proceeds of crime by buying the real estates in Thailand. Mr. B, his associate suggested him to move the money from China to Thailand through the underground banking system.

217 To move the value of this cash, there is no physical money transfer to the destination jurisdiction. Mr. Z sent limited information to Mr. B to complete an electronic transfer request. This was comprised of beneficiary account number in Thailand and amount of CNY, and then Mr. B will contact Mr. P who owned the real estate agent company in Bangkok. Mr. P informed Mr. B on the lists of beneficiary account number in China and amount of money in different accounts via WeChat application or Gmail. After that, Mr. B will send such information to Mr. Z's associates to transfer money to those account numbers in China. Transactions were made via underground banking totalling CNY 109 million.

218 When the transactions in China were completed, Mr. Z's associates sent the evidence of transfers to Mr. B then Mr. B sent the results to Mr. P. Immediately Mr. P informed his underground banking network in Thailand to transfer the money in Thai THB to Mr. Z and his associates' account numbers in Thailand. The amount of each transaction in different accounts will be not exceeding 1 million THB.

219 The process took one to two days. Mr. P made profits from the exchange rate difference and operational cost (One percent of 1 million THB).

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

BANGLADESH

220 Mr. J, a Bangladeshi expatriate living in Libya, came to Bangladesh and opened two bank accounts, one in his own name and another in his wife's name (Ms. K) in bank 'B'. A few days later, a huge amount of money was credited to Mr. J's account through on-line from different parts of the jurisdiction. One day a person came to branch 'F' of bank 'B' to deposit money to the account of Mr. J. Observing his pale face, bank officials asked him about his purpose of depositing money. Upon query, he informed that his brother who works in Libya had recently been kidnapped and the kidnapper demanded ransom. As a result, he is depositing money as ransom to release his kidnapped brother. Being informed of the matter, the bank submitted an STR against the accounts of Mr. J and his wife Ms. K.

221 BFIU analyst collected relevant documents and information regarding Mr. J and his wife Ms. K. upon analysis, it was revealed that huge amount of money (in a single deposit Tk. 0.10 million to 0.15 million) had been credited from different branches to the account of Mr. J and his wife. Based on the depositor's information given in the account statement, BFIU identified the depositors and collected information on them and came to know that all the money deposited to these accounts was the ransom. According to the victims statements, BFIU informed about some other bank accounts (three more accounts in bank A, S and M) where the victim`s relatives were instructed to deposit the ransom money. After collecting the details of these bank accounts BFIU got more information about

the account holders. These accounts were also used to take ransom from people whose relatives were kidnapped in Libya. It is also found that one of the account holders was the brother-in-law of Mr. J and another account holders worked for him.

222 BFIU froze these five accounts in order to stop the movement of funds. Based on the findings BFIU prepared an analysis report and disseminated to the LEA on an emergency basis for further investigation and legal procedures. The LEA immediately arrested the group and filed ML charges against them.

FIJI

223 A STR was filed by a local commercial bank on Person X who was identified as a potential internet banking fraud mule. The bank account of Person X showed four transactions totalling FJ$2,900 which were received into Person X's bank account and subsequently followed by three withdrawals totalling FJ$2,890 as follows:

- On 28 July 2017, Person X received a credit transfer of FJ$1,000 from the account of Person A.
- On 31 July 2017, Person X received two credit transfers totalling FJ$1,600 from the account of Person A.
- On 31 July 2017, Person X's bank account also received a credit transfer of FJ$300 from the bank account of Person B.
- On 31 July 2017, Person X made three ATM cash withdrawals totalling FJ$2,890 from local ATMs in three different locations.

224 The transfers were made from the bank accounts of Person A and Person B by fraudulent means as they were unaware of these transactions. Indicators included:

- Individuals unaware of transactions
- No relationship between victims and accused

MACAO, CHINA

225 Between April 2012 and March 2013, a Hong Kong resident had stolen important personal data of at least 6 victims in Hong Kong, and forged their signatures to transfer illegally a total of around HKD7.72 million of bank deposits. Evidence revealed that the related stolen money had flowed into Macao, the Hong Kong Police therefore requested the Judiciary Police to follow up with the investigation through INTERPOL at the end of 2013.

226 After an in-depth investigation, the Judiciary Police found that the involved man had transferred the stolen money to several bank accounts and through placement and layering, part of the illicit funds were transferred to Macao. The Judiciary Police identified the involved man, while realizing that he had been arrested by the Hong Kong Police in January 2014. He was sentenced by the Hong Kong Court to a term of 52 months imprisonment, and released at the end of 2016 after serving his sentence.

227 Since the involved man had conducted ML activities in Macao, the Judiciary Police arrested him upon his arrival at the Outer Harbour Ferry Terminal on 21 September 2017. In addition, HKD240,000 in cash and a watch worth HKD200,000 were seized from him. He admitted to have committed the above crime, and was transferred by the Judiciary Police to the Public Prosecutions Office for the charge of ML.

PHILIPPINES

228 Entities located in the Philippines operating as call centres were suspected of involvement in large scale investment fraud. The modus operandi of the scam is as follows: call centres use "Magic Jack" devices which are plugged into the USB port of a personal computer. The "Magic Jack devices" are assigned area codes corresponding to major cities in the U.S., including Chicago, New York, San Diego and Miami. These devices are used to call elderly individuals residing in the U.S. giving the victims the impression that the callers are from the U.S. when they are, in fact, physically located in the Philippines.

229 Moreover, the call centre operators have associates in the U.S., particularly from San Diego California and Hallandale Florida, who mailed fraudulent marketing materials and account statements to the victims. At least 40 U.S. residents have been victimized by this scheme within the period February 2011 – August 2013 amassing more than USD3 million. The victims were instructed to issue personal cheques for the amount of the investment to be picked up by FedEx courier; the cheques were subsequently forwarded to ADV in Muntinlupa City, Philippines. AMLCS was able to verify some of the accounts where the funds were allegedly deposited.

THAILAND

230 Thailand provided assistance to the United States on a matter regarding the use of malware to hack into bank accounts across many jurisdictions. The Royal Thai Police arrested two people in relation to the matter and 56 bank accounts were seized belonging to the suspects. AMLO filed a criminal complaint with the DSI for ML. The matter is now with the Office of Attorney General (OAG) to prosecute the defendants for ML and is pending before the court.

5.07 Use of new payment methods/systems

BANGLADESH

231 Based on a complaint, BFIU analyst searched into the bank account of Person. X - a low ranking police officer. It was found that X had a total of 30 accounts (four savings accounts, one current account, one loan account and 24 deposit schemes) in six banks ('A', 'B', 'C', 'D', 'E' and 'F') and in a non-bank financial institution (NBFI) 'G'. Ms. Y (Spouse of Mr. X) had two accounts (savings and one deposit scheme) account in bank 'B' and one loan account in 'G'. The couple also had two joint accounts (savings and loan) in bank 'F'.

232 Upon analysis, it was found that frequent cash deposits in small figures (totalling Tk. 28.10 million) had been made to the savings or current accounts of Mr. X and Ms. Y (in bank 'A', 'B', 'C', 'E' and 'F'). Money was frequently withdrawn through ATMs and for the POS payments from these accounts. When these accounts had significant balances, money had been transferred to open FDR, deposit scheme or TDR accounts in the same banks. Mr. X also opened one deposit scheme account in bank 'A' and two TDR accounts in bank 'B' with cash deposit (Tk. 1.09 million).

233 X encashed the amount of deposit scheme/fixed deposit receipt (FDR) accounts to the savings account in bank 'A'. He and his wife respectively took loan of Tk. 1.5 and 2.5 million from NBFI 'G' to buy a flat and transferred this amount to the savings account of Mr. X in bank 'A'. Then Mr. X issued cheques (Tk. 6.28 million) in favour of Mr. Q and R, opened two FDR accounts in bank 'D' with cash withdrawals (Tk. 2.7 million) from bank 'A' and opened two term deposit receipts (TDR) accounts (Tk. 1.1 million) in NBFI 'H' through EFT.

234 Mr. X and Ms. Y jointly took loan of Tk. 3.0 million from bank 'F' by mortgaging the flat and repaid the loan of Ms. Y in NBFI 'G'. Mr. X repaid his loan by transferring Tk. 0.5 million from savings account of bank 'A', transferring Tk. 0.64 million from savings account of bank 'B' and encashing a TDR account (Tk. 0.31 million) of NBFI 'G'.

235 X purchased two saving certificates of Tk. 2.0 million in his name from bank 'B' and four saving certificates of Tk. 3.50 million in his wife's name. Ms. Y also purchased one saving certificate of Tk. 1.0 million in her name.

236 . X mentioned that his profession and source of income is service, and his spouse is a housewife. But the complex transactions occurred in their accounts is not commensurate with their profession. BFIU analyst suspected that proceeds of corruption and bribery may have been transacted into their accounts. The case was disseminated to LEA for further investigation. The LEA has decided to lodge a lawsuit against the alleged persons.

5.08 Laundering of proceeds from tax offences

FIJI

Case Study 1

237 The Fiji FIU received a STR on a couple Mr. and Mrs. X for receiving large remittances and conducting transfers between their business and personal bank accounts. The Fiji FIU established that Mr X received more than FJ$1 million in remittance transactions and Mrs. X received FJ$300,000 in remittances. All these remittances were sourced from China.

238 Mr X is a director of company UVW Ltd and XYZ Ltd in Fiji. Mrs X is a director of RST Ltd in Fiji. Further checks established that Mr and Mrs X and the three companies had not filed any tax returns. Mr. X maintains two personal bank accounts, one of which had an account balance of more than FJ$1 million. Mrs. X maintains one personal bank account with a balance of approximately FJ$0.3 million. A report was disseminated to the tax authority for possible tax offences. Indicators included:

- Very significant account balance in their personal accounts.
- No tax returns lodged with the tax authority.
- Significant inward remittances received.

Case Study 2

239 The Fiji FIU received a STR on Person A, who is alleged to have been diverting business funds into his personal bank account. Person A is the director of three large manufacturing and hardware companies Company X, Company Y and Company Z. The Fiji FIU conducted financial checks and established that Person A had received significant cash and cheque deposits into his personal bank account. It was established that most of the cheques were drawn on the business account belonging to Company X.

240 The Fiji FIU further established that there were few significant deposits conducted into Company X and Company Y's bank accounts, which did not match their usual business activity. The Fiji FIU conducted further checks and noted outstanding tax lodgements for Company X and Company Y. A report was disseminated to the tax authority for possible tax and ML offences. Indicators included:

- Nil tax returns lodged with the tax authority
- Depositing of business funds into personal account

Case Study 3

241 Company X, a motor vehicle dealer was charged some FJ$8 million in taxes and penalties in 2017 for under-declaring sales revenue to avoid taxes. Company X had been manipulating its sales records overtime. The information was provided by a whistle blower and when the Tax Authority carried out a detailed investigation, it was found that the sales reported in the company's tax returns and bank accounts revealed major anomalies.

It also appears that the director of Company X, Mr. X was also involved in other businesses and had investment properties which were also under-declaring sales revenue. Mr. X and Company X have been charged and penalized for tax evasion. Indicators included:

- Business turnover is significant but appropriate income is not declared to the tax authority for tax purposes.

Case Study 4

242 Six companies have been investigated by the tax authority for alleged tax and customs duty evasion amounting to more than FJ$15 million. The companies were involved in import trades and were allegedly under-valuing their goods to evade customs duties. It is alleged that they were also understating their income to evade tax.

243 Furthermore, three companies who were also investigated for the above offences were charged FJ$25 million in taxes and have since paid their taxes and penalties in full.

a) Possible offences included:
- tax evasion and
- customs duty evasion.

b) Indicators included:
- Business turnover is significant but appropriate income is not declared to the tax authority for tax purposes

PAKISTAN

244 As per the account opening form, Mr. HN had agricultural land in rural areas of Pakistan and was also engaged in the construction business in Islamabad. His source of earning was reported to be from agricultural land and construction business.

245 Suspicion was raised by the bank over foreign remittances received in his account from an entity name M/s. EG registered in a foreign jurisdiction, a business of general trading. Since the activity in the account did not match with the nature of the business of Mr. HN, all the accounts of Mr. HN were reported as suspicious to FMU.

246 Analysis of the accounts at FMU and a search of the public domain identified that the entity M/s. EG (the remitter) was owned by Mr. HN himself and the prime business of M/s. EG was import, export and trading. Review of his statement of accounts reflected that since Jul. 2015 to Feb. 2016 USD 68,880 and Euro 115,664.90 was received in the personal accounts of Mr. HN via ten and three inward remittances transactions respectively.

247 The tax status of Mr. HN was found to be active however he had paid meagre tax for the year ending 2015. Since the amount paid by Mr. HN was not commensurate with the turnover reflected from his statement of accounts, the matter was thus reported to tax authorities.

248 Upon receipt of intelligence report from FMU, tax authorities investigated the case during which Mr. HN declared that he is a co-partner of M/s. EG, registered as a free zone entity in the foreign jurisdiction. The remittances received in his accounts were his share of the profit from the referred business, which was then utilized for the purchase of property in Pakistan.

249 As per section 101 (16) of Income Tax Ordinance, 2001 all the individuals are required to declare their foreign sources of income, which was violated in this case. Hence, the remitted amounts in foreign currency during tax years 2013 to 2016 were proposed to be taxed as a dividend income of taxpayer Mr. HN and an amount of Rs. 12.419m (USD 115,000 approx.) including fines and penalties was proposed to be recovered.

250 During the inquiry it was concluded that the taxpayer was under the impression that his income from the UAE based business was exempted from tax on account of remittances received via a banking channel.

5.09 Real Estate, including roles of real estate agents

CHINESE TAIPEI

251 X was the chairperson of K Company and other companies. These companies were not well run and were in a poor state. In order to deceive people to invest in K Company, X forged contracts and purchase orders to pretend that K Company was in good operational condition. X also lured investors with promises of 24 percent ~ 54 percent annual interest.

252 To expand the scale of business, X hired H and other eight people with high commission to assist in attracting investors. Between April 2013 and March 2017, X used accounts of K Company, other companies and employees to receive investments. The total amount of the investment was over NT$14.9 billion. To conceal the proceeds of crime, X bought real estates, cars and high value products under the name of his employees and relatives. In March 2017, X instructed his employees to withdraw about NT$30 million cash from their accounts and hand this cash over to him.

253 An amount of NT$3.7 million cash was confiscated during the investigation. After finalizing the investigation conducted by law enforcement, the case relating to violating of the Banking Act, the Money Laundering Control Act and the offences of document forgery and fraud were referred to the Chiayi District Prosecutors Office in August 2017 for prosecution.

FIJI

254 The Fiji FIU received a request for information from a local law enforcement agency to profile Person P and Company E that was brought to their attention for possible unexplained wealth as a result of corrupt practices.

255 Fiji FIU discovered that Person P entered Fiji as a foreign worker in 2010 and has been working for a government entity. While employed as a government employee, Person P created Company E and Company F. Company E operates as a real estate development company. The Fiji FIU established that Person P, Company E and Company F maintained 16 bank accounts. Person P and Company E held titles for ten properties.

256 It is suspected that Person P received certain kick-backs and bribes while employed in the government entity. Person P then used Company E to conceal these proceeds by using the illegal funds to purchase property.

MALAYSIA

257 Mr. A as a director of a utility agency in one of the states, was entrusted with an infrastructure project development worth more than USD1 billion. Mr. A abused his position of power by awarding projects to selected contractors who are related to him. Kickbacks from the deals were given to Mr. A in the form of cash and other inducements. The overall schemes were also conducted in concert with his wife and senior staff.

258 The kickbacks were mostly received in cash or other forms of luxury goods. The cash was then kept in various spaces in his house and office, or used to buy properties, cars or luxury items.

259 In the course of the investigation, approximately USD47 million was seized from the individuals involved in addition to land, luxury cars, jewellery and accessories.

260 Mr. A, his wife and two of his senior officers were charged with ML offences, and the trial is on-going. Part of the seized funds was forfeited through civil forfeiture provisions.

261 Mutual legal assistance has been sought from related jurisdictions to recover the suspected illegal proceeds channelled to overseas bank accounts. The ML methods used include:

- Use of cash;
- Purchase of valuable assets;
- Use of nominees and third parties; and
- Wire transfers / Use of foreign bank accounts.

PAKISTAN

262 Mr. X was a government contractor. As per media reports, the suspect was allegedly involved in property fraud worth millions of rupees stolen from innocent people through different housing schemes. The suspect was maintaining multiple personal and business accounts with different banks. The average monthly turnovers and the aggregated debits and credits of the suspect's accounts were very high. It was observed that during the last three years the suspect had routed funds from different accounts maintained through various banks.

263 The suspect was routing a high value of funds through his accounts by using different modes of transactions i.e. cash and clearing. It was observed that the funds deposited through cheques were subsequently withdrawn in cash. The suspect was also structuring the transactions in order to avoid the minimum reporting threshold of CTR. Furthermore, while reviewing the SOA of the suspect's USD account, it was observed that the funds deposited in cash were subsequently transferred through foreign telegraphic transfers and multiple foreign demand drafts issued in favour of unrelated individuals. In addition, the suspect was remitting high value funds to foreign-based real estate projects for the purpose of purchasing properties in that jurisdiction.

264 The matter was referred to the LEAs for the suspected offence of fraud and embezzlement of public funds.

SINGAPORE

265 A real estate agent and conveyancing lawyer were charged in November 2017 with failing to report to the authorities a suspicious property deal involving a Chinese businesswoman convicted in China for financial fraud.

266 Investigations established that the real estate agent and conveyancing lawyer had reasonable grounds to suspect that more than S$5,000,000 used by the Chinese businesswoman in her purchase of a property in Sentosa Cove might represent the proceeds of her criminal conduct. The arrest of the Chinese businesswoman for her involvement in one of China's biggest Ponzi schemes had been widely reported by various international and local media platforms. Despite the adverse news reported on their client, they failed to file any suspicious transaction reports on the said private property purchase.

267 Both the real estate agent and conveyancing lawyer were convicted and fined S$10,000 in April 2018 and June 2018 respectively.

THAILAND

268 A high ranking police officer, C and his associates committed offences related to malfeasance in office, illegal gambling business, and receiving a 3-5 million THB bribes from police officers who wanted to buy positions. The officers were also demanded to pay a sum of 10,000 – 2 million THB a month. C. also took bribes from oil smuggling gangs in amount of 2-5 million THB a month during

2011-2014. The Royal Thai Police, Revenue Department, NACC, the Army and AMLO conducted financial investigation and analysis of more than 30 persons involved with the network.

269 It was found that the proceeds of crime had been laundered through buying 111 items of land, cars, antiques, bank deposits, with an approximate value of 560 million THB (US$17.5 mill).

5.10 Association with human trafficking and people smuggling

FIJI

270 In March 2017, the Fiji FIU received an information request from the Fiji Police Force on a convicted felon Mr. A. Mr. A is a Fijian national with New Zealand residency who was convicted of human trafficking in New Zealand in December 2016. The information request received from the Fiji Police Force was a financial background check on the children of Mr. A namely: a daughter, Child S, born on 13 September 2007 and a son, Child X born on 17 June 2014. The children then aged ten and three were considered minors, but further checks confirmed that they maintained bank accounts with a local bank. Bank checks confirmed that a total of FJ$13,900 of deposit transactions and FJ$13,000 of withdrawal transactions were conducted on the bank account of Child X (three years old).

271 Furthermore, it was also established that a total of FJ$38,268 of deposit transactions and FJ$37,000 of withdrawal transactions were conducted on the bank account of Child S (ten years old). It appears that Mr. A had been using his children's bank accounts to conduct suspicious transactions.

272 The Fiji FIU issued a report to the Fiji Police Force to assist in their investigations on the alleged beneficiary of the bank accounts. Indicators included:

- Significant deposit and withdrawal transactions conducted through minors' accounts.

JAPAN

Case Study 1

273 A man engaged in a prostitution business received cash totalling 1.8 million yen by bank transfer as a commission from an adult shop. He was arrested for violation of the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

Case Study 2

274 A suspect was managing a farm through employing foreign nationals as farmers then keeping them in Japan beyond the authorized period of stay, to work at the farm and other places. (This act constituted a criminal offence of promoting illegal work). The suspect acquired certain amounts of vegetables through the promotion of the illegal work, which were the criminal proceeds in this case, and disguised the disposition of the vegetables by selling them to a bona fide third party under a false name.

275 In this case, the suspect was sentenced to both imprisonment and fine. Moreover, the suspect was also sentenced to confiscation of monetary claims derived from the criminal proceeds and property, which amounted to approximately 4 million yen (US$36,500) in total.

NEW ZEALAND

276 In September 2016, the High Court found 46-year-old Mr. F.A guilty of 15 counts of trafficking Fijians to New Zealand on false promises of NZD900 weekly wages for fruit picking. He charged the workers exorbitant fees and then exploited them upon arrival by forcing them to work illegally and live in overcrowded conditions, underpaying them and threatening them with deportation if they complained. Mr. F.A was also found guilty on 16 counts of aiding and abetting people to enter or remain in the jurisdiction unlawfully. He pleaded guilty to charges of exploitation, including failing

to pay workers a minimum wage or holiday pay, as well as aiding and abetting workers to breach the conditions of their visas. Mr. F.A, the first person to be convicted of people trafficking in New Zealand, was jailed for nine and a half years.

PAKISTAN

277 Mr. A, was listed in FIA's Red Book of most wanted human trafficker. The suspect was involved in human trafficking since 2006. FIA arrested him in January, 2006 but he escaped from custody. The suspect's name was also mentioned in World Check and various news clippings mentioned him as one of the most wanted human traffickers.

278 The suspect was maintaining an account in various branches of different banks namely ABC Bank Ltd, DEF Bank Ltd and GHI Bank Ltd and was maintaining PKR and Euro accounts. Further, he was also found to be maintaining proprietorship accounts.

279 Ms. B, one of the major counterparties of the suspect was also reported to FMU on regulatory violations by using a personal account for business transactions.

280 The details of accounts of Mr. A and Ms B, was reported to LEA for alleged involvement in human trafficking.

THAILAND

Case Study 1

281 A human trafficking network conducted incoming and outgoing transfers through commercial banks. Five bank accounts were opened under the suspect's name and his associates within the surrogacy company. Account types included savings, fixed, and foreign currency accounts.

282 The network paid a salary for a manager in Thailand by transferring funds into a bank account in Chinese Taipei and also provided in cash for expenditure in Thailand.

283 Air fares for employees and doctors' fees for pregnancy tests were paid by credit cards issued by Chinese Taipei banks. Wages for surrogacy women were transferred from abroad into employees' personal accounts and others were paid in cash at the company.

Case Study 2

284 The Royal Thai Police (RTP) Human Trafficking team undertook an investigation regarding the smuggling of illegal migrants into Thailand, after conducting searches of a vehicle and found two suspects transporting 98 illegal migrants into the jurisdiction. RTP sought assistance from AMLO in conducting financial investigations to utilise the powers available to them under the AMLA.

285 Due to the close collaboration between RTP and AMLO and their financial investigation skills as well as the cooperation of banks, the authorities were able to uncover a large network of offenders involved in smuggling as well as the financing and laundering of profits. AMLO was able to trace financial transactions from the arrested suspects back to additional key suspects by virtue of the bank statements and wire transfer details. They found that accomplices and family members were used for the purpose of their bank accounts and financial transactions. A wide range of financial enquiries were conducted into associates and family members of suspects which ultimately proved successful in tracing proceeds of crime back to the principal offenders. CCTV footage of suspects withdrawing and depositing cash, telephone records, previous human trafficking cases and significant assistance from banks proved successful in expanding investigations to the larger network.

286 Approximately 70 percent of the investigation was based on financial intelligence. Joint financial investigations between RTP and AMLO revealed two main accounts, one was the sister of

an offender and the other was an associate. The accounts had significant turnover with THB 380 million (USD 13.5 million, approx.) between them. The relevant transactions under the abovementioned accounts were fund transfers from the border areas e.g. Padang Besar, Sungai Kolok, Sadao, and from Hatyai which are unusual transactions. Banks had filed STRs indicating suspicion that the transactions are not in line with customer's profile. As a result, authorities were able to locate the mastermind of the criminal enterprise and identify high level officials and others involved in the offense.

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

HONG KONG, CHINA

Case Study 1

287 Between 2007 and 2011, a female property agent made false representations to innocent persons that an investment company would acquire various old buildings for redevelopment purposes. She asked these persons to make payments in advance to acquire these buildings in order to resell to the investment company for a profit. A total of HK$85M (approx. US$10.9M) was paid to the property agent's designated bank accounts including her boyfriend's bank accounts in Hong Kong. When some of the landlords did not receive rental payments, the investors found out the acquisitions were bogus and reported it to the HKP in November 2011.

288 Fund flow analysis by the HKP on the HK$85M criminal proceeds later revealed that some HK$20M (approx. US$2.6M) had been cashed out by the defendant. In July 2017, the defendant was convicted of seven counts of ML upon his guilty plea. He was sentenced to 42 months' imprisonment.

Case Study 2

289 Arising from a corruption investigation it was revealed that the fiancé of the defendant, who was an assistant admissions officer of an international school, asked parents seeking admission of their children to the school to make donations. The parents were asked to make payments to the defendant as it was falsely represented by the defendant's fiancé that the defendant was a senior officer of the school and that a donation was required for their children being given priority for admission to the school. The defendant received payments of HK$2.1 million from the parents.

290 In May 2017, the defendant was convicted of ML offences and received a custodial sentence of 24 months. The defendant's fiancé was convicted of fraud and was sentenced to 34 months' imprisonment.

PAKISTAN

291 Multiple STRs/CTRs were reported on four brothers A, B, C and D. Mr. A, B and C were renowned businessmen and running a company XYZ, however Mr. D was a non-resident. The group of family members was engaged in currency exchange transactions and deliberately avoided the State Bank of Pakistan threshold to purchase foreign currency in a single day, through structuring and utilizing different exchange companies. They were maintaining multiple local currency and foreign currency accounts at different banks and a particular transactions pattern was adopted by the brothers, whereby they were withdrawing funds from their PKR accounts being maintained at different banks, followed by the purchase of USD from open market in tranches and then depositing into foreign currency accounts in same bank, afterwards the funds were being remitted out of the jurisdiction to their personal accounts.

292 In addition, it was noticed that huge amount of funds were gifted by the elder brothers Mr. A and B to the younger brother Mr. D who was non-resident. Further, the tax history of family members revealed that they had not paid income taxes despite the high turnover in their accounts.

293 The intelligence was shared with the LEA and regulator SBP for action deemed appropriate.

THAILAND

294 Thai authorities investigated a drug trafficker and a significant drug producing factory was located near the Thai/Myanmar border. Authorities uncovered the fact that the defendant paid hill tribe people to transport tablets to his customers, one of which was eventually caught and confessed. The defendant and his mistress were subsequently investigated and it was found that the defendant had transferred money to his mistress.

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

JAPAN

295 A senior member of Boryokudan (Japanese violent groups) received 90,000 yen in cash as protection money from a casino manager while knowing that the money was paid from proceeds obtained through habitual gambling. They were arrested for violation of the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

THAILAND

296 AMLO received a STR from a bank and found that Mr. Z had about 1 billion THB in financial transactions, however earned an income of less than 10,000 THB per month. Mr. Z transferred funds totalling 45 million THB to the bank account of Mr. M and the transactions attempted to avoid reporting obligation. The investigation found that Mr. Z was an owner or beneficiary of an online gambling website for football betting. Prosecutors brought charges against Mr. Y, Ms. D, and Ms. L for an offence under the Gambling Act and the court ordered imprisonment and the forfeiture of property. Further information was discovered during the court proceedings on money transfers among gambling players' bank accounts and the website agent's bank account. The enquiry officer filed a petition against Mr. Z and ten of his associates for arranging online gambling (football betting). The competent officer examined financial trails of related persons and offenders and found that there was a relation between the financial trails and a STR.

297 Moreover, it was found that Mr. Z and associates visited Ms. D and Ms. L in prison. The competent officer also interrogated the administrator of the online gambling website and confirmed that Mr. Z and his associates were the website owners. The owners used the illegal proceeds to purchase assets, investments and securities in the stock market and payed large sums on life insurance.

5.13 Mingling (business investment) and investment fraud

BRUNEI DARUSSALAM

298 X was charged with 20 counts of ML and 17 counts of cheating for offering a fake investment scheme to several individuals between February 2015 and October 2016. The Commercial Crime Investigation Division, Royal Brunei Police Force found X had cheated a total of $147,581 from several victims.

299 In one incident, X met a victim at a local food court and requested the victim pay a minimum amount of $500 in order to be rewarded with a monthly investment profit of $3,000 for their lifetime. The victim proceeded to hand X cash to participate in this false investment scheme. The victim was then informed that the contribution was below the required investment amount and met X soon after to hand over two gold bracelets and three gold rings to make up the amount. X informed the victim as the items' values were assessed to be at $600, the victim would then be assured of a monthly profit of $6,000 for their lifetime.

300 In another incident, X and another individual met a victim at a restaurant and asked the victim to pay $6,350 to participate as a full member of the investment scheme. They told the victim that he/she would be rewarded with a Mercedes Benz S280 car, $200,000 in cash, $60,000 in cash every month for their lifetime, a house valued at $400,000, a Rolex watch, a trip to perform the "Haj pilgrimage", a VIP Global Card purportedly allowing the holder to withdraw up to $200,000 from any ATM at any global location and $3,000 in cash every month for 15 years.

301 In other incidents, victims were informed they were investing in charitable programmes known as 'Dana Pelaburan Amal Jariah' (Benevolent Investment Fund).

302 Generally victims were approached through face-to-face networking of personal friends, X's former colleagues or through another person. It was found that X had remitted the funds to another individual in a foreign jurisdiction through a well-known remittance service provider. X was charged on 8 April 2017 and was later sentenced to two years imprisonment for the offence of ML and three years' imprisonment for the cheating offence.

CHINESE TAIPEI

303 X, Y and Z were the chairperson, supervisor and director (respectively) of *W Company*. Between November 2015 and March 2016, in order to seek proceeds of crime and increase the shareholding, X arranged *W Company* to buy moulds and equipment from S Company and three other companies which were held by them. These products were unnecessary and of low economic benefit to *W Company*. *W Company* thus had to pay approximately NT$400 million to *S Company* and three other companies. The funds were then transferred to F Company and other two companies' accounts with the instruction of X. X allocated NT$300 million of abovementioned funds and borrowed NT$300 million from loan lenders to buy *W Company's* NT$600 million capital increase shares. The other funds were used to buy shares from other investors.

304 The newly bought shares were in the name of X, Y, and Z, F Company and other two companies etc. The shares were then transferred to H Company and another three companies controlled by X. The rest of the funds were used by X for personal purposes. In June 2016, X used the same script to make *W Company* pay about NT$500 million to companies controlled by X to buy useless moulds and equipment. X then instructed an employee to transfer the payment to F Company and two other companies' accounts. The funds were used by X to buy *W Company's* shares from other investors.

305 The funds that X embezzled from *W Company* were used by them for purchasing *W Company's* shares to increase their shareholding. *W Company* raised new capital in an amount of NT$600 million, however, it has not obtained enough funds because of the actions conducted by X which resulted in huge damage to *W Company*.

306 In order to pay back the NT$300 million loan which became due in January 2017, X arranged raising new capital with an amount of NT$300 million of H Company which controlled by X and then arranged *W Company* and its subsidiary to subscribe NT$255 million and 45 million respectively. The funds were transferred to H Company's account in January 2017. X instructed an employee to transfer the funds as the repayment to designated accounts of lenders.

307 After finalizing the investigation conducted by law enforcement, the case relating to violating of the Securities and Exchange Act and the Money Laundering Control Act, law enforcement referred it to the Taoyuan District Prosecutors Office in September 2017 for prosecution.

MALAYSIA

308 Malaysian Authorities coordinated a joint investigation on syndicate groups running illegal and fraudulent investment schemes known as 'money games'. The groups have been luring the public

domestically and internationally into their financial schemes by offering high returns over short periods.

309 In this scheme, money invested is used to purchase redeemable points in the form of "virtual coins". It was claimed that after 30-days the "virtual coins" will triple in value and will further grow depending on fluctuating unit prices plus the amount of bonus points earned. The "virtual coins" can be sold at a later time at an online market for cash or the purchase of goods and services from participating merchants.

310 The joint investigation focused on the violation of provisions related to the offering of pyramid schemes and illegal e-money businesses. Bank accounts amounting to more than USD50 million and other assets were frozen as part of the investigative process.

311 In the course of the investigation, it was identified that proceeds obtained through the scheme were used to pay for professional services such as lawyers and to purchase properties. There were also domestic and international transfers made to third party accounts without clear economic purposes. Mingling of the proceeds for business investments mainly in property development were also identified by the investigators.

312 The ML and predicate offence investigation into the syndicate is on-going. The ML methods used include:

- Use of virtual currencies;
- Use of professional services (lawyers);
- Use of internet (international banking, investment platform);
- Use of new payment methods / systems;
- Real estate;
- Use of nominees and third parties;
- Mingling (business investment); and
- Wire transfers / Use of foreign bank accounts.

THAILAND

313 A syndicate operated its trafficking business in the southern parts of Thailand, including illicit cross-border trade with a neighbouring jurisdiction. Customs officers arrested four suspects and seized 134,000 amphetamine tablets, three cars, jewellery, luxurious electrical appliances and 6,000,000 THB in cash. They also seized assets including one house and three condominiums. The customs officers found that the gang had opened a luxury car dealer enterprise in Bangkok as a place to launder illegal proceeds and to facilitate direct exchange of drug payments.

5.14 Use of shell companies/corporations

CHINESE TAIPEI

314 Mr. A was the chairperson of J Company which had no business activities. In 2015, Mr. A provided his personal account with Bank C and J Company's account with Bank E to Mr. LP who was a national of K jurisdiction and Mr. P with unknown personal information. In May, June and October 2015, Mr. P used the identification of victims to send emails to financial institutions. The financial institutions were misled by these emails and transferred funds to J Company's account from the victims' accounts. After confirming the transactions, Mr. A was instructed by Mr. LP to withdraw cash and then deliver the funds to Mr. LP. The total amount of funds transferred from fraud victims' accounts was about NT$19 million. The Taoyuan District Prosecutors Office indicted J Company, Mr. A and Mr. LP for the offences of fraud and violation of Money Laundering Control Act in August 2017.

HONG KONG, CHINA

315 Arising from a corruption investigation it was revealed that the defendant purchased a shell company at the request of her friend and was appointed the sole director-come-shareholder of the company. The defendant was also the sole authorised signatory to the bank account of the shell company. Between January 2005 and December 2008 the shell company received deposits totalling HK$250.45 million, being proceeds of Letter of Credit fraud, and disbursed HK$250.44 million to various companies and individuals during the same period.

316 In March 2017, the defendant was convicted of ML and sentenced to three years imprisonment.

NEW ZEALAND

Case Study 1

317 A New Zealand shell company was set up by a New Zealand trust and company provider based in Vanuatu. The shell company was registered on behalf of an unknown overseas client and nominees were used to hide the identity of the beneficial owners. The actual business of the shell company was not apparent and was not indicated by the company name. The address listed on the companies' register was the same virtual office in Auckland as the TCSP. The nominee director resided in Seychelles, and the nominee shareholder was a nominee shareholding company owned by the TCSP. The nominee shareholding company was itself substantially a shell company and had been used as the nominee shareholder for hundreds of other shell companies registered by the TCSP. News reports indicate that a power of attorney document transferred the directorship to a Russian national who had sold his passport details, with a bank account opened in Latvia. Trade transactions were conducted with several Ukrainian companies including a state-owned weapons trader. The contracts were then cancelled after the funds had been transferred and refunds were made to different third party offshore companies. Transactions were also made with three other New Zealand shell companies registered by the same TCSP, using the same nominee director, nominee shareholder and virtual office address as Tormex. News reports indicate that all four shell companies had been involved in laundering USD40 million for the Sinaloa drug cartel based in Mexico.

Case Study 2

318 Companies registered in New Zealand by a Vanuatu-based TCSP operated by New Zealand citizens are suspected of acting as shell companies that facilitate crime in foreign jurisdictions. The TCSP acted as nominee shareholders and provided nominee directors who resided in jurisdictions such as Vanuatu, Panama and the Seychelles – in the case of Company A, the employee recruited to act as a director likely had no knowledge of the activities taking place, as they had no previous involvement in any of the TCSP activities. Crimes include smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and ML. Company A was one company set up by the TCSP, which leased the plane that was caught smuggling arms. 73 companies registered in New Zealand by the TCSP were suspected of acting as shell companies which facilitated crime in foreign jurisdictions. Crimes included smuggling of illegal goods, arms smuggling, tax fraud, investment fraud and money laundering.

PHILIPPINES

319 Individuals representing themselves as investment advisors contacted Mr. X, an Australian citizen and owner of Y Ltd., enticing him to open a trading account with Z and Z Co. (a shell corporation), an Australian entity posing as a legitimate investing firm that provides advice and brokerage services for US securities. Mr. X engaged in the purchase and sale of stocks, which turned out to be non-existent. In a span of six months, he lost approximately USD1.8 million.

320 Mr. X remitted his payments to F Ltd. (another shell corporation and dummy broker account), an entity based in Hong Kong, which allegedly conducts securities clearing services for Z and Z Co. Portions of the remittances of Mr. X to F Ltd. were also traced to have been sent to DRR (also a shell corporation), a Philippine SEC-registered entity. The flow of funds from the victim (Mr. X) to F Ltd, then to DRR was indicative of "offshore layering". The funds remitted to DRR were immediately withdrawn after receipt of the wired funds.

321 DRR also received funds from various overseas entities tagged in several online forums including involvement in a boiler room scam. These remittance senders are G Co. (Hong Kong), CBP (Macau), A Group (USA), and SM Brokerage (USA).

322 Mr. X, through investigations done by his legal counsels, discovered that a significant number of Internet Protocol (IP) addresses being used by individuals associated with Z and Z Co. in sending emails were traced in a major city in the Philippines.

THAILAND

Case Study 1

323 Company U registered as a direct sale business but, in fact, did not run the business in accordance with the registration. Rather, it offered unit trusts through an online system under the name U-TOKEN. The company lured people to invest and promised to give returns in money or other assets at a high rate. Such return was derived from seeking more members and the increased value of the U-TOKEN without selling any merchandise. Company U's activity constituted an offence of public fraud. Moreover, the Company U operation was complex and run through several subsidiaries involving large networks as a transnational organized criminal group. The gang transferred funds into, and out of, Thailand as well as used the ill-gotten gains to buy lands, properties, cars etc. in an attempt to launder the assets obtained from the commission of the offence.

Case Study 2

324 Mr. J, a Dutch national, and his associates engaged in the drug trade as a transnational organized crime syndicate. Evidence was found for probable grounds to believe that the assets had been obtained by Mr. J and associates during engagement in an activity constituting a drug offence, which is a predicate crime under AMLA. They had opened a coffee shop chain as a front business for their illegal activity earning a yearly income of 600-800 million THB.

5.15 Association with illegal logging

THAILAND

325 Ms. C had been previously arrested for allegations involving the trafficking of tigers from Malaysia to Thailand into Vietnam via Laos although charges were never laid against her. Later, her brother Mr K was arrested in a forest north of Bangkok. It transpired that Mr K ran a significant network which smuggled protected Thai Rosewood into China as well as other networks involved in elephant ivory and live pangolin smuggling. Arresting officers discovered significant amount of cash in his possession, ostensibly to purchase the rosewood. AMLO sought assistance from the FIU of Vietnam to assist them in unveiling Mr K's complex network of businesses, associates and multi-jurisdictional money transfers. It was estimated that K's network laundered as much as USD 35 million between 2011 and 2014 using different and complex methodologies.

326 Authorities discovered that a tiger zoo owned by Mr K's sister, Ms. D in Thailand was used as a front for the smuggling.

327 Mr K and his wife were charged with conspiracy to commit illegal logging and trafficking of Siamese Rosewood, attempting to bribe officials and ML. Ms. D was charged with ML.

5.16 Currency exchanges/cash conversion

AFGHANISTAN

328 A foreign exchange dealer was arrested in December 2016 in Baghlan Province on charges of embezzlement of AFN 24,415,811 funds of Bank A in collusion of bank employees and laundering AFN 6,740,000. The primary court of the Anti-Corruption Justice Centre convicted the accused on charges of ML and sentenced him to two years custodial imprisonment, a cash penalty of AFN 50,000 and also to pay cash penalty equivalent to the laundered funds.

BRUNEI DARUSSALAM

329 Five individuals from a foreign jurisdiction arrived in Brunei Darussalam between 21 and 23 June 2016 on social visit passes and brought with them counterfeit ATM cards.

330 Between 24 and 25 June 2016 all five individuals simultaneously went to various ATM machines to use the counterfeit ATM cards and its accompanying personal identification numbers (PIN) to gain access to the computer program within the ATM machine. Once access was secured, they withdrew large amounts in cash in multiple transactions.

331 The Royal Brunei Police Force (RBPF) apprehended all five individuals at the departure gate of Brunei International Airport on 25 June 2017, based on evidence from CCTV footage at the ATM. The investigation uncovered 43 counterfeit ATM cards were left behind at one of the ATM machines as the transaction attempts were unsuccessful.

332 Three of these individuals were also found to have used a licensed money changer to convert the illegally obtained cash to a total of $34,550 to US Dollars. All converted cash was recovered by the RBPF.

333 On 26 August 2017 the individuals were sentenced to various terms of imprisonment ranging from four to 13 years for charges under Computer Misuse Act, Cap 194, and Penal Code Cap 22. Prosecutors are pursuing proceedings under the Criminal Asset Recovery Order, 2012 for the confiscation of funds stolen by the five individuals.

PAKISTAN

334 A STR was reported on individuals Mr. A and Mr. B. Reportedly, they were cousins, and Mr. A was settled abroad, while Mr. B was managing business properties in Pakistan. A STR was reported by an Exchange Company for making high value transactions of currency exchange in structured manner. During the analysis, it was found that they had purchased a high volume of US dollars from open market. The suspects were maintaining multiple joint accounts in PKR and USD at ZXY Bank. Transaction pattern in their accounts revealed that a large amount of funds were credited to their PKR account through clearing and internal transfers. The funds were being withdrawn from the PKR accounts through cash transactions, followed by purchase of USD from different exchange companies and then deposited into foreign currency accounts of the suspects. Afterwards, the funds were being remitted out of the jurisdiction.

335 On further probe it was found that, the Mr. A had sold his property and the funds were placed into the PKR accounts. However, the level of financial activities was much higher than the sale proceeds of property; hence it was suspected that they have undervalued the sale agreements to evade taxes. Further, the profession of Mr. B was also doubtful as the proof of business provided by the suspect contradicts the location and existence of the company. It was also found from internal database that Mr. B is employee of same bank where the accounts were being maintained. The authority to operate account was given as ‘either or survivor’ in all the joint accounts, which means any one singly can operate the account and it was suspected that possibly Mr. A was the true owner of the funds who was residing out of jurisdiction, while the transactions were being made by the Mr. B.

336 Furthermore, the tax status of individuals was not in line with the level of financial activities in accounts.

337 It was found that they had deliberately adopted such transaction patterns and behaviours to avoid the regulatory authorities; and they had utilized the banking channels and exchange companies to remit a huge volume of funds out of jurisdiction through structuring and other tactics.

338 On the basis of abnormal account activities it was concluded that they were involved in unauthorized capital flight and tax evasion, therefore the intelligence was shared with LEA.

THAILAND

339 Upon receiving requests from the Embassy of the Netherlands, as a matter of urgency, the OAG requested AMLO to freeze and seize assets of Mr. J and his associates who may transfer, dispose, conceal or hide their assets connected with the commission of offences. Mr. J and his associates had trafficked Cannabis, a narcotic drug, through their company network in the Netherlands which they ran as an organized crime group. The group laundered proceeds from selling narcotic drugs by funds transfer through bank accounts of legal persons overseas to Thailand and converted the money or property via cross border cash transportation, bank deposits, front companies, land sales and having nominees to hold the money or property.

5.17 Currency Smuggling

AFGHANISTAN

Case Study 1

340 On 22 January 2017, a person (person X) arrived at Kabul International Airport through a direct flight from jurisdiction Y. He was found in possession of cash exceeding the regulatory threshold that had not been declared to the Customs Department at the airport. Upon a physical search, CHF 23,000, USD 238,700, INR 141,500 and an amount of EUR 95,910 were found with person X. After a thorough investigation, the person was fined 15 percent of the total seized cash (AFN 3,569,282 approximately USD 52,313).

Case Study 2

341 On 8 June 2017, following a physical search of the bags of a suspected person (person A) at Kabul airport, four packages of gold bars weighing 11.724 kilograms were found in his bags. During the inquiry at the airport, person A has stated that: "I had placed gold bars at my shoes and after passing from x-ray machine at the exit point of Customs, I sat on the chair, took the packages off my shoes and placed those gold bars in my bags and then handed over the bags to the airline". However, after checking the security cameras of the airport, it was noticed that person A had only one bag with him while entering to the airport's terminal and the second bag was brought to the terminal by a second person. It was revealed that both persons entered the toilet of the terminal after one another and while coming out from the toilet, one of them went to airline's counter and handed over the bags. It is also noticed that after the bags are handed over to the airline counter, person A goes into the terminal's hall while person B leaving the airport's terminal. After a thorough investigation of the case by the competent authorities, the subject was fined AFN 4,980,930 (USD 72,558).

Case Study 3

On 12 December 2016, a person (person X) was ticketed on a direct commercial flight from Kabul International Airport to jurisdiction Y. The subject made no attempt to declare to an authorized officer that he was carrying USD 28,750 cash. According to the procedures, at the departure checkpoint of the airport, the subject was stopped and his bag was searched on suspicion of concealing undeclared cash in an amount above the regulatory threshold. Upon searching the subject at the first customs'

checkpoint of the airport, customs officials found an amount of 19,250 USD concealed in the suspect's shoes, travel bag, and trousers as well as 9,500 USD in his jacket pocket. After the investigation, the person was fined AFN 288,712 (USD 4,310) by the Customs Department for breaching the regulations.

FIJI

342 On 14 August 2017, Mt. Buren Randolph, a 35 year old businessman arrived with his wife on Tarawa Flight FJ230 for transit to Hong Kong. He failed to declare currencies to the value of FJ$37,719.18 (AUD & USD currency). The money was found in a suitcase and Mr. Randolph did not know how to read and write in English.

343 Mr. Buren Randolph pleaded guilty for contravening the BCR reporting requirements and was ordered to pay FJ$4,000. The undeclared cash was returned to him.

THAILAND

344 Mrs. M, of Lao PDR nationality, tried to smuggle 30 million THB in cash to Lao PDR by concealing the money in a pick-up truck. The customs officers arrested Mrs. M at the second Thai-Laos Friendship Bridge crossing point. AMLO is still looking into her network for ML.

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

FIJI

345 Two Cypriot nationals arrived in Fiji on 12 December 2017 from Hong Kong. Both nationals were arrested by the Fiji Police Force on 19 December 2017 for conducting transactions from ATMs using cloned credit/debit cards. Mr. Loizos Petridis and Mr. Cleanthis Petrides have been jointly charged with 293 counts of money laundering and attempt to obtain property by deception in Fiji.

JAPAN

346 A man made illegal money lending business through borrowing and posting bills or checks for main and interest payments to deposit-taking institutions which transferred the money to accounts opened under other parties' names. Those have been involved in ML by misusing bills or checks for quick transfer of criminal proceeds or disguising criminal proceeds as legal funds.

SINGAPORE

347 A former bank officer used the accounts of his team managers to fraudulently increase the temporary credit limits of his own credit cards from S$15,000 to S$106,500. He also made unauthorised credit balance refunds of S$9,300 on his credit cards.

348 With the increased credit limits, the bank officer purchased gold bars and immediately sold them for S$30,150. He also used the increased credit limits to purchase S$65,834.08 worth of casino chips, which he subsequently used for gambling in overseas casinos. He used the cash and credit balance refunds to finance his gambling habit and to pay off the debts he owed to banks and unlicensed money lenders.

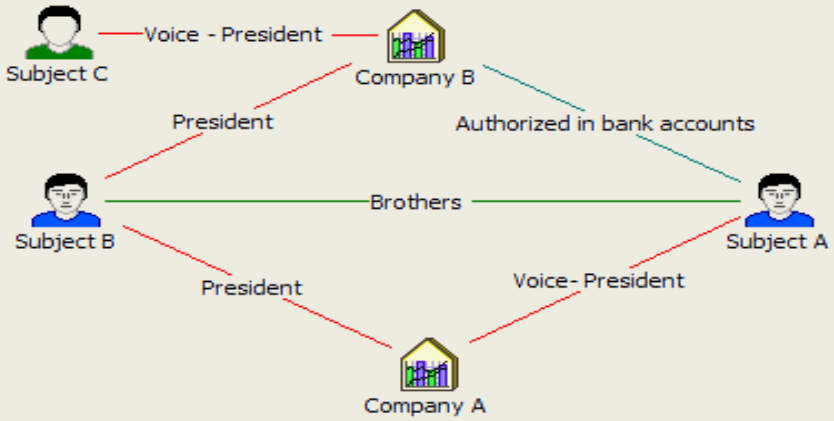
349 He was found guilty of computer misuse and ML and was sentenced to 41 months' imprisonment.

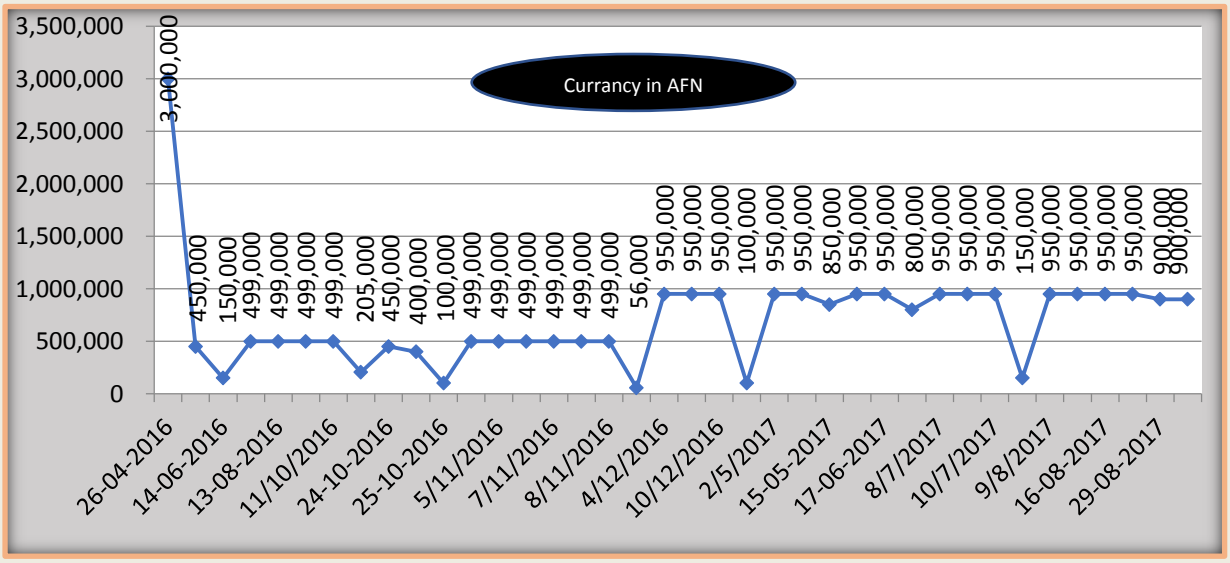
5.19 Structuring (smurfing)

AFGHANISTAN

350 Reporting threshold for Afghanistan banking institutions is AFN 1,000,000 (USD 14,500). Any two or more transactions that occur within two consecutive days of one and another, which transactions aggregate AFN 1,000,000 or greater should also be reported. Based on the STR filed by bank A, the subject was carefully structuring the placements to avoid the above reporting threshold bypassing the two consecutive days reporting requirement.

351 The subject (s) deposited the funds into the banking system which was 52 times more than the subjects declared income.





352 Although an amount of AFN 26m (USD 382,000) is placed into the banking system, but due to organized structuring (38 placements), no large cash transaction report was filed with the FIU. In addition to the structuring, additional suspicions were also identified and the case was disseminated to law enforcement authorities for investigation.

5.20 Wire Transfers/Use of Foreign Bank Accounts

BRUNEI DARRUSALAM

On 29 October 2017 a foreign national, Z, was charged for possession of contraband goods under Section 146(1)(d) of the Excise Order, 2006 as well as three charges of ML under Section 3(1)(b) of the Criminal Asset Recovery Order, 2012. Z pled guilty for possessing 118 packets and 2,058 cartons of cigarettes and three boxes containing alcoholic beverages without a permit. During investigations, Z admitted to have purchased all contraband goods from a foreign jurisdiction.

353 The investigation found that Z was involved in ML whereby some of the funds from the sale of contraband goods amounting to $2,974 were remitted to an individual in a foreign jurisdiction between January 2016 and October 2017. Z was fined a total of $1,600,000 under the Excise Order, 2006 or three years imprisonment in default, and sentenced to six months imprisonment for each ML charge to run concurrently.

CHINESE TAIPEI

354 Mr. LH was the chairperson of T Company. Between 2007 and 2008, Mr. LH set up P Company and another six companies abroad and opened accounts for these companies. During 2008 and 2009, in order to obtain the proceeds of crime, Mr. LH signed contracts of shares management or agreements of technical shares allocation with 24 employees with the claim that he was worried about the low income of the company in the future and wanted to help employees to manage the bonus. These contracts or agreements specified that T Company formally managed the shares and bonuses originally held by the employees. Mr. LH instructed these employees to sell shares in the stock market at a dedicated time and price. Deducting necessary fees, the employees transferred the settlement to P Company's account in Hong Kong, China. The total amount of the funds was about NT$100million.

355 To avoid the investigation of a law enforcement agency, Mr. LH instructed an employee to spread the funds into several legal persons' accounts controlled by Mr. LH. After finalizing the investigation conducted by law enforcement, the case involved the violation of the Securities and Exchange Act and the Money Laundering Control Act and were referred to the Shi-Lin District Prosecutors Office in July 2017 for prosecution.

FIJI

356 The Fiji FIU received two STRs on an engineering company, Company Y for conducting significant, regular cash and cheque deposit transactions. The Fiji FIU conducted analysis and established that Company conducted several unusual transactions within three months.

357 It was established that Company Y maintained five business bank accounts at two different banks. It was further established that in the last two years, the total deposit transactions that were conducted in the two bank accounts amounted to approximately FJ$4.5m.

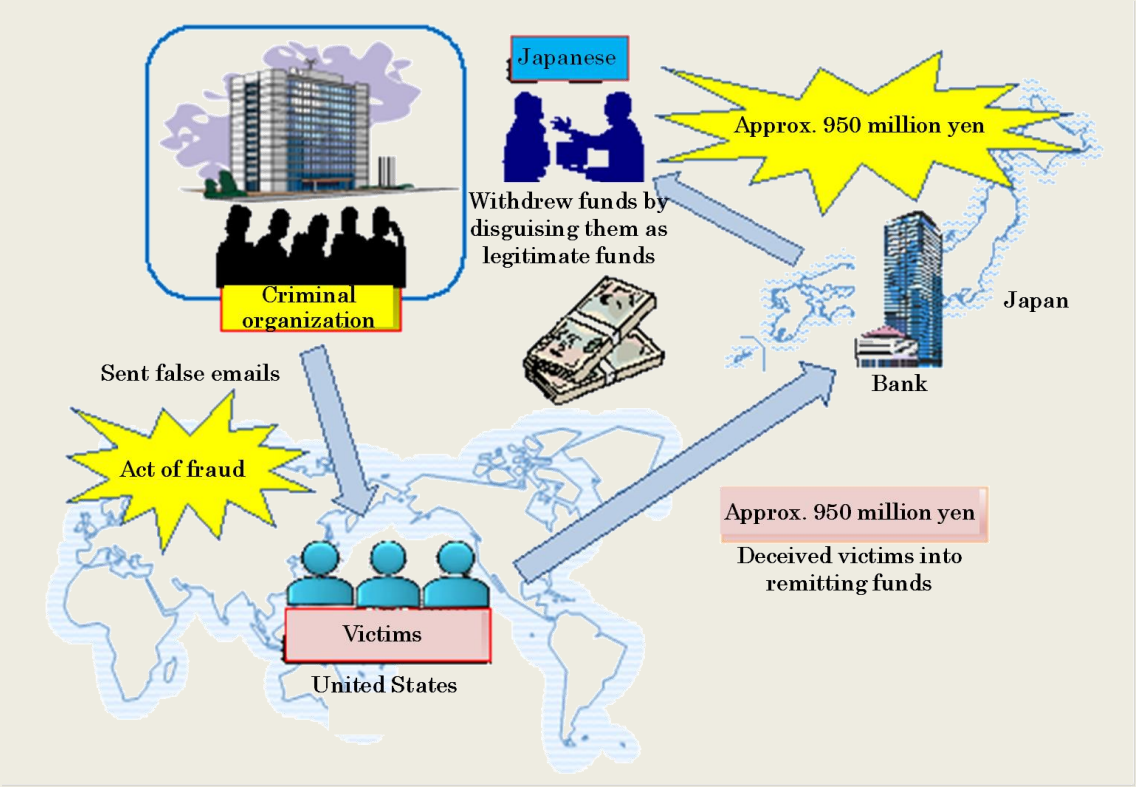
358 The Fiji FIU also established that Company Y had not lodged any tax returns with the tax authority for the past two years. A report was disseminated to the tax authority for possible tax offences. Indicators included:

- Conducting several deposits below the reporting threshold of FJ$10,000.
- No tax returns lodged with the tax authority.

JAPAN

359 Japanese men had sent falsified transaction emails to victims in U.S. causing them to remit funds of approximately 950 million yen (approx. USD 9 million) into bank accounts in Japan opened under other persons' names.

360 When withdrawing the funds, they falsely explained to a bank employee that those funds were remittances related to normal commercial transactions, in an attempt to disguise the money as legitimate business profits. As a result, they were arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds) and fraud.



PHILIPPINES

361 The National Bureau of Investigation (NBI) reported that certain Filipino individuals are creating fictitious web domains and soliciting investments online using fraudulent US Internal Revenue Service (USIRS) and Philippine Government seals and documents. Victims have been advised to transfer purported advance fees and charges to bank account 1 and bank account 2. Bank account 1 is under the account name of ABCD Trading System with address in Cebu City. Transactions in this account are characterized by international remittances (from individuals in the United Kingdom, Australia, Norway and Sweden and an entity in Indonesia) which are immediately withdrawn. One remitter also remitted funds to CD and Associates, USR Trading and XYZ Trading Services which are all based in Cebu; another remitter transferred funds to NL Distribution and Logistics located in Pangasinan. AMLC database showed the same pattern of transactions in the accounts of CD and Associates, USR Trading, XYZ Trading Services and NL Distribution and Logistics as those found in the account of ABCD Trading.

362 A bank filed an STR on USR Trading because of a complaint from a remitter in China. It was noted that the complainant remitted money upon advice allegedly by the Department of Treasury Internal Revenue Service for payment of his tax to the account of USR Trading (in connection with the recovery of an earlier investment).

THAILAND

Case Study 1

363 AMLO along with DSI, the Royal Thai Police's Crime Suppression Division (CSD) and SEC conducted an investigation into public fraud, tax evasion and ML against Mr. E, a Canadian national and former owner of a fitness company, and his associates.

364 The fitness company was sued in Thailand's Bankruptcy Court by a Thai bank seeking the repayment of a 72 million BHT loan, together with 4 million BHT in interests. As a result, the company shut down seven of its eight branches in Thailand.

365 The pattern of behaviour of the company pointed to public fraud and tax evasion which ranged from suspected false statements made to the stock market for losses sustained since 2003 to suspicious wiring of money overseas despite its constant loss reports.

366 The company's operation in Thailand was basically an illegitimate money-transaction business, which led to members receiving poor service with a loss of their membership fees and also resulted in its shareholders' loss of benefits and Thailand revenue loss.

Case Study 2

367 Authorities suspected a defendant was involved in drug related matters and launched an investigation. It was found that the defendant used accounts of his children and other people and began transferring funds into those accounts. Authorities ascertained that the defendant had full control over those accounts. Despite the prosecution not being able to prove drug offences, the court found that the defendant used the accounts for the purpose of concealing the true source of funds and convicted the defendant of ML.

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

NEW ZEALAND

368 The following case 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

369 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.

370 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.

371 ~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 ML.

5.23 Use of False Identification

FIJI

Case Study 1

372 The Fiji FIU received a STR from a foreign exchange dealer on Person Z. Person Z was reported for providing a fraudulent identification card while receiving remittances. The identification card was suspected to be fraudulent because there were no details on the expiry date and residential address. It was established that Person Z had been receiving remittances under two different names and had received international remittances totalling FJ$12,930 from April – October 2017.

373 Upon further analysis, the Fiji FIU established that Person Z had two tax identification numbers and bank accounts under both names.

374 A report was disseminated to the Fiji Police Intelligence Bureau in relation to fraud and forgery. Indicators included:

- Fake identification card.
- Two tax identification numbers for the same individual.

Case Study 2

375 The Fiji FIU received a few STRs on an individual that was alleged to be using stolen credit card information to purchase jewellery and household items at various retail and jewellery shops. Further checks with the retailers revealed that the individual has used two foreign drivers licences believed to be fraudulent. The Fiji FIU issued an alert notice requesting that financial institutions inform their EFTPOS merchants of the current methodology. A report was also disseminated to the Fiji Police Force.

376 As a result of the alert notice, a retailer identified the suspected individual and provided video footage of the individual to the FIU and Fiji Police Force. The footage showed details of a vehicle that the individual was using which gave Fiji Police Force a tangible lead to identify him. The case is still under investigation Possible Offence included fraud and forgery. Indicators included:

- Fake foreign ID.
- Purchase of large items at the same retailer in different locations.

HONG KONG, CHINA

377 A corruption investigation revealed that the defendant, a housewife, provided her personal particulars, identity documents, address, and bank account details to her friend for registering the defendant as an employee of a cleaning service contractor. The defendant had never worked for the company but received a salary totalling HK$83,408.66 between April and December 2014. From the salary received by the defendant she returned the majority of the amount to her friend.

378 Upon being convicted of ML in August 2017, the defendant was sentenced to three months and two weeks imprisonment.

JAPAN

379 Offenders used fake national health insurance cards, bank accounts, residence certificates, and postal services, which were obtained illegally to be the tools to receive criminal proceeds, and for ML purposes.

PAKISTAN

380 Mr. A, was running a shoe business in Pakistan. He opened an account in AB Bank Ltd. and closed his account just after three months. During the three month period, high value funds were routed from the account. The suspect opened another account in CD Bank Ltd. immediately after closing the account in AB Bank Ltd.

381 Moreover, his signatures in the account opening forms of AB Bank and CD Bank were also found to be different which created the suspicion that these accounts were Benami accounts. While reviewing statement of accounts, it was observed that average monthly turnovers and aggregate debit and credit turnovers were on a higher side. The suspect conducted high volume structured transactions through internal transfers, online transfers, multiple cash deposits and withdrawals and clearing cheques to avoid reporting thresholds. It was also observed that most of the transactions were conducted with unrelated counterparties.

382 Information was shared with the LEAs.

SINGAPORE

383 Two former employees of one of Singapore's oldest cooperatives were found guilty of cheating, forgery, criminal breach of trust and ML in relation to a fraud involving over S$5,000,000. They were sentenced to 144 months' imprisonment and 116 months' imprisonment respectively.

384 Investigations established that the two employees submitted to the co-operative forged loan application forms, deposit withdrawal forms and member termination letters of phantom members who were their family members and friends. Over 6 years, the co-operative was deceived into disbursing monies amounting to over S$5,000,000. The two employees thereafter laundered the stolen monies through a network of money mules consisting of their family members and friends who eventually channelled the criminal proceeds back to both of them by way of cheque encashment, cash withdrawals or electronic funds transfers.

THAILAND

385 The police requested AMLO to examine financial transactions of targeted persons who are members of a transnational crime organization committing the offence of public fraud by establishing a Ponzi scheme company. This group of people also committed this offence in People's Republic of China and more than 100,000 people were deceived with a total value of CNY 1.3 million. The Government of the People's Republic of China issued an arrest warrant against Mr. S, Mr. G, and Ms. W and found that these people also committed the same act in Malaysia, total value of MYR 300 million. It was also found that the same persons used a Burmese passport and a false Thai citizen identification card to enter Thailand to establish Y Company in Thailand.

5.22 Gems and Precious Metals

JAPAN

386 Money launderers purchased precious metals by cash derived from theft. They have conducted anonymous transactions and gave false information on customer identification (pretending to be another person or providing falsified identification documents when concluding sales contracts).

5.23 Purchase of Valuable Assets (art works, antiquities, racehorses, etc.)

MALAYSIA

Case 1 – Drugs Trafficking Syndicate

387 The Royal Malaysia Police recently charged a drug trafficking syndicate operating in the northern area of the jurisdiction which was linked to a drugs syndicate in a neighbouring jurisdiction. 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 the purchase of luxury cars, jewelleries, real estate properties and shares.

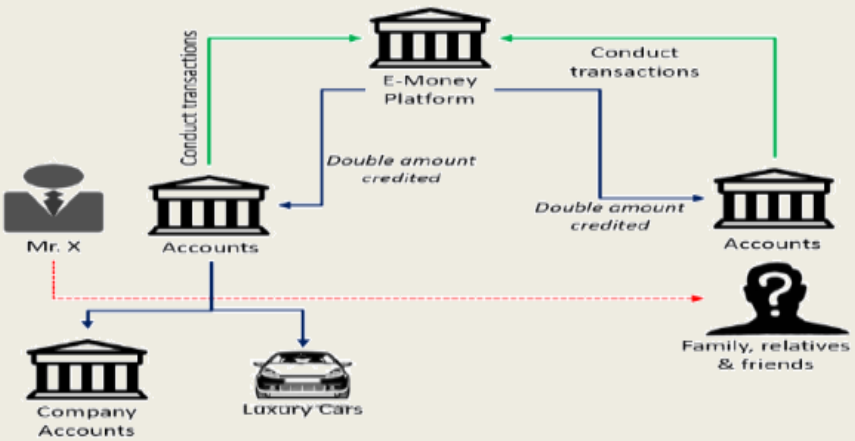
388 The financial analysis revealed that a portion of the proceeds were also used to finance other illegal activities including illegal gambling. The ML methods used included the use of nominees, trusts, family members or third parties; purchase of valuable assets (art works, antiquities, race horses, vehicles, etc.) and the use of shell companies/corporations.

Case 2 – Fraud

389 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.

390 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. To date, 24 suspects have been charged for fraud and ML offences.

391 The ML 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.).



5.24 Investment in Capital Markets, Use of Brokers

FIJI

392 Person Y is a Fijian national based in the United States and is a client of a local investment firm. Person Y was allegedly a victim of identity theft where Person Z hacked into Person Y's email and obtained personal identification documents of Person Y. Person Z emailed the investment firm and gave instructions to sell investments owned by Person Y and remit the funds to a bank account in Ireland. A total of approximately $9,981 was transferred to the bank account in Ireland.

393 The Fiji FIU conducted financial checks and linked up with its foreign counterparts, and established that bank account belonged to Person Z who was linked to certain criminal activities in Ireland.

394 A report was disseminated to the investment firm and local bank for their information. The investment firm was advised to liaise with the local bank in relation to compensation of funds of Person Z. A report was also disseminated to the Fiji Police Force for further investigation of fraud and identify theft. Indicators included:

- Fraudulent email correspondence
- Victim was not the account holder of the bank account funds were remitted into

5.25 Environmental Crimes

THAILAND

395 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 and 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

396 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 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.

397 The NSB conducted an investigation and found that the couple were involved in drug trafficking and had direct contact with 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 three 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.

5.27 Cases developed directly from suspicious or threshold transaction reports

AFGHANISTAN

Caption of the case: Ghost Public Servant

398 Individual X had opened 13 bank accounts; eleven bank accounts were opened for the purpose of salary. As per KYC forms of the subject, all accounts were opened with different phone numbers, addresses, and payroll revenue.

399 After reviewing the KYC forms and bank statements of the individual, it was noticed that the subject has received large amount of public funds as monthly salary via different bank accounts. Subject's monthly salary was USD 300, but he received USD 482,746 during four years via a payroll scam. The STR analysis report was disseminated for investigation and prosecution to the Attorney General's Office.

BANGLADESH

400 Bank 'A' submitted three STRs against the accounts of two cooperative societies and a religious institute alleging the embezzlement of public funds. Primary analysis revealed that each of these accounts had been credited by the same amount (Tk. 90,500) on the same day through clearing cheques issued by a local government agency (namely 'G') from its account title 'F' maintained in bank 'H'. Other than cheque deposits and cash withdrawals, no transactions took place in these accounts. No CTR, complaint or adverse information regarding these entities was found in the BFIU database.

401 The above scenario could not decipher what actually happened and how the funds were embezzled. Hence BFIU analyst decided to search in the BACH database of Bangladesh Bank to screen the cheques issued by 'G'. It revealed that the 'G' had issued thousands of cheques (each of either Tk. 42,000-49,500 or Tk. 90,500-98,500) in favour of different accounts from its account title 'F'. Then the BFIU analyst shrunk the time period to the previous six months and found approximately 600 cheques issued to 252 organizations including religious institutes, orphanages, educational institutes, social and cultural organizations, cooperative society etc. These 252 organizations had account in 29 banks. BFIU directed these banks to submit account opening forms, account statements and other relevant documents as well as inspection reports on the organization's location and activity. In the meantime, BFIU received 69 STRs of similar nature against 69 entity accounts of which information BFIU had already sought.

402 The documents and information obtained from the banks revealed that almost 60 percent of organizations either have no physical existence or no organizational activity or have a direct or indirect link with non-existent organizations. A two-member BFIU team also visited 10 organizations as a part of onsite inspection into bank branches on a sample basis and found that three of them do not exist physically and another three do not have any activity. Finally BFIU analyst was able to identify 180 organizations that received 479 cheques of Tk. 38.75 million from the 'G' for their infrastructural development. In most cases, money was withdrawn in cash just after the deposit and no other transaction was found in these accounts.

403 BFIU found anomalies both in the fund disbursement and account opening procedures. The same persons had been the committee members of multiple diverse organizations, s and many organizations using fake registration certificates. Few organizations beyond the jurisdiction of 'G' had got funds and most of the organizations could not show any documentary proof in support of receiving funds. Moreover, the banks failed to comply with KYC procedures as per BFIU circular and it seemed that staff of the respective bank branches had assisted with the opening of fake bank accounts. It could be mentioned that 26 organizations produced fake cooperative registration, 34 organizations produced fake voluntary society registrations and 18 organizations submitted fake membership certificates.

404 The local government agency ('G') undertook a project for the infrastructural development of local institutions. But a group of dishonest people formed paper based organizations, produced required documents, opened bank account and applied to the 'G' for allocating infrastructural development fund.

405 Since the case was related to public funds, BFIU disseminated the case to the LEA for further investigation and next steps in the legal procedures. BFIU exchanged information with Department of Cooperatives and Department of Social Services regarding the use of fake registration certificates and also with Registrar of Joint Stock Companies and Farms (RJSC&F) regarding the issuance of membership certificates by one of its registered entities to a non-existent organization. The LEA has formed an investigations team, who are now actively looking into the case. Department of Cooperatives has also taken punitive actions against the alleged cooperative societies.

CHINESE TAIPEI

406 In September 2016, the FIU received an STR from Bank H indicating that an OBU account of F Company set up in Belize, frequently received remittances from Mr. L's account in Hong Kong, China. Mr. L stated that the funds were commissions of merchandise procurement during Bank H's KYC process. However, the amount of each remittance was from US$50,000to over US$200,000. Bank H considered that the transactions in F Company's OBU account were more suspicious than usual and filed an STR to the FIU. The FIU found that Mr. L was suspected to be involved in criminal activity during the analysis and referred the case for investigation.

407 Mr. L and Mr. Y were the business managers of I Company, a successful list company, and were in charge of products selling business. They took advantage of the final decision around the selling prices and asked Mr. U, chairperson of T Company, to pay kickbacks. With the consent of Mr. U, Mr. L and Mr. Y sold products from I Company to T Company with lower prices. It caused I Company to lose chances to earn profits and made T Company obtain more profits. Mr. U provided Mr. L and Mr. Y 40 ~ 50 percent of the profits as a kickback. Between 2014 and 2015, the total amount of the kickback that Mr. U paid was over NT$ 30 million.

408 In order to obscure the proceeds of crime, Mr. L requested Mr. U to hand over cash directly or through Mr. U's wife or use F Company's OBU account or other foreign legal persons' accounts to transfer funds to Mr. L's account in Hong Kong, China. Mr. L then transferred 60 percent of the kickback to an account in Hong Kong, China of a foreign company chaired by Mr. Y or to an account of Mr. U's wife who then withdrew the cash and handed it over to Mr. Y.

409 Mr. L and Mr. Y were indicted on the charge of the offence of breaching of trust by the Hsinchu District Prosecutors Office in April 2017.

FIJI

410 In 2017, the Fiji FIU issued 448 case dissemination reports (CDRs) to the Fiji Police Force, Fiji Revenue and Customs Authority, foreign FIUs and other relevant LEA. CDRs are developed from analysis of STRs. The major recipient of Fiji FIU's case dissemination reports is the Fiji Revenue and Customs Service (FRCS) for alleged violations under the Income Tax Act and VAT Act. In 2017, 317 such reports were issued to FRCS. 84 CDRs were issued to the Fiji Police, including the AML and Proceeds of Crime Unit, Transnational Crime Unit and Police Intelligence Bureau.

411 As part of STR analysis, checks are conducted on the Fiji FIU online database which includes CTRs, electronic funds transfer reports (EFTRs) and border currency reports (BCRs).

412 In 2017, the FIU received:

- 623,213 CTRs averaging around 51,934 CTRs per month;
- 1,220,602 EFTRs averaging around 101,717 EFTRs per month;
- 792 BCRs averaging around 66 BCRs per month.

413 The Fiji FIU database can be accessed by key partner agencies through a direct data access arrangement. In 2017, LEAs accessed the database on 65 occasions to assist with investigations.

MACAO, CHINA

414 An STR was received on June 2017. Client A was an 11 years old student and opened a bank account with a local bank. His bank account was ultimately controlled by his mother Ms. B who contacted the bank for not receiving an inward remittance in her son's account. As there was doubt regarding the rationality of the above remittance transaction, the bank reviewed the account history of Client A from March to May 2017 and found that his account received 32 transfers from more than 20 different third parties and 11 cash deposits through cash deposit machines during that period. Once the above funds were received, they would be transferred to Ms. B's account in another bank through internet banking. The amount of funds received in the minor's account was more than MOP1 million.

415 Intelligence revealed that Ms. B was the suspect in several fraudulent cases from 2012 to 2017. The suspicion was that she was using her son's account to receive funds from fraud victims. The case was submitted to the Public Prosecutions Office for further investigation.

MALAYSIA

Human Trafficking Syndicate

416 The FIU initially analysed a STR reported on Mr. A whose bank accounts recorded abnormal patterns of transactions involving cash deposits from various locations and fund transfers from/to various individuals. Checking with the authorities found that he is a part of three syndicates involved in smuggling of foreign migrants via airplanes, and is facilitated by government officials.

417 Subsequently, FIU analysis focussed on another syndicate member, Mr. B who frequently transferred funds to Mr. A. The former, conducted hundreds of payments to a local airline within a year. This indicates that he may be facilitating the syndicates by purchasing airfares for the foreign migrant entering into Malaysia.

418 Further engagement with authorities discovered a further 11 individuals linked to the syndicates. Overall, FIU analysed and disclosed banking information involving transactions totalling to USD1.5 million which were mostly cash-based transactions.

419 Several arrests were made in this investigation under the Anti-Trafficking in Persons and Anti-Smuggling of Migrants Act 2007. The investigation is ongoing.

Fraud

420 Acting on a tip-off from a foreign law enforcement authority on suspected fraudulent activity, analysis was conducted on an entity and related individual. The review of STRs and related database revealed that:

- The sole proprietor's account has been receiving large inward remittances received from overseas without valid reason.
- Relationship between sender and beneficiary could not be established.
- Transaction was inconsistent with subject's nature of business, normally claimed to be involved in general trading.
- Funds received would be withdrawn nearly in full amount immediately on the same day or next few days via cash or on-line transfers to own or third parties' accounts.

Corruption

421 The following trends were observed on analysis of suspicious transactions relating to corruption:

- The suspects generally involved government officers who were in the position to make, or influence, decisions to approve development projects and misuse their position for personal benefits and monetary gains.
- The analysis on the accounts of the main suspect demonstrated frequent large cash deposits, fund transfers and cheque payments which did not match with his profile. Funds then were used to purchase unit trusts, luxury vehicles and properties. The purchases were also made on the name of the spouse or children.
- In some cases, based on the information shared by a foreign FIU, the suspect or his proxies also maintain foreign bank accounts. There were instances the funds were deposited by entities suspected to be unregistered money value transfer system operators operating in that jurisdiction.
- Checking on other databases revealed the use proxies to register businesses and companies to bid for government projects which are managed by the suspects.

NEW ZEALAND

422 The NZ-FIU makes disseminations to relevant government agencies on an individual assessment of each STR. With regards to law enforcement, individual persons or entities are escalated to a report based on a matrix that rates the person, transactions, and reason for suspicion within an STR. These reports are disseminated on an ad hoc basis to intelligence units or to individual officers. Frequently an individual will already be facing charges, or be subject to investigation. Whether or not the STR release precedes the investigation is not currently recorded.

423 In the last 12 months, there were five New Zealand Police serious and organised crime cases and 27 potential fraud cases (Ministry of Social Development) that were initiated from STRs. Additionally, there were more instances where STR information significantly contributed to cases across LEAs. For instance, STR information has been used to support organized crime investigations, including into predicate offending, associated ML, and standalone ML and asset recovery

investigations. AML/CFT supervisory agencies have also used STR information in investigations of AML/CFT Act breaches.

424 Inland Revenue Department has used STRs in the so-called Panama Papers project, Serious Fraud office found STRs useful in identifying recidivist offenders involved in scamming people in order to continue to supply money overseas to 419 scammers. The Ministry of Business and Immigration received a large influx of STRs that helped add real emphasis to pursuing Operation Spectrum relating to a large scale immigration fraud and immigrant labour exploitation on building sites. New Zealand Police's child exploitation prevention unit OCEANZ has used STR information to corroborate intelligence received from their counterparts overseas, it has also helped them to identify and profile suspects. New Zealand Customs have taken actions based on the STR information supplied by NZ-FIU in the form of scoping, alerts (passenger and freight), mailing stops and requisitions.

SINGAPORE

US$16 million seized in a bribery case developed directly from suspicious transaction report

425 In 2016, the Corruption Practices Investigation Bureau (CPIB) received a referral of a STR in relation to a Singapore bank account of Company A. In the STR, company A was linked to investigations by a foreign authority, as there was an adverse news on Company A receiving funds from Company B. Company B was alleged to have paid bribes to foreign public officials. At the same time, the beneficial owner of Company A was looking to liquidate the bank account. Acting on the STR, CPIB sought clarifications from the foreign authority and established that there were reasonable grounds to believe that funds in Company A's bank account were linked to the proceeds of crime. Accordingly, the bank account of Company A containing approximately USD 16 million was seized as part of investigations. Investigations were ongoing at the time of the report.

Recovery of S$2 million in a tax evasion case developed from financial intelligence

426 The Inland Revenue Authority of Singapore (IRAS) investigated the case after receiving financial intelligence from the STRO. Earlier, the STRO had received a suspicious transaction report (STR) on Mr L. He had frequent deposits and withdrawals of large amounts in his personal bank account. Each deposit into the bank account was followed by a corresponding withdrawal of a similar amount.

427 The STRO found that Mr L was a director in Company H and he was also linked to multiple Cash Transaction Reports (CTR) and Cash Movement Reports (CMR). As there were significant transactions in cash, the STRO suspected that Mr L could be using his personal accounts to perform business transactions with various entities possibly to evade tax.

428 Mr L and his wife were directors of Company H. Company H had paid monies from its bank account to overseas entities and Mr L. The payments by Company H were claimed as deductions against the company's income, resulting in a lower tax assessed. Company H was unable to substantiate the deductions; it could not provide valid explanations as to how these payments were incurred in the production of income. The total unsubstantiated deductions disallowed amounted to $11.7 million. IRAS recovered more than S$2 million in tax undercharged.

429 IRAS also found that Mr L did not report a trade income of $877,000 from his sole-proprietorship and recovered an additional tax of about $133,000.

Proceeds from foreign predicate offence seized following suspicious transaction report

430 STRO received an STR filed by a bank informing that Person M received two alleged fraudulent funds transfers amounting to US$112,000 from a victim overseas. Following the remittances, Person M withdrew S$48,000 in cash on the same day. The receiving bank assessed the

transaction patterns to be suspicious considering Person M was a foreign domestic worker in Singapore.

431 From the outreach done by STRO on the money mule crime trend to the financial sector and the crime alert broadcast published on the STROLLs system involving fraudulent fund transfers, the receiving bank noted that the transaction patterns appear to closely fit the modus operandi of ML activity involving a money mule and thus, submitted a STR to STRO.

432 As the information revealed possible ML from foreign predicate offence, STRO referred the information to the relevant law enforcement agency in Singapore within a day. The investigators commenced a ML investigation and immediately seized the remaining S$88,229 in Person M's bank account. The timely referral by STRO enabled the domestic agency to develop evidence to identify the owner of the receiving bank account and trace criminal proceeds, leading to the seizure of S$88,229 in her bank account.

433 Person M was convicted for dishonestly receiving stolen property and money laundering offences. She was sentenced to 8 months' imprisonment.

THAILAND

434 AMLO received a STR made by a bank that Ms. S, mistress of Mr. P, conducted many cash deposits and withdrawals involving 1-1.9 million THB in each transaction and taking only small denomination banknotes to avoid reporting to the AMLO. As a result of an investigation by the AMLO, it was found that the couple together held 70 accounts at various banks totalling a large amount of money. It was also found that Mr. P had a 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.

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

6. PUBLIC AND PRIVATE SECTOR COOPERATION INITIATIVES

AUSTRALIA

435 Australia's Fintel Alliance (FA) is a joint FIU / private sector body established to deepen cooperation on developing financial intelligence and sharing risk information. The FA was launched in 2017 with three operational goals:

- Assist the private sector partners more easily identify and report suspicious transactions
- Assist law enforcement partners with investigations
- work with academia to build knowledge and gather insight.

Panama Papers

436 The FA has been useful in identifying:

- how domestic parties use international third party intermediaries (and who they are) in finance hubs while not directly transacting with a tax haven, and
- how third party payment services are intermediating shelf-company set and servicing.

437 This new intelligence reduced the take-up time to analyse Paradise Paper data.

Child Exploitation

438 Subject matter experts from law enforcement have been seconded into the operation to brief members on the financial characteristics of child exploitation. An intelligence report co-designed by industry and law enforcement/intelligence agencies identified small value international payments to locations susceptible to child exploitation as the greatest financial indication of offending. As a result, industry members are enhancing transaction monitoring and ongoing customer due diligence to identify individuals and activities to better detect this indicator as early as possible.

439 From this operation, law enforcement and partner agencies have been provided with more reliable information for the identification of targets for referral purposes. AUSTRAC has also automated profiling of identified indicators across suspicious matter reports, a process which has identified previously unknown targets suspected to be engaged in the purchase of child exploitation material.

440 In addition, an unclassified version of the report titled "Fintel Alliance - Combating child exploitation fact sheet" has been developed and released to a national and international audience.

Money Mules

441 This operation aims to develop a capability to detect persons that may have been recruited as money mules and disseminate relevant information in near real-time to other private sector and Government partners to identify new victims.

442 Real-time sharing of information with the private sector:

- enables funds to be blocked before they are sent offshore - and Automated Alerting process is in place and reporting entities can act to retard funds
- assist persons unwittingly recruited as money mules by engaging a support service (such as iDcare) to make contact and provide advice and assistance.
- identifies high-risk accounts, jurisdictions, entities and participants running money mule networks, and
- identify leads for law enforcement and be used to profile mule recruitment networks, plus International FIU collaboration to act in identifying international money mule networks.

MALAYSIA

Public-Private Sector Partnership on TF

443 A platform has been set up between FIU, RMP and at-risk financial institutions for sharing of information on TF operational intelligence since January 2017. Periodic meetings and engagement has been conducted among the parties to share information on emerging TF risks and methods and targeted individuals and groups for joint analysis and surveillance.

444 The initiative has produced positive results, including the increase in the number of STRs related to TF (400 percent increase from 2016) and subsequently the increase in the financial intelligence disclosures made to RMP.

445 The RMP acknowledges the importance of this platform and the enhanced quality of financial intelligence disclosed to them. This has contributed to an increase in terrorism and TF investigations and the prevention of terrorism acts.

7. ABBREVIATIONS AND ACRONYMS

AML – Anti-Money Laundering
AMLC – Anti- Money Laundering Council (Philippines)
AMLO – Anti-Money Laundering Office (Thailand)
APG – Asia/Pacific Group on Money Laundering
ATM – Automatic Teller Machine
AUSTRAC – Australian Transaction Reports and Analysis Centre
BCR – Border Currency Report
CDD – Customer Due Diligence
CFT – Countering the Financing of Terrorism
CTR – Cash/ Currency Transaction Report
DNFBP – Designated Non-Financial Businesses and Professions
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
FIU - Financial Intelligence Unit
FSRB – FATF-Style Regional Bodies
FTF – Foreign Terrorist Fighters
IFTI – International Funds Transaction Instruction
JAFIC – Japan Financial Intelligence Center
KYC – Know Your Customer
LEA – Law Enforcement Agency
ML – Money Laundering
MLA – Mutual Legal Assistance
MTO – Money Transfer Operators
NBI – National Bureau of Investigation (Philippines)
NRA – National Risk Assessment
PEP – Politically Exposed Person
STR – Suspicious Transactions Report
TF – Terrorist Financing
UNODC – United Nations Office on Drugs and Crime
VAT – Value Added Tax