APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2019

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

August 2019

APG Yearly Typologies Report 2019

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) body for the Asia/Pacific. The APG produces regional typologies reports on money laundering (ML) and terrorist financing (TF) methods 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 Financial Action Task Force (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. The 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 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 2018-2019

6 The APG conducts its typologies work through the APG Operations Committee which is currently co-chaired by India and New Zealand.

1. WORKSHOPS AND PROJECTS UNDERTAKEN BY APG IN 2018 - 2019

1 This section of the report provides a brief overview of typologies related work undertaken by the APG between July 2018 and June 2019.

1.1 APG's typologies projects

Human trafficking and people smuggling project (Phase 2)

2 Phase 1 of this project was a FATF/APG project focused on human trafficking (HT) and was finalised in July 2018 (see the following section in this report: *FATF and FATF Style Regional Bodies' Typologies Projects/ FATF typology projects).*

3 Phase 2 is an APG regional project that has been built on Phase 1 which includes consideration of HT and people smuggling (PS). The project is focused on implementation support to manage both HT and PS, including public – private partnerships including civil society.

4 A HT and PS regional workshop was held in Bandung, Indonesia from 8 to 10 April 2019, which focused on implementation of public/private/civil society partnerships to counter HT and PS. The workshop was co-hosted by APG, PPATK, and AUSTRAC and was attended by 64 delegates from 12 jurisdictions, international organisations, private sector, non-government organisations and civil society. This project will conclude in 2020.

Terrorism financing & proceeds of crime (including organised crime)

5 The Eurasian Group on Combatting Money Laundering and Financing (EAG) and APG are undertaking a joint project to focus on the techniques and trends associated with the use of proceeds of crime, including from organised crime, for the financing of terrorism, whether individual terrorists or terrorist organisations (see the following section in this report: *EAG – Eurasian Group on Combating Money Laundering and Financing of Terrorism*).

1.2 2018 APG/EAG Joint Typologies and Capacity Building Workshop

6 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.

7 The APG co-hosted the 2018 Typologies Workshop with EAG in Novosibirsk, Russian Federation from 3 to 5 December 2018, involving approximately 250 delegates from 41 APG/EAG jurisdictions (with approximately 130 delegates from APG members), eight international organisations and 21 representatives from the private sector, non-government organisations and civil society.

8 The workshop included a plenary session (first and last day) and three two-day concurrent sessions on: (i) TF and proceeds of crimes (including organised crime); (ii) risks and investigative techniques associated with virtual assets; and (iii) HT and PS.

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

9 This section of the report provides a brief overview of typology reports published by FATF and other FATF-style regional bodies (FSRBs) between July 2018 and June 2019.

2.1 FATF typology projects

Financial flows from human trafficking (Phase 1)

10 In recent years, the number of victims of HT and migrant smuggling has continued to grow significantly. In August 2018, FATF and APG published a report which aims to raise awareness about the type of financial information that can identify HT for sexual exploitation or forced labour and to raise awareness about the potential for profit-generation from organ trafficking. The report also highlights potential links between HT and TF.

11 The report highlights the importance of building partnerships between public sector, private sector, civil society and non-profit communities to leverage expertise, capabilities and partnerships. The private sector and financial institutions in particular, are on the frontline.

12 Innovative initiatives at the national or regional level have demonstrated how AML/CFT measures, and those that implement them, can contribute to stopping this crime. However, globally, there has not been sufficient focus on how to use financial information to detect, disrupt and dismantle HT networks. The report provides good practices to help jurisdictions develop measures to address ML and TF from HT and includes red flag indicators to help identify those who are laundering the proceeds of these crimes.

Transparency and beneficial ownership

13 While corporate vehicles, such as companies, foundations, partnerships, and other types of legal persons and arrangements are important for supporting commercial and entrepreneurial activity, they can also be misused to conceal the ownership and control of illicitly gained assets. In July 2018, FATF and the Egmont Group published a joint report which assessed the vulnerabilities linked to the concealment of beneficial ownership in order to support further risk analysis by public and private sector.

14 The report uses over 100 case studies provided by 34 different jurisdictions of the FATF Global Network, the experiences of law enforcement and other experts, private sector input as well as open-source research and intelligence reports to identify the methods that criminals use to hide beneficial ownership. Vulnerabilities associated with beneficial ownership are analysed, with a particular focus on the involvement of professional intermediaries.

15 The report highlights that the ease with which legal persons, primarily limited liability companies (or similar), can be formed makes them particularly vulnerable, and seen to be used in building complex legal ownership structures, often involving shell companies. Moreover, trust and company service providers frequently play a role in arranging such structures. The use of nominee directors and shareholders, both formal and informal, exacerbates the risks by creating barriers between the owner or individual and laundered proceeds. Professional intermediaries often play a role in helping create or operate the structures used to conceal beneficial ownership, either complicity or unwittingly.

Professional money laundering

16 Professional money launderers (PMLs) provide services to criminals and organised crime groups by laundering the proceeds of their illegal activities. In July 2018 FATF published a report that looks at the techniques and tools used by PMLs, to help jurisdictions identify and dismantle them. Based on case studies provided from across the FATF Global Network, the report identifies a range of different ML organisations and networks, from money transport and cash controller networks to proxy networks.

17 The report finds that PMLs use a variety of ML tools and techniques such as trade-based ML, account management mechanisms, underground banking and alternative banking platforms. To lend a veneer of legitimacy to their activities, PMLs may work with corrupt individual(s) who specialise in the provision of otherwise legitimate services (e.g. bankers, lawyers, accountants) in addition to their criminal ML activity. PMLs often work for more than one criminal or criminal organisation. A successful prosecution of a PML can therefore potentially impact the activity of several criminal clients.

18 The project team also developed a non-public version of the report which explores unique investigative tools and techniques that have proved successful in detecting and disrupting PMLs.

Terrorist financing disruption strategies (Non-public)

19 In October 2018, FATF approved a non-public report on disruption of TF flows. Understanding these financial flows is important not only from an investigative standpoint, but also to ensure that authorities are able to take decisive, preventative measures to disrupt terrorist activity before a terrorist attack takes places.

20 Building on contributions from 33 members and observers from across the FATF global network, this internal report provides authorities with a toolkit of disruption tools and comprehensive strategies that will assist them to improve domestic CFT actions and identify novel ways in which competent authorities can effectively work together to disrupt TF activity.

ISIL and Al-Qaeda and affiliates financing updates (October 2017) – Non-public

21 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 information provided by the global network. These updates also cover Al-Qaeda, and ISIL and Al-Qaeda affiliates. In October 2018 and June 2019, the FATF released public statements on the evolution of the financing of ISIL following its loss of territory.

Identifying and assessing terrorist financing risks

22 Identifying, assessing and understanding TF risks are an essential part of dismantling and disrupting terrorist networks. In July 2019, the FATF published guidance which provides best practices and considerations for jurisdictions when identifying and assessing their TF risk, based on experience from across the FATF Global Network.

Criminal exploitation of virtual assets for ML/TF purposes – addressing challenges with investigations and confiscations (Non-public)

23 Virtual assets (VAs) have unique characteristics as an asset class which can frustrate financial investigations, and related confiscation, impeding authorities' abilities to detect, investigate and prosecute ML/TF offences that utilise these technologies. In June 2019, FATF approved a non-public guidance that provides best practices for practitioners in order to support them conduct effective ML/TF

financial investigations suspected of involving VAs. The report also provides case studies, and techniques that can be used by competent authorities to confiscate illicit VAs.

2.2 CFATF – Caribbean Financial Action Task Force

24 The CFATF has conducted a number of typologies reports including: Money laundering using trust and company service providers (2010); Human trafficking and migrant smuggling (2014); Illegal Lotteries (2016); Movement of cash and negotiable instruments (2016); and the proliferation of small arms and ammunition (2016).

CFATF Typologies Project on De-Risking (2019)

25 The CFATF carried out an exercise on de-risking during June 2018 to April 2019 with the goal of highlighting the negative impact it was having on the region. This exercise was conducted in two phases and involved data calls to Central Banks and private sector financial institutions.

26 The analysis of the data received through the data call revealed the following:

27 According to 71% of regional central banks, de-risking is a threat that is on the increase. Additionally, 90% of the said central banks perceive 'de-risking' as a threat that has affected and continues to affect their operational viability by, among other factors, increasing operational costs and lengthening the payment chain.

28 Based on feedback received from a total of 227 financial institutions, 158, or 70% indicated that their operations were negatively affected by de-risking (termination/restriction of correspondence banking relationships) with the main reasons being attributed to difficulty providing services/products to clients and the elevated risk rating being placed on them by their correspondent banks. Other reasons included: difficulties finding replacement correspondence banks; and increased administrative costs.

29 The two main reasons given to financial institutions for the termination/restriction of correspondence banking relationships were: low/small profit margins and the cost of compliance. However, in many instances no reason was provided. Some other reasons were: issues with AML/CFT procedures; the product/service for which the relationship was formed was no longer offered; the perceived risk of the jurisdiction; risk mitigation strategy on the part of the correspondent bank; low risk appetite; the business line not aligned with the correspondent bank's strategy and fear of regulatory sanctions in the home jurisdiction.

30 In instances where the jurisdiction of domicile for the correspondent bank were identified, half were in North America and a third were in Europe. Others were in Asia, the Caribbean, Africa and South America.

31 The products and services affected were wire transfers, loans/letters of credit, cheque clearing and settlement, e-gaming/online gambling, cash management services, credit card processing, money transfer operations and mobile banking.

32 A number of banks (55 banks) had their correspondent banking relationships terminated during the past three years. Most of these banks (80%) lost between one and three correspondent banking relationships whilst 11% lost between 7 to 10 of their correspondence banking relationships.

33 The de-risking report was approved, as an internal document, by the CFATF's May 2019 Plenary.

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

Terrorism financing & proceeds of crime (including organised crime)

34 Issues related to countering the financing of terrorism have been a standing item on the EAG agenda for many years, and are considered a top priority for the EAG and its member states. To date the EAG has completed a number of typologies projects concerning CFT. The latest is the joint project with APG (which is currently ongoing) on the links between TF and organized crime. The three jurisdictions leading the project are Bangladesh, India and Russian Federation. UNSCRs 2195 and 2322 form the basis for the project.

35 The project aims to:

- Better understand to what extent and how proceeds of crime (including organised crime) are being used, or might be used, for TF by individual terrorists and terrorist organisations.
- Identify methodologies being used to collect, move and use funds from the proceeds of crime, including organised crime, for terrorism related purposes.
- Identify best practices to detect, investigate and prevent the use of proceeds of crime by terrorists and terrorist organisations.

36 The information was gathered in two stages, one being the dissemination of questionnaires. The second being the joint EAG/APG typologies workshop held in Novosibirsk, Russian Federation in December 2018, where a separate breakout session was held on the links between TF and organized crime.

37 The outcomes of the discussions at the joint typologies workshop, as well as the responses to the questionnaires were the basis for the preliminary findings of the project report and will be discussed and adopted by APG and EAG annual meetings in 2019.

2.3 GIABA – The Inter-Governmental Action Group against Money Laundering in West Africa

Know your customer/ Customer due diligence measures and financial inclusion in West Africa

38 This report is the outcome of a study conducted directly by the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), which commenced in September 2016. The study is a follow up to an earlier study on financial inclusion carried out in 2013. It was undertaken to understand and address the challenges of implementing the ML and TF preventive measures of Know–Your-Customer (KYC)/Customer Due Diligence (CDD) with due regard to financial inclusion. On the basis of the findings of the study, recommendations have been made to assist the relevant authorities in GIABA member states to design effective KYC/CDD frameworks that promote financial inclusion, in compliance with the letter and spirit of the FATF Recommendations and Assessment Methodology (as revised). This report is available on the GIABA website https://www.giaba.org/reports/typologies/reports.html.

Money laundering resulting from the counterfeiting of pharmaceuticals in West Africa

39 This study was aimed at understanding the nature and magnitude of the ML resulting from the counterfeiting of pharmaceuticals in West Africa. The methodology employed involved the selection of four jurisdictions (Côte d'Ivoire, Nigeria, Senegal and Togo) for the purpose of in-depth jurisdiction

level study, while the remaining jurisdictions responded to a questionnaire. The linkage between ML and counterfeiting of pharmaceuticals was analysed from jurisdiction reports, responses provided by the member states to the questionnaire and the case studies provided by law enforcement authorities. This report is available on the GIABA website https://www.giaba.org/reports/typologies/reports.html.

2.4 The Egmont Group

Emerging financial technologies, money laundering and terrorist financing: A typology of virtual currencies

40 During the last 12 months the Egmont Group finalised a number of important projects including a typologies project titled *Emerging Financial Technologies, Money Laundering and Terrorist Financing: A Typology of Virtual Currencies*. The Heads of FIUs endorsed this report in May 2018 and allowed its dissemination to all FIUs, relevant reporting entities, competent law enforcement authorities, and Egmont Group Observers.

The concealment of beneficial ownership report (a joint paper with the FATF)

41 This joint FATF/Egmont Group report takes a global view assessing how legal persons, legal arrangements and professional intermediaries can help criminals conceal wealth and illicit assets. The purpose of the report is to help national authorities, including FIUs, financial institutions and other professional service providers, to understand the nature of the risks that they face.

Paper on the set of indicators for corruption-related cases

42 The Egmont Group has compiled a set of indicators in a paper that may, when considered in the context of a transaction or customer interaction, assist in the identification of corruption and of the laundering of the proceeds of corruption. The ultimate goal of this paper is to enhance the intelligence available to FIUs, which should be coordinated with law enforcement, financial institutions and other front-line reporting entities to improve the identification of suspicious transactions and activities indicative of corruption.

43 The Egmont group acknowledged the importance of other work undertaken by other international organisations on the topic including FATF, the World Bank, the United Nations Office on Drugs and Crime, and INTERPOL, which also need to be considered when looking at the identification of suspicious transactions and/or proceeds derived from corruption or any other predicate crime.

44 This paper, which has been approved by the Heads of FIUs during the Egmont Group plenary meeting in Sydney (24-27 September 2018), is not exhaustive and will be amended and supplemented in accordance with feedback received from Egmont Group members, observers, international partner organisations, different competent authorities, and reporting entities.

The ECOFEL paper on FIU operational independence and autonomy

45 This paper has been drafted to assist governments (decision and policy makers), FIUs and other key stakeholders in identifying and understanding the characteristics that define and shape FIU operational independence and autonomy.

46 The paper has been formulated in response to the Egmont Group of Financial Intelligence Units (EG) membership who have requested guidance on what characteristics should be in place to best facilitate operationally independent and autonomous FIUs. The paper focuses on describing characteristics that may foster FIU operational independence and autonomy, it is not intended to set a new standard, nor does it discuss strategies to achieve these characteristics.

3. TRENDS IN MONEY LAUNDERING AND TERRORIST FINANCING

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

3.1 Research or studies undertaken on ML/TF methods and trends by APG members and observers

AUSTRALIA

Non-profit organisations and terrorism financing red flag indicators 2018 report

48 In 2018, eight FIUs from Australia (Australian Transaction Report and Analysis Centre), Brunei Darussalam (FIU, Autoriti Monetari Brunei Darussalam), Indonesia (Pusat Pelaporan dan Analisis Transaksi Keuangan), Malaysia (Bank Negara Malaysia), New Zealand (New Zealand Police FIU), the Philippines (Anti-Money Laundering Council), Singapore (Suspicious Transaction Reporting Office) and the Kingdom of Thailand (Anti-Money Laundering Office) worked together to develop and produce a regional red flag indicators report as part of the ongoing operational efforts aligned with the Annual Counter Terrorism Financing Summit.

49 The report provides a set of red flag indicators related to non-profit organisations (NPOs) at high risk of misuse for TF in South-East Asia, Australia and New Zealand and aims to assist reporting institutions, as well as national authorities and NPOs, to better identify and mitigate suspicious activity potentially linked to terrorism financing in the region.

50 The indicators were informed by case studies and intelligence from regional FIUs, law enforcement and NPO regulators. Financial institutions that handled NPO finances and had obligations to report suspicious activity also provided input.

51 See https://www.austrac.gov.au/sites/default/files/2019-06/npo-red-flag-indicators.pdf for further information.

On-course bookmakers risk assessment

52 In late 2018, AUSTRAC published a risk assessment which examined the overall ML/TF risk for Australia's on-course bookmaking sector.

53 The services provided by on-course bookmakers were identified as being likely to facilitate low levels of ML and tax evasion, with no observations of terrorism financing recorded. The declining nature of the sector and a range of other factors limited the vulnerability of the sector to ML and other criminal misuse and as such the sector was rated as low risk. It was established that on-course bookmakers with relatively large turnovers, including those that provided online betting accounts, were more vulnerable to criminal misuse than other entities.

54 The risk assessment provided detailed information to help the sector understand and respond to the risks associated with the services provided by on-course bookmakers. Please follow this link to the risk assessment: https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/course-bookmakers-money-laundering-and-terrorism-financing-risk-assessment

Superannuation sector guidance

55 In December 2018, AUSTRAC published guidance for the superannuation sector on how to apply elements of the *Anti-Money Laundering and Counter-Terrorism Financing Act* 2006 to their business.

56 The guidance provided worked examples, designed for illustrative purposes only, to highlight how the AML/CTF toolkit for industry could be used to identify, mitigate and manage the superannuation industry's specific ML/TF risks. The worked examples provided businesses with insights into how the sector could adopt flexible approaches to using their own AML/CTF toolkit (in line with their own business and risk profiles).

57 Please follow this link to the guidance https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/industry-specific-guidance-superannuation-sector

CANADA

58 FINTRAC Terrorist Financing Assessment: 2018 - http://www.fintrac-canafe.gc.ca/intel/assess/tfa-2018-eng.asp

59 FINTRAC Operational Alert on PML Through Trade and Money Service Businesses - http://www.fintrac-canafe.gc.ca/intel/operation/oai-ml-eng.asp

FIJI

60 The Fiji FIU conducts informal research on ML/TF methods and trends. The Fiji FIU continues to provide this information through the publication of its Annual Report.

61 The Fiji FIU Annual Reports include case studies generated from suspicious transaction reports and case studies on a successfully prosecuted ML cases in Fiji. The reports also include emerging, continuing and declining ML trends. A copy of the Annual Report is available on Fiji FIU's website: www.fijifiu.gov.fj

HONG KONG, CHINA

62 Hong Kong's Joint Financial Intelligence Unit (JFIU) has published a strategic analysis report on email scams comprised of complex analysis on account information, account activities and thematic analyses on change of company directorship, account signatories and test payment. The report can be accessed via the following link –
https://www.jfiu.gov.hk/info/doc/Strategic_Analysis_Report_on_Email_Scams.pdf

INDONESIA

63 Indonesia conducts regular research and studies on ML/TF methods and trends with different themes for each study. The research and studies are held once a year. If there is a current issue or special issue regarding ML/TF methods and trends, Indonesia can hold non-routine research and studies. The research and studies, however, are only published internally, and only for limited distribution externally.

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

65 Recent research or studies on ML/TF methods and trends include the typologies relating to ML cases that have been decided in the courts in 2017. The research indicated that for the cases decided in

2017, the dominant predicate crimes reported were related to narcotics. The dominant transaction patterns were transfers via ATM, cash deposits via teller, and overbooking.

JAPAN

66 Japan Financial Intelligence Center's Annual Report, which details AML/CFT statistics, case studies and trends, was published on the Japan Financial Intelligence Center (JAFIC) website.

MALAYSIA

National Risk Assessment (NRA)

67 Malaysia's third iteration of the NRA was completed and endorsed by the National Coordination Committee to Counter Money Laundering (NCC) in July 2018. The NRA methodology has been enhanced with broader scopes and revised data points. In addition to a Threats Risk Assessment and a Sectoral Risk Assessment (FIs and DNFBPs), the NPO TF National Risk Assessment was also adopted by the NCC as part of the NRA.

68 The high-risk crimes identified in NRA 2018 are similar to those in NRA 2013, i.e. fraud, smuggling, corruption and illicit drugs trafficking, with the exception of organised crime which is assessed to have higher risks in place of tax evasion as one of the top five high risk crimes. All high-risk crimes recorded a significant number of investigations conducted, value of illegal proceeds suspected to be involved and amounts of financial intelligence generated.

69 As part of the process of the NRA, the NCC had identified areas that need to be improved to mitigate the new risks identified. In view of this, the current National AML/CFT/CPF Strategic Plan 2016-2020 (NSP) will be reviewed and recalibrated to take into account the progress of existing action plans, new mitigating strategies (including new gaps identified) and changes in the international standards.

70 At the same time, communication and awareness activities have been rolled out since the adoption, especially briefing sessions to reporting institutions.

Red flags and Typology Brief

71 In 2018 and 2019 the FIU has issued five red-flag and typology briefs on the following crimes, namely TF (April 2018), PF (May 2018), corruption (June 2018), fraud (October 2018) and drug trafficking (January 2019). These crimes are the high-risk crimes identified through the NRA and based on the needs of the private sector. The documents were issued with restricted circulation to reporting institutions (RIs) and aim to:

- provide insights and create awareness on crimes - trends, techniques, methods and channels;
- enhance and facilitate RIs' knowledge and understanding of typologies;
- assist RIs in identification of offences from red flags/indicators exhibited by their clients and financial transactions involved;
- enable early detection by RIs in order to disrupt the specific crimes-related activities and further improve the quality of suspicious transaction reports (STRs).

NEW ZEALAND

Money laundering via gatekeeper professionals and money remitters

72 The NZFIU conducted a joint project to identify money remitters and gatekeeper professionals (lawyers / accountants / real estate agents) whose services were being abused by criminals for ML. The methodology involved reviewing New Zealand Police (NZP) organised crime holdings for an 18 month period from January 2017, identifying the entities that facilitated the movement of criminal proceeds in these cases, and entering these into an analysts chart for further analysis. NZFIU data for each of these entities was then transposed into the analysts chart, with money flow analysis and proximity analysis conducted to identify those entities facilitating the highest volume and value of transactions and enable judgements to be made as to the entities' involvement in moving criminal proceeds.

73 The key themes to emerge from the project are summarized below:

74 Key nodes: A core network of approximately 65 New Zealand-based businesses, individuals and financial service providers has almost certainly been abused to launder the proceeds of organised criminal activity. This network of 'key nodes' is underpinned by several Auckland-based Money Remitters (MRs) and has facilitated more than $200 million dollars' worth of suspicious transactions since 2016. It is likely that a significant proportion of these funds have derived from drug offending, fraud, and other serious offences.

75 Culture of AML/CFT non-compliance among network of MRs: Most of the major MRs identified have previously come to the attention of Police and the Department of Internal Affairs for ongoing non-compliance with their AML/CFT obligations; including failure to carry out customer due diligence, conduct transaction monitoring or submit suspicious transaction reports. These vulnerabilities will almost certainly be exploited by criminals to place illicit funds into the legitimate economy.

76 Interdependence between MRs: MRs work closely with one another, pooling funds, using common bank accounts, and employing common cash couriers to facilitate a range of illicit and legitimate transactions on behalf of their clients. They use complex business models based on informal value transfer and transaction offsetting, which enables illicit funds to be easily commingled with legitimate funds. This often hinders the ability of law enforcement to effectively follow the money trail because illicit funds are often used to complete entirely legitimate transactions on behalf of unwitting customers.

77 Use of cash couriers: Cash couriers work on behalf of MRs to conduct cash pick-ups and disburse funds through New Zealand banks. They are high risk for ML because they deal in large quantities of cash and do not routinely carry out due diligence as to the source or beneficial owner of the funds in their possession. Some cash couriers are almost certainly conducting cash pickups directly from organised crime groups and will likely make viable targets for investigation.

78 Methods of money movement: Organised crime groups use professional facilitators as the gatekeepers to the legitimate economy. Once illicit funds are placed into the financial system via facilitators, they are commingled with legitimate funds and integrated via trusts, property purchases, or simply paid out as cash. Facilitators' extensive use of transaction offsetting and cash pooling obscures the money trail and frustrates efforts of law enforcement to trace the flow of funds back to its source.

THE PHILIPPINES

Strengthening anti-money laundering surveillance alongside advancements in financial technology

79 On 21 August 2018, the Anti-Money Laundering Council (AMLC) approved the study on the AML Regulatory Environment of Virtual Currency (VC) in the Philippines. The study was conducted to form a preliminary assessment of the transaction profile of accredited VC exchanges, particularly in relation to suspicious transactions, clients suspected of links to illicit activities, and big-ticket transactions. VC exchanges are regulated by the Bangko Sentral ng Pilipinas (BSP), when used for delivery of financial services, particularly for payments and remittances, under Circular No. 944 (Guidelines for VC Exchanges) dated 6 February 2017, in relation to BSP Circular No. 942 (Regulations for Non-Bank Financial Institutions). The study is published on the AMLC website: http://www.amlc.gov.ph/images/PDFs/Study%20on%20VC.pdf

80 The study used descriptive analysis on covered transaction reports (CTRs) and suspicious transaction reports (STRs) received from BSP-accredited VC exchanges from 6 March 2017 to 10 April 2018, which involved transactions executed on their platforms from 28 April 2014 to 6 April 2018, yielding a total of 22,366 transaction reports (composed of 1,086 CTRs and 21,280 STRs) with a combined value of PHP3.1 billion (PHP2.4 billion are CTRs and PHP0.7 billion are STRs). The study found that VC exchange reported transactions increased dramatically in both volume and value for 2017, following the issuance of BSP Circular No. 944 in February 2017 and subsequent approval of the registration of virtual currency companies in September and October 2017.

81 The BSP's establishment of a regulatory framework for VC exchanges has strengthened safeguards against risks associated with VCs, such as controls on ML and TF, technology risk management, and consumer protection. In particular, the inclusion of VC exchanges as covered persons (CPs) has allowed for more comprehensive monitoring of financial behaviour of individuals and entities possibly connected to illicit activities as well as closer coordination and information sharing among CPs in the conduct of AML surveillance, as gleaned from the narratives submitted by the VC exchange.

Risk assessment of non-profit organisations

82 On 28 November 2018, the AMLC approved the Risk Assessment of the NPO sector, and authorized its dissemination to all stakeholders. The NPO Risk Assessment was conducted in line with Recommendation 8 of the FATF 40 Recommendations. The AMLC was supported by NPO regulators, the Securities and Exchange Commission (SEC), and the Department of Social Welfare and Development (DSWD). The Philippine Council for NGO Certification (PCNC) and the Caucus for Development NGO Networks (CODE-NGO) also gave valuable inputs in said effort.

83 The NPO Risk Assessment presents and analyses the ML/TF risks of NPOs, based on investigations and actual cases, intelligence reports, and inputs from sector representatives. The ML threats for the sector were assessed as Medium; TF threats were assessed as High- Low. Vulnerability assessment for both ML and TF was rated Medium. Although regulatory framework was generally effective, enforcement of laws and regulations presented some issues.

84 The report recommends specific strategies involving both the public and NPO sectors to mitigate the ML and TF risks associated with NPOs. These strategies include sustained outreach to regulators and the NPO sector, adoption of risk-based regulations and supervision of NPOs and stronger coordination between the government and the NPO sector.

Self-funding of ISIL Southeast Asia

85 The South East Asia Counter-Terrorism Financing Working Group (SEA CTF WG), which was established during the third CTF Summit in 2017, conducted studies on funding of ISIL and ISIL-affiliated groups in South East Asia. The working groups have produced four separate reports: (a) ISIL's financing in SEA: The Regional Environment, (b) External Funding to ISIL SEA, (c) Hawala Dealers Financing of ISIL and Other High Threat Terrorist Organisations in SEA, and (d) Self-Funding of ISIL SEA. The said reports are the assessments of each of the lead project teams based on the information gathered from the SEA CTF WG members.

86 The Philippines' AMLC spearheaded the examination of ISIL-SEA's self-funding to understand it further and to put disruption strategies in place. The report on self-funding identified that these funds include those raised from criminal sources, such as kidnapping for ransom, extortion from the local population, and drug trafficking or drug smuggling. Another method of self-funding for TF is through legitimate sources, such as family support, sympathizers' donations, business profits and legitimate income. The SEA CTF WG members and guests shared information on the identified self-funding sources used by the terrorist or threat groups in South East Asia aligned with ISIL; analysed available financial intelligence, classified, and open source information; agreed to collaborate on top-priority targets to develop disruption strategies, which may be done through analyst exchange programs; and work with law enforcement agencies or regional agencies to implement these disruption strategies.

87 The report is distributed among members of the SEA CTF WG and the Financial Intelligence Consultative Group under the CTF Summit.

SINGAPORE

ACIP publications on misuse of legal persons and trade-based money laundering

88 The AML/CFT Industry Partnership (ACIP), Singapore's public-private partnership, published two industry best practice papers relating to the typologies of misuse of legal persons and trade-based ML/trade financing, including preventive measures and best practices that the industry has adopted to mitigate these risks.

89 Please see reports at: https://abs.org.sg/industry-guidelines/aml-cft-industry-partnership

3.2 Association of types of ML or TF with predicate activities

FIJI

90 Fiji has commenced a review of its NRA in November 2018. The review focussed on updating the assessment of ML threats which Fiji faces and the vulnerabilities to ML activities of the following sector: banking, remittance service providers, accounting firms, law firms and real estate agents.

91 Drug trafficking as a predicate offence for ML is trending and the FIU is working closely with Fiji Police Force investigators to assist with the financial profiling and asset tracing linked to drugs cases.

HONG KONG, CHINA

Case study 1

92 In October 2015, the Customs and Excise Department (C&ED) conducted an investigation into a syndicate selling counterfeit goods in Hong Kong. Several hawker stalls, showrooms and storages were found to be connected with storage and selling of counterfeit goods. In January 2016, the C&ED arrested nine persons and seized counterfeit goods valued at HKD 5.8 million. The financial investigation revealed that substantial cash, which was suspected to be proceeds generated from sale of counterfeit goods, had been deposited into the personal bank accounts of the syndicate and the total laundered amount was HK$5.75 million.

93 In May 2018, five syndicate members were convicted of a counterfeiting offences. Among them, three were convicted of ML and sentenced to between 11 and 26 months imprisonment. In December 2018, the court granted a confiscation order to confiscate HK$1.56 million worth of realizable properties held by the three key members.

Case study 2

94 In March 2017, the C&ED mounted an anti-narcotics operation resulting in the arrest of a couple and seizure of 4.6 kg of suspected cannabis buds and HK$1 million of suspected drug proceeds. The financial investigation showed that the couple laundered suspected crime proceeds of HK$5.4 million.

95 In March 2018, HK$3.7 million worth of realisable properties were restrained by means of a court order. In November 2018, the male in the couple was convicted to all charges and was sentenced to four years and two months imprisonment.

INDONESIA

96 According to Indonesia's most recent STR statistics, the predicate activities mostly associated to ML are fraud, corruption, and gambling, with corruption being the most significant.

JAPAN

97 In 2018, ML cases related to Boryokudan (including Boryokudan members, associates, and other related parties) accounted for 12.3% of all ML cases under the Act on Punishment of Organized Crimes.

98 A common method used by Boryokudan was to open a bank account in a fictitious name in order to obtain criminal proceeds from fraud and the sale of stolen goods.

99 One suspect engaged in the trafficking of cannabis used a home delivery service and arranged for customers to remit a total of approximately 1.6 million yen in payment to an account opened under the name of another person. He was arrested for the violation of the Anti-Drug Special Provisions Act (concealment of drug-related criminal proceeds).

MALAYSIA

100 During the validation of the initial findings of the quantitative assessments, further qualitative assessments and conclusion were also made on the results of the NRA as follows:

- Corruption, fraud and smuggling were considered to be the three most interconnected crimes with other serious crimes.
- Illicit drugs trafficking and human trafficking were found to be two serious crimes that are considered most associated with foreign sourced threats.
- Fraud is considered to be the most commonly linked serious crime to the sectors assessed, followed by corruption and tax evasion.

NEW ZEALAND

Labour exploitation and immigration fraud in the Auckland construction industry

101 NZFIU contributed to a joint-agency investigation targeting the illegal Malaysian labour market in the Auckland construction industry. The aim of the investigation was to investigate suspected immigration crimes and disrupt the illegal market in the Auckland construction industry. At the conclusion of the operation, 54 individuals were deported, 36 individuals voluntarily left NZ, 15 individuals were served deportation notices, and 190 individuals were stopped from illegally working in NZ; and charges laid included people smuggling, identity fraud, document fraud, aiding and abetting, ML and tax evasion.

102 NZFIU's contribution to this investigation centred on providing financial analysis of suspicious activity report (SAR) information and of suspects' bank account activity to assist with the identification of the criminal network and identify additional persons of interest. NZFIU analysis revealed money being passed between construction businesses and withdrawn from banks as cash for wage payments. It also identified directors operating companies in breach of their visa conditions, and identified funds being funnelled through shell companies. NZFIU continues to provide information to the investigation team on an ad-hoc basis to inform possible further investigative inquiries.

PAKISTAN

Case Study 1 - Robbery/ theft/ stolen goods

Background of the case:

103 Mr. SMARZ was an employee of a government department and maintained an account at ABC Bank in Pakistan where he was receiving a high value of funds through online cash deposits and clearing cheques. This activity was inconsistent with his profile and the bank became suspicious of his account activity. In order to confirm the source of funds, the bank tried to establish contact with Mr. SMARZ on his given mobile number and via letter to his provided residential address. The telephone contact could not be connected, and the letter was returned undelivered to the bank. Due to negative verification, ABC bank raised an STR. During analysis of the STR at the Financial Monitoring Unit (FMU), it was found that the suspect was an employee of a government department and receiving a salary of PKR 17,000. However, on the other hand the employee was receiving large sums of funds through online cash deposits and clearing from various branches of ABC Bank. Since the opening of his bank account, activities amounting to approximately PKR 17 Million were conducted through the account.

104 Through a search of public media, it was found that an individual by the name of SMARZ had been arrested by the security forces for his alleged involvement in the sale of stolen vehicles and other items. In order to confirm this matched with the suspect reported in STR, specific searches were conducted, and it was found that Mr. SMARZ had provided his mobile number on the internet for the urgent sale, and trading of, old vehicles. Based on the analysis and banking profile, financial intelligence was shared with the LEA for investigating the matter of theft, robbery and possible acts of terrorism.

Case Study 2 - Narcotics smuggling/tax evasion

Background of the case:

105 STRs were reported from Exchange Companies on three individuals on account of frequent purchasing of foreign currency in a structured manner. The reported individuals were maintaining multiple accounts in different banks. Adverse print and media news were found while searching on the public domain in relation to one of the reported individuals. It was reported that the individual had smuggled GBP 7 million worth of heroin from Pakistan to the United Kingdom for which he was jailed for twenty years. He was released from jail in 2005. The same individual had opened multiple accounts from 2011 onward in Pakistan. The accounts were located in various cities and used to park illicit funds. Further, the analysis also revealed that the two other suspects were not registered with the Federal Board of Revenue for income tax despite of high turnovers in their accounts.

Modus operandi:

106 The suspect along with other individuals linked to him by a common cell number, had purchased large amount of foreign currency in a structured manner and which were remitted out of the jurisdiction. The individuals had multiple accounts in different banks. One individual was allegedly involved in heroin smuggling. He had tactfully opened multiple accounts in different banks located in different cities by disclosing different businesses at each bank to spread the turnover and to evade the tax authorities. He had provided different business information at different banks. He would operate accounts for a short period of time and then close them. In contradiction to his stated business profile, he had conducted multiple transactions of a high value. His entire pattern of transactions in each account seemed to be suspicious as he was routing a high value of funds from one account to another. Despite the high turnover in his accounts, he was not registered for a National Tax Number (NTN). It was concluded that the alleged individual was parking illicit funds generated through drug smuggling and routing the funds through different accounts. Keeping in view all the aspects, the financial intelligence was shared with LEAs for investigating the possible smuggling of narcotics and tax evasion.

Case Study 3 - Drug smuggling

Background of the case:

107 "QRS" bank reported a STR on the basis of a media report that Anti-Narcotics Force (ANF) recovered 2.4 kg hashish from the possession of a lady ("ABC") while she was travelling in a passenger van. The bank gathered further information from sources and found a matching account in their branch. Based on this information, QRS Bank reported a STR to the FMU.

Modus operandi:

108 Suspect ABC is a photo account holder at QRS Bank, M branch since 2003. She declared herself as a housewife. Analysis of the statement of account reveals that funds were deposited and withdrawn in small amounts.

Case-IV - Corruption/tax evasion

109 STRs were reported by "Alpha" Bank and "Beta" Exchange Company on Mr. AX and Mr. JN whilst both were owners of different sugar mills. The suspects were involved in extensive currency exchange transactions and deliberately violated the State Bank of Pakistan threshold, through structuring and utilizing different forms for transactions. The individuals purchased a high value of US Dollars in a short period of time using cash without any apparent economic purpose. Meanwhile, they were maintaining multiple PKR and foreign currency accounts at Alpha Bank, where transactional

activity was reported unusual. The analysis of STRs showed that the individuals were withdrawing funds from their PKR accounts and purchasing USD from the open market and then depositing the amount into foreign currency accounts. Further, the funds were remitted out of the jurisdiction to their personal accounts.

110 Moreover, it was found that the individuals are close relatives of politically exposed persons (PEPs), the brothers of Mr. AX. During the analysis, it was observed that along with Mr. AX, his brothers and parents were also maintaining accounts at the same branch of Alpha Bank. A high volume of turnover was noticed in the accounts of family members during a particular period, comprising of inter account transactions and high value cash withdrawals and deposits which were not in line with the stated profile of individuals' declared income at time of account opening. The transactions in these accounts were conducted in a manner to break the trail of funds and hide beneficial ownership. The tax history of the family members revealed that the amount of tax paid was not commensurate with the transactional activity observed in the accounts.

111 Based on the above, it was suspected that the accounts of Mr. AX and Mr. JN might have been used for comingling of funds from different sources to confuse the audit trail and evade tax authorities. Further, due to the involvement of PEPs, suspicions were raised that the financial activities conducted from the Exchange Companies and banks may involve misuse of authority or corrupt practices. Therefore, the intelligence was shared with LEAs for further probing of the matters and further, appropriate action.

THAILAND

112 Cigarettes smuggling proceeds were used to fund incidents in the southern border provinces. The smuggling was carried out by members at an operational level. A shop owner who trades various types of smuggled goods was also closely related to the perpetrator group. It was also found that a religious school was used as a venue to recruit, promote their ideology and training to facilitate a number of terrorism activities in the jurisdiction. The group also received financial support from drug smugglers as the operation prevented the detection of smuggling.

3.3 Emerging trends; declining trends; continuing trends

BRUNEI DARUSSALAM

113 A major continuing trend seen in STRs received by the FIU in 2018 included a large percentage of reports filed with the following red flag indicators:

- Account holders are from zero or low-income backgrounds;
- Multiple electronic fund transfers deposited into the account from another account within the same bank;
- Multiple electronic fund transfers out of the account to another account within the same bank;
- Multiple below-threshold cash deposits within the same day;
- Cash withdrawals immediately following a cash deposit or electronic fund transfer deposit;
- Use of personal savings account for business activities (particularly for sole-proprietorships and micro enterprises); and
- Suspicious customer behaviour (account holders refuse to provide the bank justification for account activity and proceed to close their own account).

114 The above trends appear to be common elements of criminal activity including illegal deposit taking, fraud (investment scams), unlicensed money changing and, occasionally, unlicensed remittance

activities. In addition, the indicators also allude to potential illicit activity such as money mules or online trading where the account holder is possibly investing funds on behalf of third parties.

CHINA

Money laundering through network crowdfunding platforms and live-broadcasting platform

115 With the development of technology and financial innovation, internet finance has emerged. Internet finance, network crowdfunding platforms and live-broadcasting platforms are playing a vital role in the financial market these days, as they particularly attract new customers and open new channels for business. However, criminals may use these two platforms for ML.

Money laundering using network crowdfunding platforms

116 Concealing the illegal purpose of ML with “legal” network crowdfunding: Criminals may set up false crowdfunding projects on the platform to raise funds from so-called “investors” and investors will collect the funds through online payments.

117 Use of cross-border network crowdfunding as new channels of TF: Terrorists or supporters may use false names or false registered IPs to set up a network crowdfunding project. Through this means, they may attract cross-border funds.

118 Use of network crowdfunding platforms as an investment intermediary to raise funds.

Money laundering using live-broadcasting platform

119 Criminals may use false identity information to set up live-broadcasting platforms and arrange fake fans to reward large amounts of money or charge money through future investment analysis platform with so-called investment experts. All the rewards and charges will be remitted to the designated account through online payment. After a certain percentage of "platform fees" are charged by the network broadcast platforms, criminals may withdraw the remaining funds. This kind of low-cost ML method can evade tax liability and AML supervision.

AML measures of network crowdfunding platforms and live-broadcasting platforms

- Focus on information integrity and identify customers effectively.
- Pay attention to abnormal transactions and effectively identify ML risks.
- Establish a customer rating mechanism and customer money laundering evaluation index system.
- Strengthen monitoring and analysis of STRs.
- Improve monitoring and analysis standard of AML data.

Money laundering trends and new characteristics of underground banks

120 As one of the main methods of ML, underground banks usually have the characteristics of a family operation, a strict organisation system, hidden operation modes and fixed capital channels. In recent years, with the continuous innovation of transaction modes, underground banks have developed some new features in the use of tools and operation modes:

- Money laundering through offshore accounts. Offshore accounts could conceal the actual controller and source of funds. Meanwhile, funds from domestically held offshore accounts are easy to control, which makes them a new tool for underground banks to absorb and transfer overseas funds.

- Domestic banks open non-resident accounts for overseas institutions, but it is difficult for banks to judge the authenticity of original account opening information submitted by non-resident accounts' customers, and the true source of non-resident accounts' funds.
- New financial trends (represented by internet finance) provide convenience for underground banks to launder money. By using third-party payments as the transaction platform, E-commerce has characteristics such as high efficiency, non-face-to-face transactions and are difficult to monitor, therefore such platforms have become a popular transaction mode for underground banks.

FIJI

Continuing trend: Email compromise and email spoofing

121 Commercial banks, financial institutions, businesses and members of the public were continuously advised by the Fiji FIU to exercise caution when handling email payment instructions for import trade transactions and large value personal outbound foreign remittance transactions. The Fiji FIU noted a continuous increase in cases of individuals and businesses falling victim to email compromise and spoofing scams in 2018.

122 Recent case examples reported to the Fiji FIU in 2018 on email compromise and email spoofing cases include:

- In March 2018, an email account of a local bank customer was compromised, and a fraudulent payment instruction was sent to the local bank. Approximately FJ$575,000 was transferred to a foreign bank account belonging to a cybercriminal syndicate.
- In September 2018, in a case involving cyber ML, FJ$556,000 was fraudulently transferred from a local business bank account to an offshore "incorrect" bank account number. In this case the foreign supplier's business email was compromised.
- In October 2018, proceeds of approximately FJ$27,000 from the sale of investment shares of a local investor who is residing abroad, were remitted to a cybercriminal's bank account in another jurisdiction as a result of an email compromise.
- In October 2018, proceeds of the settlement of estate property, totaling approximately FJ$845,000 was remitted to the foreign bank account of a cybercriminal who pretended to be the beneficiary of the estate. It appears that email accounts of the beneficiary and the local party were compromised.

123 Any suspicious overseas trade transaction or large personal remittance that could be linked to email compromise and spoofing scams should immediately be reported as a suspicious transaction report to the Fiji FIU. Commercial banks and remittance service providers were reminded to conduct enhanced due diligence for suspicious payment instructions.

The Fiji FIU has noted a decline in the following trends:

- the use of fraudulent documentation to conduct financial transactions; and
- the number of impersonation cases reported to the FIU.

INDONESIA

124 The banking industry is still being used by ML perpetrators to launder proceeds of crime. Based on court verdicts; transfers via ATM, cash deposits through tellers, transactions using electronic data capture (EDC), and transfers via mobile banking showed an upward trend. Cash transactions (i.e. giving

and receiving money directly), showed a declining trend based on Indonesian research on results of court verdicts decided in 2017.

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

JAPAN

126 Instances of concealment of criminal proceeds in 2017 consisted largely of cases in which offenders attempted to transfer funds to bank accounts under the name of other persons. This is a major trend seen in ML crimes.

127 In addition, criminals use various methods to keep investigative authorities off track including; selling stolen items using a false name, hiding criminal proceeds in a warehouse under a contract executed in the name of another person.

LAO PDR

128 During February 2018 to December 2018, cheque counterfeiting or the use of counterfeit cheques in ML is a declining trend according to statistics of predicate offences. However, fraud is a trend which continues to occur.

MACAO, CHINA

129 Throughout the period from January to June 2018, a total of 2,187 STRs were received by Financial Intelligence Office (GIF), with 1,128 STRs from the gaming sector, 617 STRs from the financial sector (including banking, insurance and financial intermediaries) and 442 STRs from other sectors.

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

- Chips conversion without / with minimal gambling activities;
- Irregular large cash withdrawals;
- Purchase of portable commodities and valuables;
- Suspected underground banking / alternative remittance services;
- Significant cash deposit with non-verifiable source of funds;
- Suspected use of credit card / debit card to purchase high value goods and discount for cash;
- Chips conversion / marker redemption on behalf of third party(ies);
- Use of ATM, phone banking, cash deposit machines;
- Currency exchange/ cash conversion;
- Attempted but unsuccessful transactions;
- Foreign exchange transactions with unidentified source of funds;
- Use of cheques/account transfer etc. to transfer funds;
- Unable to provide ID / important personal information; and
- Suspicious wire transfer.

131 From January to June 2018, 60 STRs were disseminated to the Public Prosecutions Office. These cases were mainly related to fraud.

132 According to the observations of STRs received, the rising fraud in remittances and the use of cheque/account transfers, have been the focus of the banking industry's specific attention in the past few months. Apart from the typical cases that the local beneficiary bank received telegraphs from the

ordering bank or an email from the victim claiming the relevant remittances were related to fraudulent acts, some cases were reported to the Prosecutions Office based on local/overseas intelligence received. This shows that effective international cooperation and information sharing did contribute to efficient and successful investigations, prosecutions and convictions in some fraudulent cases.

133 A number of cases, such as the social media deception, online romance scam and e-shopping fraud emerged in the first half of 2018. Judiciary Police have maintained close co-operation with overseas enforcement agencies, and have reminded the public to be more skeptical, and not to disclose account information and transaction verification codes to anyone so as to avoid suffering pecuniary loss.

MALAYSIA

STR analysis continuing trends

134 The upward trend in STR submissions with a compound annual growth rate of 23% since 2008 is attributable to increased awareness and generally heightened transaction monitoring by reporting institutions. It is also attributed to the effectiveness of public and private sector engagements, including sharing of the risk information on high-risk crimes, TF risk profiling and frequent public-private sector information sharing platforms. STRs are mainly contributed by banking, casino and money services business sectors.

135 The main suspected offences reported by reporting institutions were fraud/scam, tax evasion, organized crime and corruption.

STR analysis emerging trends

136 Fraudsters moving from using personal accounts to setting up business accounts to avoid suspicion.

Investigation (ML, TF and predicate offences) continuing trends

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

138 Usage of third-party accounts including mule account holders for receiving and transferring illegal proceeds.

139 Laundering through high value goods, such as jewellery and branded items.

NEW ZEALAND

Money laundering threat to the South Pacific

140 NZFIU analysis indicates that banking institutes in the South Pacific islands are being targeted for ML, fraud and potential criminal infiltration. In one instance, a NZ citizen with suspected links to organised crime was observed attempting to establish ML structures in a number of South Pacific jurisdictions. He is a company formation agent and has extensive knowledge of international banking, legal and AML systems. The NZFIU holds concerns this individual is attempting to facilitate transnational ML through the South Pacific on behalf of organised crime groups.

141 In another scheme which is unrelated but in which there have been similar attempts to establish a bank, the government of a South Pacific jurisdiction was recently presented with a proposal regarding

rights to natural resources of commercial magnitude, in exchange for the issuance of a banking licence to a company registered in a third jurisdiction. The NZFIU assessed that this proposal was almost certainly fraudulent, and was possibly an attempt to gain access to the South Pacific banking sector for nefarious purposes.

Increasing gang presence in the South Pacific

142 Increasing numbers of gang members are travelling to South Pacific jurisdictions, providing an optimal setting for gangs to conduct a range of organised criminal activities, particularly moving illicit substances in and out of the region and into New Zealand. NZ's organised criminal groups (OCG) have strong familial links to the South Pacific, increasing recruitment opportunities and the connectivity of networks to NZ. ML techniques observed by NZFIU include cash smuggling, wire transfers, structured cash deposits, and use of South Pacific jurisdictions as tax havens.

Money laundering via online gambling platforms

143 Reporting to NZFIU indicates an ongoing trend of ML via online gambling platforms. SAR reporting shows individuals with connections to drug networks and OCGs continue to use online gambling websites, receiving large payments to their NZ bank accounts as 'refunds'. As these sites are operated offshore, they are almost certainly being misused to circumvent NZ's AML controls and allowing offenders to move illicit funds in and out of the jurisdiction undetected.

PAKISTAN

144 An increasing trend in the receipt of tax evasion related STRs has been observed in 2018.

145 A continued trend in receipt of Hawala/Hundi related STRs was observed in 2018.

4. CASE STUDIES OF ML AND TF

4.1 Terrorism Financing

MALAYSIA

146 Investigators identified a total of more than USD7,000 raised through local sympathizers since 2016, upon the instruction of Malaysian terrorists in Syria through a close encrypted messaging application. Subsequently, a key portion of the raised funds were remitted by financial facilitators in the network via remittance companies to jurisdictions near Syria and Iraq or through other transit jurisdictions.

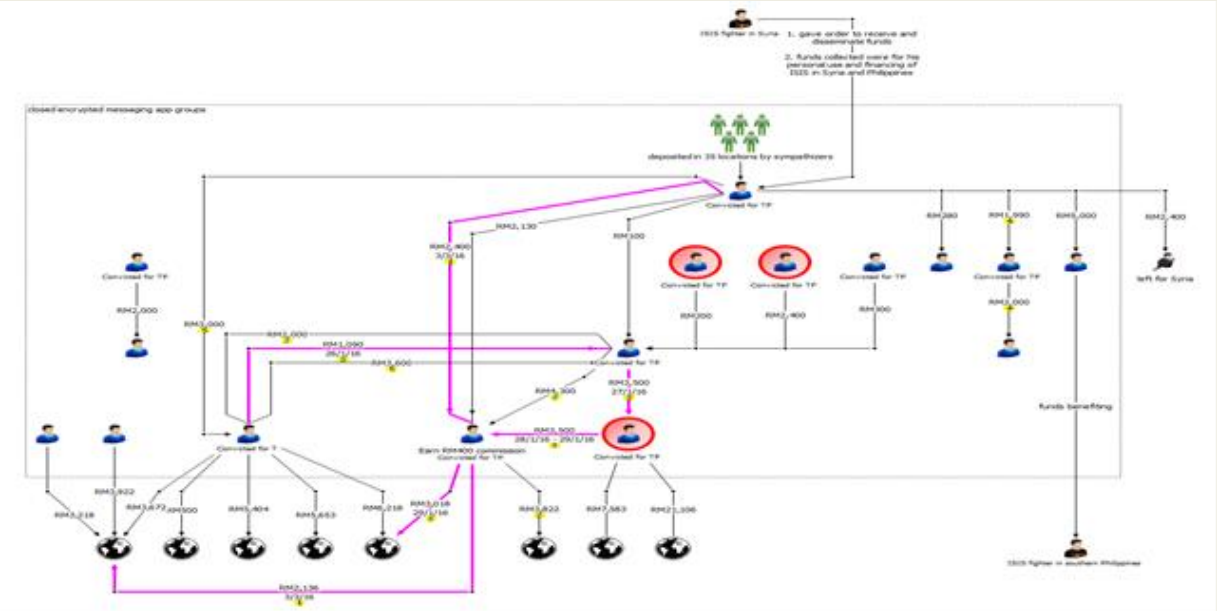
147 The financial facilitators attempted to obscure the trails by transferring funds among themselves multiple times before those funds were channelled abroad. It is believed that the potential use of the funds includes purchasing of a lorry for transportation of goods, explosive bags or supporting the travelling and living cost of terrorists bound for, or in, Syria.

148 One of the suspects was identified by a reporting institution after its transaction monitoring system found a financial trail between facilitators whose names were flagged by authorities earlier.

149 Overall, a total of nine financial facilitators in this network were sentenced to a total of 65 years' imprisonment (ranging from four to ten years) for terrorism financing activities stipulated under sections 130N(b), 130O(1) and 130Q(1) of the Penal Code.

150 The TF methods used include:

- Wire transfers/Use of foreign bank accounts.
- Underground banking/alternative remittance services/Hawala.



THE PHILIPPINES

The MG and the M City Siege

151 The Maute Group (MG) is a Daesh/Islamic State of Iraq and Syria (ISIS) inspired group based in the Southern Philippines. The group consists of known clans in the area belonging to prominent families.

Identified Money Moving Networks

152 Based on the analysis and findings, CJ (a foreign terrorist organisation) cell members sent international fund transfers to the Philippines from January to February 2017. These transactions were all received through the same remittance agency and network of who was using an international remittance platform.

153 Information from the foreign police officials indicated that funds were made available in Jurisdiction I through a form of hawala whereby Jurisdiction I's foreign fighters for ISIS based in Syria were directed to sell assets in Jurisdiction I. The funds from these sales were directed to CJ situated in Jurisdiction I, while the value of the funds from these sales were made available through ISIS to Jurisdiction I's foreign fighters in Syria. Using this system, foreign fighters in Syria were able to access funds, and funds were made available in Jurisdiction I without the need for international funds transfers, remittance or physical movement of currency. Additional information also indicates that, Jurisdiction I's foreign fighters for ISIS that departed for Syria left their bank accounts and bank cards for use by CJ members.

MG linked network sending from Jurisdiction T to the Philippines

154 Information from Jurisdiction I indicated that funds in support of the M City Siege were sent to the Philippines from a network of individuals based in Jurisdiction T. Additional information also indicates that the same network of individuals in Jurisdiction T also sent funds to Jurisdiction T approximately US$20,000.00 was sent to the Philippines from Jurisdiction T. The said individuals received the funds in the Philippines through two separate remitters.

MG linked network-sending funds to Jurisdiction I

155 A network of individuals was identified sending funds from M City to Jurisdiction I at the end of 2016. The funds were sent primarily using two remittance businesses, CMAL and EMT. The owner of CMAL and his possible wife, along with another individual, sent 12 transactions from the Philippines to Jurisdiction I between July 2016 and January 2017. It is possible that these transactions are linked to legitimate business activities, with the recipients in Jurisdiction I each operating a business however, these transactions do not appear to be business related. The said businesses are not registered, and there are no records of any imports or exports associated.

Network of Female Financial Facilitators based in the Philippines

156 It is probable that there is a network of female financial facilitators based in the Southern Philippines moving funds on behalf of ISIS and ISIS linked groups in South East Asia.

157 Female financier ME received funds from Jurisdiction M and Jurisdiction K from individuals who have also sent funds to female financier MM. Both female financiers ME and MM received funds in the Philippines from a certain individual in Jurisdiction M and a certain individual in Jurisdiction K between 2015 and 2016. This network has also sent funds to the second wife of certain Dr. MA. Female financier ME and another female financier EI both sent funds to the second wife of Dr. MA in Jurisdiction M in 2016.

Foreign Terrorist Fighters

158 Seven foreign fighters of Jurisdiction I have been identified and travelled to the Philippines prior to the siege of M City. Analysis has determined that it is unlikely these individuals would have the funds or resources to arrange travel, including passports, visas and the purchase of tickets on their own. Information indicates that certain nationals of Jurisdiction I admitted to having facilitated the travel of the seven identified foreign fighters of Jurisdiction I who travelled to the Philippines. It is also suspected that another citizen of Jurisdiction I facilitated the travel of the remaining three foreign fighters of Jurisdiction I. Authorities of Jurisdiction I have arrested the said individuals on terrorism financing charges.

Identified High Risk Remittance Business

159 CMAL is considered a high-risk remitter for TF. CMAL is no longer registered as an MSP but appears to be registered prior to the siege. CMAL has never been registered with AMLC as a MR and has not submitted any transaction reports. The owner of CMAL is recorded as HPM who does not operate a business account for CMAL but uses his personal bank account to facilitate remittance transactions. CMAL was also identified by Jurisdiction A's FIU as a remittance agency receiving funds from a group in their jurisdiction and has sent structured transactions to the Philippines in April 2013. The group in Jurisdiction A is suspected to have links to terrorism financing. These transactions represent the majority of transactions received through CMAL up to 2016.

160 Between November 2013 and June 2018, the international remittance platform filed 22 SARs that identify CMAL as either the sending or paying agent for 49 suspicious money transfers transacted from 11 July 2013 up to 20 March 2017. The majority of SARs filed were for suspected TF.

161 CMAL acted six times more as the paying agent than as the sending agent based on the suspicious money transfers. Most of the suspicious money transfers sent to CMAL, as the paying agent, originated within the Philippines followed by Indonesia, which sent the highest value of money transfers.

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

CHINA

162 In December 2017, the supervisory authority, tax bureau and police investigated a suspect, who falsely used foreign exchanges receipts in trades to obtain a subsidy rebate and conceal gains from tax offences through underground banking and multiple registered corporations in City H.

163 In February 2018 the case was solved. Suspect X established a shell company Y, purchased VAT invoices through a third party, then falsely made out invoices for tax to company Y. Suspect X and Suspect Z also executed tax offences by falsifying invoices, purchased customs declaration, made false outputs and illegal foreign exchange. According to the police, the total value of VAT invoices and tax rebate have reached more than millions of yuan. At present, the case has been transferred to the prosecutor for prosecution.

PAKISTAN

164 Mr and Mrs XYZ (well-known Pakistan business family) were involved in unauthorised capital flight and tax evasion using offshore companies. STRs were reported by different Exchange Companies on the basis of structured currency exchange transactions (USD) and deliberate violation of the Central Bank's threshold for currency purchases through structuring and utilizing different exchange companies. The amount involved (identified through CTRs) was significant, which triggered a suspicion. The FMU identified that the suspects maintained multiple foreign currency accounts at different banks. The overall transactional pattern revealed that they were withdrawing funds from their local currency accounts, followed by a purchase of foreign currency and then depositing into foreign currency accounts, which were finally remitted out of jurisdiction. During analysis of the STR, the names of suspects were also found in leaked papers as the owners offshore companies and that they were in the process of selling their companies to a foreign company. Mis-declaration was also observed in the sale of companies to a foreign buyer. It was suspected that Mr. and Mrs. XYZ were involved in dishonest and fraudulent declarations, breach of foreign exchange regulations, unauthorized flight of capital, tax evasion, and other offences. The Director General of FMU ordered the freezing of the accounts. The financial intelligence was shared with multiple agencies under the AML Act.

165 On the basis of FMU's referral, the tax authorities recovered the tax liability in the amount of PKR 6.2 billion.

PHILLIPINES

166 In May 2017 Jurisdiction U's FIU requested information through Egmont Secure Web (ESW) on various individuals and entities allegedly involved in ML, securities and wire transfer frauds.

167 The information involved GLADS, a Philippine-registered entity wholly owned by GRALE. The information revealed that Mr. DT, a majority interest holder of GRALE, sponsored the formation

of G Income Fund (the "Fund") in October 2011. Mr. DT served as trustee, chairman, president, and co-investment manager of the Fund between 2012 and 2014. The Fund was intended to produce income for its investors/shareholders by investing primarily in individual promissory notes signed by post-graduate and professional students and recent graduates in high-income fields of employment. In January 2012, GRALE became the Fund's custodian of all relevant loan-related documentation including the original promissory notes via a Loan Servicing Agreement.

168 GRALE allegedly began losing money and Mr. DT devised a scheme of creating fictitious loans paid for by the Fund in order to keep his company afloat and maintain his lavish lifestyle. Under Mr. DT's fraudulent scheme, loan proceeds were wired to TF-LLC, a limited liability company that Mr. DT also controlled, rather than to a bank that formally issues loan to the borrower.

169 The fraud was discovered when employees of GRALE mistakenly sent a loan statement to Mr. DT's former college roommate, who was listed as having a loan with a principal balance of USD342,000.00. In December 2014, Jurisdiction U's Investigation Bureau interviewed Mr. DT's former roommate who denied ever conducting business with, borrowing money or obtaining a loan from Mr. DT, GRALE, or the Fund. This led to the launching of an investigation by Jurisdiction U's securities commission, Mr. DT's arrest and the filing of criminal charges and multiple civil lawsuits against him. One of the independent trustees of the Fund, Mr. MS, executed an affidavit alleging that Mr. DT advised the independent trustees of the Fund to invest indirectly in a series of factoring transactions in the Philippines. This would involve loaning monies to one of two potential limited liability companies that would act as intermediaries in Jurisdiction U – LCLLC or LC2LLC ("LC Entities"). These LC Entities would in turn loan the funds to counterparties in the Philippines as part of a series of factoring transactions. Interest payments and repayments of the principal by the factoring transaction counterparties would then be made back to the Fund through the LC Entities. The Fund allegedly loaned a total of USD8,065,759.44 from April 2013 to October 2014 to the LC Entities. However, the proceeds wired from the Fund to the LC Entities were not invested but were instead wired to GRALE's operating account. From there, some of the proceeds were retained for GRALE's operating expenses and some were wired to GLADS, a Philippine corporation wholly owned by GRALE. Aside from Mr. DT, among the incorporators of GLADS are Filipino lawyers connected to a known law office in the jurisdiction.

170 Certain funds were allegedly laundered in ELI Corp., a Philippine registered entity. Mr. DT apparently fabricated false promissory notes which suggests that LC Entities, represented by a Mr. BS, loaned monies to ELI Corp, represented by a certain Mr. WD. The fictitious promissory notes issued from April up to November 2015 totalled PHP210.30 million. Said funds were purportedly loaned by ELI Corp. to various Filipino business entities via Working Capital Agreements ("WCA"). These WCAs also turned out to be fictitious.

171 The Philippine FIU acted on the request and provided response which includes possible ultimate beneficiaries of the funds which originated from the entities controlled by Mr. DT from Jurisdiction U.

172 In November 2017, Jurisdiction U found the new information provided by the FIU very useful, and, thus, made another request this time focusing on the new participants identified by the FIU in its previous response for inclusion in their investigation of the case. The FIU also acted on the case and provided the information sought within three months from receipt of the subsequent request.

4.3 Use of virtual currencies

AUSTRALIA

Suspension of cryptocurrency business registrations over links to organised crime

173 AUSTRAC suspended the registrations of two digital currency exchange businesses following the arrest of a man by the Australian Federal Police (AFP).

174 The AFP's arrest followed an investigation into those responsible for allegedly importing border-controlled drugs via international mail. Investigations led AFP officers to execute search warrants seizing steroids, Australian currency and cryptocurrency related items, in early 2019. Charges were laid on a number of individuals related to the importation, trafficking and possession of approximately 30 kilograms of illicit drugs, including MDMA, cocaine, methamphetamine and ketamine.

175 It was alleged the criminal syndicate, used various dark net sites, bitcoin accounts and legitimate business for the sourcing, payment and distribution of the illicit drugs.

176 In a separate action, the AFP-led Criminal Assets Confiscation Taskforce (CACT) successfully sought the restraint of assets related to the investigation. Orders were obtained from the County Court of Victoria to restrain property valued in excess of AUD2 million.

177 This included several bank accounts, real estate properties, motor vehicles, a motorbike, cash and cryptocurrency. The restraining orders were made under the *Proceeds of Crime Act* 2002 (Cth)

178 Following the arrests, AUSTRAC suspended the registration of two digital currency exchange businesses where one of the men arrested was a key member, removing their ability to continue to conduct business.

CHINA

Case Study 1

179 Corporation A deals with U-bao which is a digital currency circulation system. The related suspects used U-bao to collect money illegally, with those funds flowing into the system from multiple accounts. Hundreds of parties were involved, and the notes/reference for the transactions were "U-bao". There are many negative public opinions about Corporation A, including pyramid selling. The accounts of one suspect has many fund transactions which are related to the company of Corporation A. The total value involved in this case has reached millions of yuan, and relevant information about this case have been referred to the police.

Case Study 2

180 WEIKA is a virtual currency issued by a cross-border network platform. This type of currency can be used for consumption and can raise its value through purchasing equities which are related to certain amounts of WEIKA. WEIKA charges fees for membership. The account of Suspect B had funds flowing in and out frequently, and the money crossed different sectors and regions. The transaction notes/references of Suspect B and counterparts were "Onecoin", "WEIKA activation code", "Purchase motivation package", etc. They were suspected of using WEIKA for pyramid selling and ML, the total amount in this case has reached millions of yuan.

CHINESE TAIPEI

181 IRS, a legal person established in Jurisdiction S in 2016, ran a Ponzi Scheme of Bitcoin investment to defraud investors. Since October 2016, Mr. A had been the responsible person in the area of Chinese Taipei and China and in charge of the overall operation of the group, recruitment of investment, bonus distribution, etc. Mr. A and the accomplices held briefing seminars to explain investment plans, profit and reward mechanisms of IRS to the participants. They ensured that the

invested products would be valued daily and the maximum profit that investors could obtain would be 255% of the amount of the investment after one year. In this way, Mr. A defrauded about 30 thousand investors and the value of funds amounted to approximately US$ 51 million.

182 Mr. A et al. converted the proceeds of crime into the form of VC and real estate. During the investigation, these properties, where were held by Mr. A et al, were seized. In December 2018, the Taichung District Prosecutors Office indicted Mr. A and accomplices in violation of the Banking Act and the Multi-Level Marketing Supervision Act.

HONG KONG, CHINA

183 In July 2017, 136.9 Bitcoins (valued at about HKD 13.64 million) were stolen by hackers in a Bitcoins exchange platform based in Jurisdiction A. The stolen Bitcoins were eventually transferred to Mr. A in August 2017. Mr. A subsequently sold the Bitcoins and transferred the proceeds to a bank account in Hong Kong, China. Upon request of Jurisdiction A, the proceeds of HKD 4.6 million and USD 0.73 million in the bank account were withheld in Hong Kong, China. The investigation is in progress.

JAPAN

184 A male office worker purchased VAs (i.e. virtual assets) using an account and credit card information of another person, which were obtained illegally. He changed the virtual asset to Japanese yen through an overseas exchange website and transferred the money to a bank account in the name of another person. He was arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

NEW ZEALAND

Illicit drug purchases via the dark web using bitcoin

185 In 2018 an individual was convicted for importing and supplying large amounts of class C controlled drugs. The individual purchased the substances from dark net websites using Bitcoin. He then on-sold them to customers within New Zealand and internationally via advertisements posted on the dark net; accepting Bitcoin, Ethereum and cash as payment.

186 On termination, NZP located more than NZD400K in cash and approximately NZD180K worth of crypto currency on the offender's wallet. In total, more than NZD1.5 million of assets was restrained under NZ's criminal proceeds legislation.

THE PHILIPPINES

187 An individual used his company originally registered as a sole proprietorship under a different purpose to operate a pyramid scheme using Bitcoin as a front to explain the company's source of earnings and VC exchange platforms to facilitate payments and investments. Under the scheme, investors were promised double-digit interest rates every few weeks. As the suspects resorted to pyramiding and employed intermediaries to serve as recruiters of new investors, the scheme's geographical reach extended nationwide. The perpetrators were eventually arrested. Months prior to the arrest, the VC exchange's systems flagged suspicious account activities, transactions, and individuals associated with the scheme, leading to the filing of STRs on the group and their associates/cohorts.

SINGAPORE

Use of virtual currency – Proceeds from transnational email fraud used to purchase Bitcoins

188 Proceeds from an email fraud perpetuated against a victim in the United States were transferred to a Singaporean bank account used by a Singaporean company offering an online trading platform and payment gateway for virtual currencies. Using forged documents, the perpetuator opened an online trading account that was subsequently credited with criminal proceeds. The perpetuator then purchased Bitcoins, regardless of the price, through the online trading platform. Due to the unusual trading pattern, the online trading account was blocked by the Singaporean company. Upon receiving a recall letter from the bank, the Singaporean company liquidated the Bitcoins that the perpetuator purchased. The funds were seized by the Police. Investigations are ongoing.

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

FIJI

Use of a Gatekeeper to allegedly facilitate unusual EFTPOS transactions

189 The FIU received a suspicious transaction report from a local bank on significant transactions conducted on a single EFTPOS terminal over a weekend. It was deemed suspicious since the EFTPOS terminal was a newly installed facility at a small local law firm.

190 The FIU established that a Fijian national, Person A, residing in Jurisdiction B approached Person X, principal of the local law firm to acquire an EFTPOS machine to receive investment funds on behalf of his entity, Company A.

191 The local law firm acquired the EFTPOS facility despite no apparent economic viability for an EFTPOS machine. A week later, two foreign credit cards were fraudulently used to conduct seven transactions within a span of three weeks totalling approximately FJ$2 million through the EFTPOS terminal at the local law firm. The funds were transferred to the law firm's trust account.

192 It was established that Person X was supposedly involved in the elaborate scam with Person A and Company A to fraudulently obtain funds using the EFTPOS machine. Person X received approximately FJ$221,000.00 from the fraudulent transfers while Company A received approximately FJ$650,000.00 into its local bank account. The remaining FJ$1,129,000.00 was retained in the law firm's trust account.

193 Funds were swiftly withdrawn from Company A's local bank account to pay individuals and invest in assets. It was also established that expensive Rolex wristwatches were purchased from the proceeds of crime. There was good coordination and communication between local border law enforcement agencies and the FIU in this matter.

194 The FIU issued an enforceable instruction notice to the local bank to restrict all bank accounts involved in the elaborate scheme including beneficiaries of the funds to secure and minimize the loss of the proceeds of crime. The FIU provided a case dissemination report to the Fiji Police Force and the case is still under investigation.

Possible Offence:

- Fraud.
- Possession of property suspected of being proceeds of crime.
- Money laundering.

Indicators:

- Use of lawyer as a gatekeeper to facilitate fraud.
- Use of unfamiliar business transacting methods which was not commensurate with nature of business.
- Purchase of valuable assets and luxury items.

Fraudulent VAT Returns

195 A local accounting firm is alleged to have been lodging fraudulent tax returns with local tax authorities. It is suspected that the firm inflated the reported expenses in VAT return claims of their clients. The firm also submitted copies of fraudulent invoices and receipts to substantiate the fraudulent expense claims. The clients of the accounting firm then received VAT refunds from the local tax authority indicating that they were not entitled to any refund. This has also resulted in the loss of a substantial amount of money by Fiji's local tax authority. The likely offences are ML, obtaining property by deception and general dishonesty obtaining a gain/causing loss. This matter is currently under investigation by local LEAs.

NEW ZEALAND

Accountant incorporating NZ companies on behalf of OCGs

196 A New Zealand accountant has incorporated several companies which have subsequently been used by OCG to facilitate importation of drugs into the jurisdiction. The accountant filed the company incorporation documents and registered himself as the director and/or shareholder of the companies. The companies' bank accounts are used to fund drug imports and/or repatriate the proceeds of drug offending internationally. It is possible that the accountant is also falsifying the financial records of these companies (i.e. 'cooking the books') to obscure the illicit activity, though this has not yet been established.

Use of lawyer to conceal purchase of property by OCG member

197 A member of a New Zealand OCG entered into an agreement to purchase a property using lawyers to obfuscate the funds and arrangement. The OCG member's mother is a solicitor who obtained a mortgage against an existing property and provided these funds to settle the OCG member's property purchase via another solicitor's trust account under the guise of a "property refinance". The OCG member makes regular payments to a newly established transactional account in his mother's name, from which the mortgage is serviced. An acknowledgement of debt between the member and mother separates the OCG member's funds from the property transactions, limiting law enforcement's ability to disrupt the purchase by seizing funds and/or assets.

SINGAPORE

Use of Professional Services – Company incorporated to receive bribe payments from overseas

198 A law firm that offers corporate secretarial services assisted a foreign businessman to incorporate a company and its lawyers served as directors of the registered company. In their capacity as directors, the lawyers then applied for bank accounts for the company and granted full control of the bank accounts to the foreign businessman, whom they dutifully declared to the banks as the beneficial owner of the company.

199 The foreign businessman then used the company as a conduit for receiving bribes on behalf of foreign officials. He also held himself as an employee of the company to give legitimacy to the withdrawals that he made from the company's bank accounts to his personal account or other accounts

under his control. The alleged corrupt proceeds channelled to his accounts were eventually paid to the foreign officials.

200 Corrupt Practices Investigation Bureau (CPIB) proactively engaged foreign authorities to conduct a joint investigation against the corrupt officials who had received the bribes in Singapore. Investigation is ongoing.

THAILAND

201 A private religious school in a southern border province commissioned an accounting firm for "window dressing" of school's account, in order to receive the *per student* financial support from the government that was then used to support terrorism activities in the area.

4.5 Trade-based money laundering and transfer pricing

AFGHANISTAN

Case Study 1

202 Upon verification with Customs and Revenue Department, it was found that the trading Company X's customs documents were forged. It was a 'company on paper' which had no record of any imports or exports with Customs and Revenue Department, yet money was credited into the company's accounts in a systematic manner by several individuals. The company's accounts were then debited by Mr. Y who used the money for money transfer and exchange purposes. Mr. Y also smuggled physical cash through domestic airports to other provinces of the jurisdiction. The FIU intelligence led to open investigations by LEA.

Case Study 2

203 Results of financial analysis conducted on companies showed that the companies have transferred a large amount of cash abroad mainly to Jurisdiction A and Jurisdiction B against imported goods. However, the value of the imported goods was verified by the Customs department to form only a tiny fraction of the total amount sent abroad. The companies also transferred a large amount of money to Jurisdiction C and Jurisdiction D against which no goods were imported into the jurisdiction.

204 Financial verification of invoices by the reporting entities of the FIU also showed that the companies transferred money via invoices from different banks for importing the same goods.

205 Upon dissemination of the case by the FIU to LEAs, the Major Crime Task Force opened an ML investigation on the case.

206 This investigation not only confirmed issuance of different payment invoices for the same goods, but also showed that the companies had forged payment invoices. The invoices presented by the owners of the companies in court were subjected to verification and an expert panel was formed to determine whether the invoices were real. The expert panel confirmed that the invoices were forged.

207 During investigation, the accused individuals offered a bribe to the officials to clear them of charges and drop the case, which resulted in their immediate arrest and detention for attempting bribe officials.

208 While the subjects were in detention, the ML investigation was completed and an ML prosecution was opened.

209 The FIU, upon request made by the concerned LEA, compiled and dispatched 30 files, approximately 1500 pages of value-added products to the LEA.

210 These value-added products included:

- Supporting documents money transfer transaction alongside information about delivery channels, beneficiaries and jurisdictions to which the transfers were made.
- Information on gifts offered by these companies to employees of banks in exchange for carrying out transactions.
- Introduction of FIU employee for consultation and provision of expert opinion to the LEA.
- Information regarding Tax Identification Number (TIN) numbers of companies being prosecuted.
- Provision of information about the purpose of transfers, received from jurisdictions to which transfers were made.
- Freezing of bank accounts involved in the case as per LEA request.
- Provision of information on the differences between the amounts transferred via real invoices and amounts shown in forged invoices.
- Information on the content of forged invoices, transfer procedures from banks, and the total amount transferred by convicted individuals along with invoices.
- Formation of a board of technical inspection which comprised of representatives from three banks and was chaired by the FIU, and dispatching a technical inspection report of this board to the LEA.
- Information regarding specification of individuals who acted on behalf of these companies to transfer money abroad during the period 2013 – 2015.
- Information regarding signatory authorities of these companies, and authorized persons of these companies in the absence of a company director and deputy director.

211 It is worth mentioning that the abovementioned value-added products were dispatched to the LEA by the FIU upon a total of 15 requests made by the LEA.

212 As a result of this prosecution, the accused individuals were subjected to ML convictions and sentenced to four years imprisonment with immediate effect. This conviction was made based on the AML Law and resulted with a confiscation of a certain amount of fund. The case is open for appeal (as for the time of preparing this typologies report 2019).

FIJI

213 The Fiji FIU received a STR in relation to Person M receiving significant amounts of funds from Company D.

214 It was established that Person M was also a director and shareholder of Company D. Company D had received approximately FJ$510,138.00 in remittances from Company E located in Jurisdiction B. These remittances were allegedly for bill payments, purchase of goods and trade payments. Fiji FIU discovered that Person M was also a director and shareholder of Company E in Jurisdiction B and that there were no exports from Company D to Company E to match the remittance payments. The funds were then transferred to Person M's local bank account and used to purchase property.

215 The FIU further established that Person M had received approximately FJ$897,913.00 from Person N located in Jurisdiction B. These funds were then used by Person M to purchase another property.

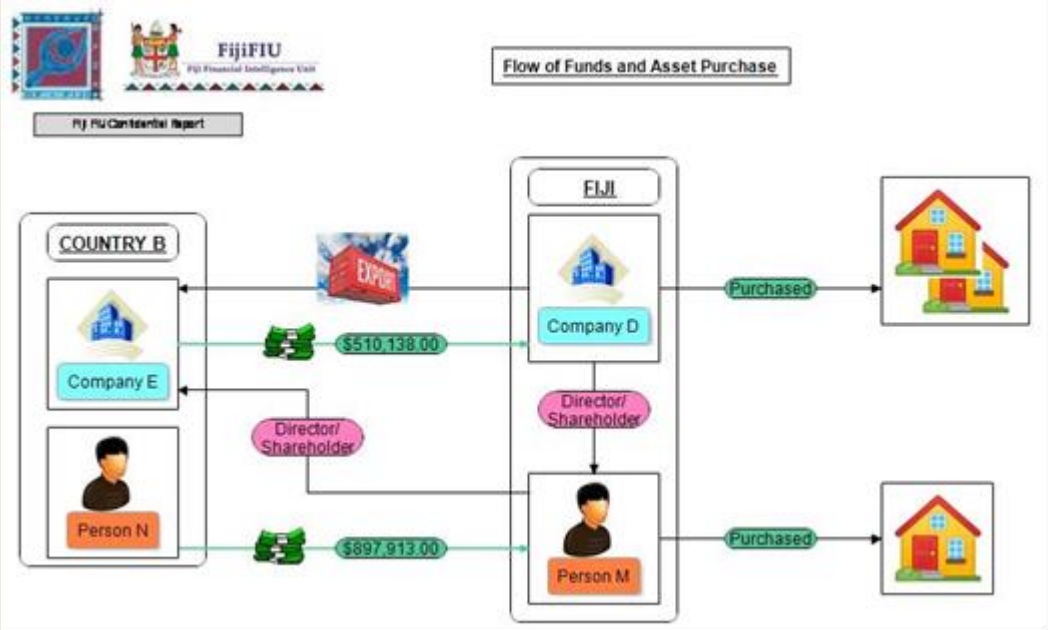
216 A case dissemination report was provided to the FIU of Jurisdiction B and Fiji Revenue & Customs Service (FRCS) for further profiling and investigation.

Possible Offence:

- Trade based ML
- Tax offences.

Indicators:

- Significant inward remittances.
- Rapid movement of funds from business to personal accounts.
- Numerous related entities utilized to move funds.
- Property investment.



INDONESIA

217 JT was sending funds overseas in large amounts recorded in 5419 International Fund Transfer Instructions (IFTI) reports with total amount IDR3.6 trillion (USD254 million) to 2,365 parties (individuals and companies). JT was one of the owners of an import trading company, money changer, and freight forwarding company. Based on an examination of JT's accounts, it was found that for any overseas transfer of funds, JT always attached invoice documents related to the purchase of goods imported from offshore supplier companies. China, Hong Kong- China and Japan were the jurisdictions that received the largest amount of funds from JT. Transfers of funds to China amounted to Rp1.085.182.450.627 (USD74,840,169) consisting of 710 parties.

218 When the data relating to goods imported by JT was matched against Directorate General of Customs and Excise (DGCE) Customs data, there appeared to be a difference between the invoices attached by JT in the banks with the existing data in DGCE. After the matching data process, it could be seen that the invoices in the banks had never been recorded in DGCE data (i.e. false or fictitious).

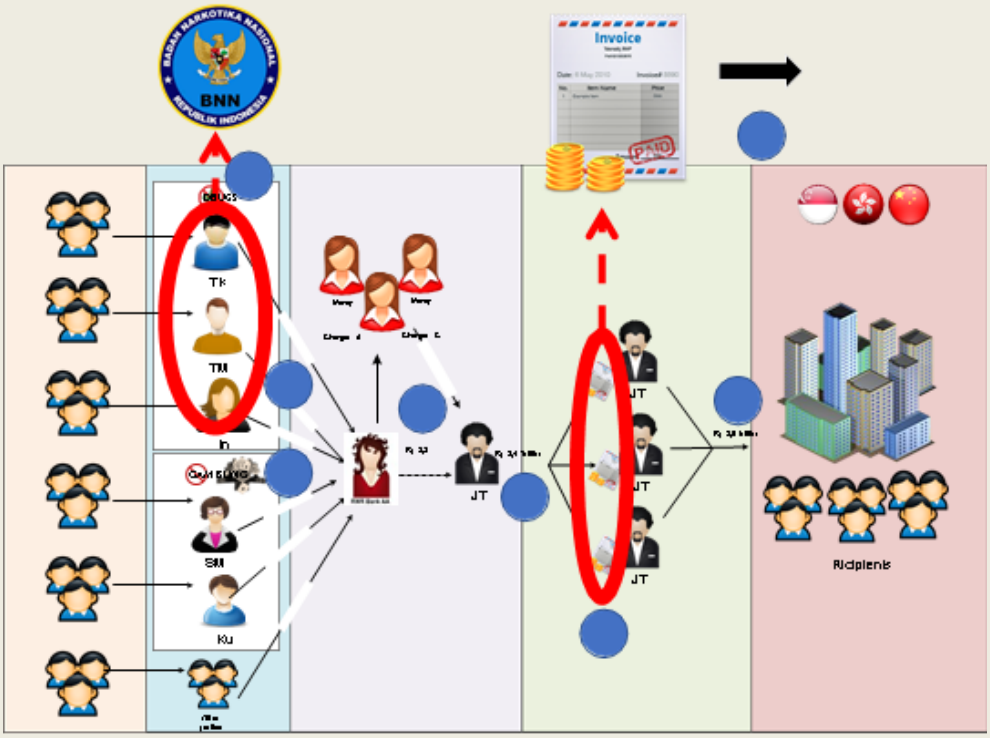
219 There were 2,365 overseas recipients of funds. Most of them (1,246 parties) were companies that did not engage in import activities, and 494 of them were individuals. The rest was companies engaging in export and import activities.

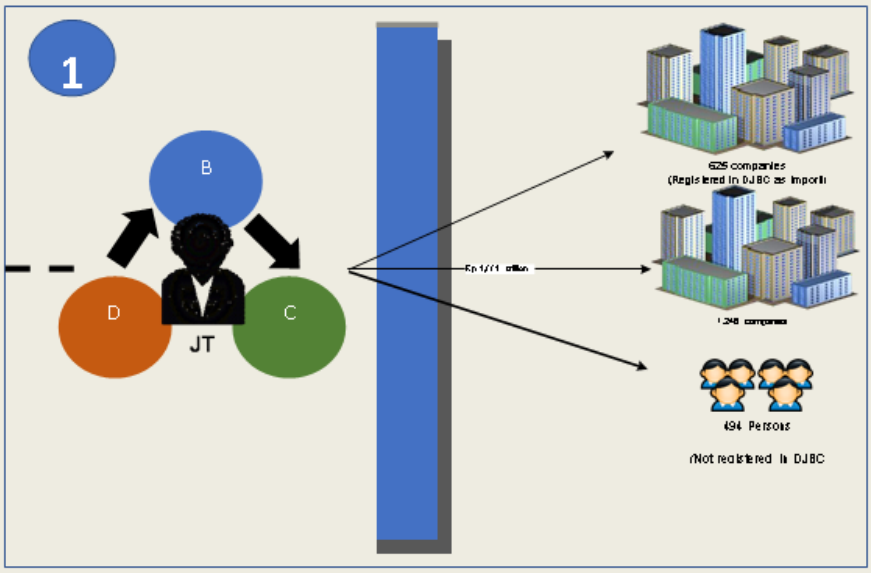
220 RWR was one of the sources of funds for JT's account in A Bank. RWR transferred Rp772 billion (USD53,241,379) to JT's account in A Bank. The funds were subsequently sent to B Bank in the amount of Rp354,8 billion, C Bank in the amount of Rp1,34 trillion (USD92,413,793) and D Bank in the amount of Rp796,17 billion (USD54,908,275).

221 Based on PPATK's analysis on RWR's account in A Bank for the period 2014-2015, the total incoming funds in the account amounted to IDR9,62 trillion (USD663,448,275) from several parties. Some parties were identified to be involved in a criminal activities linked to narcotics, namely, TK in 965 transactions amounting to IDR313,2 billion (USD21,600,000), TM in 328 transactions amounting IDR114,53 billion (USD1,002,068) and AAS amounting IDR9,86 billion (USD680,000) and USD45.000. The National Anti-Narcotics Board (BNN) was advised about those parties' involvement in narcotics crime.

222 RWR accounts were also allegedly used to receive funds from the parties involved in online gambling, and further sent the funds overseas through JT's account. JT's accounts allegedly used for the benefit of RWR. This is reinforced by the pattern of transactions on the JT's account in the form of pass by transactions.

223 The transaction patterns on JT and RWRs personal accounts, in the form of pass by transactions, ranged in the millions to billions of rupiah and were predominantly conducted via internet banking. Based on bank information, the purpose of JT and RWRs account opening was for business transactions.

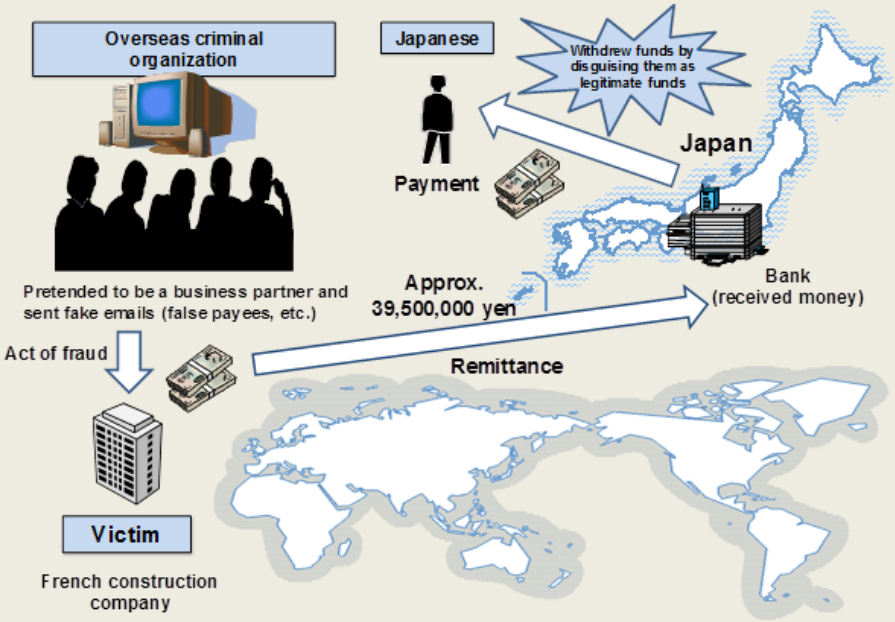




JAPAN

224 When selling a stolen car, an unemployed man placed the vehicle number of another car on the stolen car and exported it to a foreign jurisdiction through an export management company which did not know that the car had been stolen. He was arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

225 A Japanese man had sent falsified transaction emails to a construction company in France and made them remit funds into bank accounts in Japan opened under other persons' names. When withdrawing the funds, he falsely explained to a bank employee that those funds were remittances related to normal commercial transactions, thereby disguising the money as legitimate business profit. As a result, he was arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds) and fraud.



NEW ZEALAND

Trade goods used as payment in illegal fishing operation

226 A New Zealand fishing company was charged with a complex and large-scale fraud involving under-reporting of its catch. This involved two types of offences – making false statements on catch returns and selling fish that had not been declared to the Ministry for Primary Industries. Some of the illegal catch was subsequently exported to an Australian company which provided the New Zealand exporter with a new boat as payment for the illegal catch. This methodology saw the exchange of value (a new boat as payment for illegally caught fish) via the international trade stream rather than exchange of cash.

PAKISTAN

227 FMU received a STR on a suspect regarding trade based ML. The suspect Mr. A, was conducting business in Karachi and had opened a bank account. Sometime after opening the account, the suspect submitted an EIF (electronic import form) for certification from the bank. Upon enquiring, the bank identified that the importer was involved in trade based ML. The suspect imported grey cloth from a jurisdiction through companies based in another jurisdiction by falsely declaring that the grey cloth was imported from China. Customs Intelligence also seized the cloth and a total of 106 containers in substitution of smuggling.

228 The suspect is maintaining a bank account in Karachi and Customs Intelligence is investigating the matter. The financial intelligence was then forwarded to LEAs, for further investigation and for their necessary action under the provisions of AML Act, 2010.

PHILIPPINES

229 Philippine Drug Enforcement Agents arrested ZTC, a national of Jurisdiction C, in a buy-bust operation. ZTC was caught in *flagrante delicto* selling methamphetamine hydrochloride, locally known as shabu, to a government agent. Aside from the drugs, various financial documents in his possession were also seized, particularly deposit slips of suspected drug proceeds deposited to the bank accounts of several persons/entity namely QH, XQ, WL, CG, WH, RDS, MAD, BJC, JE and YSMW Enterprises.

230 The drug operations of ZTC dates prior to 2009 when he was arrested by government agents, also for selling large quantities of illegal drugs.

Several Requests for Financial Investigation

231 The Philippine FIU received requests from several government agencies to conduct a financial investigation on QH, WH and YSMW Enterprises relative to illegal drug activities. Accordingly, several financial documents pertaining to QH, WH and YSMW Enterprises were seized by government agents in the possession of arrested drug personalities in Central Philippines. Moreover, cellular phones seized from inmates in different jail facilities contained text messages specifically alluding to YSMW Enterprises and QH bank accounts as being used to facilitate the proceeds of illegal drug activities.

232 The FIU conducted bank inquiry on the identified bank and investment accounts of the subject personalities. Coordination was also made with: (1) different government property registries to verify property ownership and business holdings of the subjects; and (2) law enforcement agencies to determine derogatory records and assistance in the conduct of surveillance operations.

Results of financial investigation

233 There was no identified financial transaction of ZTC except that deposit slips to other persons were found in his possession.

234 YSMW Enterprises' bank accounts were used to facilitate drug proceeds as evidenced by text messages extracted from the cellular phones of inmates. The company was registered to be engaged in wholesale/retail of hand bags. Financial transactions in its bank accounts recorded numerous large denominated amounts, which were not typical in the ordinary course of such a business. Moreover, it was found that the bank accounts of the company were not materially controlled by its registered owner, LTE, but by DS and TS, both of which are also nationals of Jurisdiction C.

235 On the other hand, QH, XQ and WH are related by blood and all citizens of Jurisdiction C. They declared as sources of income, (a) a computer shop which was later determined to be non-existent, and (b) HK Corporation, a company whose declared business is to engage in the sale of computer ink and accessories. Financial investigations on their accounts revealed that billions of pesos flowed into their accounts, which were atypical to the declared nature of their business.

236 CG, a national of Jurisdiction C, owns several businesses which recently ceased operations. In his identification documents, he declared salaries as his main source of income. In 2018, he established travel and real estate businesses. It can be seen that, from the transaction profile of the businesses that billions of pesos flowed into the companies' bank accounts even at their infancy stage. On the other hand, WL, likewise a national of Jurisdiction C, declared that she is a financial manager of GPT Company, known to be engaged in online-gambling. Financial investigations revealed that hundreds of millions of pesos flowed into her accounts. She also made several fund transfers to the bank accounts of WFG, wife of CG.

237 Identified through outward fund transfers from the accounts of subjects were numerous persons of interests possibly related to illegal drug activities. The propriety of the transactions was not established and was not justified to be made in the ordinary course of business.

238 The recovery of the deposit slips in the possession of ZTC showed the link of QH, XQ, WL, CG, WH, YSMW Enterprises, RDS, MAD, BJC and JE in illegal drug activities. Relationships were established between and among them because of their exchanges of funds through bank to bank transfers and the use of money service businesses. Moreover, their financial transactions were discovered to be linked with other individuals and entities who are respondents in different civil forfeiture cases filed by the FIU, in relation to violation of the Philippine drug laws, based on the wire transfer transactions they made through the banking system.

239 The material amounts transacted to their accounts, unsupported with legitimate sources of income that would generate hundreds of millions of pesos would lead to the conclusion that they have other sources of income. The transactions to their accounts were not typical transactions for the types of businesses. The inconsistent behaviour of the accounts and the nature of the sources of their income shows an absence of any underlying justification of the said financial transactions.

240 A total of six hundred fifty (650) bank accounts maintained in thirteen (13) financial institutions, containing Php773,003,483.06 and USD142,407.25 were frozen and is currently subject of civil forfeiture.

SINGAPORE

Supplying designated luxury items - Company and its director prosecuted for the supply of designated luxury items to the Democratic People's Republic of Korea (DPRK), cheating and ML

241 Person N is one of the directors of Company T. Between 2010 and 2017, Company T supplied designated luxury goods worth over S$6 million, including wine, perfumes and cosmetics, to a department store in the DPRK on 80 occasions.

242 When the DPRK department store delayed payments for the goods ordered and caused cash flow problems in Company T, Person N devised a fraudulent scheme and used Company T to submit fictitious commercial invoices to five banks to fraudulently obtain financing on 81 occasions, totalling more than US$95million.

243 In July 2018, Person N and Company T were charged for supplying designated luxury items to the DPRK under the UN-DPRK Regulations. Person N was also charged for cheating in relation to the invoice financing fraud. Company T was also charged for laundering of the proceeds from the invoice financing fraud.

244 The prosecution of Person N and Company T is ongoing.

4.6 Underground banking/alternative remittance services/Hawala

CHINA

Case Study 1

245 In July and November 2014, the supervisory authority provided STRs to the police. The police filed the case in May 2015, and investigated Suspect Y and his associates.

246 This case involved three underground banking organisations: card swiping by POS machine, illegal trading of foreign exchange and cross-border cash withdrawals by ATM. They formed an integrated underground banking criminal chain. Until June 2018, all the 41 suspects involved in this case have been sentenced for the illegal operation.

Case Study 2

247 In September 2018, the supervisory authority, jointly with local police, uncovered an underground banking case. Suspect C and his associates were illegally trading foreign exchange in two cities. They used accounts of one suspect in City J, foreign exchange was collected from overseas accounts and funds were collected from domestic accounts. The total amount in this case has reached more than one billion yuan.

CHINESE TAIPEI

248 In May 2017, a Ponzi scheme developed by Group Y was introduced into Chinese Taipei by Mr. B with the assistance of a Malaysian citizen. Mr. B et al. held several briefing seminars to claim that Group Y had invented software which could be used to gain profit from sport lotteries. Depending on the amount of investment, the annual interest rate that investors could gain was ranging from 84% to 180%. In order to deceive more investors and receive more funds, Mr. B et al. developed feedback programs to provide high number of incentives or other prizes that make investors willing to introduce new investors to join or invest. As of September 2018, Mr. B et al. had defrauded about 3,000 investors and the amount of victimization was about US$ 198 million.

249 In order to evade the investigation, Mr. B et al. hid the cash received from investors at the residences of Mr. B and his accomplices, this cash amounting to approximately NT$ 200 million. About NT$ 232 million was transferred abroad through underground banking operators. Some of the funds

were used for other investments in their names or converted into foreign currency or VA. During the investigation, case related assets such as cash, virtual currency, cars, real estate, and bank accounts were seized. In November 2018, the Prosecutors Office indicted Mr. B and his accomplices for violating of the Banking Act, the Money Laundering Control Act, and the Multi-Level Marketing Supervision Act.

250 When investigating an unrelated kidnapping case, the CIB found H company, which runs electronic trading led by Wu, actually operates underground banking, including an illegal exchange on foreign currencies including such as CNY, USD and NTD in jurisdictions and regions covering Chinese Taipei, Hong Kong, China, and Southeast Asian jurisdictions. The suspects committed ML offences via opening OBU accounts and abusing the corporate personality of unrelated paper companies. The remittance amount was up to NT$20 billion and the illicit gains were up to 180 million NTD. The CIB successfully brought a motion to the court on 25 September 2018, pursuant to the Money Laundering Control Act (Expended Confiscation) and the Code of Criminal Procedure. An equivalent 430 million NTD in the related bank account was seized. Under the collaboration between Chinese Taipei and China, five suspects were arrested in China and seven suspects were arrested in Chinese Taipei.

INDONESIA

Case Study 1

251 In July 2014, HF declared his allegiance to ISIS. He then communicated through telegram to BS (an ISIS Commander for Southeast Asia from Indonesia). HF obtained an instruction from BS to assist the needs of the MIT Group (a Terrorist Group of Indonesia affiliated with ISIS) and carry out an attack. Based on the results of a search of IFTI data, PPATK found that there was an inflow of funds in July 2015 from the Middle East amounting to USD3,789.77.

252 In addition, HF is known to have controlled other individuals' accounts, which were used to receive funds from domestic terrorist groups. According to the authorities, the funds were sent to several parties in the Philippines in July 2015, in particular, USD10,500 was sent through MSP for purchase of weapons to be used by terrorist organisations. In January 2016, the police arrested HF in relation to the shooting and bombing of Thamrin, Boulevard Jakarta. HF has since been imprisoned for six years for terrorism and terrorism financing offences.

Case Study 2

253 On May 2015, AS met AJ, both are affiliated with ISIS, while visiting AA in prison. At the meeting, AJ asked to help dispatch parties in Indonesia to Syria to join ISIS. The source of funds entered into bank accounts in the name of AJ were mostly sourced from domestic parties and were in the amount to IDR 300 million (~USD21,428). The funds were used to purchase tickets to Syria. In the period of April 2016, AJ instructed the US to send money to SM by using the equivalent amount of Philippines pesos amounting to IDR 200 million (~USD14,285) through MSB remittance for the purpose purchasing weapons to be used in military training in Indonesia.

JAPAN

254 Vietnamese suspects had customers who wanted to send money from Japan to Vietnam. They had the customers send money to their bank account in Japan, which was opened under another person's name. They bought convenience goods and food with the money and exported them to Vietnam under the guise of a legitimate transaction. The exported goods were then sold in Vietnam and thereby converted into cash. This scheme was in effect equivalent to an international remittance. The suspects were arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds) and of the Banking Act (underground banking).

255 A case where money remitted by a customer to an account opened in another person's name was used to purchase heavy machinery and agricultural equipment, with the purchased machinery and equipment exported to a foreign jurisdiction in a deal disguised as a legitimate transaction and converted into cash. This arrangement was in effect equivalent to an international remittance.

PAKISTAN

256 A complainant reported that he was receiving phone calls from Afghan telephone numbers and a local number demanding a sum of Rupees 1 million as extortion money. The callers was revealed to be members of Taliban Movement of Pakistan (TTP) and warned that if the amount is not paid, their house will be bombed. The complainant and his nephew went to a place in Peshawar and handed over extortion money to an unknown individual.

257 The investigation revealed that the money was transferred through hawala to Afghanistan. A Joint Investigation Team (JIT) was constituted. Cash Dissemination Report (CDR) analysis revealed contacts between two parties and further investigation found that both the accused were linked with JuA. Upon arrest, both confessed to being involved in the transfer of the extortion money. The investigation revealed other individuals involved who are still at-large and have been declared as proclaimed offenders. Further investigations are in progress.

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

FIJI

Business Email Compromise resulting in significant loss

258 The FIU received an STR from Bank D that Company C was a victim of a business email compromise. The FIU discovered that Company C's business email correspondences with their foreign supplier were compromised by a hacker in Jurisdiction F. The hacker intercepted the email correspondences and instructed Company C to transfer approximately US$266,000.00 to a foreign bank account number. The hacker emailed Company C with an email address similar to Company C's foreign supplier.

259 The FIU provided a case dissemination report to the respective foreign FIU for their investigation. It was established that the funds were subsequently dissipated to different entities on the same day. However, the ultimate destination of the funds could not be ascertained.

Possible offence:

- Obtaining financial advantage through deception.
- General dishonesty.

Indicators:

- Poorly constructed emails in order to convince the recipient to ignore mistakes.
- Changing payment details and beneficiary details at the last minute.

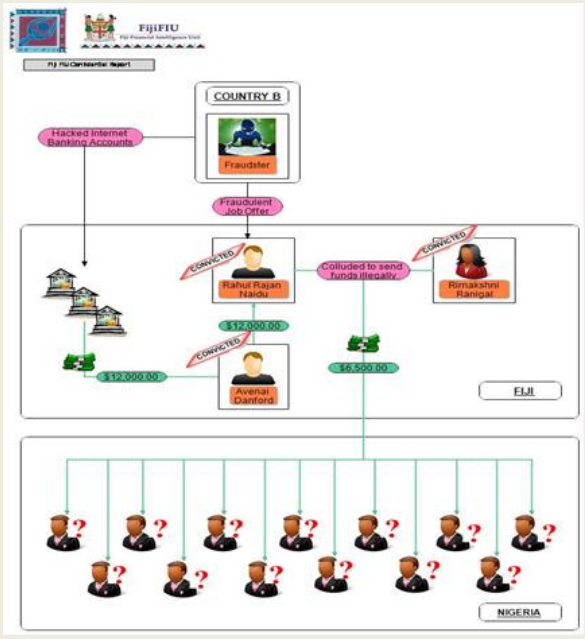
Colluding to facilitate illicit gains via unauthorized internet banking transfers

260 Mr. Rahul Rajan Naidu received a job offer from a "Jasmin Olich of Global Link Money Services" to purportedly conduct a confidential evaluation on Western Union services by sending and receiving money through Western Union. Mr. Rahul Rajan Naidu was advised that the funds would only be transferred to a Westpac bank account which he would then withdraw, deduct his commission and remit the remainder to various individuals in parts of Nigeria.

261 Since Mr. Rahul Rajan Naidu did not hold an account at Westpac he approached his friend, Mr. Shoeb Nur Ali, a pay master at Fiji Meats Limited to assist him find Westpac account holders who were not using their bank accounts. Mr Shoeb Nur Ali asked his friend, Mr. Avenai Danford, if he was willing to allow Mr. Rahul Rajan Naidu to use his account to receive funds. Mr. Avenai Danford agreed and received $12,000.00 into his Westpac bank account from unauthorized internet banking transfers from three victims. Mr. Avenai Danford withdrew and gave these funds to Mr. Rahul Rajan Naidu.

262 Mr. Rahul Rajan Naidu then asked Mr. Shoeb Nur Ali for copies of his ID and copies of ID of three of Mr. Shoeb Nur Ali's colleagues. Ms. Rimakshni Ranigal, Front Line Officer at an exchange dealer outlet, used these documents as well as copies of other ID that Mr. Rahul Rajan Naidu obtained to send 12 remittances to Nigeria.

263 None of the 12 individuals who were recorded as the senders of these remittances were present when the funds were sent and were not aware that funds were sent using their names and ID. On 4 September 2018, Mr. Rahul Rajan Naidu was found guilty of four counts of ML and Mr Avenai Danford and Ms. Rimakshni Ranigal were found guilty of one count of ML each. On 18 September 2018, Mr Rahul Rajan Naidu, Mr Avenai Danford and Ms. Rimakshni Ranigal were given sentences of six years nine months, three years and five years respectively.



4.8 Use of new payment methods/systems

AUSTRALIA

264 In June 2018, the Minister for Home Affairs confirmed that AUSTRAC and Commonwealth Bank of Australia (CBA) had reached an agreement, in which CBA has admitted to 53,750 breaches of Australia's Anti-Money Laundering and Counter Terrorism Financing Act 2006 (AML/CTF Act). The CBA agreed to pay a financial penalty of AUD700 million, the largest civil penalty ever ordered in Australia.

265 The CBA acknowledged there were failures related to its Intelligent Deposit Machines (IDMs), more specifically, failures with management of risks around its IDMs and failures to provide timely threshold transaction reports and suspicious matter reports. CBA also admitted failures around appropriate monitoring of customers and accounts.

266 CBA's compliance failings translated into serious and organised criminals exploiting the financial sector to launder the illicit proceeds of their criminal activities, including proceeds from the sale of illicit drugs in the community.

267 This case provides an example of the very real nature of organised criminal activity and ways in which criminals can exploit the financial sector when reporting entities fail to adhere to their AML/CTF obligations.

268 The penalty was the largest civil penalty in Australia's corporate history. In June 2018, AUSTRAC issued several media releases on this matter: http://www.austrac.gov.au/media/media-releases.

269 The outcomes of this case sent a strong message to industry that serious non-compliance with Australia's Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (AML/CTF Act) would not be tolerated, with the result of the civil penalty proceedings providing a real example of the consequences of poor compliance.

270 The case also reiterates the responsibility of financial institutions, their boards and senior management to ensure a business takes AML/CTF obligations seriously, and that they have implemented an organisational culture to support this.

CHINA

Case Study 1

271 In June 2017, Suspect D provided his Alipay QR code with real name authentication to his girlfriend (who has been sentenced) to receive drug proceeds, and transferred the money to the game ID of his girlfriend. Suspect D used his account to conceal the source and nature of criminal proceeds, and was involved in the crime of ML. In April 2018, the court sentenced Suspect D to a two-month detention along with a penalty.

Case Study 2

272 In 2017, Suspect E was involved in drug trafficking, and received payment for drugs using WeChat or cash. Suspect E transferred the money to his ex-wife (Suspect F) through the same means. The court determined that Suspect F provided her WeChat account to Suspect E, concealed the source and nature of criminal proceeds, and assisted to transfer the proceeds. They were convicted of ML offences. In March 2018, the court sentenced Suspect F to seven months imprisonment along with a penalty.

FIJI

Manipulation of Internal Systems and Processes

273 Ms. Vika Sadrau was employed with Post Fiji Limited as a Customer Service Officer responsible for processing Electronic Money Orders (EMO).

274 From March to May 2015, Ms Vika Sadrau dishonestly obtained $55,779.32 by manipulating the EMO system. Ms. Vika Sadrau processed an EMO transaction for a customer and used the same EMO key ID to create multiple payments for the same transaction.

275 Ms. Vika Sadrau then altered the payment amounts and payee details and obtained approval from her supervisor to make payments to herself. Ms. Vika Sadrau processed payments to herself totalling $55,779.32. She then deposited $21,000.00 into her bank account.

276 Ms. Vika Sadrau pleaded guilty to one count of theft and one count of ML. On 22 August 2018, Ms. Vika Sadrau was sentenced to 18 months for theft and four years imprisonment for ML. The case study demonstrates breach of internal control procedures.

HONG KONG, CHINA

277 A number of Stored Value Facilities (SVF) accounts were found to record frequent cash top-ups or transfers from other accounts between December 2017 and June 2018. The deposit funds were not used for making any purchases, instead they were mainly withdrawn from linked personal bank accounts and a small amount of the funds were then returned to the original senders. Transaction monitoring discovered that some of the terms of transfer messages were references to football betting and the names of national teams participating in an international football tournament. Suspecting that the SVF accounts might be used for illegal gambling, the SVF service provider made a disclosure to the JFIU.

278 Having been analysed by the JFIU, it was found that some account holders had reported addresses in the same residential complex, and one account holder's mobile number was directly linked to an illegal football betting website. The SVF accounts were used to receive gambling bets, by cash top-ups and transfers, related to illegal online football betting by a syndicate. The bets were consolidated through the SVF accounts and subsequently transferred to either the personal bank accounts held by the syndicate members or the originating SVF accounts, depending on the outcome of matches. The information was disseminated to a local law enforcement agency for follow-up actions.

INDONESIA

279 Following an attack on Surakarta (a regional city in central Java), several fund transfers used to finance the attack were identified from the bank accounts of individuals who were in communication with Mr. Y, an Indonesian ISIL Commander for Southeast Asia who was residing in Syria. FIU and Law Enforcement Agencies identified Mr. Y (Syria) transferring approximately USD 1,000 to PayPal the account of Mr. H (Indonesia). Mr. H withdrew the PayPal balance to his bank account and transferred it to Mr. M (Indonesia). Mr. M then transferred the money to multiple bank accounts, those funds were to be cashed and delivered to terrorists. Mr. M who was involved in financing the attack was convicted under the CFT Law. In addition, Mr. Y has been added to the UNSCR 1267 sanctions list and the Indonesia's Domestic Terrorist List.

JAPAN

280 A male office worker received information on electronic money by email from a fraud group member knowing that the information was obtained illegally. He was arrested for violation of the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

4.9 Laundering of proceeds from tax offences

CHINA

Case Study 1

281 In December 2017, the supervisory authority received STRs for four corporations from certain financial institutions. After further investigations, the supervisory authority provided the information to

the local police. The police found that Corporation G falsely made out invoices for VAT. In April and May 2018, six suspects were arrested. At the time of writing, three suspects remain in custody and the other three are out on bail pending trial.

282 During January 2017 to April 2018, the companies involved in this case falsely made out more than one thousand special invoices for VAT, evading millions of yuan in taxes.

Case Study 2

283 In February 2018, the supervisory authority provided STRs that falsely made out special invoices for the police. In June 2018, the police and local tax authority set up a joint team to investigate this case. In July 2018, the team successfully destroyed four crime dents, five criminal gangs and arrested 23 suspects. The team also detained more than one thousand company seals, hundreds of bank cards and USB keys, more than 80 financial books, 90 business licenses of shell companies, 50 tax-control disks, thousands of falsely made out invoices for VAT and freeze more than millions of yuan.

FIJI

Laundering business proceeds via cash intensive business

284 Company A was reported for conducting significant cash deposits and subsequently purchasing bank cheques with cash.

285 The FIU established that Company A had not lodged its tax returns in 2016 and 2017. However, it received approximately FJ$6.4 million dollars in deposits. Further analysis established that the shareholder, Person O and his wife Person P received approximately $740,000.00 as deposits into their bank accounts and had also not lodged tax returns.

286 A case dissemination report was provided to the tax authority on Company A, Person O and Person P for investigation.

Possible Offence:

- Tax offences.

Indicators:

- Large cash deposits.
- Use of family member to facilitate tax evasion.
- Use of cash intensive business to launder funds.

Alleged tax evasion by diversification of business operations and use of family members

287 The 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 Company X and also operates a fuel pump station on the same premises.

288 The FIU conducted financial checks and established that Person A had used his personal bank account to make payments to Company Y for fuel supplies for the pump station. The FIU conducted further checks and established that Person A received significant cash and cheque deposits into his personal bank account. It was established that most of the cash and cheques were drawn on the business account belonging to Company X.

289 The FIU had previous intelligence holdings on the son of Person A, who was also reported for possible tax offences. The FIU conducted further checks and noted outstanding tax lodgements for Person A and his son.

290 A report was disseminated to the tax authority for alleged tax offences.

Possible Offence:

- Tax Evasion.

Indicators:

- Nil tax returns lodged with the tax authority.
- Depositing of business funds into personal account.
- Use of family member to evade taxes.
- Diversification of business operations to evade taxes.

Use of third parties to evade taxes

291 Company Y, was reported for depositing a significant amount of cash as a 'loan repayment' from an employee. The FIU had received a previous report on Company Y for similar activities.

292 The FIU established that Company Y had received deposits totalling approximately FJ$12 million from 2016 to 2018 and had not lodged tax returns for the same period. Further profiling revealed that the directors of Company Y were directors of other companies that were strongly suspected of tax evasion activities.

293 A case dissemination report was issued to the tax authority for investigation.

Possible Offence:

- Tax evasion.

Indicators:

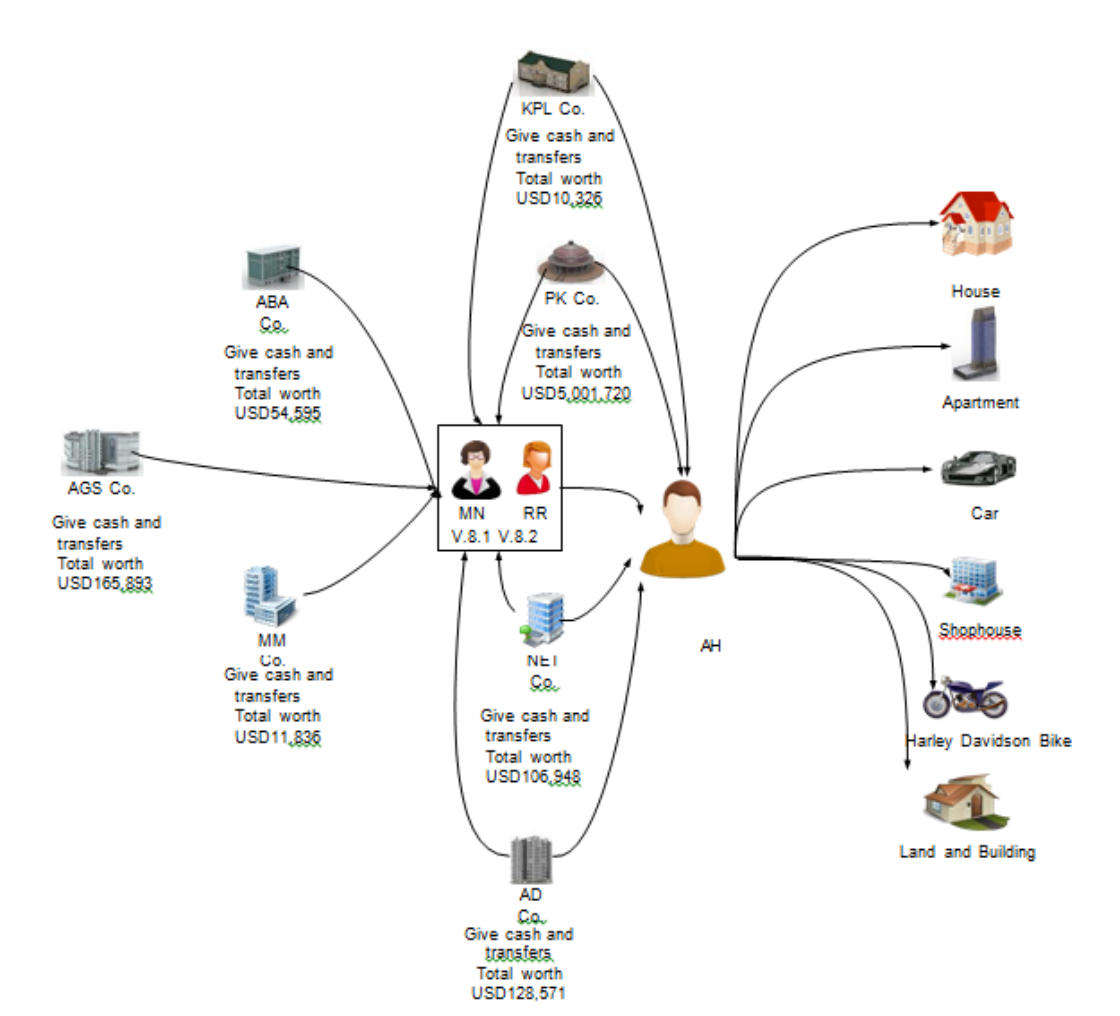
- Significant cash deposits.
- Use of third parties.
- Associated companies.

INDONESIA

294 AH is the CEO of LPS Co. He produced tax invoices based on false transactions and sold them to seven companies. He received profits totalling to ~USD3,510,621. Most of the money he received from the sale of false tax invoices were received in cash and the rest were received in his personal bank accounts. He also asked his employees to receive cash and deposit it to his personal bank accounts.

295 After funds were received in his personal bank accounts, AH purchased assets using his name and his family/relatives' names (for example, his wife and children). He purchased land and properties using cash amounting to ~USD71,428 in a day. He also built share houses or offices on the purchased land to obtain more money and invested in other companies. To further conceal the origin of the money, he combined the illicit funds with his company's funds.

296 Based on the information obtained from the Tax Authority, he stored the money in IDR but withdrew it in USD.



PAKISTAN

Background of the Case:

297 Accounts were opened by the suspect in different banks and in the name of his spouse, daughter and sons. Large volumes of funds relating to a textile business both in local and foreign currencies were routed to the family members' accounts in order to evade taxes.

Modus Operandi:

298 An individual, Mr. X, opened individual and partnership accounts in different branches of different banks. One of the several accounts was reported by a bank to the FMU because an unusual pattern of cash deposits into the account over a short period of time was identified.

299 The cash amounting to around PKR 62 M was deposited through 80 transactions out of which 77 transactions were structured. The accumulated funds were then withdrawn through four instruments on the same day in favour of an individual named "Z" for the purpose of purchasing a property. It was noted that all structured cash deposit transactions were conducted in a period of half an hour through numerous deposit slips. Moreover, the signatory of the deposit slips was also found to be the same person. Such activity in the account did not make any logical or economic sense. Furthermore, the

customer did not provide any details about the source of funds which were deposited by cash into the account and the customer did not provide documentary evidence to the bank in relation to the purchase of the property.

300 During the analysis, it was identified that the above proceeds were from the business of the suspect. Those proceeds had been routed through his spouse's proprietorship account by way of structured cash transactions to avoid reporting to FMU.

301 The suspect's family members' accounts were identified through a search of FMU's internal database and high turnovers were detected in those accounts. Interestingly, the suspect and his family members were found to be registered for National Tax Numbers. Only the suspect himself had paid income taxes while none of his family members paid income taxes, despite the fact that they were making high value transactions in their respective accounts.

302 From the activity described above, it was suspected that the reported individuals were involved in income tax evasion. Financial intelligence was therefore disseminated to the tax authorities.

4.10 Real Estate, including roles of real estate agents

CHINA

303 Suspect V is the legal representative, shareholder and supervisor of many investment and technology companies. One of these companies promoted a project, which required house owners to use their houses to guarantee loans from the bank. The company would pay a fixed income to the house owner, and also pay the loan interest and principle. The transaction counterparties also included investment companies, micro-loan companies and commercial companies. It was identified that, this project had the characteristics of illegal fund-raising and it would have high risks if the capital chain broke down. Information and intelligence form this case has been provided to the police.

PAKISTAN

304 The accused Mr. X obtained six properties in the UK worth GBP 6,885,625 during the period 2004-2006. These properties were then transferred the properties between companies controlled by accused persons at prices inflated to between five and 16 times the original price. On the basis of the inflated prices, the accused persons managed to obtain mortgage advances totalling GBP 49,276,250 through dishonest property valuations. During the period 2004 to 2006, 20 transactions were carried out transferring a fraudulently obtained amount of GBP 28,883,098 to Pakistani banks. Mr. X was sentenced to 13 years imprisonment by a UK court in 2011. Whereas the accused, Mr. Y, managed to flee to Pakistan. Mr Y, reportedly, brought in excess of GBP 25 million of stolen assets with him to Pakistan. UK authorities requested assistance to recover criminal assets held illegally by the accused persons in Pakistan. Having started an inquiry, the National Accountability Bureau (NAB) gathered relevant financial information from various agencies and financial institutions and consequently 12 residences and agricultural land had been cautioned under s 23 of Pakistan National Accountability Ordinance (notice by NAB to void transfer of property). The case is currently at the inquiry stage.

4.11 Association with human trafficking and people smuggling

AFGHANISTAN

305 Money Service Provider (MSP) X was acting as a guarantor by receiving money in instalments from Afghan citizens for their recruitment abroad. MSP X coordinated recruitments, with a foreign organisation (XYZ) irrespective of the regulations governing recruitment of workers abroad. The recruited Afghans deposited the instalments in MSP X's bank accounts, for which MSP X failed to

provide any supporting documents. The recruited Afghans were then were smuggled abroad via extremely high risk routes at the border provinces of Afghanistan.

306 As a result the company's license was suspended and the aforementioned case was sent to the concerned LEA for further legal proceedings.

FIJI

307 Ms GC and her twin sister, Ms. SR were separately operating travel agencies and placed advertisements in the newspaper requesting interested individuals to go to New Zealand for fruit picking and construction work. The advertisement attracted 17 individuals who were promised high wages, accommodation, food, transport and six days' work from 7 am to 5 pm. The 17 individuals were issued with New Zealand visitors visas and advised that work permits would be issued when they arrived in New Zealand. They were also required to pay consultation fees, lodgement fees, administration fees, release of passport and ticket fare totalling approximately FJ$3,768.00 per person.

308 The 17 individuals were required to only sign a blank visa application while Ms. GC and Ms. SR filled the application forms with false or misleading information.

309 Upon reaching New Zealand, the 17 individuals were mostly picked up from the airport by Mr. F A. The victims were then taken to their accommodation where they were required to share bedrooms with strangers of the opposite sex, sleep on mattresses or on the floor, and change clothing in the same room. The victims were also required to pay for transportation and food which was sometimes raw and unhygienic. The individuals were also paid very little.

310 Some of the victims were able to contact NZP and informed them of their conditions. Investigations were conducted simultaneously in New Zealand and Fiji.

NEW ZEALAND

Orchard worker charged with slavery and human trafficking

311 A Hawke's Bay orchard worker was recently charged with slavery and human trafficking for offences committed in Samoa and across the Hawke's Bay region. He is alleged to have lured Samoan nationals to New Zealand with the promise of well paid jobs, but when they arrived he confiscated their passports, controlled and closely monitored their movements, and subjected them to physical assaults and threats. He contracted the victims out to various orchards throughout Hawke's Bay, receiving payments to his personal bank accounts for labour contracting services rendered.

THE PHILIPPINES

312 The Philippine FIU received a referral from a Philippine law enforcement agency on three Filipino citizens and eight foreign nationals for alleged involvement in trafficking of persons and child pornography. Respondents were operating a cybersex den in Central Visayas and recruiting minors to engage in pornographic acts. In 2014, the Metropolitan Police in jurisdiction U seized and confiscated computers, tablets, cell phones, cameras, hard drives and DVDs containing indecent images and videos of Filipino children in the possession of foreign national, Mr. C. The videos show Filipino children being sexually/physically abused by Mr. C and adult Filipino females. Documents recovered also showed several money transfers to three Filipino citizens. Tracing of the money showed that it originated from jurisdiction U and jurisdiction C and transferred to the Philippines through two remittance agents and one local bank, averaging Php212 thousand per money transfer. The total detected amount was Php2.38 million involving various remittances and cash deposits and Php2.06 million of

withdrawals. The findings resulted in the issuance of a freezing order, petition for civil forfeiture and the filing of a ML case against the respondents in 2016.

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

CHINA

Case Study 1

313 Through investigation, the authorities found that Suspect U embezzled millions of yuan by taking advantage of his position. Suspect U then asked Suspect B to deposit the money in Suspect B's account. Under the arrangement of Suspect U's wife (Suspect O), Suspect D withdrew the money, and then transferred most of the money to Suspect P, who was Suspect O's brother in law. Then Suspect P transferred the money to Suspect O's son in the name of his hotel. Suspect O subsequently asked Suspect D to transfer the remaining amount to Suspect P's wife (which was controlled by Suspect O), and then Suspect O gave the bank card to her son.

314 In November 2018, Suspect O was convicted of ML and sentenced to two years imprisonment with two years' probation, and along with a penalty. Suspect P was convicted of same offences and was sentenced to ten months imprisonment with one year probation, along with a penalty.

Case Study 2

315 Suspect Q accepted bribes and was convicted of a bribery offense. During the investigation, Suspect Q and his wife asked their brother Suspect K to transfer millions of yuan and thousands of Hong Kong Dollars. Suspect K then gave some cash to Suspect T. In April 2018, the court sentenced Suspect K to two years and ten months imprisonment, along with a penalty. Suspect T was sentenced to three years and ten months imprisonment, along with a penalty.

Case Study 3

316 During an investigation of Suspect R's bribery, Suspect R's sister Suspect G was suspected of ML. During the period 2012 to 2016, although clearly aware if Suspect's R's activities, Suspect G continued to keep and deposit the proceeds of Suspects R's bribery in her bank accounts. Suspect G then purchased houses and vehicles in accordance with R's arrangements. In December 2018, Suspect G was sentenced to one year imprisonment with one year probation, along with a penalty.

CHINESE TAIPEI

317 In 2016, the share price of Company T, a listed company, was depressed for a period of time. Mr. C decided to manipulate the share price of Company T. Mr. C cooperated with stock market speculator Mr. D and used 42 securities accounts controlled by them to buy and sell large amounts of shares of Company T. They used these securities accounts to conduct corresponding transactions to create an impression of brisk trading on Company T's shares. They also released fake news which stated that foreign capital would be invested in Company T. So that the unwitting public investors mistakenly believed that Company T's stock was worth investing in and traded Company T's shares. The share price of Company T was manipulated from around NT$ 6 per share in August 2016 to around NT$20 per share in February 2017.

318 The board of directors of Company T were re-elected in May 2017. Mr. C falsely announced to the public that he would participate in the election and seek management rights to make unwitting public investors participate in the investment. However, Mr. C et al. successively sold Company T's shares, which they bought earlier at lower prices, to public investors in February or March 2018 (i.e.

when the share price of Company T was high and the trading was brisk) and gained a large profit. The total amount of the profit that they realized was about NT$ 1.1 billion. Mr. C et al. were indicted for violation of the Securities and Exchange Act in August 2018.

FIJI

Breach of Employer Trust and Manipulation of Internal Systems and Processes

319 Ms. Rosheen Praveena Raj and Ms. Rine Munivai Sorby were employed as finance officers at the Pacific Theological College (PTC). They were responsible for processing cheques for wages and bills. From 2006 to 2011, Ms. Rosheen Praveena Raj and Ms. Rine Munivai Sorby manipulated this system to fraudulently obtain proceeds totalling FJ$582,244.42. Ms. Rosheen Praveena Raj was responsible for all accounts payable including payroll. She tampered with the weekly payroll spreadsheet, payment vouchers, and cheques to process excess wage payments of FJ$96,576.86 and FJ$73,099.93 to herself and Ms. Rine Munivai Sorby respectively.

320 The fraud was detected when Mr. Nilesh Avinesh Sharma was appointed the Director of Finance and Administration in 2012. He discovered major anomalies in the financial records and conducted an internal investigation and audit to identify the causes of these anomalies. Ms. Rosheen Praveena Raj and Ms. Rine Munivai Sorby also tampered with bill payment cheques to make payments totalling FJ$412,567.61 to themselves. On 18 September 2018, Ms. Rosheen Praveena Raj and Ms. Rine Munivai Sorby were found guilty of two counts of ML each. On 19 September 2018, Ms. Rosheen Praveena Raj and Ms. Rine Munivai Sorby were sentenced to 11 and 10 years imprisonment, respectively.

Significant funds movement among unrelated individuals between jurisdictions

321 The FIU received an STR on Person Y for receiving remittances totalling approximately FJ$167,000.00 from an unrelated individual, Person X in Jurisdiction D.

322 Person Y claimed that the funds were for the construction of Person Y's property. Fiji FIU established that Person Y bought land in 2018 valued at $100,000.00. Person Y had not declared any income in the last two years and did not seem to be employed.

323 The FIU also discovered that Person X was potentially a person of interest to law enforcement authorities in Jurisdiction D and may have used Person Y to launder funds in Fiji.

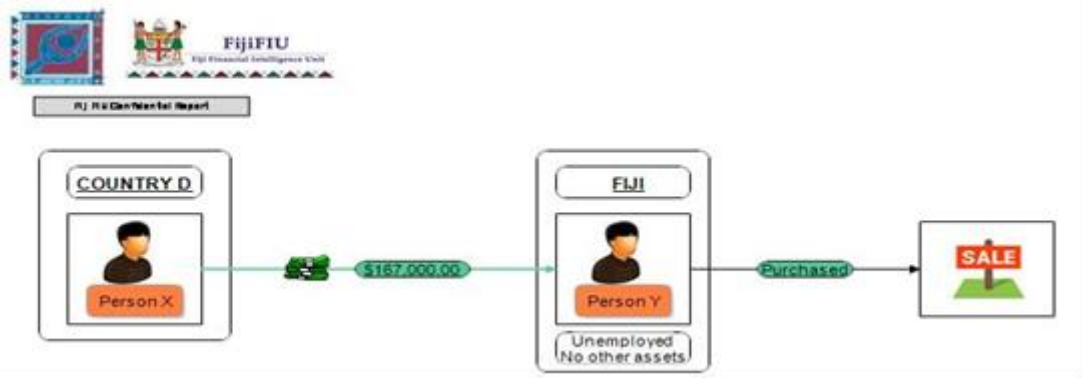
324 A report was disseminated to the Fiji Police Force Intelligence Bureau and the FIU in Jurisdiction D for further profiling.

Possible Offence:

- ML offences.
- Tax evasion.

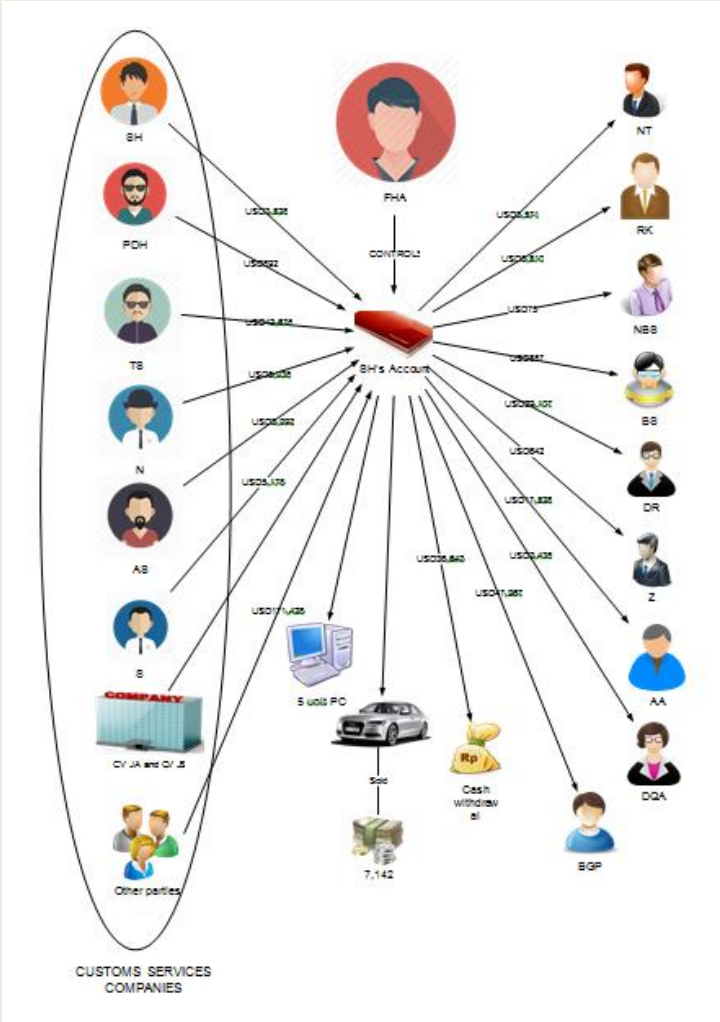
Indicators:

- Significant remittance of funds between local and overseas individuals without any apparent established relationship.



INDONESIA

325 FHA is an analyst at the Directorate General of Customs and Excise. He borrowed SH's account, owner of AMJ Co, to store money received from bribes from the Customs Services Companies he analysed. AMJ Co. was also one of the companies being analysed. Money from SH's accounts was laundered by transferring it to different accounts which were subsequently used to purchased assets, such as cars and computers.



JAPAN

326 A man working for a trading company concealed a stolen car in a warehouse in a container yard under a contract executed in the name of another person, knowing that the car had been stolen. He was arrested for concealment of stolen items and violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

327 The suspect knowingly received illegal proceeds derived from prostitution as protection racket remitted to the bank account opened under the name of a daughter of a member of Boryokudan (Japanese organized crime groups).

MACAO, CHINA

328 An STR revealed that Mr. A, who worked as a deputy manager of the accounts department in a shipping company in the Jurisdiction H, received numerous remittances totalling approximately six million from his bank account in Jurisdiction H between September and October 2015. Following this, Mr. A made purchases in jewellery stores in Macao, China with his own debit card and had funds transferred to his former girlfriend, Ms. B. Ms. B's bank account was reviewed and it was found that a large number of cash deposits were made using deposit machines and inward remittances were received from her boyfriend since 2015.

329 In March 2016, the shipping company found that Mr. A was suspected of embezzling around HKD380 million during the period 2010 to 2016. The shipping company reported this to LEAs in Jurisdiction H. After learning some illicit funds were transferred to Macao, China, the shipping company sent a representative to Macao, China to file a case with Macao's Judiciary Police. In January 2018, the news reported that Judiciary Police arrested Ms. B. Members of her family were also charged with ML through purchases of properties, cars and valuables. Assets valued at around HKD40 million, including cash, was seized.

330 To facilitate the case investigation, the FIU observed that Ms. B's bank account had irregular incoming funds and suddenly increased to over HKD21 million in 2015. The funds were then used for the purchase of properties and valuables for the purposes of reselling. Ms. B remitted back the sales proceeds to Mr. A. It was highly suspicious that Mr. A used his former girlfriend Ms. B and her family to place and layer proceeds of crime in Macao, China after Mr. A's misconduct was uncovered in the Jurisdiction H. The Judiciary Police finally passed the case to the Public Prosecutions Office.

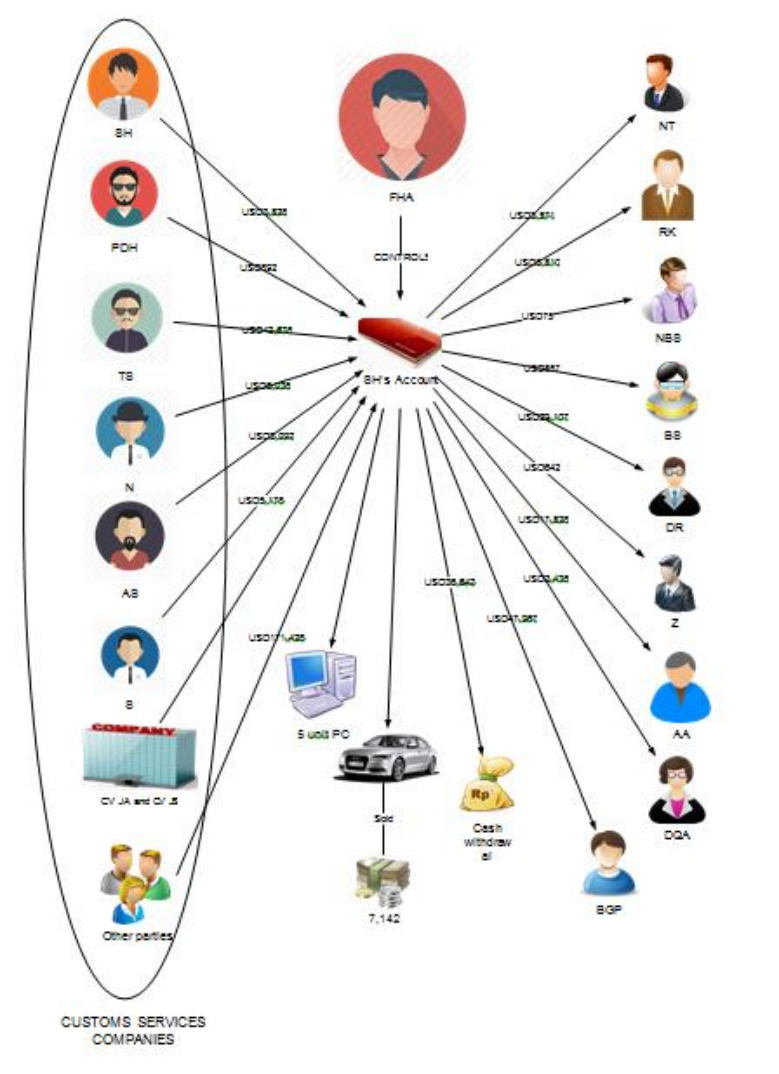
SINGAPORE

Use of Nominees – for incorporation of shell companies to receive bribe payments from overseas

331 Acting on leads received, CPIB established through analysis of financial intelligence that there is a network of Singapore companies that might be controlled by foreign persons for use to receive or launder significant funds from questionable sources from foreign jurisdictions. Two of the Singapore companies might have received funds linked to bribes made to foreign politically exposed persons.

332 An investigation was initiated into the two Singapore companies and the associated directors linked to the network of Singapore companies. Preliminary investigations revealed that the directors were nominees who offered their names for incorporation of companies and the opening of bank accounts for the companies, in return for fees. The nominees then rendered the beneficial owners full control of the corporate bank accounts. The Singapore companies were seemingly shell companies. Their registered addresses belong to a registered filing agent ("RFA"), which aided the incorporation of the companies. CPIB partnered with the regulator of the RFA for joint inspection of the RFA.

Requests were also made to foreign authorities for financial intelligence on various individuals and entities. Investigations are ongoing.



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

CHINA

Case Study 1

333 Four suspects opened bank accounts and transferred funds to many customers through online banking, and conducted testing transfers before each transaction. The funds went in and out of accounts quickly, the balance was very low and the IP addresses changed frequently in many places. Upstream counterparts included clients who were being investigated by authorities as suspects of online gambling participants. The amount of money linked to the case has reached millions of yuan and the intelligence has been provided to the police.

Case Study 2

334 Fourteen companies linked to this case opened accounts at the same time and at the same location. All the accounts shared the same identical characters and all the contact numbers were newly registered. Transactions notes/references included words such as "top up" and "similar 6-digit membership number". Transactions could be made at any time of the day, and some occurred around midnight and early hours of the day. IP addresses were concentrated on high risk regions for gambling. The amount of money connected to the case has reached millions of yuan and the information/intelligence has been provided to the police.

CHINESE TAIPEI

335 The 4th Investigation Corps of CIB raided betting websites. After tracking down the online betting website of "Beijing PK10" led by suspect Hsu on 5 September 2018, the 4th Corp tracked the source to find another suspect, Yao (behind-scene webmaster and bookie). After screening CCTV footage and tracking suspects by vehicles, the corps found that they lived in the same community. To prevent the suspects from moving to another area, the corps immediately applied for a search warrant in the District Court. As the second search of premises was conducted on 17 September 2018, the corps arrested another suspect named Peng in the parking garage. The suspects confessed to operating an online betting website. During a search of his residence, the corps found that Peng had used his own "cash-counting machine" to check the weekly betting amount. Counting the weekly betting amounted to approximately NT$10 million a week of each of its six exclusive agents, the betting amount of that website exceeded NT$1 billion over six months. The corps seized evidence including cash NT$1,982,000, two mobile phones, books, and the cash- counting machine. The case led to charges for gambling offences.

HONG KONG, CHINA

336 In September 2017, HKP's intelligence identified Mr. A to be a mastermind of a bookmaking syndicate engaging in an online casino, horse racing and football bookmaking activities in Hong Kong, China. Mr. A may also have expanded its operation to other nearby jurisdictions. A parallel financial investigation was commenced.

337 In June 2018, enforcement actions were taken resulting in the arrest of 45 persons for bookmaking related offences and five persons for both bookmaking and ML with HKD 2 million cash seized as well as HKD 1.68 million in the account withheld. The investigation is in progress.

JAPAN

338 Ex-members of Boryokudan (Japanese organized crime groups) knowingly received criminal proceeds in cash (JPY 950,000) derived from an illegal game gambling shop as protection racket. They were arrested for violation of the Act on Punishment of Organized Crimes (receipt of criminal proceeds).

KOREA, REPUBLIC OF

339 Person J and 64 other people are the operators and members of a ring that was engaged in the operation of illegal online gambling websites. Between about 2011 and September 2018, they launched and operated sports betting websites, such as "Cola", "Pasta" and "Y", in China, Thailand and some other places, and allegedly concealed the proceeds generated from operating those illegal gambling websites via transfers to accounts held in borrowed or fake names or via purchases of real estate properties by cash and transfers of ownership afterward.

340 On 24 May 2017, a preliminary investigation was initiated upon receipt of a report concerning alleged criminal activities. During the investigation, a total of 82 warrants and permissions were executed: 25 search and seizure warrants (against financial accounts), 27 search and seizure warrants (against residential premises, etc.), and 30 communications log access permissions. About 15,000 individual gamblers and KRW 109.2 billion of gambling money were uncovered and found to have been involved. The criminal proceeds identified (cash withdrawals) were in the amount of KRW 8.9 billion, and approximately KRW 13.1 billion of the criminal proceeds were preserved. Details are as below.

Details (Real estate, cash, etc.)		Amount Preserved
4 apartment units (112 m^2, 188 m^2, etc.)		KRW 5,475 million
Land (1,150 m^2), indoor golf simulator (rental deposit), 3 internet cafes		KRW 1,850 million
8 imported cars (Mercedes Benz, Audi, etc.), 3 Korea-made cars, 6 imported two-wheel vehicles		KRW 1,054.7 million
Cash 229 proceeds-hidden accounts		KRW 3,3458.6 million KRW 1,883.8 million
Indoor golf practice facilities (golf clubs, computers, etc.)		KRW 187 million
Total	KRW 13.1 billion (Seized: KRW 4,017.8 million; Preserved prior to prosecution: KRW 9,083 million)	

341 As shown above, the police identified KRW 109.2 billion of gambling money, and seized or confiscated the following: i) four apartment units, ii) real estate properties including land sites, iii) imported luxury cars and iv) accounts in which cash and criminal proceeds were hidden. Authorities recovered a total of KRW 13.1 billion of criminal proceeds and returned it to the National Treasury, while arresting 140 people (with 11 under detention) and sending them to the prosecutors' office for indictment.

NEW ZEALAND

OCGs laundering criminal proceeds through NZ casinos

342 During an 18 month period, at least six NZP organised criminal investigations involving suspected laundering of criminal proceeds through NZ casinos. The basic ML methodologies included using criminal proceeds to gamble, loading gaming machines with illicit cash before 'refunding' the funds as a casino cheque, and crediting illicit funds to casino accounts and transferring them to conventional bank accounts. Cash couriers working for suspected ML syndicates are also conducting cash 'drop offs' to casino patrons. It is suspected that a proportion of the cash being dropped off at the casinos has derived from domestic drug dealing. It is unknown whether the casino patrons receiving these funds are actively involved in the laundering scheme or unwitting end users of an informal value transfer system.

VIETNAM

343 In 2017, through prosecution and investigation of subjects using the internet to appropriate property, Vietnam Police prosecuted a case related to gambling and conducted investigations of a large number of subjects and a variety of participants including law enforcement agencies in many provinces and cities in Vietnam. In the case, the subjects established an IT enterprise and abused operation of an IT field to organize online gambling such as betting or card games. These subjects used many practices

to conduct criminal activities such as telecommunication cards, game cards to top up card games in to gambling games, connecting with payment portals of other companies, establishing agents to receive profits from gambling, etc.

344 This gambling network had a big scale to hide and rationalize illegal profits. The subjects used different practices such as investment into projects, capital contribution into business, real estate purchasing, making deposits, converting into gold, foreign currency and transferring to foreign jurisdictions. The investigators indicated that the total amount of money used for ML was about 38,000 USD.

345 In November 2018, the Supreme People's Court of Vietnam proceeded and convicted 92 persons of the crimes of; "Organizing gambling", "Gambling", "Money Laundering", "Illegal invoice acquiring", "Abusing positions and/or powers in enforcement", "Using internet, telecommunication, electronic devices to appropriate property." Of these four persons were convicted of "Money Laundering". Competent authorities recovered about 90% of proceeds from the persons who were convicted of ML.

THAILAND

346 Internet gambling was illegally organized. Bank accounts were used to receive money to buy playing credits and were regularly changed to avoid high volume triggers, resulting in accounts being frozen. The organizer used the proceeds to buy assets. In 2019, there are 28 cases with total assets seized or frozen over 20 million baht (USD 660,000).

4.14 Mingling (business investment) and investment fraud

MALAYSIA

Case Study 1: Illegal and Fraudulent Investment Scheme

347 Malaysian authorities disrupted the activities of syndicates suspected to have conducted illegal and fraudulent investment schemes. The joint investigation involved the Central Bank of Malaysia (BNM), Royal Malaysia Police (RMP), Inland Revenue Board (IRB), Companies Commission of Malaysia (CCM) and Malaysia Co-operative Societies Commission.

348 The groups have been luring the public domestically and internationally into their financial scheme by offering high returns over a short period of time.

349 The modus operandi of the illegal scheme involved the following:

- Public were lured to enter into a short term contract to purchase cryptocurrency produced by the syndicated groups, which were purported to be backed by gold.
- The schemes claimed that the gold was retained by the syndicated groups for trading purposes.
- The schemes also purported to offer high monthly returns as high as 15% per month.

350 The joint investigation by the authorities focused on violation of provisions related to illegal and fraudulent investment schemes. The investigations are still on-going. The syndicates were also investigated by the authority of neighbouring Jurisdiction A for the offence of illegal deposit taking due to their transnational involvement in Jurisdiction A.

351 Bank accounts amounting to more than USD4 million and other assets such as luxury cars were seized as part of the investigation process.

352 The ML methods used include:

- Purchase of valuable assets;
- Wire transfers / Use of foreign bank accounts;
- Use of virtual currencies; and
- Co-mingling of funds (business investment).

4.15 Use of shell companies/corporations

AUSTRALIA

Utilising a web of labour intensive companies

353 A person of interest (POI) was recorded as undertaking more than AUD15 million in cash withdrawals from 2015 to 2018 in connection with seven corporate entities operating in the cleaning, security and construction industries.

354 The POI's financial activity was characterised by a large volume of cash-based transactions into company and personal accounts, and displayed the following ML risk indicators:

- multiple bank accounts held by each corporation, simultaneously;
- a lack of company registration for goods and services tax (GST); and
- a lack of registration for pay as you go (PAYG) tax contributions for employees.

355 In addition, the POI possibly attempted to obfuscate the affairs of the companies: with a lack of transparent booking keeping practices (i.e. minimal records provided to the liquidators of failed companies); the establishment of new companies with similar names to the failed entity shortly after liquidation; back-dating office holder commencement dates and the possible use of dummy directors.

356 The activity suggested the POI was utilising these corporations to facilitate ML, engaging in illegal phoenixing activity and potential tax avoidance.

CHINA

357 Suspect D frequently transferred money to a number of companies and individuals. During a short period, the amount of money involved in unilateral transactions added up to millions of yuan. The money was rapidly and separately transferred in and out of accounts, most of the transactions were across provinces, and the amount of transferred money had some multiple relationships. Transactions always occurred at early hours and through online banking. IP addresses concentrated on high risk regions of drugs. All the financial counterparts were local banks, and most of them were registered in the middle of 2018, and some of the institutions have been revoked. The authorities suspected that under the cover a shell company, Suspect D and his associates transferred drug proceeds through poorly regulated financial institutions.

CHINESE TAIPEI

358 Company A, a ship-building corporation, won a tender for approximately NT$ 34.9 billion to construct six vessels in October 2014, with contracts signed in November 2014. However, Company A had a serious shortage of operational funds since its capital was only NT$ 530 million and it had purchased substantial investments in China. Mr. E, the president of Company A, considered that the significant funds shortage of Company A might not pass the credit investigations conducted by the banks that syndicated the loan. So Mr. E and other accomplices forged relevant documents to falsely

increase the capital of Company A from NT$ 530 million to NT$ 4 billion. The nine banks providing this syndicated loan, were trapped into approving credit lines with a total of NT$ 20.5 billion in February 2016.

359 In order to apply for bridge loans, appropriation, etc., Mr. E and his accomplices forged business documents, including purchase contracts, commercial invoices, payment requisitions, etc., to pretend that Company A purchased relevant equipment based on the necessity of building vessels from foreign shell companies AZ, OK, L3, HS, and QY, all of which had Mr. E's son as the registered chairman. In 2015, Mr. E and other accomplices fraudulently applied bridge loans five times with a total amount of about US$68 million. In 2016, Mr. E et al. fraudulently applied for revolving funds several times with a total amount of about US$134 million.

360 In order to avoid investigation, Mr. E transferred part of funds in foreign bank accounts of abovementioned foreign shell companies to natural or legal persons' accounts controlled by Mr. E in Chinese Taipei. The funds were then transferred into Company A's account. The rest of funds in foreign shell companies' accounts were used for investment or other purposes.

361 In February 2018, the Prosecutors Office indicted Mr. E and his accomplices for violation of the Company Act, Business Entity Accounting Act, Criminal Code, and the Money Laundering Control Act.

JAPAN

362 A suspect deceived a financial institution and had the financial institution deposit funds in a shell company's account in the name of a financing loan.

NEW ZEALAND

NZ shell company used in money laundering scheme involving Bulgaria, UK, The Marshall Islands and Belize

363 The NZFIU received information from a partner FIU regarding a NZ-registered company which had come to overseas law-enforcement attention due to suspected involvement in transnational ML. The NZ Company was the sole shareholder of a UK company whose bank accounts had received suspected criminal proceeds from a Bulgarian-based company. The NZ Company's directors and shareholders were a group of Russian nationals who were well-known to the NZFIU for incorporating NZ company structures that had subsequently been involved in ML schemes in overseas jurisdictions, principally in Eastern Europe. It is almost certain that the NZ Company was a shell company which formed part of a complex series of company structures designed to obscure beneficial ownership of assets and financial transactions in overseas jurisdictions.

NZ shell companies suspected to be operating as part of North Korean and Iranian arms trafficking network

364 Partner FIU reporting identified a NZ shell company facilitating overseas transactions on behalf of third parties based offshore. It alleged the NZ shell company was involved in a North Korean and Iranian arms trafficking network. The counterparties to the transactions were other shell companies based in tax haven jurisdictions. The NZ Company was incorporated by a small group of NZ-based Russian nationals operating a trust and company incorporation service primarily to high wealth clients based offshore. Many of the NZ companies set up by these individuals have subsequently come to the attention of overseas law enforcement agencies as part of transnational ML / tax evasion investigations.

THE PHILIPPINES

365 The A Commission (AC) requested assistance in obtaining documents for bank accounts used by certain individuals and entities currently facing proceedings in Jurisdiction A. The AC's request for assistance was made pursuant to a Multilateral Memorandum of Understanding Concerning Consultation and Cooperation and Exchange of Information (MMoU), to which the Philippines' Company Registry is a signatory.

366 Allegedly, the accounts stated in the request were used in facilitating the commission of unlawful activities, particularly those of carrying on a financial services business without holding the necessary financial services license, misleading or deceptive conduct and unconscionable conduct.

367 Through its investigation, AC uncovered a scheme whereby investors - which included local residents - were enticed to put money into binary options product offered. The investors were directed to deposit funds into a bank in Jurisdiction A under the name of AMPL. Within 48 hours, the money was transferred, through international fund transfers, to different jurisdictions around the world. In effect, AMPL was responsible for facilitating the remittance of the investments to various international entities. Estimates show that around USD2.8 Million had been deposited into AMPL's bank account during the first half of 2016, and that approximately USD2.1 Million of the funds were dispersed worldwide. AC understands that money had been transferred overseas to entities and bank accounts controlled by EAS, SS, CDS and YI.

368 AMLI appears to have been a recipient of remittances from AMPL. Thus, AC comprehends that AMLI may be related to, owned and operated by the same persons as AMPL. Hence it requested the bank documents of AMLI and other related individuals or entities for the period July 2014 up to present.

369 Examination of the bank documents of ST, AMLI and DTI revealed that they had transactions with individuals and entities which were mentioned by AC as having participated in the alleged unlawful activities. These transactions were characterized mostly by outward remittances from domestic bank accounts.

370 Equally important, there were remittances from Jurisdiction A to domestic banks which came from individuals who may have been victims of the fraudulent scheme. These shall be taken up in detail in the following discussion. The information shared by AC did not mention the foreign entity W Corporation. Investigations, however, yielded information that YI transferred substantial amounts to said corporation.

371 The Articles of Incorporation of AMLI show that ST, a national of Jurisdiction I, is one of the incorporators of AMLI. AMLI, according to AC, is among the entities which received funds from AMPL. Furthermore, internet searches revealed that ST is the Chief Operating Officer of TGL, another corporation which allegedly received funds from AMPL. Investigations revealed that ST was the beneficiary of numerous remittances from corporations – some of which are controlled by ST himself - and individual which, as stated by AC, are linked to AMPL.

372 ST was also the beneficiary of remittances from TGPL, one of the corporate defendants before the Court of Jurisdiction A. These remittances were discovered in the course of examination of their bank transactions with the local bank. IMC, which is likewise one of the corporate defendants before the Federal Court of Jurisdiction A, was observed to have made remittances in favour of ST in his local bank account.

373 It must be recalled that ES was allegedly one of the recipients of the funds from AMPL's WB Corporation account, and one of the individual defendants against whom AC filed cases. It was determined that ES made two remittances in favour of ST in the latter's local bank account.

374 ST is also the president of ALALI. ALALI was issued a Certificate of Incorporation on 18 December 2014. Its principal place of business is at XX, Condominium, M City. The authorized capital stock is unusually low at USD190.00, which is divided in into five shares with a par value of USD38.00 per share. This amount is patently insufficient to support its purpose or any business carried on in a corporate capacity for that matter.

375 The Certificate of Incorporation was issued to AMLI on 30 September 2014. Its principal place of business is located at XX Condominium, M City. It should be emphasized that; this is the same principal office address of ALALI as stated in its Articles of Incorporation. The authorized capital stock, similar to AMLI, is abnormally minimal at USD190.00, which is divided in into five shares with a par value of USD38.00 per share. Notwithstanding the minimal authorized capital stock, AMLI maintains numerous bank accounts under its name.

376 It should also be emphasized that; according to AC, customers from Jurisdiction A were required to deposit funds to certain local bank accounts in the Philippines. Examination of the statement of account revealed six remittances, all substantial in amount, originating from Jurisdiction A and which were credited to said local bank accounts. Noticeably, all this transpired in June 2015.

377 Investigations further revealed that AMLI was transacting with several persons and entities identified by AC as carrying on an unlicensed financial services business in Jurisdiction A and against whom court orders were obtained. AMLI made nine outward remittances in favour AMPL. In addition to the foregoing suspicious activity, it was also discovered in the course of investigation that there were international remittances between AMLI and TGL.

378 IMC, with an address in Jurisdiction A, is one of the entities against whom AC obtained court orders which prohibited it from carrying on unlicensed financial services business in Jurisdiction A. Another local bank account of AMLI was discovered to have made a remittance, with IMC as the beneficiary.

379 US is one of the entities which was prohibited, by the Federal Court of Jurisdiction A, from carrying on unlicensed financial services business. Examination of AMLI's local bank account showed a fund transfer to US purportedly for administrative fees.

380 The Certificate of Incorporation was issued by the Philippine Company Registry to DTI on 29 July 2011. It is interesting to note that ST presented a Certificate of Employment in opening a local bank account, which provides that DTI is one of the subsidiary companies of IMC. Investigations of the accounts of DTI with local banks showed that it had received international remittances from IMC.

381 YI is one of the defendants in the proceeding that ASIC instituted before the Federal Court of Jurisdiction A. According to ASIC, the money that was deposited to AMPL's bank account had been transferred overseas to entities and bank accounts controlled by YI, among others. Investigations revealed that YI made four remittances in favour of a local bank, the amounts of which are all significant.

382 After a thorough examination of the bank documents and connected transactions of the aforementioned persons, their interconnectedness and participation in the evident ML scheme has been comprehensively established. Individuals from Jurisdiction A were observed to have made significant remittances to AMLI's local bank account. AMLI's bank transactions, in turn, showed remittances to AMPL, TGL, IMC, US and ST.

383 ST, who is the incorporator of AMLI and ALALI, was the beneficiary of several remittances from AMLI, TGL, IMC and ES. IMC and YI, on the other hand, made international remittances to DTI and W Corporation, respectively.

384 Investigations further revealed that AMLI and ALALI have the hallmarks of a shell corporation. The two companies have remarkable similarities which are evident when juxtaposed. For example:

	AMLI	**ALAL**
Date of Incorporation	30 September 2014	18 December 2014
Primary purpose	To develop software applications for our clients; to support their business process including systems integration, provided, (h)owever that (it) shall not engage as internet service provider.	To (d)evelop (s)oftware (a)pplications for our clients, to support their business process including systems integration provided, however that (it) shall not engage as internet service provider
Principal place of business	XX Condominium, M City	XX Condominium, M City
Incorporators	1. ADR 2. AH 3. AP 4. ST 5. DWR	1. ADR 2. AH 3. AP 4. ST 5. GC
Authorized capital stock	One Hundred Ninety USD (USD190.00), which is divided in into five (5) shares with a par value of Thirty Eight USD (USD38.00) per share	One Hundred Ninety USD (USD190.00), which is divided in into five (5) shares with a par value of Thirty Eight USD (USD38.00) per share

385 The fact that these companies are obviously engaged in highly questionable undertakings becomes all the more apparent when their financial transactions are examined. Despite having unusually low capital, these corporations have transacted in substantial amounts. Significantly, almost all were remittances.

386 While it is true that the request of ASIC mentioned only documents pertaining to local bank accounts, it is probably unaware of the extent in which Philippine financial institutions were utilized in the ML scheme. There is, therefore, a necessity to share the information acquired in the course of the instant investigation and the relevant documents. This is in keeping with our declared policy, as enshrined in Sec. 2 of Republic Act (R.A.) No. 9160, otherwise known as the Anti-Money Laundering Act of 2001, as amended, which is to extend cooperation in transnational investigations and prosecutions of persons involved in ML activities wherever committed.

387 Furthermore, in view of the fact that the Philippine's legal persons have been exploited in the apparent criminal activity, the same emphasizes the need to share the results of the present investigation to the Company Registry pursuant to its Memorandum of Agreement with the FIU.

4.16 Currency exchanges/cash conversion

CHINA

Case Study 1

388 Suspect E was the actual controller of four associated accounts owned by him and three individuals. Cash in Australian dollars, Canadian dollars, US dollars and other foreign currency were deposited in those accounts. Suspect E then exchanged the money for HK dollars through online banking, and withdrew cash at multiple branches. The amount of each withdrawal was less than five thousand HK dollars so as to avoid detection. Suspect E was suspected of illegal foreign exchange trading. The amount of money involved in this case was millions of HK dollars. Suspect E was arrested in July 2018.

Case Study 2

389 In January 2018, the authorities found that bank accounts of Suspect F and G were involved in foreign exchange trading. A number of unusual transactions occurred between September 2011 and December 2017 and millions of yuan was transferred over the counter and through ATMs. This was inconsistent with information available which showed that Suspects F and G were unemployed.

390 During an investigation, the authorities found that a large amount of money was transferred in and out of Suspect F's and Suspect G's accounts, regardless of the exchange rate loss. Foreign currency was frequently deposited and then withdrawn in cash in HK dollars. The amount of deposits was less than five thousand dollars per day to avoid detection. Suspects F and G were suspected of illegal foreign exchange trading. Suspect F was arrested in December 2018.

FIJI

Undeclared Currency Exchange

391 The FIU received an STR from a foreign exchange dealer in relation to Person M, a naturalized Fijian citizen who is a frequent traveller to Jurisdiction Z. Person M conducted three foreign exchange transactions totalling approximately FJ$30,000.00 on behalf of Person X and Person Y.

392 The Fiji FIU conducted financial profiling and established that the FJ$30,000.00 was not sourced from Person M, X and Y's bank accounts. It was suspected that the individuals were keeping cash at home and laundering funds out of the jurisdiction. A case dissemination report was provided to the FRCS for their profiling and investigations.

Possible offence:

- Non-declaration of BCR.
- ML.
- Possible tax related offence/tax evasion.

Indicators:

- BCR form not filled by individual.
- Individual exchanged funds under the name of other persons, especially minors.

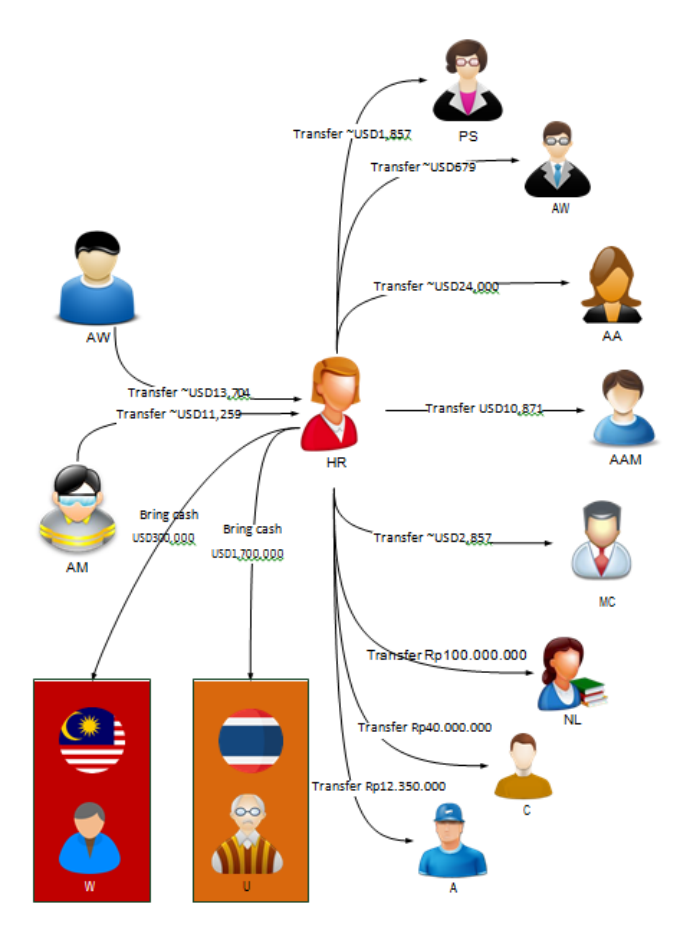
HONG KONG, CHINA

393 A sales manager of a company in the gift trading business falsely represented to his employer that he had received 50 sales orders from customers located in various jurisdictions. The sales manager applied to his employer for advance payments of RMB 2.77 million (over HK$ 3.4 million) payable to two suppliers in China. Believing that the applications were genuine, his employer remitted RMB 2.77 million into the designated accounts of the two suppliers in China, held by two representatives of a licensed money service operator (MSO) in Hong Kong, China. Between 23 November 2012 and 26 November 2014, the representatives of the MSO arranged for the transfer of the corresponding sum HK$ 3.1 million and HK$ 310,000 from their bank accounts to the sales manager's bank accounts in Hong Kong, China.

394 On February 2018, the sales manager was convicted of two counts of dealing with property known or believed to represent proceeds of an indictable offence and was sentenced to four years imprisonment.

INDONESIA

395 HR is the wife of KM a k a PR. HR was working in a money remittance service owned by PR. HR's account was used to store money from the sale of narcotics. HR also took the money abroad to be exchanged into other currencies. The money given to HR in cash or transferred was converted to USD and was taken in Thailand and Malaysia. HR took with her USD250,000 to USD350,000 on each trip, totalling approximately USD2,000,000.



4.17 Currency Smuggling

AFGHANISTAN

Case Study 1

396 Mr X's bag was subjected to a thorough search conducted in the presence of government officials from relevant departments at an international airport of the jurisdiction. The search showed that the suspect had hidden more than 1.7 million Indian Rupees inside baby diapers which he was carrying in his hand bag. Since the suspect could not provide any documentation for the discovered cash, he was arrested.

Case Study 2

397 Upon their arrest for currency smuggling, which was discovered in their handbag at an international airport, Mr X and Mr Y claimed that they were to be assisted by certain officials at the airport in transferring the cash abroad. Based on this claim made by the suspects, further investigations were carried and it was discovered that the subjects had lobbied airport officials to assist them in smuggling a certain amount of USD and KSA Riyals out of the jurisdiction. Ultimately, four airport officials were arrested along with the suspects.

Case Study 3

398 Person A arriving from Jurisdiction A passed the security screenings in the airport, however suspicions were raised shortly after the suspect exited the airport terminal. As per the suspicion by border police the person's luggage was subjected to a physical search, upon which it was discovered that the person had packed certain amounts of USD and KSA Riyals in cosmetic materials. The security screenings at the terminal, including X–ray scans failed to detect foreign currencies packed as cosmetics. The case was referred to law enforcement agencies for further investigations.

Case Study 4

399 Border police at an international airport suspected persons X and Y, when Mr. X's luggage was suspected at a baggage screening checkpoint at an airline counter. Based on this suspicion, Mr X's luggage were subjected to a physical search upon which it was discovered that gold bars weighing more than 11 kilograms were contained in the luggage.

400 Mr X claimed to have brought these gold bars into the airport inside his shoes and then placed them in his luggage after passing the X-ray scans. However, the CCTV footage shows that Mr X and Mr Y entered a washroom at the same time, each carrying a bag. Upon exiting the washroom, Mr X was shown in the footage carrying two bags, while Mr Y exited the washroom empty handed. Moreover, the footage also showed Mr. Y leaving the terminal as soon as Mr X submits the luggage at the airline counter. In this case, the gold bars were brought into the airport by Mr Y, possibly with the assistance of airport officials.

401 After a thorough investigation of the case by competent authorities Mr X was fined 4.9 million AFNs (equivalent to 72,558 USD) in accordance with prevailing laws and regulations.

BRUNEI DARUSSALAM

Case Study 1

402 In February 2018, three foreigners were found travelling through the Brunei International Airport with various currencies above the declaration threshold without making a declaration. The currencies involved included Malaysian Ringgit, Vietnamese Dong, Thai Baht and Singapore Dollars. The cash was concealed in their luggage. The activity was detected through a routine inspection and X-ray scanning by customs officers. It was later found that the individuals intended to transport the funds across the land border to the neighbouring jurisdiction. The individuals were prosecuted and then fined for offences under Section 37(2) of the Criminal Asset Recovery Order, 2012 (failure to declare) which carries a penalty of BND 5,000 or five months imprisonment per person.

Case Study 2

403 In March 2018, a foreigner was found travelling across the land border to Brunei with Brunei Dollars and Singapore Dollars above the declaration threshold without making a declaration. The cash was concealed in a backpack on the front passenger seat of the car. The activity was detected through a random stop and search at the control post by customs officers. The individual was prosecuted and then fined for offences against Section 37(2) of the Criminal Asset Recovery Order, 2012 (failure to declare) which carries a penalty of BND 5,000 or five months imprisonment.

JAPAN

404 Four Korean suspects imported six gold ingots (total six kilograms worth JPY 27,500,000) from Incheon International Airport in Korea to Fukuoka Airport in Japan on 13 April 2017. The suspects also attempted to take cash (JPY 735,220,000) abroad without declaration or license. Fukuoka District Court sentenced them to two years and six months in prison, suspended for four years.

NEW ZEALAND

Chinese males attempting to smuggle approx. $65K cash from South Pacific jurisdiction to NZ

405 Two Chinese males were stopped at a South Pacific island's international airport attempting to smuggle approximately $65K cash into New Zealand. The funds were comprised of approximately $50K USD and $15K NZD and were concealed on their persons. The two individuals travel regularly between NZ and China, and one of them regularly frequents NZ casinos where he has lost more than $20K since 2015. It is suspected that these individuals were attempting to repatriate the proceeds of drug imports back to NZ and China.

PAKISTAN

406 Information was received that an organized gang involved in foreign currency smuggling would attempt to smuggle foreign currency from Islamabad International Airport on an international flight. An operation was conducted which led to the recovery of various foreign currencies totalling PKR 38.69 million (approx. USD 276.168). Two accused persons, namely Mr. AK and Mr. GD, were also arrested on the spot. One of the accused persons namely Mr. AK had already boarded the aircraft with the foreign currency, ready to take off, at the time of his arrest.

SINGAPORE

Currency Smuggling – Cash Courier imprisoned 36 months for smuggling millions into Singapore

407 Person A worked as a courier for a money-changing operation in a neighbouring jurisdiction. Between 2013 and 2014, on 100 occasions, he brought into Singapore physical currencies amounting to S$12 million without providing full and accurate cross-border cash movement reports. Person A wilfully provided false declarations claiming that he was unaware of the actual sources and recipients of the physical cash. This was the highest amount of cash brought into Singapore illegally.

408 In February 2018, Person A was convicted and sentenced to 36 months imprisonment.

THAILAND

409 In 2019, a Laos national carried undeclared Thai currency across the border. This act is customs evasion for ML purposes, which is a predicate offense. The assets of approximately 100 million baht (USD 3,300,000) were traced, seized and frozen.

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

FIJI

Cheque Washing

410 The FIU received an STR from a local bank in relation to a suspected high level fraud attempt on a publicly listed entity, Company E. The FIU established that Person F altered/washed 14 cheques that were issued by Company E to pay Person F.

411 The local bank's verification process identified that the payees on the cheques were altered and had not cashed the cheques.

412 The FIU further established that Person F was related to one of the high ranking officials of Company E.

413 A case dissemination report was provided to the FPF, Cybercrime Unit for their investigations. The matter is now before the Suva Magistrates Court.

Possible offence:

- Obtaining financial advantage through deception.
- Fraud.

Indicators:

- Stains or discolorations on the cheque possibly caused by erasures or alterations.

JAPAN

Case Study 1

414 A second-hand dealer, who also managed illegal loans, planned to make illicit profits by deceiving a credit card company, by using its customer's credit card. The dealer provided the credit

card company with fictional sales data, detailing sales paid for by a credit card that never occurred. The credit card company then deposited funds into an account opened in the name of another person but actually controlled by the dealer.

Case Study 2

415 A person concerned to Boryokudan (Japanese organized crime groups) received a credit card, which his acquaintance obtained illegally and for free. He used the card to withdraw cash and paid for living expenses and amusements expenses.

MACAO, CHINA

416 According to a bank's card acquiring business, it was noticed that Client A used 11 cards issued outside Macao, China to conduct a large amount of transactions in three jewellery shops since January 2018. A total of over MOP1.8 million was transacted in three months. It raised the bank's suspicion that Client A withdrew cash from the card to purchase valuables in these jewellery shops.

417 Shortly after the above transactions, intelligence revealed that Client A was involved in fraud and was subsequently arrested by the Judiciary Police. After an in-depth investigation, it was suspected that Client A had colluded with the staff of the jewellery shops to make the above card transactions and launder illicit proceeds derived from scams in other jurisdictions. Some of the illicit funds were transferred to Macao, China through debit card transactions in order to conceal the source of the funds. The case was also submitted to the Public Prosecutions Office for further investigation.

4.19 Structuring (smurfing)

AUSTRALIA

Cross-border bulk cash smuggling

418 The Australian Border Force (ABF) Border Related Financial Crimes Unit (BRFCU) observed aspects of structuring within various ML methodologies. In particular, the identification of structured bulk cash smuggling as a significant border risk in the aviation traveller/crew stream.

419 Aircrew transiting through onshore airports have been used to carry amounts of currency just below the AUD10,000 reporting threshold. This activity is coordinated by a controller, who will utilise their networks to provide the funds prior to the venture and will consolidate them on arrival.

420 This typology has been observed to be linked to capital flights from markets that are deemed to be more volatile than those of the destination jurisdiction as well as financing of narcotics supply.

CHINA

Case Study 1

421 Telecommunication fraud led by an offshore gang led to a loss in the millions of yuan. With the support of the FIU, the police carried out an investigation, and collected evidence from more than 20 cities. A number of suspects, including foreigners were arrested and related bank cards were frozen. The offshore gang laundered illicit funds through structuring. In just a few days, funds from two bank accounts were transferred to several first-level accounts, hundreds of secondary accounts and fifth-level accounts and thousands of third-level and forth-level accounts through online banking. All the funds were transferred and withdrawn overseas.

Case Study 2

422 A and B lived as a couple. A knowingly assisted B to transfer illegal proceeds in the following ways:

- Used personal accounts. A opened two bank accounts to transfer illegal proceeds and both accounts remained at a low balance.
- Purchased property and vehicles.
- ML using cash.
- ML by investment.

423 In September 2018, the court convicted A of ML and sentenced A to ten months of imprisonment, along with a penalty.

MALAYSIA

424 The case study involves a PEP (Suspect B) who is also a high-ranking government official who misused his position as the Chairman of a NPO, namely ABC Foundation. Suspect B's wife's credit card spending on luxury items were paid by ABC Foundation. The payments for personal expenditures by the NPO strongly indicate the subject had committed the offence of criminal breach of trust.

425 ABC Foundation maintains a current account at a local bank, with Suspect B as the sole signatory.

426 The account detected frequent cash deposits from various locations below the value of CTR requirements, possibly to avoid CDD and reporting requirements. In addition, multiple large cheques deposited into the account from various entities without reasonable justification were also observed. The cheque amounts ranged between RM16,000 to RM1,000,000.

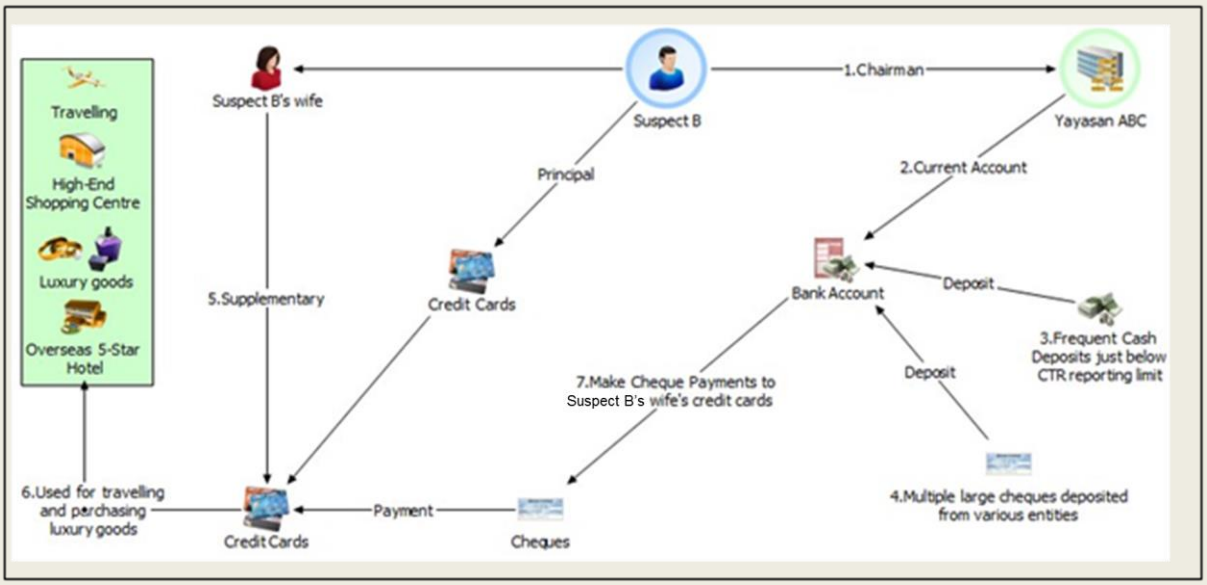
427 At the same time, Suspect B's wife holds multiple supplementary credit card facilities under the combined limit with the principal card holder. The cards were actively used for travelling, purchasing luxury goods and staying at expensive hotels overseas.

428 The cards were paid through a third party cheque issued by ABC Foundation. Multiple large cheque payments were made and the cheque signatory is Suspect B who is also the Chairman of ABC Foundation.

429 Suspect B has been charged for multiple counts of criminal breach of trust, ML and abuse of power. The court case is currently ongoing.

The ML methods used include:

- Purchase of valuable assets;
- Use of bank accounts/ credit cards/ cheque;
- Use of cash; and
- Involvement of NPO.



NEW ZEALAND

Drug importation network using structuring/smurfing and third party bank accounts

430 A drug importation network engaged in structuring and use of third party bank accounts to fund their importation activity. Third parties deposited $27.5K in cash to an individual's bank account during a two week period – in amounts of between $9K and $9.5K cash at a time. The deposits were made at different branches in the Auckland area. These funds were then transferred to another third party bank account where they were consolidated with $60K worth of electronic credits which had been made by a number of additional third-party accounts before being forwarded as a lump sum to another third party bank account under the guise of a loan payment.

4.20 Wire transfers/use of foreign bank accounts

FIJI

Law Firm Victim of a Business Email Compromise Scam

431 The FIU received an STR in relation to a bank account held at Bank Z in Jurisdiction A which was used to fraudulently obtain funds from a local law firm.

432 The law firm was engaged to facilitate the sale of a property on behalf of four individuals. The email address of one of the individuals, Person V was compromised and a fraudulent email was sent to the local law firm advising them that the funds should be sent to the bank account held at Bank Z. The local law firm sent approximately FJ$845,000.00 to the bank account held at Bank Z in two separate transactions in October 2018.

433 The local law firm did not realize they were victims of a "business email compromise scam" until Person V followed up on the payment. The financial institution in Fiji that sent the funds attempted to recall the funds but was unsuccessful.

434 It is believed that the account signatory of the bank account held at Bank Z in Jurisdiction X may be involved in computer related offences and a party to a business email compromise scam.

435 The FIU liaised with its overseas counterparts to recover the funds. The case is still under investigation.

Possible Offence:

- Business Email Compromise/Email Account Compromise.

Indicators:

- Sudden change in account details for remittance payment.
- The use full names instead of nicknames and a language structure may not match how the supposed sender normally communicates.

PAKISTAN

436 An STR was submitted in relation to suspect XYZ from ABC Exchange Company based on adverse media that; the suspect was allegedly involved in child abuse via making and selling videos online. Suspect XYZ was arrested by the Federal Investigation Agency. The police of a foreign jurisdiction arrested a man allegedly linked to child abuse activities. During the investigation, the accused revealed that the Pakistan citizen, Suspect XYZ, was also involved in the illegal activity. This information was shared with Pakistani authorities by the foreign jurisdiction's embassy and based on this information Suspect XYZ was arrested by the LEA.

437 Suspect XYZ received remittances of small amounts from six jurisdictions from different individuals. It was suspected that Suspect XYZ received illicit proceeds from selling videos. The accused also confessed that he received small amounts for selling one video.

438 The FMU shared financial intelligence with LEAs. The suspect was found guilty and sentenced for seven years and fined Rs. 1.2m by a special court for cybercrime.

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

NEW ZEALAND

Suspected TBML barter scheme involving export of vehicle parts as payment for importation of methamphetamine

439 A New Zealand-based vehicle parts exporter came to the attention of NZPFIU for suspected involvement in a trade-based ML barter-trade scheme involving the shipment of stolen vehicle parts offshore as payment for the importation of methamphetamine from West Africa. The individual has been linked to an international drug importation syndicate spanning NZ, Australia and West Africa, and is suspected of using his NZ-based vehicle wrecking business to facilitate payments (in the form of vehicle parts as well as actual cash telegraphic transfers) to West Africa in exchange for shipments of methamphetamine into NZ via the mail stream.

4.22 Use of false identification and documents

AFGHANISTAN

Case Study 1

440 A targeted MSP used forged identification documents to obtain a license, in order to avoid identification and skip responsibilities in the future. Through discovering the misconduct of the MSP the relevant authorities were not able to locate the true identification of the subject.

441 As a result the FIU revoked the license and notified the licensing body to verify the identification document before issuance of license.

Case Study 2

442 Verification of a bidding application submitted by Engineering Company X to the National Procurement Authority showed that the company's bank statement were forged. Verifications showed that the actual closing balance of the company's bank statement was 155,486 AFN. However, the company forged its bank statement showing a closing balance of 2 million AFN. This was done to fulfil the bidding requirement. As a result, the company was blacklisted from participation in National Procurement Authority's bidding process.

JAPAN

443 A senior male Boryokudan member illegally obtained cell phones, etc. from a distributor of cell phones, etc., and sold them using identification documents of other persons. He then transferred the illicit proceeds to bank accounts opened in the names of other persons and controlled by him. He was arrested for violation of the Act on Punishment of Organized Crimes (concealment of criminal proceeds).

4.23 Gems and precious metals

AUSTRALIA

Trade-Based Money Laundering – Precious metals market

444 Due to its anonymity and intrinsic value, the precious metals market has been identified as an attractive alternative to the financial system for ML. The ABF Border Related Financial Crimes Unit (BRFCU) recently worked with the USA Homeland Security Investigations (US HSI) to undertake a joint trade transparency initiative utilising analytic software "Data Analysis for Research and Trade Transparency System" (DARTTS).

445 This work enabled the analysis of imports and exports to identify trade data discrepancies. The results identified Australian entities suspected of employing trade-based money laundering (TBML) methodologies using gold bullion and false invoicing as a vehicle to move illicit funds offshore under the guise of wholesale bullion trading. Investigative efforts including cargo examinations and purity testing are ongoing.

446 The ABF BRFCU conducted a discovery project into the risk presented by gold and gold products. Here it was observed that the trade in precious metals and gems was being increasingly adopted by entities looking to conceal the transfer of value.

447 This project found that precious metals and diamonds, in particular, were routinely being used to transfer the proceeds of crime and to layer and manipulate the true source, destination and purpose of financial transactions. Border interdiction activity aimed at identifying the undeclared or illicit trade of gold revealed a large number of import and exports dealing with this commodity and significant revenue leakage issues due to false-invoicing, smuggling and other illicit trade activity.

CHINA

Case Study 1

448 The Customs and Police in City N set up a joint team and investigated 14 cases of precious metals smuggling. The team has dismantled five criminal gangs. Members of these gangs repeatedly

smuggled gold by concealing it inside human bodies. Several kilograms of gold were seized, and 22 suspects were arrested. The case is under further investigation.

Case Study 2

449 In November 2018, Customs and its subsidiary in City M have investigated a case about precious metals smuggling. A criminal gang has smuggled hundreds of kilograms of precious metals by hiding golds inside human bodies over 40 times. Five suspects were arrested and the case is under further investigation.

Case Study 3

450 In July 2018, Customs in City L found dozens of gold bars in the tool box of a private car. The suspect was arrested, and the case is under further investigation.

NEW ZEALAND

Prolific fraudster purchasing gold / precious metals

451 A prolific fraudster was using stolen cheques to make a range of purchases of high value goods around New Zealand, including more than $100K worth of gold and jewellery. He deposited the stolen cheques to retailers' bank accounts and ordered goods from the retailer's before banks identified the cheques as invalid. He used this *modus operandi* to 'purchase' more than $100K worth of gold and jewellery which he had shipped to his and his associates' addresses. When police conducted a search warrant they were unable to locate any of the gold/jewellery – it is suspected the offender forwarded the gold/jewellery to local organised crime groups as repayment for drug debts.

4.24 Purchase of valuable assets (art works, antiquities, racehorses, etc.)

AUSTRALIA

Purchases of artwork by organised criminal entities

452 The ABF Border Related Financial Crimes Unit (BRFCU) identified a number of instances where the purchase of valuable goods had been used to facilitate illicit transfers.

453 In 2018, the ABF identified an Australian-national with significant connections to onshore-organised crime entities travelling to arrange purchase of an artwork by a well-known artist.

454 During intervention, the person of interest was in possession of a number of documents, including a sales agreement and valuation request. It is possible that the sale and purchasing of high value goods is being used as a mechanism for legitimising the flow of significant value. It is also possible that these documents may have been fabricated for this purpose.

CHINA

Case Study 1

455 Suspect A was an employee of a logistics company. His account received frequent cash deposits from a high risk region. The funds were then transferred to a number of personal accounts. Suspect A also purchased low-value used cars in multiple cities. Suspect A was suspected of TF, and the abnormal transactions could not be explained by Suspect A's occupation. The value of funds related to the case has reached millions of yuan. This information has been reported to the relevant authority.

Case Study 2

456 Suspect B manufactured and sold drugs several times during 2010 and 2011, and the whereabouts of the proceeds was not clear. His mistress, Suspect C and Suspect C's parents had a large amount of money going in and out of their accounts. The police filed a case against Suspect C and her parents on suspicion of ML. According to the evidence, the court affirmed that Suspect C had no source of income, and that the money used for the purchase of financial products, a house and car as well as cash were from Suspect B's drug proceeds. In September 2018, Suspect C was convicted of ML and was sentenced to five years imprisonment, along with a penalty.

FIJI

457 Mr. Z, a businessman in Fiji entered into a business venture with Mr. Y, an overseas investor. As part of the business venture Mr. Z was instructed by Mr. Y to find a property suitable for investing in as a supermarket. Mr. Z suggested Property B and sent a sale and purchase agreement for FJ$5.5 million (US$2.75 million). Mr. Y remitted approximately FJ$5.3 million (US$2.7 million) to two separate bank accounts for the purchase of the property. After a while Mr. Y became suspicious of Mr. Z and asked his wife, Mrs. X to visit Fiji and investigate the purchase of the property. Mrs. X discovered that the original sale and purchase agreement stated that Property B was purchased for FJ$3.3 million (US$1.65 million). When Mr. Y queried this discrepancy with Mr. Z he insisted that the property was sold for FJ$5.5 million (US$2.75 million) but the sale and purchase agreement was for FJ$3.3 million (US$1.65 million) to evade taxes.

458 It was established that Mr. Z inflated the price of Property B to fraudulently obtain FJ$1.2 million (US$0.6 million) from Mr. Y. The funds were then used to make a part payment on two vehicles, two houses and establish a fixed term deposit. Mr. Z has been charged and is awaiting trial. The properties have also been restrained.

4.25 Investment in capital markets, use of brokers

AUSTRALIA

Off-market transfers of securities on small exchange markets

459 An off-market transfer (OMT) is the transfer of ownership of securities (including interests in managed investment schemes) bilaterally between parties outside of an exchange market.

460 In 2018, the Australian Securities and Investments Commission (ASIC) commenced surveillance of the ML/TF risks associated with OMTs on small exchanges.

461 Through this work, ASIC identified that 'Australian Company A' had disproportionate trading activity compared to other securities on the exchange.

462 'Company A' operated in the retail sector with several offshore markets, and the controlling shareholder of this company had transferred over AUD1 million to an Australian casino.

463 ASIC notes that small exchanges could be vulnerable to ML through OMTs, which may be considered a potentially attractive vehicle for the transfer of wealth for criminal enterprises. Risk factors include the fact that they can operate outside the Australian banking industry and are predominately affected by unregulated share registries with no mandatory reporting requirement for the off-market transfer of ownership or due diligence obligations.

JAPAN

464 A suspect deposited criminal proceeds derived from fraud in a security account opened under a false name and converted the money into stocks.

4.26 Cases developed directly from suspicious or threshold transaction reports

AFGHANISTAN

465 Based on STRs received by the FIU from reporting entities a suspicion was formed on activities of certain trading companies. These STRs received from reporting entities were prioritized based on risk matrix classification. The STRs from trading Company A and trading Company B were subjected to financial analysis.

466 The FIU began financial analysis of these companies and disseminated financial intelligence data to LEAs.

467 During 2018, FinTRACA disseminated (47) proactive and reactive cases to domestic law enforcement agencies for investigation or further action to be taken.

AUSTRALIA

468 Operation Astatine focused on a NSW-based criminal syndicate involved in drug trafficking and tobacco smuggling. The syndicate was involved in importing 50 million cigarettes and conspiring to import 200 kilograms of methylenedioxymethamphetamine (MDMA) via sea cargo.

469 The Australian Commission for Law Enforcement Integrity and NSW Joint Organised Crime Group (JOCG)—conducted a parallel investigation into a Department of Immigration and Border Protection (now Department of Home Affairs) officer, who was charged for allegedly using his position to assist the syndicate.

470 In August 2017 the NSW JOCG executed 13 search warrants across NSW entities connected to the syndicate. Approximately 80 kilograms of cocaine and a total of AUD740,000 cash were seized across four properties. During the course of the investigation, the JOCG seized a further AUD2 million. The JOCG arrested nine people including eight in Sydney. The alleged head of the syndicate was arrested in Dubai and extradited to NSW in relation to drug importation offences.

471 AUSTRAC provided onsite intelligence support throughout the investigation. Financial intelligence identified key links between previously unknown domestic and overseas entities, and uncovered frequent significant cash deposits conducted by various syndicate members.

CHINA

Case Study 1

472 Financial institutions found that more than 100 customers opened accounts over a short period of time. Each account purchased about 50 thousand US dollars through online banking and then transferred those funds to individual accounts in other places. The total amount has reached millions of dollars. The controller of these accounts was suspected of illegal operation underground banking.

473 Triggered by the STRs, the authority analysed more than a million large transactions and ten layers of parties involved. The authority classified the modes of transaction, personnel characteristics and crime types and discovered hundreds of parties involved.

474 In July 2018, the law enforcement authorities successfully arrested 26 suspects involved in this case, destroyed six large underground banking gangs and 21 dens and seized criminal tools such as computers and frozen bank cards.

Case Study 2

475 In October 2018, financial institutions reported to the authority that the legal representative of Company A applied for transfer 80 million yuan. The authority provided related information to the police immediately. After investigation, the authority found that the transactions of Company A had following characteristics:

a) Company A had investment platform and private fundraising platform.
b) The financial manager of Company A was also the legal representatives of four related companies. He had 27 joint bank accounts and clients came from all over the jurisdiction.
c) Settlement with personal accounts to evade supervision or tax.
d) The counterparties were mainly young and middle-aged people who were familiar with the Internet, and they were mostly friends or acquaintances.
e) The features of the small amount regular rebate transaction were obvious.

476 Later, the police filed the case, and froze hundreds of millions of yuan and six suspects have been arrested.

CHINESE TAIPEI

477 In July 2015, the Anti-Money Laundering Division (AMLD) learned from the financial intelligence filed by a bank that Mr. S's account had recently received several large cash deposits. The financial activities were inconsistent with the financial background and transaction history of Mr. S. The AMLD decided to conduct further analysis. After analysing relevant documents provided by financial institutions, the AMLD considered that these transactions might involve illegal activities.

478 In November 2015, the AMLD disseminated this case to the MJIB. The MJIB launched an investigation and found the following fact: Mr. T and Mr. W were the predecessor and successor chairman of the Company T, a listed company in Chinese Taipei. Mr. L was the director of the Company T. In May 2015, Mr. T et al. set up a foreign paper Company F and assigned unwitting Mr. S as the chairperson and used Company F to buy accounts receivable of Company T and equity of subsidiaries of Company T. However, the process of appraisal and conclusion of agreements were not handled in accordance with normal procedures and the related documents were not reviewed or approved by the board meetings. In July, Company T revealed material information that stated that Company F bought the aforementioned assets of Company T with a total amount of about NT$ 204 million and that Company F would pay by instalment plan. After paying several instalments, Company F was unable to continue to pay for some reason. Mr. T et al. didn't actively request Company F to perform the contract. It caused Company T to receive a loss of approximately NT$33.3 million.

479 After finalizing the investigation conducted by the MJIB, the case which involved a violation of the Securities and Exchange Act was referred to the Prosecutors Office in April 2018 for prosecution.

FIJI

480 In 2018, the Fiji FIU issued 321 CDRs to the Fiji Police Force, Fiji Revenue & Customs Authority, foreign FIUs and other relevant law enforcement agencies. CDRs are developed from analysis of STRs. The major recipient of Fiji FIU's CDRs is the Fiji Revenue & Customs Service (FRCS) for alleged violations under the Income Tax Act and VAT Act. In 2018, 207 such reports were

issued to FRCS, 62 CDRs were issued to the Fiji Police Force, including the AML & Proceeds of Crime Unit, Transnational Crime Unit and Police Intelligence Bureau.

481 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).

482 The Fiji FIU database can also be accessed by key partner agencies through a Direct Data Access (DDA) arrangement.

MALAYSIA

Terrorism Financing Case

483 As part of the regional CFT initiative, the FIU participated in the regional analyst exchange programme to analyse suspicious transactions involving the ISIL-linked Maute armed group based in the Southern Philippines. The programme was held between May and August 2018 involving analysts from the Australian Transaction Reports and Analysis Centre (AUSTRAC), Pusat Pelaporan dan Analisis Tansaksi Keuangan (PPATK), BNM and the Anti-Money Laundering Council (AMLC). The exchange program produced a comprehensive financial intelligence report on the Maute group based on the transactions involving the concerned jurisdictions. The report has been disseminated to the respective law enforcement agencies in all jurisdictions for further enforcement action.

Fraud – Business Email Compromise

484 The FIU received an alert from the LEA of Jurisdiction Y that a sum of USD1.5 million (MYR5.8 million) had been fraudulently transferred via five transactions from Victim A in Jurisdiction Y to a bank account belonging to Subject X in Malaysia between January and March 2018. Victim A received a letter purportedly written by its trading partner, Subject Y instructing its staff to transfer money to Subject X in Malaysia. From January to March 2018, imposters using fake email addresses misled staff from Victim A into initiating five transactions totalling USD1.5 million to Subject X's bank account at Bank C in Malaysia.

485 Arising from the alert by the LEA of Jurisdiction Y, the FIU immediately contacted Bank C to block the account from performing any withdrawals. However at that point of time, it was noted that Subject X had partially withdrawn the funds via cash cheques and funds were transferred to three local counterparties leaving the account with a balance of approximately RM3.15 million.

486 Preliminary analysis of the case revealed the following findings:

- Subject X's name is almost similar to the name of Victim A's trading partner;
- Subject X and the local counterparties were newly established around the same time in late 2017 and early 2018. Upon registration of the businesses, the entities immediately opened bank accounts to facilitate the receipt and movement of the fraudulent funds;
- Most of the funds received from Victim A were withdrawn immediately within the same day or next working day via cash cheques, ATM withdrawals and online fund transfers to counterparties, which are common patterns noted in scam cases; and
- It was observed from Subject X and the counterparties' accounts that all funds were eventually withdrawn via cash making it difficult to trace the ultimate beneficiary.

487 The case was forwarded to the relevant law enforcement authorities and resulted in Subject X's account being frozen and the subjects being investigated.

NEW ZEALAND

Case Study 1

488 The NZFIU received an SAR regarding a member of a NZ OCG depositing extremely large amounts of cash at a NZ casino. An NZFIU analyst conducted a financial profile and identified assets and funds far in excess of what would be expected given his profile. The NZFIU released a report to the local NZP Criminal Investigation Branch which initiated an investigation into his activities. The individual was subsequently arrested for involvement in methamphetamine manufacture and supply, and approximately $770K worth of assets was restrained under NZ's Criminal Proceeds legislation.

Case Study 2

489 NZFIU received an SAR regarding an unknown individual who was paying extremely high household electricity bills using large amounts of cash. NZFIU conducted inquiries with the electricity company to identify the holder of the account into which the funds were being paid. NZFIU released a report to the NZP District in which the individual resided, which included an assessment that the individual was likely operating an indoor cannabis growing operation. The NZP District commenced an investigation into the individual and established that he was indeed running an indoor cannabis growing operation from his house; he was arrested and charged with cannabis-related offending.

Case Study 3

490 NZFIU received an SAR regarding an electronic goods importer/exporter with suspicious financial activity occurring in its NZ accounts, including unexplained cash deposits, credit card overpayments, and transactions to/from high risk jurisdictions. The NZFIU conducted inquiries with partner agencies and assessed that the company was possibly involved in a form of trade-based ML. The NZFIU released an intelligence report detailing the case and released it to a specialist investigative unit, which initiated a formal criminal investigation into the company's activities.

SINGAPORE

Recovery of S$2.9 million in a case of criminal breach of trust developed from suspicious transaction reports

491 The STRO received several STRs on Person A, who was an accountant of a Singapore-registered company, Company B. STRO's analysis revealed that there were multiple cheque deposits from offshore companies going into Person A's personal accounts in Singapore. This is unusual as the offshore companies were under the care of Company B and Person A did not have an ownership interest in these companies. It was noted that the funds were subsequently withdrawn via cash and cheques and not transferred to other corporate entities.

492 The STRO disseminated the information from the STRs and the results of its analysis to the relevant law enforcement agency in Singapore. Investigations revealed that Person A had misappropriated the equivalent of S$46.2 million from Company B and its offshore companies by preparing false payment vouchers and making use of blank cheques signed by the authorised signatories. The proceeds of crime were primarily used to fund Person A's gambling activities. An amount of S$2.9 million was recovered from Person A by the relevant law enforcement agency.

493 Person A was sentenced to 18 years' imprisonment for offences including criminal breach of trust and ML.

5. EFFECTS OF AML/CFT COUNTER-MEASURES

494 This section of the report provides a brief overview of recent results from legislative, regulatory or law enforcement counter-measures.

5.1 The impact of legislative or regulatory developments in detecting and / or preventing particular methods

AFGHANISTAN

495 FinTRACA has established a Watch-List which is accessible to reporting entities for their consideration while dealing with customers. The designations have been very useful to alert reporting entities of evolving threats.

AUSTRALIA

AUSTRAC Regulation of Digital Currency Exchanges

496 New laws for digital currency exchange (DCE) providers operating in Australia were implemented by AUSTRAC, Australia's financial intelligence agency and anti-money laundering and counter-terrorism financing (AML/CTF) regulator in 2018.

497 The new AML/CTF laws covered the regulation of service providers of cryptocurrencies, including bitcoin, the agency's compliance and intelligence capabilities to help DCEs implement systems and controls to minimise the risk of criminals using DCEs for money laundering, terrorism financing and cybercrime.

498 DCEs with a business operation located in Australia are now required to register with AUSTRAC and meet the Government's AML/CTF compliance and reporting obligations, allowing them to protect their business operations from money laundering and terrorism financing, whilst helping to strengthen public and consumer confidence in the sector.

499 The changes also increased opportunities to facilitate the sharing of financial intelligence and information relating to the use of digital currencies, such as bitcoin and other cryptocurrencies, with industry and government partners. This has provided Australia with immediate benefits in the fight against serious crime and terrorism financing.

CHINA

500 According to the requirements of the *Notice on Regulating Overseas Large Amount Cash Withdrawal Transactions by Bank Cards of the State Administration of Foreign Exchange*, as of 2018, a person's overseas bank card cash withdrawal should not exceed the equivalent of 100 thousand yuan per year. After the implementation of this policy, the withdrawal of large amounts of cash abroad has been effectively curbed. The maximum amount for an overseas cash withdrawal, for a single person, has been reduced from one million to 20 or 30 thousand yuan. In 2018, the cumulative amount of overseas cash withdrawal for domestic bank cards has been reduced by 44% compared with 2017.

CHINESE TAIPEI

501 In accordance with the scope of the financial leasing enterprise designated on March 5, 2018, the Financial Supervisory Commission (FSC) promulgated the "Regulations Governing Anti-Money Laundering of Financial Leasing Enterprises" on 20 June, 2018. On 9 November, the FSC promulgated

the regulations governing internal audit and the internal control system of anti-money laundering and countering terrorism financing of financial leasing enterprise, banking business, securities and futures business, and insurance companies. The FSC also promulgated amendments to "Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Certified Public Accountants" on the same day.

502 In order to strengthen AML/CFT mechanisms of Chinese Taipei, the FSC promulgated amendments to the "Regulations Governing Anti-Money Laundering of Financial Institutions" and "Regulations Governing Reporting on the Properties or Property Interests and Locations of Designated Sanctioned Individuals or Entities by Financial Institutions" on 14 November, 2018.

503 The FSC will continue to supervise the financial industries to comply with AML-related regulations and implement AML/CFT work, and continue to review the related regulations so as to conform to international norms.

504 On November 7, 2018, Chinese Taipei passed the Amendments to the Money Laundering Control Act (MLCA) and Counter-Terrorism Financing Act (CTF Act). The Amendments to MLCA mainly includes enterprises handling virtual currency platforms or transactions in the AML/CFT regime. Besides, based on the newly released Amendments, Financial institutions and the designated nonfinancial businesses or professions (DNFBPs) should establish the AML/CTF internal control and audit system based on its ML/TF risk as well as the business scale. Amendments to CTF Act specifies that the scope of TFS applies to assets wholly or jointly owned or controlled, directly or indirectly, or to funds or other assets of persons and entities acting on behalf of or at the direction of designated persons and entities.

FIJI

505 Fiji is currently reviewing its Public Order Act to further strengthen its legal provisions on TFS for TF (R.6) and proliferation financing (R.7). The review of these provisions commenced in February 2018. The review is currently in the consultations phase. Comments on the draft provisions have been sought from APG and CTED.

506 The Reserve Bank of Fiji (RBF) enhanced the AML/CFT onsite inspections of remittance service providers and moneychangers and has revised its AML Supervision Policy over this sector.

507 The Fiji FIU enhanced its AML/CFT onsite inspections of the DNFBP sector. In 2018, the FIU conducted the onsite AML/CFT inspections of five real estate businesses and eight law firms.

508 Review of the Companies Act and Regulations is currently underway, which is intended to address the key legal gaps on transparency of beneficial owners of legal entities.

INDONESIA

509 BAPPEBTI (Futures Trading Oversight Commission) issued four regulations on Crypto Assets and Digital Gold. Indonesia, through the Central Bank (BI), bans the use of all Virtual Currencies in payments and payment systems. However, for investment and/or trading purposes, Virtual Currencies/Crypto Assets are still allowed. The regulations require the Crypto Assets and Digital Gold Traders in the Futures Trading Market to comply with AML-CFT regulations.

MALAYSIA

Reduction of Cash Transaction Reporting ("CTR" for the purposes of the follow paragraphs) threshold

510 Effective 1 January 2019, BNM, as the competent authority under the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001 (AMLA) reduced the cash transaction reporting threshold from RM50,000 (approx.USD12,000) to RM25,000 (approx. USD6,000).

511 The decision was derived from the findings of the 2017 NRA, where corruption poses the second highest net crime risk to the jurisdiction. Based on case studies and STR analysis, the amount of proceeds from corruption placed with financial institutions and non-bank financial institutions varies but is usually below the cash threshold limit imposed. This has made it increasingly difficult for enforcement agencies to detect laundering of corruption proceeds unless an STR is raised. Additionally, the previous threshold of RM50,000 was disproportionately high relative to other jurisdictions, and did not accurately reflect the size and prevalence of cash usage in the Malaysian economy.

512 Reducing the threshold would make it difficult for criminals to continue to launder the proceeds through reporting institutions. The extensive use of cash by criminals to store, move and disburse illegal proceeds underscores the importance of CTRs as a preventive measure against ML and TF risks. By lowering the threshold, such behaviour can be more easily detected through enhanced monitoring and better visibility on suspicious transaction patterns.

NEW ZEALAND

513 Prescribed Transaction Reporting (PTR) regime is enhancing the quality of NZFIU assistance to domestic and international partners.

514 Under the updated AML/CFT legislation, reporting entities are now required to report large cash transactions (LCT) of $10,000 and above, and international funds transfers (IFT) of $1,000 and above to the NZFIU. The below examples illustrate the increased benefits PTR reporting is having on NZFIU's ability to build the intelligence picture across the entire financial system in support of serious and organised crime investigations:

- A NZP specialist investigative unit submitted a request for NZFIU holdings on a number of individuals suspected of arranging importations of methamphetamine into the jurisdiction. These individuals were not previously known to NZP and had not engaged in any suspicious transactions. In the following weeks the NZFIU received PTRs on the suspects detailing cash deposits to third parties' bank accounts. The NZFIU released a report which assisted with developing leads for the investigation team and inquiries are ongoing. As there was no elements of suspicion to these transactions on the part of reporting entities, these transactions would have remained unreported under the old regime.

- A partner FIU based in jurisdiction A submitted a request to NZFIU regarding suspected proceeds of crime being deposited to a NZ-based MR's (i.e. money remitter's) bank account held in jurisdiction A. The partner FIU requested details of the movement of funds once they entered the remitter's bank account in jurisdiction A and who the beneficiaries of the transaction were. Based solely on PTR information, NZFIU was able to trace the suspected criminal proceeds to an account in jurisdiction B and identify who the beneficiary of the transaction was. NZFIU released a report to the partner FIU to assist with its inquiries.

SINGAPORE

Enhanced access to information on Beneficial Ownership

515 Under the new beneficial ownership regime, foreign companies are also required to capture information on their beneficial owners through the mandatory requirement of making available the registers of controllers to the Registrar. With the amendments to Section 386A of the Companies Act in 2017, the registers of controllers must be made available to the Registrar and public agencies administering or enforcing any written law (including CAD, CPIB and IRAS) upon request. In effect, these changes enhance the access to basic information held by domestic authorities where it can be obtained from financial institutions and from corporate service providers (CSPs) and other DNFBPs (e.g. lawyers and accountants).

516 With the above development, law enforcement agencies can have access to beneficial ownership information from the registered filing agents. And, for this reason, CPIB has partnered with ACRA for joint inspection of the CSPs for a more holistic approach towards combating ML offences.

6. ABBREVIATIONS AND ACRONYMS

ABF – Australian Border Force
AFP – Australian Federal Police
AML – Anti-Money Laundering
AMLA – Anti-Money Laundering Act
AMLC – Anti- Money Laundering Council
AMLD – Anti-Money Laundering Division
ANF – Anti Narcotics Force (Pakistan)
APG – Asia/Pacific Group on Money Laundering
ATM – Automatic Teller Machine
AUSTRAC – Australian Transaction Reports and Analysis Centre
BCR – Border Currency Report
C&ED – Customs and Excise Department (Hong Kong, China)
CDD – Customer Due Diligence
CDR – Cash Dissemination Report
CFT – Countering the Financing of Terrorism
CIB – Criminal Investigation Bureau
CIPB – Corrupt Practices Investigation Bureau
CTR – Cash/ Currency Transaction Report
DGCE – Directorate General of Customs and Excise (Indonesia)
DNFBP – Designated Non-Financial Businesses and Professions
EAG – Eurasian Group
ECOFEL – The Egmont Centre of FIU Excellence and Leadership
EFT – Electronic Funds Transfer
ESW – Egmont Secured Web
FATF – Financial Action Task Force
FINTRAC – Financial Transactions Reports Analysis Centre (Canada)
FIU – Financial Intelligence Unit
FMU – Financial Monitoring Unit (Pakistan)
FRCS – Fiji Revenue & Customs Service
FSRB – FATF-Style Regional Bodies
GIF – Financial Intelligence Office (Macao, China)
HT – Human Trafficking
IDR – Indonesian Rupiah
ICRG – International Cooperation Review Group
IFTI – International Funds Transaction Instruction
INTERPOL –International Criminal Police Organisation
JAFIC – Japan Financial Intelligence Center
KYC – Know Your Customer
LEA – Law Enforcement Agency
MIT – Mujahidin Indonesia Timur
MJIB – Ministry of Justice Investigation Bureau
MG – Maute Group (Philippines)
ML – Money Laundering
MR – Money Remitter
MSP – Money Service Provider
NAB – National Accountability Bureau (Pakistan)

NCC - National Coordination Committee to Counter Money Laundering (Malaysia)
NGO – Non-Government Organisation
NNB – National Anti-Narcotics Board (Indonesia)
NPO – Non-Profit Organisations
NRA – National Risk Assessment
NZP – New Zealand Police
NZFIU – New Zealand Financial Intelligent Unit
OCG – Organised Crime Groups
PPATK – Pusat Pelaporan dan Analisis Transaksi Keuangan (Indonesia)
PS – People Smuggling
PEP – Politically Exposed Person
PKR – Pakistan Rupee
PML – Professional Money Launderers
POI – Person of Interest
PTR – Prescribed Transaction Reporting
RI – Reporting Institutions
RMP – Royal Malaysia Police
SAR – Suspicious Activity Report
SEA CTFWG - South East Asia Counter-Terrorism Financing Working Group
SEC – Securities and Exchange Commission (Philippines)
STR – Suspicious Transactions Report
SVF – Stored Value Facilities
TF – Terrorist Financing
TRACFIN – Traitement du renseignement et action contre les circuits financiers clandestins (France FIU)
TTP – Taliban Movement of Pakistan
VAT – Value Added Tax
VC – Virtual Currency