APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2020

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

(Adopted out-of-session)

September 2020

Applications for permission to reproduce all or part of this publication should be made to:

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

© September 2020/All rights reserved

DISCLAIMER:

Under Article 1 of the APG Terms of Reference 2012, the APG is a non-political, technical body, whose members are committed to the effective implementation and enforcement of the internationally accepted standards against money laundering, financing of terrorism and proliferation financing set by the Financial Action Task Force. This document, any expression herein, and/or any map included herein, are without prejudice to the status of, or sovereignty over, any territory, to the delimitation of international frontiers and boundaries and to the name of any territory, city or area.

CONTENTS

INTRODUCTION

1 The APG is the FATF-style regional body for the Asia/Pacific. One of the mandates of the APG is research and publish regional ML and TF typologies reports to assist governments and other stakeholders to better understand the nature of existing and emerging ML and TF threats and pursue effective strategies to address those threats. 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. 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.

2 The APG Operations Committee has oversight of the typologies research programme and is Co-Chaired by Samoa and New Zealand (2020).

3 The publication of yearly reports is a requirement of the APG's Strategic Plan and the Operations Committee Terms of Reference. The reports are intended to assist APG members to identify suspicious financial activity. Case studies and indicators of ML and TF 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 those crimes. APG typologies research and report publication is undertaken in coordination with the Financial Action Task Force (FATF) and other partners in the global AML/CFT network and includes regional and global priority areas.

4 Each year APG members and observers provide case studies, observations on trends, research, information on regulatory enforcement action and international cooperation. The information collected provides a basis for further study on particular and high priority topics. The information also supports other experts and stakeholders.

5 The case studies featured in this report are 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.

6 This report includes a brief section on the preliminary analysis of the impact of the COVID-19 pandemic (2020) on ML/TF in the Asia/Pacific region.

1. COVID-19 IMPACT ON ML/TF TYPOLOGIES

On 11 March 2020, the 2019 novel coronavirus (COVID-19) was declared a global pandemic by the World Health Organisation.[1] The COVID-19 pandemic has forced governments to introduce a range of unprecedented measures to help control the spread of COVID-19 such as banning international travel, business closures and requiring passengers arriving from international jurisdictions to self-isolate or quarantine. There has been a severe disruption to normal business activity that in many APG jurisdictions has required governments to provide substantial and rapid fiscal stimulus and support to companies and workers. While it may be too early to understand the full impact that COVID-19 will have, the APG Yearly Typologies Report offers an opportunity to canvas the ways in which this pandemic has changed the ML/TF landscape.

Criminal groups have already sought to exploit the COVID-19 pandemic and adjust their ML/TF typologies in response to border closures, social distancing requirements, greater reliance on digital communications / payment channels and the increased criminal opportunities arising from the misappropriation of government financial support payments. There are also opportunities for terrorist organisations to spread extremist views across a large proportion of the population increasing their use of online technologies and to exploit distrust and fear in the community to draw individuals into supporting their organisations.[2]

COVID-19, however, may provide a unique opportunity for law enforcement and financial intelligence units (FIUs) to detect and disrupt certain ML operations, including serious organised crime groups having to stock-pile cash due to an inability to launder through regular methods because of the closure of casinos or other gambling venues as one example.

In addition, as profits of retail and hospitality industries for instance are negatively impacted, the co-mingling of funds may be an impractical layering technique. Due to a disparity with similar businesses in the industry, it may be possible to identify entities who continue to co-mingle illicit funds through businesses

1.1 Work by FATF and Global Network

The FATF secretariat has taken a proactive role in keeping its members and the global network informed regarding challenges, good practices and policy responses to threats and vulnerabilities arising from the COVID-19 pandemic. In a statement issued by the FATF President on 1 April 2020[3], the President highlighted the importance of continuing to implement the FATF standards to ensure the integrity and security of the global payment system during and after the COVID-19 pandemic through appropriate and transparent channels. Similar statements have also been issued by FATF-style regional bodies (FSRBs) and FIUs.[4]

[1] https://www.who.int/news-room/detail/27-04-2020-who-timeline---covid-19
[2] See the UN CTED report, 'The impact of the COVID-19 pandemic on terrorism, counter-terrorism and countering violent extremism' https://www.un.org/sc/ctc/wp-content/uploads/2020/06/CTED-Paper%E2%80%93-The-impact-of-the-COVID-19-pandemic-on-counter-terrorism-and-countering-violent-extremism.pdf
[3] http://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html
[4] For example, see statement by GAFILAT on COVID-19 and its associated ML and TF risks dated 8 April 2020

The FATF issued an information note, *COVID-19 related ML/TF risks and potential policy responses*[5], on 3 April 2020 in response to the impact of the COVID-19 pandemic on global AML/CFT efforts which focused on:

- New threats and vulnerabilities arising from COVID-19 related crime and impacts on ML and terrorist financing TF risks.
- The current impact COVID-19 has on the AML/CFT efforts by government and the private sector.
- Suggested AML/CFT policy responses to support the implementation of measures in response to COVID-19 while managing new risks and vulnerabilities that have been identified.

1.2 Pandemics and ML/TF

Pandemics, economic recessions and natural disasters have long impacted criminal activity and the methods by which money is laundered and terrorist activities financed. Lessons may be learned from the Spanish Flu of 1918-1920, the tsunami in Indonesia in 2004,[6] H1N1 (also known as the swine flu) of 2009-2010, and the exploitation of non-profit organisations (NPOs) during natural disasters, humanitarian crises, or pandemics.[7]

During these times of national and international disasters, there is often an outpouring of humanitarian aid offered by governments and charity organisations. Alongside this aid and charity lies the risks of corruption, misappropriation of funds by serious and organised crime groups, and diversion of funds to terrorist entities.

1.3 Experiences of APG members

The majority of illicit activity associated with COVID-19 relates to proceeds generating offences such as financial fraud and exploitation scams with criminals attempting to profit from the pandemic through fundraising for fraudulent charities. FATF members have reported an increase in fundraising scams with criminals posing as international organisations or charities and requesting donations via email to raise money for COVID-19 related campaigns.

APG members have reported that serious and organised crime groups have targeted new government pandemic response programs. This includes cyber criminals fraudulently claiming government benefits by stealing personal and business identity information or directly targeting businesses and individuals receiving support from pandemic response programs. APG members have also reported a significant increase in online fraud scams with criminals posing as manufacturers and distributors of essential COVID-19 materials such as personal protective equipment (PPE) and testing kits and various pharmaceutical products. These materials are either counterfeit or the materials are never received by the customer.

Changes in normal business activity, and pace of financial transactions, have been observed by members as reflected in the levels and types of reporting. Some members reported that numbers of suspicious transaction reports are down, and the analysis conducted by FIUs on trends has

[5] <http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>
[6] <https://www.oecd.org/site/adboecdanti-corruptioninitiative/partnerships/36770989.pdf>
[7] See 2014 FATF report *Risk of Terrorist Abuse in Non-Profit Organisations* – <https://www.fatf-gafi.org/Media/fatf/documents/reports/Risk-of-terrorist-abuse-in-non-profit-organisations.pdf>

had to adapt accordingly. At least one member noted that the value reflected in CTRs is significantly higher in 2020 compared to 2019, triggering inquiries into the transactions. Members have also noted that the reductions in staffing by businesses in response to the COVID-19 pandemic may have an impact on the quality of CDD conducted.

APG members have also noted increasing public concern over accountability of governments for public funds used to address COVID-19 with some allegations of corruption and procurement fraud in the Asia/Pacific region. COVID-19 restrictions have also affected the commission of predicate offences, such as drug trafficking and gold smuggling, with members identifying alternative methods being used by criminal groups to continue these smuggling operations and generate illicit proceeds. At least one member provided several examples of criminal activity being detected as a consequence of the enforcement of border closures.

FATF has highlighted other potential ML/TF risks emerging from the COVID-19 pandemic:[8]

- Criminals may find ways to bypass customer due diligence (CDD) measures by exploiting temporary challenges in internal controls caused by remote working situations, in order to conceal and launder funds.
- Criminals may exploit weak information technologies (IT) systems to gain access to customer contact and transaction information which is then used in targeted phishing scams with the criminals posing as the compromised business.
- As more individuals move money out of the banking system due to financial instability, it may lead to an increased use of the unregulated financial sector. Criminals may seek to invest money in real estate or troubled businesses to generate cash and hide illegitimate proceeds.
- International financial assistance may be misappropriated by corrupt officials or transferred to other jurisdictions, particularly in jurisdictions with weak AML/CFT controls and poor accountability and transparency measures.

A non-public FATF information note released on 23 April 2020 also provides additional details on illicit activities associated with COVID-19.

1.4 Specific Cases/Observations

Online fraud related to PPE

Example 1 – Case provided by Chinese Taipei

Mr Zhang falsely claimed to be the owner of S Company which sold PPE such as masks for medical use. After downloading random pictures of factory production lines from the internet he posted these pictures on social networking platforms to create the false impression that S Company was capable of manufacturing medical masks in massive quantities and was able to ship those masks to China. Consequently, many customers placed orders with S Company during the COVID-19 pandemic. Mr Zhang claimed he would provide the customers with a 'bill of lading number' so that they could track the shipping progress. The customer would then assume the transaction was legitimate and transfer payments to S Company.

[8] <http://www.fatf-gafi.org/media/fatf/documents/COVID-19-AML-CFT.pdf>

Example 2 - Case provided by Hong Kong, China

In January 2020, Ms A posted advertisements on various e-commerce platforms claiming to have a large quantity of surgical masks and alcohol sanitisers for sale. Between January and March 2020, more than 200 victims purchased these goods and paid for them by depositing cash or making electronic fund transfers. A total of HKD 1.4 million (USD180,600)[9] was deposited into three Hong Kong bank accounts and four e-wallets held by Mr B (Ms A's spouse) and his associates. In early March 2020 reports were made by victims as they had not received their goods and were unable to get in touch with Ms A and Mr B. Investigations revealed that the money was withdrawn quickly after victims deposited the money into the designated bank accounts and e-wallets. Ms A and three members of her syndicate were arrested in April 2020. The investigation is currently ongoing.

Example 3 - Case provided by Hong Kong, China

Mr A is the owner of a clinic who received an unsolicited email from Mr B claiming to be a surgical mask and personal medical protective equipment supplier from Jurisdiction X. In early February 2020, Mr A placed an order for PPE and transferred a total of HKD 20 million (USD2.5 million) to 14 overseas bank accounts in seven jurisdictions. Mr A made a police report when he was unable to get in touch with Mr B. The Hong Kong Police Force promptly liaised with banks via INTERPOL and withheld over HKD 16 million (USD2 million) from the accounts. The investigation is ongoing.

Example 4 – Case provided by Thailand

A victim filed a complaint with police after she had contacted a Facebook user called "Phukong Met" to purchase face masks and was told to transfer 1.46 million baht (USD47,100) over eight separate transactions into Ms S's bank account. After the payments were made, the victim did not receive any face masks. An investigation uncovered that there were two suspects involved in the fraud, Mr T and Ms S who were subsequently arrested. Mr T confessed that he used a police officer's photo as a profile photo on his "Phukong Met" Facebook page to con people into buying the masks. The money swindled from the victims was spent by Mr T on gambling and personal expenses.

Example 5 – Case provided by Singapore

On 25 March 2020, a 39-year-old man was arrested on suspicion of laundering scam proceeds relating to COVID-19 medical supplies in the amount of S$10.2 million (USD7.3 million). A foreign pharmaceutical company was deceived into transferring this sum to a Singapore bank account for the payment of large supplies of surgical masks and hand sanitisers. The pharmaceutical company was a victim of a Business Email Compromise Scam, where scammers used the spoofed email address of their business partner to re-direct payment transfers to the bank accounts controlled by the scammers. The first alert was raised by a Singapore-based bank on Saturday, 14 March 2020. The bank received a funds recall message from the victim and notified the Singapore authorities of their suspicion. Singapore authorities immediately notified their French counterparts of the suspicious money flow and possibility of fraud. To prevent any dissipation of illicit proceeds, the Singapore authorities acted immediately. Through quick intervention and collaboration with banks, the Anti-Scam Centre

[9] All conversions to USD equivalent are based on conversion rates at 1 July 2020

of the Singapore Police Force seized more than S$6.4 million (USD4.5 million) on the same day of the alert. This is a testament to the close partnership and trust between the private sector and the authorities built through extensive public-private collaborations over the years. The Singapore authorities are working with the French authorities to gather evidence for the ML investigation and determining the destination of the remaining funds.

Example 6 – Case provided by Bangladesh

The Bangladesh FIU received an email from a local bank, Bank X advising that a counterfeit letter bearing the bank's letterhead and officials' signatures had been sent to an international bank, Bank Y, requesting a transfer of funds. The letter required Bank Y to accept and execute instructions supposedly given by Bank X via facsimile or email instead of using the SWIFT network which was usual for international funds transfer requests. The letter stated that the SWIFT network was unavailable as a result of the COVID-19 pandemic.

In the letter, Bank X agreed to indemnify Bank Y against any losses (including losses due to fraud), if Bank Y agreed to make payment of the funds in the way Bank X had outlined in their letter. Once the letter was sent, a fake fund transfer request in Bank X's name was sent to Bank Y through email requesting urgent payment for the procurement of ventilators to a firm in Jurisdiction A. Bank Y became suspicious of the letter as the letter and fund transfer request were both sent to Bank Y on a public holiday. Bank Y contacted its local office in Bangladesh who then confirmed Bank X that the request was an attempted fraud.

Scams related to medical treatment

Example 7 – Case provided by China

A bank manager received a call from his client who said that he had received a request for money from his daughter who was studying abroad. His daughter claimed to be infected with COVID-19 and asked her father to transfer RMB 100,000 (USD14,150) for medical treatment directly into her online social media account. The bank manager asked his client for further details and established the client had not spoken to his daughter via phone to confirm she had actually sent the message. The bank manager asked his client to verify the authenticity of the information before making a payment. After speaking with his daughter, the father learned his daughter's social media account had been hacked and she was not infected with COVID-19. No payment was made.

Impersonation of law enforcement officials

Example 8 – Case provided by Hong Kong, China

In April 2020, while Ms A was in quarantine at a local hotel after her arrival in Hong Kong from Jurisdiction X, she received a call from Mr B who claimed to be a police officer from Jurisdiction X. Mr B claimed that Ms A was involved in economic crime and demanded Ms A prove her innocence by surrendering her e-banking username and passwords so the police could undertake 'asset scanning'. Ms A complied and later found that an amount of HKD 1 million (USD129,000) was transferred from her bank account to a bank account held by an unknown person. Fund flow analysis was conducted on multiple bank accounts and eventually, HKD 1 million (USD129,000) was withheld. Investigations are ongoing.

Identity theft

Example 9 – Case provided by Thailand

The offenders offered job opportunities to job seekers via websites. Upon their registration on the website, the job seekers were required to fill in their personal data including a bank account number. The offenders then used this information to commit identity theft by hacking into the victim's bank account and/or into their Facebook account and then requesting money from the victim's friends. This fraudulent activity was committed by a network of offenders. The proceeds of crime, approximately 200,000 baht (USD6,460), was transferred to their e-wallet. After the arrest of some of the offenders, proceeds of crime with approximately 105,000 baht (USD3,390) was returned to the victims.

Fake charity scams

Example 10 – Case provided by China

Mr W posted on an internet platform a request for public donations for the fight against COVID-19. Mr W provided a QR code which people could scan to receive bank account details for where they could send their donation. During the pandemic, over 100 people from all over China made donations mostly in RMB 10 yuan (USD1.41) or 100 yuan (USD14.15) amounts. The total value of the donations exceeded RMB 100,000 (USD14,150). Shortly after the money was credited to nominated bank account it was transferred out to Mr W's personal bank account. The case has been reported to the police for investigation.

Breach of COVID-19 restrictions

Example 11 – Case provided by Australia

Ms. A runs a beauty business that under Australian COVID-19 restrictions was not permitted to provide beauty services due to the risk of spreading the virus. Ms. A's bank reported that in the period of a fortnight, she deposited AUD22,600 (USD15,570) of cash into her business account at multiple branches while her business would have been closed due to COVID-19 restrictions. Ms. A also then conducted funds transfers to multiple third parties for the value of AUD1,300 (USD900) per transfer. Additionally, earlier that month a second business account received AUD40,000 (USD27,550) in transfers over four days. These funds were then transferred by Ms. A to another person at another bank. It is suspected the source of these funds may have also come from illegitimate sources and are being channelled through the business in an attempt to legitimise them.

The case has been reported to the police for investigation.

Misuse of public funds

Example 12 – Observations provided by Papua New Guinea

There has been elevated attention from the public on the expenditure by government bodies to address the COVID-19 crisis. Internal investigations and an independent committee have been established in PNG to respond to allegations that funds allocated to the COVID-19 response were expended without the appropriate procurement processes being followed, including

through fraudulent payments. Allegations spread via social media, and there was also a complaint lodged with the Police against the Health Minister who had allegedly issued instructions in favour of a fraudulent payment.

2. APG WORKSHOPS AND PROJECTS 2019 - 2020

This section of the report provides a brief overview of typologies related work undertaken by the APG between July 2019 and June 2020.

2.1 Typologies Projects

Digital Know Your Customer (KYC) Workshop

At the 22nd Annual Meeting in 2019, members approved a two-phase project on the implementation of digital KYC in the Asia/Pacific region. The objective of the project is to support the implementation of digital KYC including outreach and capacity building on applying the FATF Guidance on Digital Identity (ID) published in March 2020.

- Phase one of the project was to be a regional workshop on digital KYC to be held collaboratively by the Alliance for Financial Stability with Information Technology (AFS-IT), a non-profit organization based in Hong Kong, China and the APG Secretariat. The initial plan for phase one was to conduct the workshop in Seoul in late March 2020, however, due to the impacts of COVID-19 the workshop has been postponed and will be held within the APG typologies workshop planned for late 2020.
- Phase two of the project will include the development of a scoping paper of proposed further activities informed by the outcomes of the workshop to be developed in partnership between AFS-IT and APG. Any future work on this issue would depend on resources available in the secretariat and member needs.

Financing and Facilitation of Foreign Fighters (FFs) in Southeast Asia

At the 22nd Annual Meeting in 2019, members approved a project with the Global Center on Cooperative Security to explore what is known about the financial profiles of FFs and returnees in Southeast Asia. The project will produce a typology report on the use of financial intelligence related to FFs emanating from, returning to, or traveling within the region, as well as offer recommendations on how financial intelligence can be better used to support the detection, disruption, or prosecution of FFs.

A questionnaire was distributed to APG members in December 2019 and 19 responses were received. This questionnaire collected information from jurisdiction's FIUs on the scope and nature of financial intelligence collected, gathered, and disseminated related to FFs in Southeast Asia. It was originally planned to supplement the information collected from the questionnaires with field consultations and interviews with law enforcement agencies (LEAs), security agencies, and other national and regional stakeholders in the region in mid-2020. In light of the challenges and restrictions posed by the COVID-19 pandemic, the project team will explore the possibility and capacity to conduct virtual meetings/consultations with individual jurisdictions to follow up on the questionnaire and solicit jurisdiction-specific feedback to feed into the draft report. The draft report is planned to be shared with APG members in November 2020 for their feedback and review in advance of the 2020 APG typologies workshop, where the project may also form a workshop stream.

Human trafficking and people smuggling project (Phase two)

Phase one of this project was a FATF/APG project focused on human trafficking (HT) and was finalised in July 2018. Phase two is an APG regional project that has been built on phase one 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. 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.

A regional workshop was intended to be conducted in early 2020 to develop a training package for use by APG members to showcase the importance of partnerships between the public, private and non-government sectors in the prevention, detection, analysis and response to HT and PS; outline mechanisms and opportunities to enhance partnerships in the Asia/Pacific region; and highlight indicators for laundering the proceeds of these crimes. Due to the COVID-19 pandemic, this regional workshop to complete the HT and PS project has been postponed.

Terrorism financing & proceeds of crime (including organised crime) - Non-public

The Eurasian Group on Combatting Money Laundering and Financing of Terrorism (EAG) and APG conducted a joint project focussing 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. The joint report was adopted by APG members in August 2019 and EAG members in November 2019 (see the following section in this report: EAG – Eurasian Group on Combating Money Laundering and Financing of Terrorism).

2.2 2019 Typologies and Capacity Building Workshop

Each year the APG typologies workshop brings together AML/CFT practitioners from investigation and prosecution agencies, FIUs, regulators, customs authorities and other agencies to consider priority ML and TF risks and vulnerabilities.

Due to resourcing challenges, the APG typologies workshop was not held in 2019. While the APG is planning to hold its annual typologies workshop in 2020 in Malaysia, this may be disrupted by travel restrictions due to COVID-19.

3. FATF, FSRBS AND OBSERVERS' PROJECTS

This section of the report provides a brief overview of typology reports published by FATF and other FATF-style regional bodies (FSRBs) between July 2019 and June 2020.

3.1 FATF Typology Projects

ML and the Illegal Wildlife Trade (June 2020)

This typologies report built on earlier research into the connection between the illegal wildlife trade (IWT) and ML undertaken across the global network. The report found IWT to be a major transnational organised crime, not only in source, transit and destination jurisdictions but also involving other jurisdictions worldwide. A lack of understanding, and targeted pursuit of parallel financial investigations in line with risk profile, across jurisdictions was also a major finding of the report. The report recommended a number of key actions, including:

- Improve risk understanding, policies and legislation relating to ML and IWT.
- Pursuit of parallel financial investigations and ML charges related to IWT.
- Improve international cooperation around IWT.
- Private sector supervision and public-private collaboration.

The report is available on the FATF website at:

<http://www.fatf-gafi.org/publications/methodsandtrends/documents/money-laundering-wildlife-trade.html>

ISIL and Al-Qaeda and affiliates financing updates (June 2020) – Non-public

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.

COVID-19-related ML and TF risks and policy responses (May 2020)

This paper drew on submissions from FATF members and the global network in relation to three thematic areas:

- New threats and vulnerabilities originating from COVID-19-related criminal activities and flow-on effects to ML/TF risks.
- The impact of COVID-19 on governments and private sector entities to perform their AML/CFT functions.
- Suggested AML/CFT policy responses to manage emerging threats and vulnerabilities whilst also responding to COVID-19.

The paper is available on the FATF website at:

<http://www.fatf-gafi.org/publications/fatfgeneral/documents/covid-19-ml-tf.html>

Best Practices on Beneficial Ownership for Legal Persons (October 2019)

This paper is designed to provide practical advice for jurisdictions on the effective enforcement and supervision of beneficial ownership (BO) obligations. It draws on the joint FATF and Egmont Group Report on the Concealment of Beneficial Ownership (July 2018) and provides case studies and examples of best practices to guide jurisdictions in ensuring compliance with BO obligations. The report recommends a multi-faceted approach to ensuring accurate and up-to-date BO information is accessible in a timely manner and highlights the importance of collaboration and information-sharing. The key features of an effective BO system for legal persons are identified as:

- Comprehensive risk assessment of all types of legal persons.
- Access by competent authorities to BO information.
- Adequacy, accuracy and timeliness of BO information.
- Prohibiting or immobilising bearer shares and nominee arrangements.
- Effective, proportionate and dissuasive sanctions.

The paper is available on the FATF website at:

<http://www.fatf-gafi.org/publications/methodsandtrends/documents/best-practices-beneficial-ownership-legal-persons.html>

3.2 Caribbean Financial Action Task Force

The CFATF has conducted a number of typologies reports including: ML using trust and company service providers (2010); HT and migrant smuggling (2014); illegal lotteries (2016); movement of cash and negotiable instruments (2016); the proliferation of small arms and ammunition (2016) and a CFATF typologies project on de-risking (2019).

CFATF Risk, Trends and Methods Group ML and TF Cases

This report is an update on the compilation of ML/TF case studies compiled by CFATF in 2018. It consists of a compilation of 13 sanitized cases received from seven CFATF member jurisdictions, two of which show clear elements related to terrorist financing. These case studies relate to corruption, structuring, fraud, drug trafficking, and the suspected abuse of NPOs.

The report is available on the CFATF website at:

<https://www.cfatf-gafic.org/documents/resources/13298-cfatf-2019-cases-update-on-money-laundering-and-terrorist-financing/file>

3.3 Eurasian Group

TF & Proceeds of Crime (including organised crime) – Non-public

Issues related to countering the financing of terrorism have been a standing item on the EAG agenda for many years, and are considered a high priority. The EAG has completed a number of typologies projects concerning CFT. The latest is the joint project with APG on the links between TF and organized crime. The three jurisdictions who led the project are Bangladesh,

India and Russian Federation. United Nations Security Council Resolutions 2195 and 2322 form the basis for the project. The project aimed 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.

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. 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 was adopted by APG and EAG annual meetings in 2019.

3.4 Eastern and Southern African Anti-Money Laundering Group

Procurement-related Corruption in the Public Sector and Associated ML

The Council of Ministers approved a typology study on 'Procurement Corruption in the Public Sector and Associated Money Laundering in the ESAAMLG Region' in September 2017 to better understand the dynamics of procurement corruption and associated ML in the region. The study aimed to:

- Understand the manner in which the public sector procurement process is manipulated and the stages and sectors most vulnerable.
- Identify the key actors involved in corruption and ML within the procurement process.
- Analyse the methods and trends for laundering the proceeds of procurement corruption.

This report was informed by case studies and questionnaires distributed to both public and private sector entities with responses received from 17 member jurisdictions and 11 member jurisdictions respectively. The study found corruption was prevalent in procurement across the member states and this most commonly occurred at the awarding of the tender stage. A number of recommendations to combat ML at the agency, domestic and regional levels were also developed. The report is available on the ESAAMLG website at:

<https://www.esaamlg.org/index.php/methods_trends/readmore_methods_trends/12>

3.5 Inter-Governmental Action Group against Money Laundering in West Africa

Money Laundering and Terrorist Financing Linked to the Extractive Industry / Mining Sector in West Africa

The extractive industry/mining sector represents a large component of GDP for a number of GIABA member jurisdictions and is considered to be at high risk for ML and TF. The study set out to:

- Comprehensively assess the ML/TF risks, including assessing the adequacy of existing legal, supervisory and regulatory frameworks to prevent, deter, investigate and prosecute illegal exploitation of the extractive industry/mining sector.
- Identify the most common methods and trends used to launder illegal proceeds from the sector
- Analyse the main techniques used to finance terrorist activities from the sector.

Provide practical recommendations and policy advice to address ML/TF in the sector and support financial institutions, designation non-financial businesses and professions (DNFBPs) and other reporting entities (REs) to identify and appropriately respond to ML/TF. This typologies project involved input from members and relevant stakeholders through questionnaires and workshops. The report found that regulatory and law enforcement efforts have not yet managed to curb ML/TF in the sector. A number of obstacles to improving AML/CFT measures remain, including weak regulation, corruption, cash-based economies, porous borders, and under-resourced and poorly trained LEAs.

The report is available on the GIABA website at:

<https://www.giaba.org/reports/typologies/reports.html>

3.6 Egmont Group

Egmont and WCO Customs-FIU Cooperation Handbook (2020)

This handbook is designed to serve as a practical tool for FIUs and Customs Services (and other law enforcement agencies) to effectively collaborate and combat financial crime, ML and TF. The handbook looks at common ML methodologies including:

- Smuggling and concealment of currency, currency equivalents, gems and precious metals.
- Trade-based money laundering.
- Money or Value Transfer Services and alternative remittance systems.

The handbook is available on the Egmont Group website at:

<https://egmontgroup.org/en/document-library/11>

3.7 European Commission

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities

This report is an update on the Commission's first supranational ML/TF risk assessment conducted in 2017 (required every two years). The assessment identified cash as the ML instrument-of-choice for criminals despite its waning popularity across the broader population. The report also found that financial subsectors or products that deal in cash remain areas of significant ML risks. The main vulnerabilities in the DNFBP sector related to failing to identify beneficial ownership information and the lack of STR reporting by self-regulatory bodies (SRBs) to FIUs. The gambling sector and NPOs were also found to have varying degrees of risk which highlighted the importance of understanding the nature of their activities to better mitigate these risks. Professional football, free ports, and investor citizenship and residence schemes were identified as new sectors posing ML/TF risks. The risk assessment noted horizontal vulnerabilities such as anonymity in financial transactions, identification and access to BO information, supervision, and cooperation between FIUs.

The report concluded with an overview of mitigating measures and recommendations for member states to improve their AML/CFT systems and is available on the European Commission website at:

<https://op.europa.eu/en/publication-detail/-/publication/0b2ecb04-aef4-11e9-9d01-01aa75ed71a1/language-en/format-PDF/source-search>

4. TRENDS

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

4.1 Research or Studies by APG Members and Observers

Australia

Risk Assessment: Mutual banking Sector

AUSTRAC published its risk assessment of Australia's mutual banking sector in 2019. For the purposes of AUSTRAC's assessment, Australia's mutual banking sector includes approved deposit-taking institutions that are owned by their customers (such as mutual banks, building societies and credit unions). AUSTRAC assessed the overall ML and TF risk associated with Australia's mutual banking sector to be medium.

The report can be found on AUSTRAC's website:

<https://www.austrac.gov.au/business/how-comply-guidance-and-resources/guidance-resources/risk-assessment-mutual-banking-sector>

Report: Combating the sexual exploitation of children for financial gain activity indicators report

AUSTRAC's Fintel Alliance (a public-private partnership incorporating government, law enforcement, private sector and academic organisations) published its 'Combating the sexual exploitation of children for financial gain – Activity indicators' report in November 2019. Recognising that financial service providers play an important role in combating child sexual exploitation for financial gain, Fintel Alliance works collaboratively with law enforcement and industry partners to proactively identify transactions that relate to child sexual exploitation. This report aims to assist financial service providers and LEAs to detect suspect transactions by providing updated financial and environmental indicators to more effectively combat child sexual exploitation.

The report can be found on AUSTRAC's website at:

<https://www.austrac.gov.au/sites/default/files/2019-11/Fintel%20Alliance%20_Financial%20Indicators%20Report_Combating%20the%20sexual%20exploitation%20of%20children.pdf>

Report: Illegal phoenix activity indicators report

AUSTRAC's Fintel Alliance published its 'Illegal Phoenix Activity Indicators' report in October 2019. Illegal phoenix activity involves a business owner creating a new company to continue the business of a company that has been deliberately liquidated to avoid paying its liabilities and taxes. This report identifies and explains the key indicators of illegal phoenix activity in the labour hire and payroll industry. While the indicators in this report are specific

to labour hire, they are also relevant to businesses that predominantly conduct cash transactions for paying staff and suppliers.

The report can be found on AUSTRAC's website:

<https://www.austrac.gov.au/sites/default/files/2019-10/Fintel%20Alliance%20phoenix%20activity%20report.pdf.>

Exploitative practices in labour hire arrangements

The Australian government is examining challenges posed by labour hire structures used by legitimate enterprises to exploit labour and avoid detection. The use of third-party accounts and companies in workers' names obfuscate control of entities to create distance from criminal responsibility and allow for further offending around phoenix activity for the GST revenue that is payable to the Australian Taxation Office. Therefore typologies utilised regarding 'phoenix' behaviour may be of assistance in identifying entities of concern within the labour hire cohort. At the extreme end of the scale, when workers are not paid they have no interaction with the financial system. When exploited workers are paid the use of cash and the lack of interaction with traditional financial system remains a known weakness in using ML provisions to identify human trafficking.

Common cuckoo-smurfing methodology

Australian authorities have been building awareness of a common methodology used in ML through offsetting accounts. Common names for this method are 'mirror banking', 'black market peso exchange', 'cuckoo smurfing' and 'hawala'. This method normally involves a party (A) based internationally wanting remittance of money into Australia. Arrangements are made through a person (ML1) in that region to send the money. ML1 may have connections to an Alternate Remittance Sector in that region. ML1 also has connections to persons in Australia who maintain an amount of cash and wish for that cash to be moved offshore without any disclosure (Z) as well as someone who can act as their representative to handle physical matters within Australia (ML2).

ML2 has multiple functions. They firstly arrange to meet with Z or a representative of Z and collect an amount of cash as arranged between ML1 and Z. Upon ML2 confirming receipt of the money with ML1, ML1 will forward banking instructions to ML2. These banking instructions relate to the deposit/remittance requests arranged by A. ML2 will then make those deposits into the nominated accounts. Money is structured in amounts under AUD10,000 (USD6,940) to ensure that no information of ML2 is recorded that can then place them under suspicion with AUSTRAC and other authorities. Once deposits are made, ML2 will advise ML1 that they are completed. A common practice to show unequivocal proof is by photographing the deposit slips and sending them to ML1. Communication is usually through the use of encrypted chat applications. This feature is also used to prevent detection from interception by law enforcement and other authorities.

Brunei Darussalam

The FIU of Brunei Darussalam is a member of the Financial Intelligence Consultative Group (FICG) which is made up of FIUs from Association of South East Asian Nations (ASEAN) members, Australia and New Zealand. Together FICG has produced the following:

- TF Disruption Toolkit – to identify ways to disrupt terrorist financiers by exploring participant jurisdictions' counter-terrorism financing capabilities and information sharing principles.
- Regional Corruption Threat Assessment – a threat assessment conducted based on input from participating FICG members to identify corruption typologies and possible regional counter-measures to tackle it.
- Operational Guidance of Virtual Assets (VAs) – a project that surveys the regulatory landscapes of VAs and virtual asset service providers (VASPs) in the Southeast Asia, Australia and New Zealand region, to produce a comprehensive operational guidance on dealing with VAs and providers.

In addition, Brunei Darussalam is currently in the process of updating its 2016 ML and TF National Risk Assessment (NRA).

Indonesia

Indonesian authorities regularly conduct research on ML/TF methods and trends which are published internally and for limited distribution. Their most recent research on ML cases from 2018 indicated that the dominant predicate crimes reported are narcotics-related. The most common transaction patterns are via ATM, cash deposit via teller and overbooking.

Japan

The National Public Safety Commission publishes an annual report on ML and/or TF risk assessments on the website of JAFIC, Japan's FIU. Also published on this website is the Annual Report on the Prevention of Transfer of Criminal Proceeds. This report is a compilation of statistics, case studies and trends related to ML and TF.

Malaysia

The Malaysian FIU has issued four red-flags and typologies reports on corruption, illicit drug trafficking, smuggling, and HT in 2019. These crimes are the high risk and medium-high risk crime identified through the 2017 NRA. These documents were issued with restricted circulation to REs with the aims to:

- Provide insights and create awareness of crimes (trends, techniques, methods and channels).
- Enhance and facilitate REs' knowledge and understanding of typologies.
- Assist REs in the identification of offences from red flags/indicators exhibited by their clients and involved financial transactions.
- Enable early detection by REs to disrupt crime.
- Further improve the quality of STRs.

Thailand

Thai authorities are undertaking research on ML/TF methods and trends to be finalised in late 2020 relating to:

- Case studies.

- ML through legal persons and shell companies, legal professionals and accountants, tour companies, foreign trusts operating in Thailand, Ponzi schemes and NPOs.
- ML through Fintech and financial inclusion.
- Fundraising, TF network expansion and measures to disrupt FFs focussing on communication through computer networks, social media, and trade-based TF.

4.2 Association of Types of ML or TF with Predicate Activities

Hong Kong, China

In early 2016, the Customs and Excise Department (C&ED) identified an illicit cigarette selling syndicate in Hong Kong, China. Investigations uncovered the storage location and operations of the syndicate, as well as links to a couple who deployed certain store keepers and couriers to undertake the illicit activities. After the sale of the illicit cigarettes, the store keepers/couriers would either deposit the cash into the bank account held by the female of the couple or hand the cash directly to the couple.

In August 2016, the C&ED arrested the couple and four other members of the syndicate, and seized illicit cigarettes valued at approximately HKD2.1 million (USD271,000). Financial investigations revealed the syndicate had laundered approximately HKD8.2 million (USD1 million) of crime proceeds between June 2013 and August 2016. In October 2017, the couple and two of the syndicate members were convicted of illicit cigarette offences. The female of the couple was also convicted of ML and sentenced to 33 months' imprisonment. In May 2019, the court granted a confiscation order to confiscate HKD2.95 million (USD380,600) of realisable properties held by the female.

Indonesia

According to the most recent statistics related to STR reporting, the predicate activities most commonly associated with ML are fraud, corruption and gambling. According to analysis results, corruption is the predicate offence most commonly associated to ML.

Japan

In 2019, Boryokudan members and related parties were involved in 9.7% of all ML cases cleared in accordance with the Act on Punishment of Organised Crime and Control of Crime Proceeds. Some of these individuals used bank accounts opened in the names of third parties to acquire criminal proceeds from predicate offences (such as fraud), while others received criminal proceeds from gambling crimes in the name of protection money.

Lao PDR

Since February 2019, Lao PDR authorities reported three convicted cases of ML which relate to the predicate activities of fraud and drugs.

Malaysia

Malaysian authorities have identified fraud, smuggling and corruption were high-risk crimes with significant interlinkages to other serious crimes as part of the preparation of their 2017

NRA. Tax evasion was substantially linked with smuggling offences. It was also noted that smuggling-related crime, i.e. TBML, HT and drug trafficking, may have been facilitated by corrupt border officials. Malaysia is currently preparing a 2020 NRA which will cover the development of trends and patterns of ML and TF since the 2017 NRA.

Pakistan

A case was registered against persons for corruption, fraud and forgery and ML was later identified. The accused management of X Institute purchased various properties at exorbitant rates, violating the procurement rules. Kickbacks of PKR 1 billion (USD6 million) were paid. A benami investment[10] amounting to PKR 38 million (USD229,200) in the name of one of the co-accused was traced to the stock market. Following the collection of evidence and the taking of statements, the personal bank accounts, lockers and property of the accused persons and their dependents were seized by LEAs. The value of seized assets was approximately PKR 641 million (USD3.8 million).

Chinese Taipei

Suspect Lin recruited 15 members for a fraudulent computer room operation from within a rented facility engaged in swindling. Members disguised themselves as delivery drivers and told victims that their deliveries were involved in ML activities before other members of the syndicate continued to scam these victims. The case was reported to the Taitung District Prosecutors Office (Sheigu) where after investigating the patterns of activity, a search warrant was issued in May 2019. At the execution of the search warrant, 16 suspects, including Lin, were arrested and a number of computers, electronic devices, mobile phones and other items confiscated. 13 suspects were placed into incommunicado detention.

During the search, conversation records were identified and, in conjunction with victim statements, it was identified that the fraudulent computer room had been in operation since February 2019 and an amount exceeding NTD20 million (USD679,100) had been swindled. This included money from two Chinese citizens living in the United States who had remitted USD76,000 and USD78,000 (NTD4.5 million) to the suspects. Investigations are continuing.

4.3 Emerging, Declining and Continuing Trends

Brunei Darussalam

Brunei Darussalam sees a continuing trend of STRs filed with the following red flag indicators:

- Involves personal or joint accounts.
- Account turnover (debit/credit) is more than the expected income of the individual(s).
- Multiple inward/outward electronic fund transfers with no clear purpose.
- Transactions are of similar amounts or similar range of amounts.
- Any cash transactions conducted are typically well below cash threshold reports (CTRs) threshold (but there is no indication of trying to report just under the threshold to avoid detection).
- May involve purchases/payments to companies.

[10] Transactions where the beneficiary of a transaction is not the same person that provides consideration.

- May involve international wire transfers (small amounts).

The above indicators allude to possible activities of which the highest likelihood is gambling through online gambling sites. Thus far, no sites have been found to be operating from Brunei. Sites operated from other jurisdictions may be unregulated and have possible links to criminal activity. Other possible offences include fraud through false investment schemes, unlicensed money lending, the involvement of third party (anonymous) use of accounts or laundering proceeds from drug trafficking.

In addition to the above, Brunei Darussalam has noted an emerging trend relating to the 'renting' of SIM cards of local mobile phone numbers by unknown third parties to send messages to promote online gambling. As a result of the detection of this trend, the authorities in the jurisdiction have worked together with the telecommunications sector to limit the acquisitions of SIM cards per person to reduce the risk of it being 'rented' out to unknown third parties.

Indonesia

The banking industry continued to be used to launder proceeds of crime with transfer via ATM, cash deposits through tellers, and transfers via mobile banking showing an upward trend based on court verdicts. Cash transactions, however, declined based on analysis of court verdicts. Predicate crimes of fraud and narcotics-related offences were increasingly associated with ML, although corruption remains the predicate offence most commonly associated with ML.

Japan

The majority of criminal proceeds concealment cases cleared in 2019 involved the transfer of criminal proceeds into bank accounts opened in the names of third parties indicating this has become one of the main methods for ML. Other common methods of concealment included hiding stolen goods in coin-operated lockers before selling these stolen goods under false names.

Lao PDR

Between February 2019 and February 2020, Lao PDR has identified drugs as an emerging trend with the identification of the first ML case related to drugs and a large number of drug-related predicate offences convicted. Fraud continues as a ML trend, with a decline in the number of robbery-related ML cases.

Malaysia

The use of mule accounts and a shift from personal to business accounts to move illicit funds continue to be widespread in 2019. Malaysia remains highly exposed to telephone scams involving the impersonation of law enforcement officials forcing victims to transfer their savings to mule accounts. In response to this trend, enforcement actions have been taken with several successful raids on syndicates involving foreign nationals based in Malaysia.

Pakistan

Emerging trends include:

- STRs related to the use of VAs for illegal activities.
- Use of branchless banking for carrying out transactions related to frauds, etc.
- STRs on HT were also reported.

STRs related to hawala/hundi declined in 2019. Receipt of tax evasion-related STRs is a continuing trend in 2019.

Singapore

Business Email Compromise Scams as a continued trend

Business email compromise (BEC) scams continue as a trend of cyber-enabled crime involving cross border funds flows into and out of Singapore, adversely affecting financial institutions (FIs), businesses and individuals. The victims believed that they were transferring funds to their business partners or for their employees' salaries, only to discover that the request for payments was made by scammers, and the accounts did not belong to their business partners nor workers. Authorities have also observed a new variant modus operandi - scammers no longer limit themselves by posing as business partners of the company or employers, but also as the company's employees.

There has been a surge of BEC scams in Singapore from 2017 to 2019, and BEC fraud remains one of Singapore's top ten scam types. Most recently, in 2019, there were 385 cases of BEC scams in Singapore resulting in losses of S$45.4 million (USD32.6 million). Given the transnational nature of this scam type, BEC scam is a global problem. To this end, Singapore is part of a global initiative under the Egmont Group involving 14 participating jurisdictions, which aims to prevent the dissipation of funds arising from such scams. Participating jurisdictions partake in swift information sharing which allows authorities to act on timely intelligence from partner jurisdictions to stop/disrupt the flow of criminal proceeds from BEC scams.

Since October 2018, Singapore authorities have also partnered with FIs, through a public-private partnership initiative, known as the AML/CFT Industry Partnership (ACIP), to combat BEC scams. The Commercial Affairs Department of Singapore (CAD), working closely with the eight ACIP member banks, has to-date seized more than USD2 million in illicit funds entering the jurisdiction. Singapore has also actively engaged foreign jurisdictions to which criminal proceeds have been transferred. Singapore further contributed to the INTERPOL Global BEC awareness campaign, where educational material was shared via various platforms to raise the public's awareness of the BEC scam and its warning signs.

Virtual assets as an emerging trend

VAs were first identified as an emerging risk in Singapore's NRA in 2014. Since then, law enforcement has seen an upward trend of reported cases involving virtual currencies with a total of 383 of such reports lodged from 2016 to 2018. The majority of these cases reported in

Singapore related to cheating (e.g. scams) and offences under Singapore's Computer Misuse and Cybersecurity Act (which includes unauthorised access to computers and accounts).
There are three broad ways that VAs can be exploited in Singapore: as a payment method, marketed product, and as a targeted item. See details below:

- Payment Method: Ransomware malware cases where ransom payment (in the form of VAs like Bitcoin) is demanded, and impersonation scams where scammers impersonate foreign officials (e.g. government law enforcement officials) to demand a settlement fee in VAs for offences victims had allegedly committed. In some cases, tainted assets had flowed through VA exchanges.
- Marketed Product: Schemes involving initial coin offerings (ICOs), e-commerce scams selling VAs.
- Targeted Item: Unauthorised transactions involving VAs (e.g. hacking).

Apart from the three categories identified above, LEAs have also seen the emergence of cases that use VAs to launder illegal proceeds. Two emerging typologies are described below:

Scam Victims Turned Mules - Laundering Proceeds Using VAs

In certain types of cheating cases (e.g. love scams, and officials impersonation scams), the victims may also be deceived into receiving tainted proceeds in their bank accounts without knowledge of their illicit origins. Traditionally, the modus operandi was to request the victims to transfer these funds to other 'pass-through' accounts via a remittance service or wire transfer. Lately, a new typology in several cases has emerged where the perpetrators instructed the victims to purchase and transfer Bitcoins to the perpetrators instead.

VASP Accounts Set Up Using Stolen Identities to Launder Proceeds

In cheating cases involving compromised bank accounts (e.g. where victims were deceived into revealing their banking login details), scammers were observed to have layered proceeds by creating a VASP account in the name of the victims without their knowledge. During account opening, a VASP may require the account holder to take a photograph of themselves holding on to their identification document (e.g. passport or national identification card). Scammers hijack this process by first tricking the victims into taking such a photograph under false pretences. The criminals would thereafter use this photograph to create an account with a VASP, unbeknownst to the victim. The scammer would then empty the victim's compromised bank account by transferring monies to the VASP to purchase Bitcoins. As the scammer had control of the VASP account, they would be at liberty to transfer the criminal proceeds to other accounts under their control, and to launder them through even more layers.

In such cases, the VASP would also be kept in the dark despite proper CDD. From the VASP's perspective, it would appear that the victim was purchasing Bitcoins using funds from their own bank account.

Thailand

Continuing ML trend of convincing a large number of people to invest or pay collateral before starting work with a promise of large returns or income. The money is never repaid and no returns or income received.

Continuing TF trends of robbery (including high value assets from soft targets), drug trafficking, illegal oil trading and customs evasion to finance terrorism. The use of religious schools to receive government grants in order to finance terrorist activities also continued as a TF trends.

5. CASE STUDIES

5.1 Terrorist Financing

Australia

In November 2019, a Melbourne man was convicted of two counts of giving support for a foreign incursion (under Australia's *Crimes (Foreign Incursions and Recruitment) Act 1978*) in relation to the remittance of over AUD2,700 (USD1,880) to an American supporter of ISIL who was fighting in Syria in 2014. The funds were sent over multiple remittances in 2014, and were intended to be used to support a website service operated by the fighter in Syria. Taking into account earlier time served on remand, the Melbourne man was released with a recognisance order upon conviction.

The Philippines

Use of non-profit organisations

A local NPO sought funding from foreign donors (FD) for projects aimed at improving livelihoods for the poor, assisting victims of typhoons and other calamities, and human rights training etc. The FD sends the funds to the NPO's foreign currency (forex) deposit account maintained in a local bank, through international remittance facilities. The NPO maintains several peso currency deposit accounts, which are used to move the funds from the FD. Transfer of funds to the peso deposit account is made through direct credit (fund transfer via credit memo) of the withdrawal. The NPO also makes a cash withdrawal from the forex account, sells the foreign currency to the same bank, and deposits the proceeds to peso deposit account also maintained with the same bank.

To fund the implementation of approved project, the NPO withdraws funds from its deposit accounts through authorized personnel. Once withdrawn, the funds will be again turned over to another person who will distribute the same as follows: forty percent (40%) to the actual project and sixty percent (60%) to the local terrorist group (LTG), which is also designated as a terrorist organization by several foreign jurisdictions and supranational bodies. The funds that went to the LTG are used for the purchase of arms, medical equipment, food, clothing, and other necessities, for tactical offensive operations against government forces and civilians.

On the basis of the sworn statements executed by the witnesses, and the financial intelligence provided by the AMLC Secretariat's (AMLCS) Financial Investigation and Analysis Group (FIAG) the Investigation Report (IR) was concluded in August 2019, and a process was commenced ('bank inquiry') to seek bank records.. The said IR was transmitted to AMLCS' Legal Evaluation Group (LEG) for their evaluation also in August 2019. In October 2019, officials were able to secure authority from the AMLC to inquire into several bank accounts of the NPO. An IR on the results of the bank inquiry was concluded in December 2019, recommending the freezing of the subject accounts. On 26 December 2019, the AMLC issued a resolution directing the concerned bank to freeze three main accounts and other related accounts of the NPO, for a period of 20 days.

To date, the bank had frozen 15 bank accounts under the name of the NPO with an aggregate outstanding balance of PHP14.9 million (USD302,000). The Verified Petition to Extend the Freeze Order to six months for the 15 bank accounts was granted by the court.

Singapore

Person jailed 33 months for TF

In April 2019, CAD prosecuted Person K for providing S$450 (USD323) via a money remittance service provider to another individual in a third jurisdiction in 2014. The money was intended to support the publication of ISIL propaganda. The beneficiary of the funds was an exact name and jurisdiction match of an individual who was designated in 2016 by the United States for providing logistical support and facilitating the movement of tens of thousands of dollars and foreign fighters to ISIL. Person K was convicted under the Terrorism (Suppression of Financing) Act and sentenced to 33 months' imprisonment for TF in January 2020.

Person jailed 30 months for TF

In September 2019, CAD prosecuted Singapore national A for providing financing to Sheikh Abdullah al-Faisal, a radical preacher in Jamaica who supports the use of armed violence by ISIL. Singapore national A had established communications with the preacher through social media platforms. He intended to support the preacher's cause by transferring a total of S$1,145 (USD823) of his own funds to two intermediaries through a licensed remittance agency and an online payment platform. Singapore national A was convicted in October 2019 under the Terrorism (Suppression of Financing) Act for providing funds to benefit Sheikh, who was facilitating terrorist acts, and was sentenced to 30 months' imprisonment.

Thailand

Use of the internet for TF

Perpetrators used social media to disseminate their extremist ideology and finance their recruitment which often involved small amounts of money. Investigations and intelligence gathering activities have identified encrypted messaging applications as a challenge for authorities to trace and investigate illegal activities. Thai authorities, including the FIU, have been improving their relevant skills and working closely together to share information and monitor illegal activities.

Use of new payment methods for TF

Three persons designated under the Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559 (2016) were reported as attempting to conduct electronic transactions. These designated persons (two from the Thailand list and one from the UN sanctions list) attempted to top-up their e-wallet of an electronic payment service business but their transactions were refused.

Use of third parties

A domestic designated person under the CFT law granted power of attorney to an appointed person for the purpose of conducting financial transactions on his behalf. The attempt was refused by the financial institution.

5.2 Offshore Banks, International Business Companies and Offshore Trusts

Indonesia

RT collaborated with HA and AT in an effort to obtain a number of public funds through securities activities, namely a fixed fund investment discretionary fund mutual fund conducted by SC through Bank CC for Rp1.45 billion (USD100,550). The results of the corruption by RT were converted into several assets including for the interests of Company S through SC in the amount of Rp3.26 billion (USD225,550), a mall complex (in bankruptcy filing), a housing complex, land and a building originating from Securities Co funds through check/Bilyet Giro amounting to Rp4.28 billion (USD295,700) used for the benefit of Company C. In addition, asset placements in the form of investment trusts in several tax-free jurisdictions were identified with total assets worth USD16.5 million. The beneficiaries of the trust structure were RT's family members. These assets generally included property, cash and investment portfolios and insurance policies.

Mongolia

In November 2018, FIU received an information request from a foreign FIU of jurisdiction L concerning domestic citizen B who is an ultimate BO of a legal entity incorporated in jurisdiction A and maintained financial activities in jurisdiction L. The FIU conducted analysis and disseminated information to LEAs within the framework of permission given by a foreign FIU as it was concluded that the information was suspicious. The LEA's investigation revealed that a citizen B, a public official of a state-owned enterprise, while concluding a contract for USD6.5 million, abused his public position and supplied products with a value much higher than the market price and transferred his illicit proceeds to a bank account belonging to a legal entity incorporated in an offshore zone (jurisdiction A). Further analysis by the FIU found that Mr. B had received 25% in his bank account in jurisdiction L out of the contractual amounts the state-owned enterprise sent to foreign suppliers. The LEA opened a criminal case against five subjects conducting further investigations and requested the mutual legal assistance (MLA) from jurisdiction L. Moreover, accounts, savings, withdrawal transactions, movable and immovable assets which may have obtained as proceeds of a crime were restricted from 13 December 2019. In detail, the total amount of approximately USD1.2 million subjects hold in their savings, current accounts at three banks and 11 apartments, three expensive vehicles were seized. The prosecutor's office is preparing to transfer this case to the court.

Pakistan

It was suspected that a suspect was involved in concealing true ownership of funds through benami accounts and channeling of funds. A STR was filed by Bank A on the account of company ABC, which was registered in BVI but maintaining account with Bank A in Pakistan. The suspicion was raised about the true beneficiary of funds as high amounts were routed from the account. The directors of the company were foreigners, while two Pakistanis were

authorized to operate the account in Bank A. During the analysis, high turnovers were noticed in the reported account comprising deposits through clearing of cheques, followed by immediate issuance of banker's cheques. Further, one of the authorized signatory of the account was identified as CFO of another Pakistani company (Company XYZ), and Mr. J the director/chairman of XYZ Company was found to be under investigation by one of the anti-graft LEAs regarding corrupt practices and scams in Pakistan. Moreover, both the individuals (Suspect and Mr. J) were also found connected through common contact details. Therefore, it was suspected that Mr. J was the true beneficiary of account and the funds (as a whole or part) were linked to any scam or corrupt practices by the individual. The financial intelligence was shared with the anti-graft LEA.

5.3 Virtual Currencies

China

From 2016 to early 2018, knowing that offender A had committed financial fraud through the "Energy Californium" operating platform, the four defendants provided him with bank accounts to remit funds abroad and assisted in purchasing real estates, vehicles, insurance and other assets with the proceeds of crime. The total amount involved was more than RMB 120 million (USD17 million), of which nearly RMB 10 million (USD1.4 million) was transferred overseas. The People's Bank of China cooperated with LEAs in conducting ML investigations on more than 3,000 bank accounts involved in the case, and verifying the account information of more than 80,000 bank accounts of 50,752 victims. In November 2019, the local people's court convicted four defendants of ML offences. Among them, defendant B was sentenced to three years in prison with a fine of RMB1.7 million (USD242,350), defendant C two years in prison with a fine of RMB 3 million (USD427,670), defendant D one year in prison suspended for one year and six months with a fine of RMB 155,000 (USD22,100), as well as defendant E eight months in prison suspended for one year with a fine of RMB 105,000 (USD15,000).

Hong Kong, China

Mr B started conducting VA trades for Ms A in 2017. After a few months, Mr B gained the trust of Ms A and persuaded her to set up a cold wallet (i.e. a wallet that is inaccessible online). Ms A then transferred 1,000 Bitcoins to the cold wallet and stored the cold wallet in her safe along with the recovery key. Ms A later found all Bitcoins stolen and reported the case to Hong Kong Police (HKP). An investigation by HKP revealed Mr B had stolen the private and recovery keys of Ms A's cold wallet during the set-up process. Some of the stolen Bitcoins were sold and the proceeds (in fiat currency) were transferred to different bank account in Mr B's name. Mr B was arrested with approximately HKD10 million (USD1.29 million) in bank accounts and Bitcoin accounts withheld. The investigation is ongoing.

Indonesia

In March 2017, the Indonesian Post Office received package shipments intended for Person A originating from the Netherlands. Customs and Excise officials conducted an inspection of the package and found ecstasy which was then reported to the police. The police then disguised themselves as package deliverers (postal officers) and made arrests of Person A. Person A claimed to buy 68 items of ecstasy from a Dutch citizen he knew on Facebook for the price of

1 Bitcoin. The intention and purpose of the suspect to buy the ecstasy pill from the Netherlands was distribution in Indonesia, where one pill from the Netherlands will produce 10 extra pills.

Japan

Criminal proceeds from a specialised fraud were remitted to a bank account opened under the name of Suspect A. Suspect A withdrew this cash and remitted the amount to a VA account opened in an online bank in the name of Suspect B. Subsequently, these criminal proceeds were used to purchase VAs which were then transferred into different accounts.

Korea

KoFIU received and analysed an STR involving the executive director of a VASP (Person A) that flagged high risks of ML and market manipulation between VA dealers. Analysis of financial transaction patterns and problems with accounting transparency revealed potential embezzlement, tax crimes and mixing of funds. KoFIU traced transactions with another VA exchange through the company's accounts and found large transfers to the private bank accounts of the CEO and Person A. The STR and analysis by KoFIU were disseminated to SPO who commenced an investigation. The SPO's investigation revealed that two suspects (Persons A and K) who operated virtual currency exchanges had manipulated the computerised system to make it appear as though billions of KRW in cash had been deposited, thereby deceiving 7,060 victims and illegally acquiring approximately KRW38.2 billion (USD31.9 million) worth of VAs in profit. The SPO prosecuted and detained Person K and others for violating the *Act on the Aggravated Punishment, Etc of Specific Economic Crimes* and other charges in March 2018 and confiscated approximately KRW4.5 billion (USD3.76 million) worth of criminal proceeds from Person K.

Pakistan

The entities ABC Company and XYZ Company were suspected to be involved in mining, trading and providing platform for sale purchase of virtual currency in Pakistan, which is prohibited by the regulators (SBP & SECP). STRs were filed by ABC Bank on the account of company ABC and company XYZ, which were apparently involved in trade of VAs and providing platform to facilitate trading of VAs. Both the companies were registered as software houses but engaged in prohibited activity of mining and trading of VAs. The directors of company ABC were of young individuals and one of them was close associate of a domestic politically exposed person (PEP.) While the directors of company XYZ were husband and wife and both were NICOP (National Identity Card for Overseas Pakistanis) holders and were staying in a foreign jurisdiction. During the analysis, high turnovers were noticed in the reported accounts which comprised of International Bank Fund Transfers (IBFTs) and internet transfers, deposits and withdrawals through ATMs and Cash deposit machines (CDMs). Further, transactions in the accounts were mostly of small amounts but frequency of transactions remained exceptionally high. Moreover, it was reported that the company had received funds from various individuals through internal funds transfers as investment in virtual currencies (Bitcoins).

Based on suspicion raised by the RE and the high volume of transactional activity in the accounts of company ABC & company XYZ, it appeared that the companies were facilitating/ providing platform for trade of VAs in Pakistan. Further, keeping in view the potential involvement of third-party individuals who had invested in such companies for trade in VAs,

the financial intelligence was shared with Federal Investigation Agency (FIA) and Securities and Exchange Commission of Pakistan (SECP) under the AML Act-2010 for action deemed appropriate, to mitigate the apparent risk arising from such type of dealings. Based on the FMU's intelligence the SECP issued warning letters to the concerned companies and initiated the audit of their financial books, while the FIA is investigating the matter in context of ML.

Thailand

Case Study 1:

The Thai Anti-Money Laundering Office (AMLO) in collaboration with the Office of the Attorney General (AGO) and the Royal Thai Police (RTP) investigated a foreign national (Swedish) living in Thailand on a VA (Bitcoin) investment fraud case, following informal information request from the US Internal Revenue Service. The subject was suspected of defrauding victims in the US to invest in Bitcoin with him and subsequently transferred the invested Bitcoin to his wallet opened with a Thai VASP.

AMLO obtained information including bank accounts and wallet transaction information from banks and VASPs. The estimated VAs involved is valued at over a million USD. With the obtained financial information, the Thai authorities were able to facilitate the MLA request from the US to issue warrants for seizing bank accounts and confiscated assets (including the VAs held in the wallet). The subject was arrested and extradited to the US for trial.

Case Study 2:

A multi-national joint LEA operation (i.e. Thailand, Canada & the US) was set up to investigate a case concerning a subject who ran an internet trading platform selling illegal goods from 2014-2017 and used VAs (e.g. Bitcoin) as a mode of payment - both for its members' convenience and anonymity. The investigation revealed that the postal service was used as a channel to deliver goods to overseas. The subject first laundered the illicit proceeds of VAs to fiat currency (Thai baht) before purchasing properties (worth hundreds of millions of baht) in his name. The subject was arrested as a result of multi-national efforts and the assets identified during the investigation were seized by the Royal Thai Police. The Thai authorities are currently handling a subsequent asset recovery request through MLA.

5.4 Professional Services (Lawyers, Notaries, Accountants)

Hong Kong, China

During an investigation of a fraud-related third party ML case, an account holder was convicted of ML involving HKD10 million (USD1.29 million) and sentenced to 30 months' imprisonment in late 2018. A follow-up investigation revealed that a consultant company in Hong Kong, China (Company A) may have been assisting individuals in Jurisdiction X establish companies and open bank accounts in Hong Kong, China for ML purposes and Company A had received over HKD5 million (USD645,150) in 2016 and 2017 for these services. The investigation revealed Mr C (director and shareholder of Company A) had worked in partnership with a secretarial company in Jurisdiction X (Company B). Company B was responsible for linking individuals in Jurisdiction X with Mr C and arranging them to meet in order to establish companies and bank accounts in Hong Kong, China.

Mr C was subsequently arrested with over HKD2 million (USD258,060) withheld in his bank accounts as suspected proceeds of crime. The investigation is ongoing.

Japan

Suspect A raised capital to establish a legal person as the incorporator using criminal proceeds from fraud. The judicial scrivener entrusted to set-up the legal person was not informed by Suspect A that the source of funds was from criminal proceeds.

The Philippines

In 2018, an ASEAN jurisdiction (Jurisdiction A) requested assistance from the Philippine government in relation to an ongoing investigation on two of its nationals alleged to have funnelled funds or accused of funnelling funds to other jurisdictions including the Philippines. The case concerns a ML investigation on the subjects who were allegedly involved in illicit drug trafficking. The matter was referred to the AMLC for appropriate action. In the provided summary of facts, it was stated that nationals of Jurisdiction A conducted large and suspicious money transfers to various jurisdictions involving fictitious import of goods from the Philippines. The subjects allegedly transferred proceeds from illicit drug trafficking to various beneficiaries comprising of 21 entities and two individuals in the Philippines totalling approximately Php1.53 billion (USD30.8 million).

A total of 23 entities and individuals were listed as alleged beneficiaries in the Philippines of the remittances originating from two nationals of Jurisdiction A. However, results in the AMLC database showed that only 14 entities from the list appeared as beneficiaries of funds, which totalled Php1.77billion (USD35.7 million). It is possible that the remittances to the other entities named in the request are below the reporting threshold. Of particular interest are seven entities which have a common contact person or officer / director based on registration documents filed with the Securities and Exchange Commission (SEC). A Filipino lawyer was the identified contact person of six entities. He is also one of the officers/directors of one entity. The nationalities of the partners/incorporators of the seven entities are mostly nationals of Jurisdiction A followed by nationals from two other ASEAN jurisdictions (Jurisdiction B and Jurisdiction C).

The case also revealed that the seven entities affiliated with the Filipino lawyer have several addresses, however, all have a common address in a Makati Building. This is likely the registered office or business address provided by the law firm or lawyer which/who acted as the formation agent of the entities. Further, based on submissions with the SEC, five of the entities provided the corporate e-mail address of the lawyer likely for electronic correspondences. The Filipino lawyer, who is the resident agent/contact person of six entities and an incorporator of one entity, is not registered with the AMLC. The law firm where he is connected is also not registered with the AMLC. Based on the findings it is apparent that the lawyer and the law firm provided services which are within the scope of the DNFBP guidelines.

5.5 Trade-Based Money Laundering and Transfer Pricing

Afghanistan

Upon verification of customs documents, FinTRACA found that the customs documents of company X were forged. FinTRACA developed an analysis of the case and identified that large amounts of USD were credited into the company's accounts in a manner of structuring by several individuals. The bank accounts were then debited by the president and vice-president of company X and large amounts of USD were transferred to different jurisdictions in order to import goods. The company provided commercial banks with invoices, contracts of sale, embarking documents, and customs documents as supporting information for the purposes of importing goods from other jurisdictions. The verification of invoices by FinTRACA showed company X had transferred money through fake invoices from different banks overseas. There was also a significant difference between the customs value of the imported goods and the amounts transferred overseas. FinTRACA disseminated the case to the Major Crime Task Force for further investigation.

Hong Kong, China

In 2015, one of the core members of a drug trafficking syndicate, Mr. A, was charged for manufacturing and importing methamphetamine in Jurisdiction X. Mr. B who worked closely with Mr. A to facilitate the drug trafficking was surfaced. Mr. B resided in Jurisdiction X and his residence was rented under the name of Mr. C, the director and secretary of a trading company (Company D). In the office of Company D in Jurisdiction X, a number of documents which detailed the compilation of false export invoices were seized. A total of HKD100 million (USD12.9 million) crime proceeds in multiple deposits and each transaction below the reportable threshold of Jurisdiction X were found in the Company D's bank account in Jurisdiction X. Part of the money was subsequently remitted to the bank accounts of Mr. C and his family members in HKC. Investigation is ongoing with over HKD1 million (USD129,000) in bank accounts withheld.

Indonesia

Company S is a manufacturing company engaged in the textile industry. Company S has a bonded zone facility where the facility is provided to support the textile industry. Bonded zone facilities are facilities provided to industrial / manufacturing companies whose production is export oriented.

FL as the main director and owner of Company S together with BS as the finance director are known to have committed customs violations in the form of notifying export values greater than the value of goods actually exported. This violation is known from the results of the arrest made by Customs which shows the amount of goods notified by Company S in the export document is greater than the value of the actual goods to be exported. In the period of December 2015 until June 2016, FL has issued approximately 205 incorrect or falsified export declarations, where the amount of goods in the declarations is not in accordance with the number of goods real value exported, the amount in the declarations is far greater than the real goods exported.

Company S has issued processed goods or finished goods whose raw materials come from imported materials without completing their customs obligations and also without the approval of Customs And Excise, where the FL act is a customs crime resulting in state losses in the form of import duties and taxes in the framework of imports (VAT and income tax) amounted to IDR118 billion (USD8.1 million).

Pakistan

Mr. XY is the husband of Ms. XX and both of them are directors in a company which imports parts for its various electronic consumer products from a foreign jurisdiction and assembles such parts locally. Both the individuals are registered for income tax with the tax authorities and their company is also registered with the local company registry. However, very low amounts of tax were paid by both husband and wife while their company did not pay income tax to the tax authorities.The accounts of Mr. XY and Ms. XX and their company were being maintained at the branches of the same bank. Two of the company's local currency accounts were identified, of which one was maintained in jurisdiction where the company's plant is located while another account was maintained in the area where the individuals were residing. Mr. XY and Ms. XX were maintaining their individual accounts in foreign currency separately at the same branch of the bank.

The credits in the company accounts were mainly made via clearing cheques and cash deposits and the withdrawals from the accounts were mainly made via cash cheques and import payments. All the cash withdrawals from these accounts were deliberately made just below the reporting threshold of CTRs which is PKR 2 million (USD12,000), apparently to avoid reporting of CTRs.

High value foreign currency cash deposits were made on a frequent basis in their accounts which were then remitted to another jurisdiction (a tax haven offshore jurisdiction) bordering the jurisdiction from where imports were being made. In aggregate, around USD7 million was remitted abroad via 58 transactions and the remittances were made in two personal accounts of Mr. XY being maintained in these offshore jurisdictions. These remittances were made in a structured manner on a regular basis keeping the amount of transactions remitted mainly of USD150,000 or USD100,000 each with the purpose declared as 'personal use'. It appears that cash for purchasing the USD was withdrawn from their company accounts, as structured cash withdrawals were witnessed from the company accounts on the dates on which cash deposits were made into their USD accounts. Most of the cash transactions were made by an individual working as an accountant in the company.

After analysis of such activity and other supplemental available information, it was inferred that the remittances made from the accounts of Mr. XY and Ms. XX to the offshore jurisdiction were related with the settlement of business payments to evade taxes/duties by incorrectly recording the price of the imported goods and to settle the remaining amount through the FCY accounts maintained in offshore jurisdiction. The predicate offences suspected in the above case were tax evasion and under-invoicing and TBML. The matter was referred to the local tax authority and customs authority simultaneously for investigation.

Singapore

Use of sub-contractors as third parties to launder criminal proceeds

Investigations revealed that a group of employees had cheated their employer, Company A, by awarding contracts to a company they had set up on their own (Company B). This group of employees used Company B to submit inflated invoices to Company A. Concurrently, this group of employees approached several sub-contractors to issue fake invoices to Company B. After payments were successfully disbursed from Company A, Company B would pay the amount due on these fake invoices to the sub-contractors, who would then withdraw the monies in cash and pass them back to the group of employees. These sub-contractors were later given a cut of these illegal profits for their role in the elaborate scheme to layer the monies. Investigations are ongoing in this case.

Thailand

AMLO worked closely with the Office of the Narcotics Control Board, the Royal Thai Police and Thai Customs. A joint operation of RTP and AMLO led to the arrest of Mr. R, an accused person on drug-trafficking charges, in Chiang Rai Province. The case was revealed from Ms. W, one of the suspects of drug trafficker in Rayong Province, who had transferred drug proceeds totalling 200 million baht (USD6.39 million) to Mr. R's bank accounts. According to the money trail, Mr. R transferred money to the bank accounts of Mr. S, a petrol station operator in Mae Chan district of Chiang Rai Province. As a result, AMLO seized Mr. S's assets worth 150 million baht (USD4.79 million). The civil court had the final decision that all the proceeds is vested in the State. According to the financial investigation, AMLO also found that Mr. S transferred large amounts of money which were suspected to be the proceeds of drug trafficking to Myanmar Companies bank accounts which he claimed that the transactions were made for commodities payment such as agriculture products, cars, gold, silver and oil. ML methods used in this case were using a front business to register, conflicting documentation as in invoice, shipment, import invoice, or other documents, phantom shipment of goods and false description of goods. However, the financial intelligence revealed that the commodities payment was used to launder proceeds of drug trafficking from Ms. W.

5.6 Underground Banking / Alternative Remittance Services / Hawala

Australia

AUSTRAC unregistered remittance dealers campaign

Unregistered remittance dealers are committing a serious offence and are at a high risk of being targeted to launder money gained from the proceeds of criminal activities such as: terrorism, human trafficking and forced labour child exploitation, illegal firearm sales, drug trafficking, tax evasion, telephone and email scams, and other types of fraud. AUSTRAC recognises that most remittance service providers want to do the right thing; to assist with this, from September to December 2019 AUSTRAC visited individuals and businesses providing money transfer services across Australia.

AUSTRAC financial intelligence in ML investigation into remitters

AUSTRAC supplied financial intelligence to assist a law enforcement investigation into an extensive international network of remittance service providers laundering millions of dollars out of Australia on behalf of organised crime syndicates and cancelled the registrations of several remittance providers.

Australia-based crime syndicate members used the remittance network to exchange funds obtained through criminal activities for legitimate, or 'clean', funds held overseas. The network, which operated mainly out of India but also had connections to the UK and the US, used Australian bank accounts, corporate structures and complicit remitting agents in Australia and overseas to launder the funds. The investigation identified Australian bank accounts that were receiving multiple cash deposits, structured to avoid triggering any threshold transaction reports by the banks. Further investigation connected the account holders with property purchases, and large amounts of cash suspected to be the proceeds of crime. The funds in the accounts were also shown to be inconsistent with the income tax declarations of the account holders.

Law enforcement in Australia, India, the US and the UK made a number of arrests. Two offenders in Australia were arrested and charged with offences relating to dealing in the proceeds of crime, while three offenders in India were charged on drug trafficking and ML offences. Authorities seized around AUD10 million (USD6.9 million) in assets.

Queensland / Netherlands / Belgium investigation and prosecution

AUSTRAC identified that persons of interest (POIs) were structuring transfers overseas to avoid detection. Structured international funds transfer instructions (IFTIs) were conducted via money remitters identified as providing unregistered remittance services. Remitters, POIs, addresses, patterns in transfers, threshold monitoring, and remitter patterns to same beneficiaries were also identified. As a result of this investigation, eleven persons were charged and illicit drugs totalling AUD301.6 million (USD209.2 million) were seized.

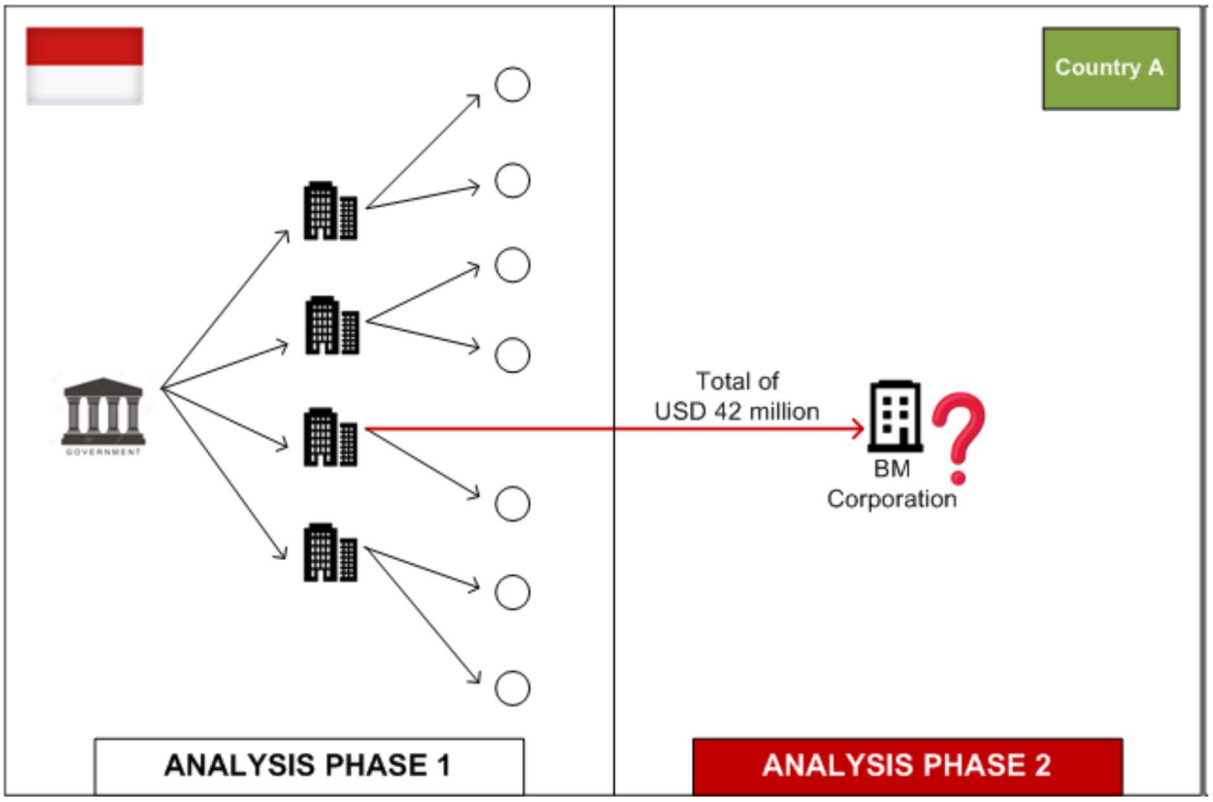
Hong Kong, China

HKP launched a joint investigation with Jurisdiction X against a ML syndicate based in Jurisdiction X using couriers to smuggle drug proceeds into HKC by checked-in baggage. Mr. A was identified as the person to receive the drug proceeds from another cash courier at the Hong Kong International Airport. The cash courier was subsequently interviewed and identified Mr. A as the receiver in HKC to take over the foreign currencies amounting to around HKD5 million (USD645,140). Mr. A took a portion of the cash as his reward and then exchanged the foreign currency to HKD at a remittance agent. Mr. A was subsequently arrested in HKC. Investigation is ongoing.

Indonesia

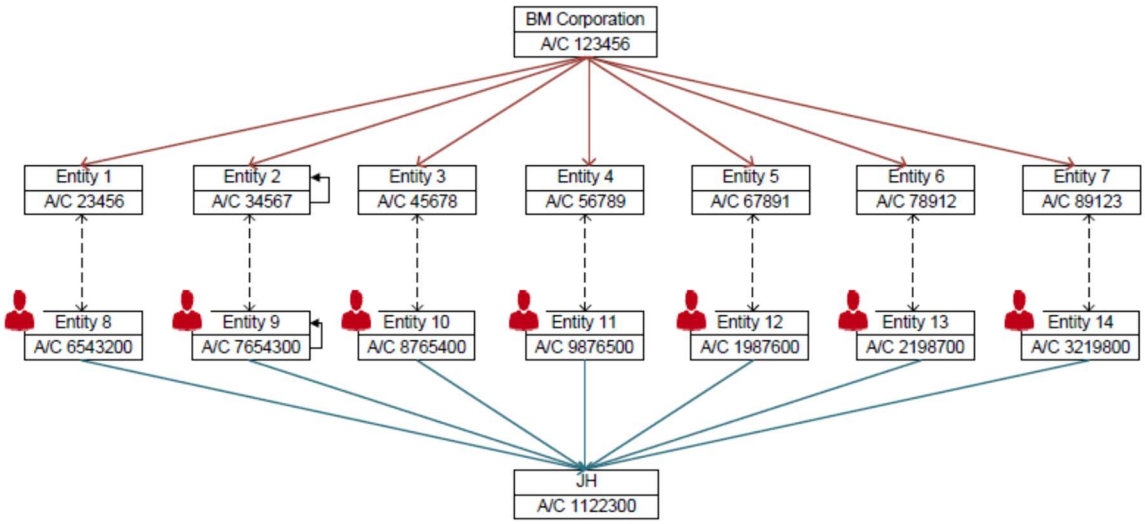
This case is related to the procurement of electronic identity card (E-KTP) in the period 2011-2013 which allegedly amounted to losses reaching IDR2.3 trillion (USD159.2 million). This case involved legislative members, several high-ranking officials from related Ministries and several parties from the private sector. From the investigation process, it was found that there was information regarding the involvement of the Chairman of Legislative Assembly, SN, as

the main offender in this corruption case. From the mapping of the distribution of recipients of project funds, there were significant flow of funds amounting to USD42 million in aggregate as of November 2011 to April 2012 to BM Corporation, a company located in Jurisdiction A (see Figure 1). BM Corporation is a project sub-contractor in charge of providing software tools for the Electronic ID card.



According to information obtained from FIU located in the Jurisdiction A, it was identified that from that amount of USD42 million, BM Corporation transferred an amount of funds of USD7 million to several accounts owned by a number of companies and individuals located in Jurisdiction B. The information was then submitted to the investigator as an entry information for further investigation continued. The investigators then tracked the recipients located in Jurisdiction B. From the results of the investigation, it was found that out of the USD7 million received by several parties in Jurisdiction B, an amount of USD3.5 million were intended as payments for business transactions conducted with their counterparts, which are several entities, located in Indonesia. The investigators then investigated then such counterparts located in Indonesia, and at the same time the Indonesian Financial Transaction Reports and Analysis Center was also tracking transactions on the entities' accounts. At that time the following facts were revealed:

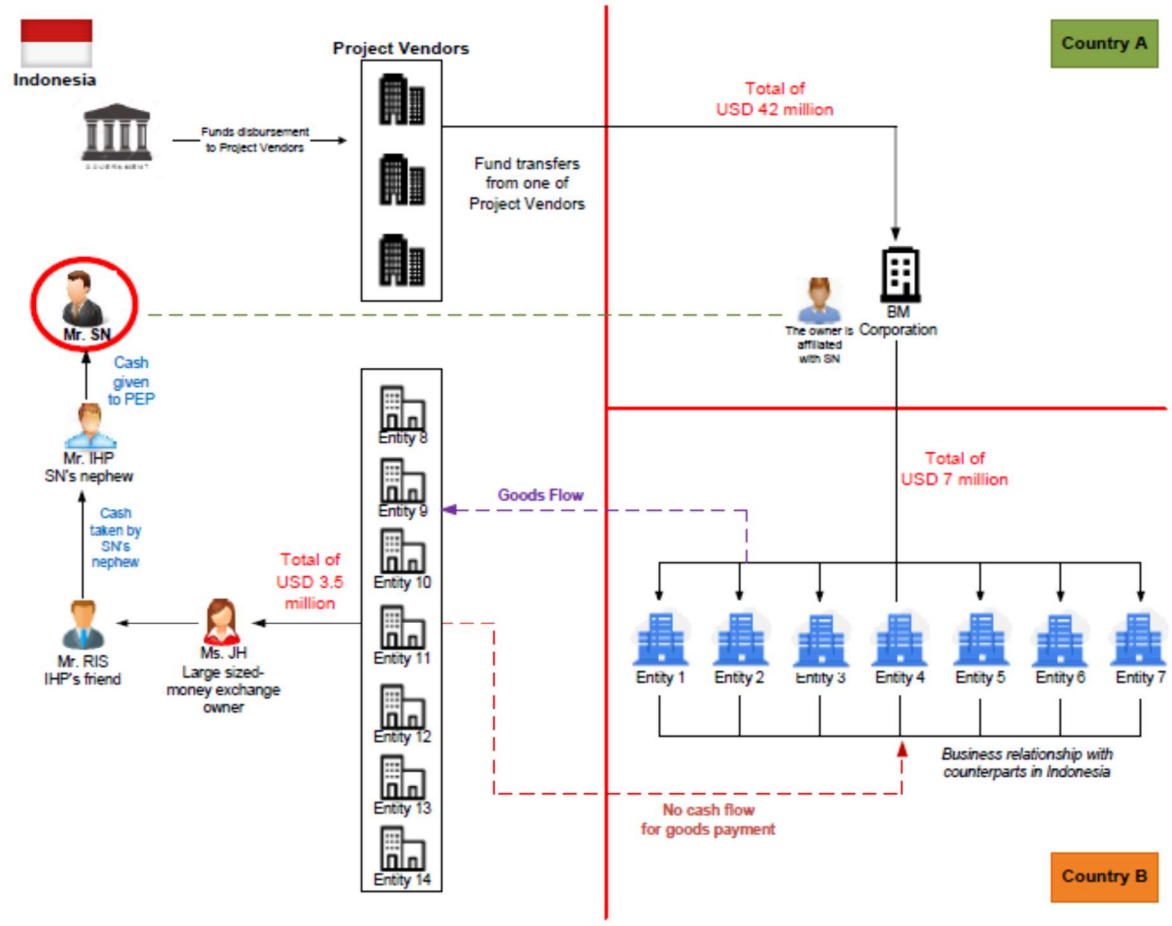
- During that period, the entities in Indonesia were conducting business activities with their counterparts in Jurisdiction B. They requested the assistance of JH (the owner of a large money changer in Indonesia) to pay their business transactions to their counterparts in Jurisdiction B. They transferred the funds to JH to be transferred to Jurisdiction B.
- In fact, colleagues in Jurisdiction B did not receive any payments from JH accounts. Instead, they received payments from BM Corporation.



The investigators then questioned JH and found that the transactions that he received were carried out at the request of IHP, a nephew of SN. The funds are then given in cash to SN. The background of the transaction scheme is as follows:

- IHP ordered BM Corporation to transfer an amount of USD3.5 million as part of the kickback that SN should have received. IHP asked for the assistance of his colleague RIS and said that there were funds abroad that needed to be immediately transferred to Indonesia, but he did not want to use any conventional bank to make the transfer.
- RIS then contacted JH (the owner of a large money changer in Indonesia) to find several entities in Indonesia who were interested/needed to transfer any funds to their partners in Jurisdiction B for business transactions. JH, through RIS, provided the entity's account number in Jurisdiction B to IHP. IHP then advised BM Corporation of that account number.
- BM Corporation then transferred the requested funds to several entities in Jurisdiction B for business transactions that should have been received by the entity. On the other hand, in the same period, the entities in Indonesia also transferred funds to JH's accounts in the same amount as they should have paid to their counterparts in Jurisdiction B. In short, the entities in Indonesia have officially paid for their business transactions, and the entity in Jurisdiction B have also received these payments, even though the source of payments were not their counterparts in Indonesia, but from Jurisdiction A.
- After JH received the funds, the funds then were given to RIS, and RIS gave the funds to IHP in cash. Eventually, IHP received the funds and gave them in hand to SN as the main beneficiary.

The following diagram shows the flow of funds in the scheme:



With reference to the above figure, the funds in Indonesia which were earned through a criminal act (proceeds of crime), were transferred abroad through two jurisdictions (Jurisdiction A and Jurisdiction B), then they were transferred back to Indonesia (reversal pattern), and finally the funds were used as a bribe and paid to SN as a PEP. In principle, the funds abroad remain abroad, and the funds in the jurisdiction remain in the jurisdiction (no official remittance had ever been recorded).

However, the entity abroad managed to send the funds, and the parties in Indonesia succeeded in receiving the requested funds. The transfer schemes are usually used by money changers in Indonesia. Usually, they use such mechanism to facilitate entrepreneurs in making payments for their business transactions, to avoid high transfer fees when using normal banking/transfer services, avoiding taxes or to seek higher profits (using foreign exchange rates). IHP, who knows the mechanism, misused it because he received a kickback from the project. The transaction scheme is clearly an attempt to disguise the transactions to impede tracking and detection of banks and any authorities. Most parties in the scheme were also not aware that the transactions they made were part of a disguised transaction scheme arranged by a third party.

Singapore

CAD investigated three persons for carrying out an unlicensed remittance business between December 2015 and December 2017. Persons A and B were helping Person C to collect the money from persons seeking to transfer money overseas, then Person C would use the money to purchase electronic goods in Singapore and export the goods to Jurisdiction B through

courier companies to resell them for a profit. Thereafter, Person A's brother and Person C would disburse the money to the intended beneficiaries overseas.

Persons A and B were convicted of offences under the *Money-changing and Remittance Business Act* and were fined S$24,000 (USD17,200) and S$12,000 (USD8,600) respectively. Person C was issued a stern warning under the *Money-changing and Remittance Business Act*.

Chinese Taipei

Mr K, the head of a criminal group, and classmates used a legal trading company as a cover to conduct illegal foreign exchange services in order to clean money from unknown sources. They provided a daily RMB remittance service to their clients through dummy Chinese accounts and then provided equivalent amounts in NTD in cash, charging 1-4% in commission. In a single day, NTD39 million (USD1.3 million) was processed resulting in a profit of NTD800,000 (USD27,150) in commissions. From October 2018 to January 2019, NTD600 million (USD20.3 million) was processed with preliminary investigations estimating NTD11 million (USD373,200) in commissions made. A special taskforce investigated the group and in March, Mr K and seven accomplices were arrested with Mr K taken into custody after interrogation.

5.7 Internet (Encryption, Access to IDs, International Banking Etc.)

Afghanistan

Millions of USD were collected from a number of people by a group, with the claim of offering people online services for the sale of currency, shares, gold, fuel, etc. through a fake online system. FinTRACA conducted an analysis of the suspects and found that these individuals were also operating with multiple business licences. These licences and tax identification numbers were the same, despite each company being required to have a separate tax identification number for the settlement of tax duties. Based on the findings of FinTRACA, these individuals were operating with an invalid licence and cash collected through their foreign exchange dealership. The case was disseminated to law enforcement agencies for further investigation.

Australia

AUSTRAC reveals overseas investment scam defrauding Australians

An Australian came to the attention of Romanian authorities for transferring millions of dollars to a business based in Romania. Upon request, AUSTRAC investigated the financial activities and found the person was the victim of an 'advance fee' investment scam. In this type of scam, victims are approached and deceived into sending 'advance fee' payments or giving their bank account details with the promise of money from unlikely sources such as overseas lottery wins or inheritances. The Australian, a man in his 70s had been withdrawing large sums of money from his retirement savings to make the transfers, which AUSTRAC discovered were being made to five businesses in Hong Kong, Bulgaria and Romania. AUSTRAC found multiple complaints about these businesses online, alleging their involvement in an advance fee fraud. A review of their international funds movement revealed another 125 Australians who were likely to be victims. AUSTRAC shared financial intelligence with Fintel Alliance partners,

alerting them to the scam and leading them to blacklist the five overseas businesses. Intelligence was also provided to counterparts in Romania, Hong Kong and Bulgaria to enable them to carry out criminal investigations and help Australian banks and the victims to recover funds.

Northern Territory ML investigation and prosecution

In Australia's Northern Territory (NT), an investigation arose following the NT Police's receipt of reports from the Australian 'Cybercrime Online Reporting Network' about NT residents holding bank accounts that received online fraud proceeds. Investigations determined suspects were holders of accounts that had received the proceeds of cybercrime. All had dealt with portions of these proceeds through international transfers. Investigations uncovered further instances of unreported cybercrime associated with these offenders. There were a diverse cross section of victims with losses up to AUD250,000 (USD173,500). Investigators used search warrants to seize the suspect's devices containing records of communication between co-offenders. This demonstrated the offenders were part of a wider network sourcing stolen identity information, using this to create fraudulent bank accounts and then on selling these to other cyber offenders. The offenders were charged with state-based ML offences and dealing in the proceeds of crime offences.

Hong Kong, China

The electronic system of a money service operator (MSO) in Jurisdiction X was hacked by an unknown culprit via the internet and around HKD41 million (USD5.29 million) was fraudulently transferred to bank accounts of Company A, Company B and Company C in HKC. A second layer account holder was prosecuted for ML offences and was sentenced to 4 months' imprisonment in late 2018. The MSO recovered over HKD3 million (USD387,100) from the account temporarily frozen by HKP. Investigations into other account holders is ongoing.

Macao, China

Several STRs received by FIU revealed that an advertising planning company in Macao received several remittances totaling around USD760,000 from other overseas jurisdictions in the period of October 2016 to July 2017. All the remittances were later requested for refunds since they were reported as having related to fraudulent activities, yet part of the fund had already been withdrawn.

By analyzing the account transaction patterns of the company, the FIU discovered that the company only received several remittances shortly after the account opening, then the funds would mainly be withdrawn in cash. The account movements were not in line with normal business activities and the BO was a non-resident. The FIU inferred that it was a shell company and that the accounts opened were used for laundering criminal proceeds by receiving remittances and then immediately cashing out. Furthermore, the FIU had verified with foreign counterparts that the funds received by the company were related to fraudulent activities. The risk of ML by the company was relatively high. Therefore, the cases were passed to the Public Prosecutions Office.

The Public Prosecutions Office then requested the Judiciary Police to investigate this ML case. A non-resident was found using the name of an advertising planning company to open multiple accounts in two Macao local banks, assisting overseas fraud syndicate to receive criminal

proceeds. Five batches of fraudulent funds had been received from October 2016 to July 2017, three of which totalled around USD490,000 and had been withdrawn by other members of the syndicate. After in-depth investigation, the Judiciary Police discovered that the above fraud syndicate hacked into the computer systems of some companies in other overseas jurisdictions, and sent out fraudulent emails to commit the offence. They also recruited members to open bank accounts in Macao to launder money. From July 2016 to January 2019, the syndicate received a total of 22 batches of fraudulent funds which was equivalent to approximately USD2.84 million. The Judiciary Police had previously apprehended three members of the fraud syndicate, all were involved in ML and fraud offences.

On 20 November 2019, under the aid of the Public Security Police Force for border control, the Judiciary Police arrested the above-mentioned non-resident at the Macao port of the Hong Kong-Zhuhai-Macao Bridge. He confessed committing the crime, claiming to have gained a small profit for laundering the money through bank accounts. The Judiciary Police transferred the involved man to the Public Prosecutions Office for three offences as criminal syndicate, fraud and ML.

Mongolia

A reporting entity submitted a STR to the FIU in April 2019 suspecting that Citizen A had been making suspicious transactions and might be involved in a cyber fraud case. FIU conducted STR analysis on this case collecting information and requesting information from four foreign FIUs, as possible victims were from different jurisdictions, and disseminated the case to a law enforcement agency for further investigation.

It was identified that from June 2018 to December 2018, three citizens and a citizen of Jurisdiction X unlawfully accessed computer systems of a number of foreign legal entities (suppliers). Then, they requested the ordering legal entities to wire payments to their bank accounts of the falsified legal entities which have very similar names with the original supplier entities deceiving that the account number has changed. In order to receive payments to their accounts, subjects incorporated 16 legal entities with similar names in home jurisdiction and opened accounts at domestic banks.

Using their fraudulent accounts, subjects illegally obtained MNT3.6 billion (USD1.27 million) through wire transfers from six legal entities from jurisdictions I, T, I, U and G. During the course of the investigation, the law enforcement agency froze EUR234,000 (USD263,700) in bank accounts and seized two properties worth MNT800 million (USD 282,900) and one mining license. On December 2, 2019, the District court convicted the four offenders on charges of fraud and ML and imposed sentences of six to ten years' imprisonment and confiscation of MNT1.2 billion (USD424,400) for the purpose of compensating damage to a foreign legal entity.

5.8 New Payment Methods/Systems

Australia

Suspicious deposits lead to arrests and frozen bank accounts – Intelligent Deposit Machines

As part of an investigation into criminal networks laundering money in Western Australia (WA), AUSTRAC and WA Police identified two offenders who were depositing and receiving large amounts of cash into their bank accounts. Further investigation showed the funds came from the proceeds of illegal cannabis-growing, and the offenders were arrested and charged.

AUSTRAC and WA Police were investigating the use of intelligent deposit machines by criminal networks to launder money from the sale of methamphetamine in WA. Intelligent deposit machines are a type of ATM that accepts cash and cheque deposits and credits them to the recipient's account. The funds are then available for immediate transfer to other accounts both domestically and internationally.

During the investigation, AUSTRAC identified two people who were making significant cash deposits and receiving large structured ATM deposits into their bank accounts in Perth, WA. Financial investigators and police analysed the bank accounts and found that more than AUD1.2 million (USD832,400) had been deposited over nine months. The investigation linked the funds to cannabis production across WA.

The bank accounts were frozen and police executed search warrants at the offenders' homes, finding and seizing more than AUD10,000 (USD6,940) in cash. The two offenders were charged with dealing with property reasonably suspected of being the proceeds of crime valued at AUD100,000 (USD69,370) or more.

AUSTRAC disrupts large-scale international money laundering syndicate – ATM cash deposits
Bank reporting of Threshold Transaction Reports enabled AUSTRAC to identify patterns of transactional activity consistent with ML. AUSTRAC's financial intelligence and expertise were pivotal in helping law enforcement understand the syndicate's sophisticated ML methodologies and in identifying new suspects throughout the investigation.

AUSTRAC initiated an investigation into a ML syndicate suspected of moving large amounts of cash through a complex network of Australian bank accounts. Sharing financial intelligence with law enforcement agencies resulted in 10 arrests and the imprisonment of a key Australia-based syndicate member. AUSTRAC identified a suspected Hong Kong–based ML syndicate operating in Australia. Over six months a key Australia-based member of the syndicate travelled from Sydney to Perth numerous times to help launder the proceeds of their organised crime. He received money on 13 occasions, collecting up to AUD500,000 (USD346,850) in cash at a time. He then took other syndicate members to banks and ATMs across Perth to deposit cash into a variety of accounts belonging to newly established Australian companies whose directors were Hong Kong nationals living overseas. The money was ultimately transferred to China. A total of 163 bank transactions estimated to be worth AUD29.5 million (USD20.4 million) were made, with the depositors visiting as many as 10 bank branches a day.

A joint-agency task force was set up between AUSTRAC, Australian Federal Police, Australian Border Force and Western Australia Police to identify the source of the deposited

funds and to disrupt the ML. Authorities arrested 10 offenders on ML and drug charges, with the syndicate's key Australia-based member sentenced to 10 years' imprisonment.

Complex State-based ML investigation

Between 2009 and 2015 an individual used card-skimming equipment on ATMs to dishonestly obtain the bank card numbers and personal identification numbers of individuals who used the compromised machines. During this period the individual transferred, or caused to be transferred by other people, over AUD550,000 (USD381,500) in proceeds of the card skimming offending to recipients. The Australian Commonwealth Director of Public Prosecutions prosecuted the individual for a range of offences under the Australian *Criminal Code Act 1995* (Criminal Code), including:

- Dishonestly obtaining or dealing in personal financial information.
- Dealing in proceeds of crime worth AUD100,000 (USD69,400) or more.
- Possession or control of a thing with intent to dishonestly obtain or deal in personal financial information.
- Importation of a thing with intent to dishonestly obtain or deal in personal financial information.

China

In May 2018, the police had arrested a drug transporter, Defendant A, with 96 grams of heroin. During the investigation, it was identified that Defendant A had been arrested several times for drug crime and was jailed twice for drug trafficking. Defendant B, his wife, helped him with ML. Defendant A received drug funds through the mobile payment QR code provided by Defendant B, and Defendant B occasionally transferred the criminal proceeds from the mobile payment account to the connected bank account, and then transferred proceeds of crime to other bank accounts. On June 26 of 2019, Defendant B was sentenced to the crime of transferring drug criminal proceeds and sentenced to eight months in prison.

Hong Kong, China

Case Study 6

Ms. A, a resident of HKC, noted some unauthorized transactions from her credit card monthly statement and reported the case to HKP. Investigation revealed that Mr. B, had impersonated her to open a Stored Value Facility (SVF) account and linked this SVF account with her credit card. Mr. B then used this SVF account to make purchases of high-end products / cash coupons / game points and settled payments with Ms. A's credit card. The merchandises were delivered to Mr. B's associates in Jurisdiction X. Mr. B also transferred funds that were withdrawn from Ms. A's credit card to his associates via P2P funds transfers. The investigation is ongoing.

Case Study 7

Mr. A, with a view to concealing his true identity, submitted bogus KYC documents including identity documents and proof of address of different individuals to the issuing SVF licensee for SVF prepaid cards application. Upon approval, Mr. A would top up these SVF prepaid cards with large amounts of illicit funds from a company in cryptocurrency-related business. These

cards would then be sent to Mr. B, Mr. A's associate in Jurisdiction X. Multiple ATM cash withdrawals were subsequently noticed from these SVF prepaid cards in Jurisdiction X. The investigation is ongoing.

Japan

Case Study 1:

Suspect B converted criminal proceeds from the sales of counterfeit products into electronic money. This electronic money was then transferred via a money transfer service into an account opened in the name of Suspect B's family member.

Case Study 2:

Suspect C, a foreign national illegally in Japan, sold stolen goods under a false name. Suspect C used a new money transfer service to transfer these criminal proceeds to an overseas criminal organisation.

Case Study 3:

Suspect D and accomplices fraudulently acquired the right to use Electronic Money A and subsequently used the right to then purchase the right to use Electronic Money B. The right to Electronic Money B was then resold to a trader who transferred the funds into a bank account opened in the name of a third party. Suspect D then withdrew these funds from the bank account via an ATM.

5.9 Laundering Proceeds of Tax Offences

Australia

Business owner jailed for 'phoenixing' to avoid tax

An Australian Taxation Office (ATO) investigation involving AUSTRAC identified an offender who was carrying out illegal trading known as 'phoenixing'. This involves creating a new company to continue the business of a company that has been deliberately liquidated to avoid paying its debts. Over a 12 year period, the offender operated a labour hire business through four different companies, mainly providing welders to engineering construction companies in Western Australia. After the ATO wound up the first company for non-payment of Goods and Services Tax (GST) and Pay-As-You-Go withholding (PAYGW), the offender created the second company. Once again, he failed to report and pay GST and PAYGW, then abandoned the company without paying its debts and created the third company. He repeated this process to create a fourth company.

To distance himself from the companies, the offender installed family members and associates as directors. He claimed to be managing the business on behalf of these directors and earning a salary of around AUD41,000 (USD28,450) a year. AUSTRAC's analysis of financial data showed that over a number of years the offender had made several significant cash withdrawals totalling AUD1.8 million (USD1.24 million) from ATMs, including an AUD650,000 (USD450,900) cash withdrawal from ATMs at a casino. He also transferred AUD831,000

(USD576,450) from business bank accounts into his personal credit card accounts and other non-company bank accounts. He was charged with three counts of dishonestly causing a loss and 17 counts of obtaining a financial advantage by deception. The offender was found guilty of all charges. He was sentenced to five years and four months' jail, and ordered to pay AUD890,112 (USD617,460) to the ATO.

Complex tax fraud and ML investigation

Operation Elbrus was an Australian Federal Police investigation into tax fraud and ML using complex company structures to facilitate the offending. Eight alleged co-conspirators were charged with fraud and six co-conspirators were also charged with ML. Plutus Payroll Pty Ltd (Plutus) was set up by co-conspirators and offered payroll services on behalf of corporate employers (the client companies). Plutus received gross payroll from the client companies to pay wages/salaries, tax, super etc. Plutus Payroll purported to subcontract with companies incorporated and controlled by the conspirators, collectively known as "Second Tier Companies". Contrived payroll services agreements between Plutus and Second Tier companies purported to make the Second Tier Companies responsible for processing the Client Companies' employees and contractors' payroll funds and paying the requisite PAYGW to the ATO.

ATO states the PAYGW has to be remitted by the entity paying the salary/wages – not necessarily the legal employer. The Second Tier Companies were incorporated by the co-conspirators using straw directors (officeholders in name only). They were controlled by one of the co-conspirators and instructed to open bank accounts in names of Second Tier Companies. A separate office was maintained at a different location where the co-conspirators processed the payroll and laundered the money. Plutus and the Second Tier companies withheld a percentage of the PAYGW owed to the Commonwealth. The funds retained by Plutus and Second Tier companies were transferred to the co-conspirators using false invoices and/or third and fourth tier companies. The key aspects, or means, by which the co-conspirators utilised complex ML methodologies to deal with the proceeds of crime, include:

- Complex corporate structures, false invoicing and legal trusts were used to facilitate phoenixing of companies and to conceal the source and destination of proceeds of crime.
- Professional facilitators such as lawyers, accountants and liquidators were used to layer funds through shell companies and opaque accounting networks, including offshore bank accounts to launder proceeds and avoid law enforcement interest.
- Phoenixing of companies involving winding up a company when it accrued too much tax debt.

Hong Kong, China

Case Study 8

In mid-2016, HKP conducted a fund flow analysis of the companies and bank accounts owned or controlled by a national of Jurisdiction X (Mr. A) and his wife (Ms. B). Investigation revealed that these companies had no actual business operations in HKC that could justify the flow of funds via their accounts. Mr. A and Ms. B may have transferred substantial assets from Jurisdiction X to HKC with a view to evading tax in Jurisdiction X. Mr. A and Ms. B were

arrested and charged with criminal offences in Jurisdiction X. HKP conducted asset recovery action and withheld over HKD140 million (USD18 million) from their accounts. The investigation is ongoing.

Case Study 9

In mid-2016, Jurisdiction X noticed that a syndicate, with a view of evading tax in Jurisdiction X, was arranging its clients to travel to HKC to set up offshore purported "service companies" and "financial holding companies" and to open company bank accounts in HKC. Investigations revealed that the pre-tax profits would be taken from Jurisdiction X to HKC as purported "operating expenses" or "service fees" and then returned to the Jurisdiction X without declaration to overseas tax authority. For clients that did not set up the aforementioned offshore company structure, the syndicate would arrange pre-tax profits to dissipate via their controlled offshore company bank accounts in HKC before funds were returned to the Jurisdiction X. In return, the syndicate charged their clients for a service fee. It was estimated that the syndicate had dealt with a total of HKD150 million (USD19.3 million) by use of the fraudulent schemes. The investigation is ongoing.

Indonesia

LH is suspected to have issued a tax invoice not based on the actual transaction (fictitious tax invoices or FPTBTS) to reduce the amount of VAT owed through a fictitious company namely PT. To facilitate the action, LH is assisted by several FPTBTS sales and couriers. LH sells the FPTBTS at a price of 25% to 40% of the VAT value stated on the invoice. The total value of VAT on FPTBTS that was successfully issued was Rp235,536,504,798 (USD16.3 million).

In addition to the surrender of the LH suspect, the Directorate General of Tax investigators also surrendered the confiscated evidence in the form of documents and assets belonging to the suspect. Assets handed over include, two housing units and one car with the value of the assets approximately Rp5,500,000,000 (USD380,680) related to the ML case.

Korea

An unregistered Korean-Chinese Businessman A, and his older brother Businessman B, purchased Korean duty-free cosmetics without authentic documentation. These cosmetics were then sold in Korea and overseas via social media networks, including WeChat. Payment was received into the accounts of Businessman A, Businessman B and their parents' names without reporting income.

KoFIU identified that Businessman A's account had a deposit of KRW8.6 billion (USD7.19 million) and withdrawal of KRW8.7 billion (USD7.27 million) and most parties to the transactions were non-Korean. Businessman A's account was suspected of being an unregistered foreign currency exchanger and financial transaction information was disseminated to the National Tax Service (NTS). An inquiry by the NTS into the account of Businessman A identified that Businessman A and Businessman B sold cosmetics without authentic documentation (no tax invoices issued) and failed to report income amounts. The NTS detected they failed to report KRW22.3 billion (USD18.6 million) in sales (KRW15 billion (USD12.5 million) by Businessman A and KRW7.3 billion (USD6.1 million) by Businessman B) and collected taxes totalling KRW4 billion (USD3.3 million) (KRW2.7 billion

(USD2.25 million) by Businessman A and KRW1.3 billion (USD1 million by Businessman B).

Pakistan

FMU received an STR from ABC Bank against Mr. S who was conducting a marble business and had very high turnover in his accounts. Based on the STR, FMU conducted a detailed analysis of all reported STRs/CTRs against Mr. S and his business. During analysis, very high turnover was observed in the suspect's multiple accounts maintained with different banks, whereas no tax was paid by him. Based on this analysis, FMU shared financial intelligence regarding Mr. S with relevant LEAs, for suspected predicate offence of tax evasion and ML.

The LEA initiated an enquiry against the suspect and the news of the inquiry also came in the newspapers. Based on adverse media news, additional STRs were reported to FMU by different banks against multiple accounts of Mr. S, along with details of his major counterparts. During analysis of these additional STRs on Mr. S, multiple STRs were found against many of the counterparts with whom Mr. S was conducting transactions, reported by different banks for having inconsistent activity in their accounts. Most of Mr. S's counterparts were general order suppliers and turnover in their accounts was found to be quite high. Based on FMU's analysis, Mr. S and his counterparts were suspected to be involved in Hawala, smuggling and tax evasion.

Moreover, FMU received a request of information from one LEA regarding some accounts which were allegedly being exploited for transnational TF. A search was conducted against these accounts across FMU's database and STRs/CTRs were found against a few of these accounts which were maintained by three different individuals (Mr. X, Mr. Y and Mr. Z). Two of these individuals (Mr. X and Mr. Y) were identified to be the counterparts of Mr. S. Thus, a suspicion was raised against Mr. S and his counterparts for their possible involvement in TF.

Based on new information, analysis of STRs/CTRs of all the suspects was done and a collective very high turnover was noticed in the accounts of all the suspects. The transactional activities in the suspects' accounts were not in line with their profile and transaction with unrelated counterparties in far flung areas (including high risk regions) of the jurisdiction were observed. Many of the suspects were found to be transacting with each other on a frequent basis. Based on FMU analysis, all the suspects appeared to be part of an organized network involved in TF, Hawala/Hundi and smuggling. Thus, financial intelligence on all the individuals was shared with the relevant LEAs and the financial regulator. Based on FMU's intelligence the concerned LEAs initiated inquiries and following outcomes were achieved:

- Taxation Authorities (FBR-IR) registered a case against Mr. Sun and his associates under Income Tax Ordinance 2001 along with Anti Money Laundering Act 2010. The suspects were charged for committing tax theft of more than PKR 1.26 billion (USD7.5 million) over the period of last 5 years.
- Customs Court issued arrest warrants for four accused suspects. The Customs and Taxation's Special Court granted permission to attach ten immovable properties and ten bank accounts of four accused. Further investigation is ongoing.
- Counter Terrorism Wing (CTW) of LEA, initiated an investigation against Mr. Sun and his associates for their involvement in TF and ML. CTW lodged an FIR against Mr. Sun and his associates under different laws including AML Act 2010 and Anti-

Terrorism Act 1997. During the course of enquiry, sufficient incriminating evidence substantiating that the said individuals committed the offence of TF, using channels of Hawala and employing tactics of ML and forgery was identified. The case is under investigation.

- The regulator conducted a thematic inspection covering multiple banks and carried out focused onsite review of the bank accounts and as a result, imposed monetary penalties on multiple banks for violation of AML/CFT Regulations.

5.10 Real Estate, Including Roles of Real Estate Agents

Hong Kong, China

In mid-2017, HKP arrested a drug trafficker with the seizure of 5kg cocaine. The residence of his syndicate head, Mr. A, was raided with a seizure of HKD430,000 (USD55,500) in cash. Investigation also revealed that Mr. A's wife, Ms. B, had purchased a HKD19 million (USD2.45 million) flat in early 2017 and made a down payment of HKD10 million (USD1.29 million). Mr. A and Ms. B were arrested for ML. Further investigation revealed that between 2010 and 2017, eight bank accounts of Ms. B (six personal and two company accounts) recorded total deposits and total withdrawals amounting to around HKD56 million (USD7.2 million) and HKD57 million (USD7.35 million) respectively, with cash deposits over HKD26 million (USD3.35 million). The investigation is ongoing.

Pakistan

XYZ Trading (Pvt.) Ltd (XYZ Company) opened a bank account in ABC Bank and three individuals were identified as signatories to the account. XYZ Company was registered with the Securities and Exchange Commission and engaged in the business of real estate, construction and development. The ABC Bank noted transactions involving large amounts of funds in the account which appeared to be unusual and did not have economic sense with respect to customer's disclosed line of business. The customer was approached by the reporting bank for plausible justification. However, despite repetitive follow-ups, the customer did not provide any valid justification to the reporting bank for the unusual transactions conducted.

The funds were routed among 130 bank accounts maintained by different counterparties of XYZ Company engaged in the real estate businesses. These counterparts included an entity, QRS Company, believed to be the owner of XYZ Company as one of its signatories was common between them. There was also an adverse media report published in a daily newspaper of the jurisdiction that the anti-graft authority of the jurisdiction was investigating the owners of QRS Company in a case regarding encroachment and illegal allotment for a project. The financial intelligence was then shared with LEAs on account of corruption and tax evasion, respectively under the provisions of *AML Act 2010*.

Singapore

Use of criminal proceeds to purchase shares and properties

In February 2019, Person Y, a former employee of Company S, was sentenced to 3 years and 11 months' imprisonment for offences including cheating, falsification of accounts, criminal breach of trust and ML. Investigations revealed that between December 2006 and June 2013,

Person Y had deceived the director of Company S into signing 404 cheques amounting to S$1.9 million (USD1.36 million) and another 37 cheques amounting to about MYR106,000 (USD24,800) issued by a related foreign company. Person Y subsequently used the misappropriated company funds to purchase shares, a car and two apartments. Approximately S$2 million (USD1.4 million), comprising of funds in Person Y's bank accounts, as well as proceeds from the sale of the two apartments, were seized during the course of the investigation and subsequently restituted to the victims.

Vietnam

Brothers A and C were the Director and Chairman of the Real Estate Company M and many of its affiliates. They promoted the sale of real estate projects without the approval of competent authorities and promised to pay high interest rates to customers who deposited cash with the company's treasurer, Treasurer D. Instead, later investments by other customers were used to pay some interest to earlier customers but no land projects were delivered. Under the direction of Brother C, Treasurer D gave the money received from customers to Brother B and other individuals to deposit into their personal accounts. After a short time, Brother B and these individuals transferred these funds back to Treasurer D to deposit in the company account. Some of these funds were then used by Brothers B and C to purchase houses and land with transactions amount to hundreds of billions of dollars.
Brothers A, B and C, Treasurer D and other related individuals have been arrested by authorities under investigation of fraud, property appropriation and ML. Documents for prosecution are being finalised by authorities.

5.11 Trade Gems and Precious Metals

Brunei Darussalam

On nine separate occasions between August and September 2019, Person A induced a victim to deliver to him a total of BND13,980 (USD10,000) by deceiving the victim to believe that the money was used for a gold investment scheme which did not exist. Instead, the money was used by Person A to purchase a boat, a boat engine and to pay off his debt. Only the engine purchased by Person A for BND2,800 (USD2,000) was recovered by the authorities. Person A was charged with nine offences of cheating under section 420 of the *Penal Code Cap 22* and one offence of ML under section 3(1)(b) *Criminal Asset Recovery Order 2012*. Upon pleading guilty, he was sentenced to 8 months' imprisonment for each offence of cheating and 12 months' for the offence of ML. In total, he was sentenced to 36 months' imprisonment. The engine is the subject of a civil forfeiture application under the *Criminal Asset Recovery Order 2012.*

Singapore

Use of family member and precious metals to conceal criminal proceeds

Between 2018 and 2019, 12 people were prosecuted in the largest complex public fraud in Singapore. They were prosecuted for predicate offences and ML offences under the *Companies Act, Penal Code and Computer Misuse and Cybersecurity Acts*. Though four persons had left Singapore before investigations commenced, they returned to Singapore to face prosecution through close collaboration with foreign LEAs.

A public agency responsible for disbursing training grants was defrauded of S$40 million (USD28.67 million) through false claims. The syndicate used nine legal persons to create a veneer that three training institutions had delivered training to more than 25,000 persons. This veneer facilitated the fraud on the public agency and the agency disbursed S$40 million (USD28.67million) in false claims to the bank accounts of these legal people. The illicit proceeds were laundered through cash withdrawals, or layered through a network of mules' bank accounts controlled by the syndicate and withdrawn in cash.

Person N, a key member of the syndicate, enlisted his spouse, Person L's to assist with concealing part of the proceeds handed to her in cash. She in turn converted part of the proceeds into 11 kg of gold, and proceeded to hide S$6.7 million (USD4.8 million) in cash and the 11 kg of gold in her brother's home. Person L's brother played an active role in concealing these illicit proceeds by transferring these proceeds to his friend's home for safekeeping. Around S$18.5 million (USD13.26 million) in illicit proceeds was seized in the course of investigations. Seven people have been sentenced to imprisonment, ranging from 33 months' to 104 months.

Court proceedings for the other five persons are ongoing.

5.12 Association with Human Trafficking and People Smuggling

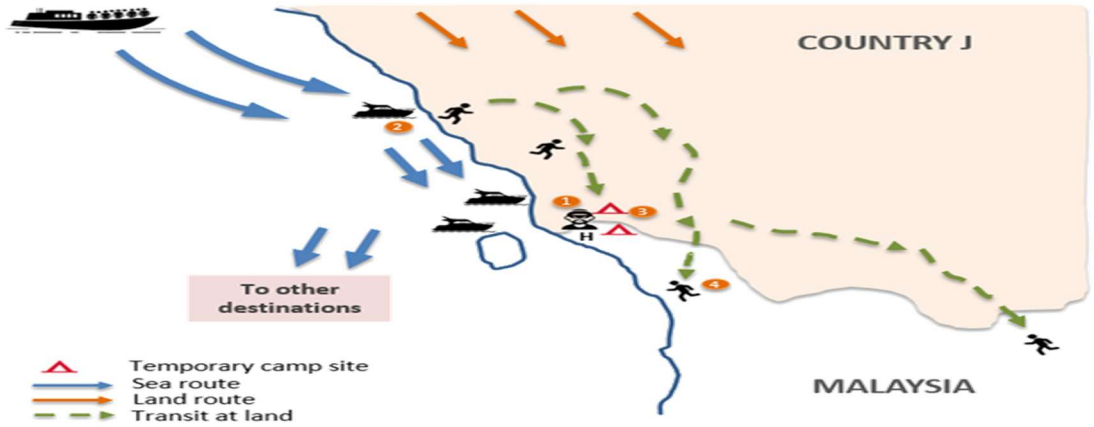
Hong Kong, China

A cross-border human smuggling syndicate member, Ms. A, was arrested. She admitted assisting the syndicate to collect the crime proceeds from human smuggling in HKC and remit to Jurisdiction X on several occasions via a local money service operator. Ms. A pleaded guilty to ML charges (involving a total of HKD 200,000 (USD25,800)) in court and was sentenced to four months' imprisonment in late 2017.

Malaysia

Smuggling of Foreign Workers into Malaysia by sea and transit land route

Mr. H was the mastermind of a human smuggling/trafficking syndicate who had dual citizenship of Malaysia and a neighbouring jurisdiction. He owned/arranged for transport (by boat) to bring in workers from neighboring jurisdictions to Malaysia. Each of the workers would be charged around MYR5,000 (USD1,170) to MYR9,500 (USD2,220) per person. Most of the workers who came in by maritime route were transported to the border and temporarily placed at a jungle camp until the workers made full payment of the fees / cost to the syndicate. Usually the outstanding payments were made by the family members in the home jurisdiction to the syndicate. The common payment methods are by cash, money transfers and illegal remittance. Workers who have made full payment were released and moved along hidden trails before being sent to their next destination. Runners from the syndicate will be waiting for the workers at the entry points in Malaysia to send the workers to various destinations in Malaysia in a car or van. Workers who were not able to complete the payment will be kept in the camp where they may be subject to abuse, torture, killings at the hand of smugglers. Mr. H, the agents, runners and transporters who have linkages with Mr. H were arrested under the Malaysian law.

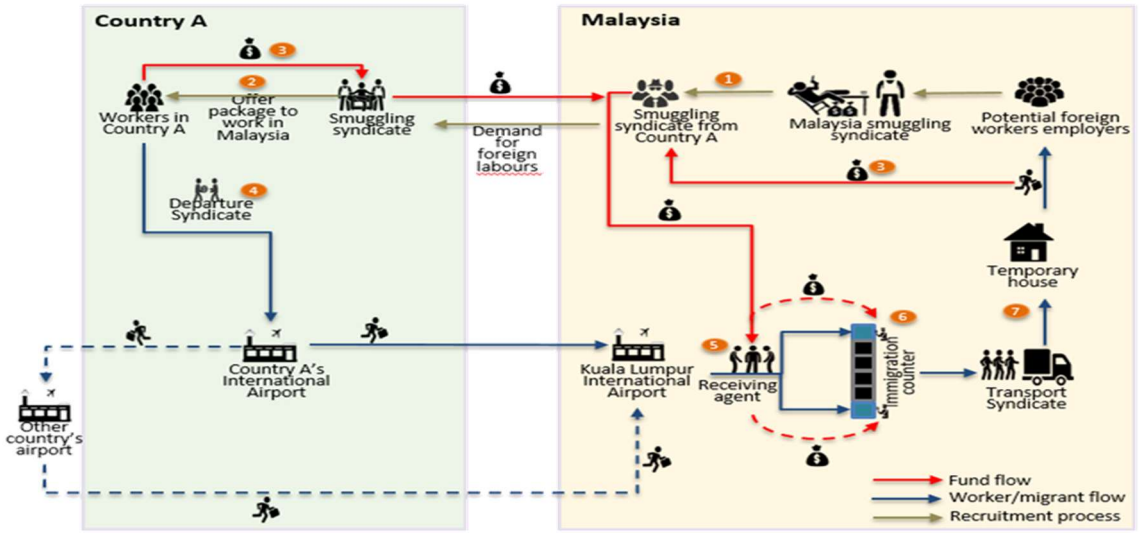


Smuggling of Foreign Workers into Malaysia by Air

Human smuggling syndicates in Malaysia tend to go through human smuggling syndicates of the same nationality of the potential workers i.e. syndicates from Jurisdiction A based in Malaysia would recruit workers in Jurisdiction A, through syndicates in Jurisdiction A. Human smuggling syndicates in Jurisdiction A (or via its agents) source workers who want to come to Malaysia using a social visit pass or study pass to work illegally in Malaysia by offering attractive packages which include flight ticket, passport, social visit visa, sim card for phone, accommodation, offer of lucrative income, employment opportunity around the Klang Valley area in construction, services, manufacturing, etc., to the potential workers.

Workers who agree with the package are required to pay about MYR15,000 – MYR17,000 (USD3,500 – USD3,970) per person. They can pay the amount in a lump sum or half in cash upon agreement with the package. Alternatively, they can pay by installment prior to departure to Malaysia, or once they have started working in Malaysia. There may be more than one syndicate involved to ensure smooth clearance at the immigration counter during departure or arrival process. Once the workers arrive at a Malaysian airport, they will contact the syndicate in Jurisdiction A or in Malaysia to inform them of their arrival. The workers will be requested to wait at certain locations at the airport, while the receiving agent makes arrangements with the immigration counter to ensure smooth clearance for the workers. The receiving agent will inform the workers to use immigration counters, manned by specific corrupted immigration officers who have colluded with the receiving agent. As such, the workers appear to have gone through normal immigration checks carried out by the immigration officers.

Workers who managed to illegally enter Malaysia will be received by the syndicate and transported to temporary housing.



Thailand

In February 2020, seven Thai surrogates and two Chinese nationals were arrested on transnational commercial surrogacy ring. The raids came after the Royal Thai Police found a gang of Chinese nationals hiring Thai women as surrogate mothers. They face charges of colluding in transnational criminal activities and engaging in commercial surrogacy, which is illegal under Thai law. The probe followed a tip-off from the Health Service Support Department about a transnational commercial surrogacy operation. It arranged for the women they hired to be impregnated with donor sperm in a neighbouring jurisdiction, and then returned to Thailand. When they were due, the women were flown to China to give birth and returned to Thailand alone, while the babies were taken by the syndicate. AMLO is in the process of freezing and confiscating the proceeds from the case.

5.13 Nominees, Trusts, Family Members or Third Parties

Hong Kong, China

In late 2014, HKP identified a cross-border bookmaking racket active in HKC and Jurisdiction X. Investigation revealed that the relevant accounts contained suspicious transactions totalling HKD228 million (USD29.4 million) between 2009 and 2015. A joint operation was mounted by the HKP and Jurisdiction X in early 2016 resulting in the arrest of eight people in HKC for ML offences and seizure of over HKD10 million (USD1.29 million) in cash and valuables. Approximately HKD10 million (USD1.29 million) was withheld in bank accounts. The investigation is ongoing.

Indonesia

NL together with his partner, PTH, opened the TM Financial Credit Institution which collected funds from the community with 10% interest for the depositors and then used the funds by lending them to the community with 10% interest. The TM Financial Credit Institution

apparently did not get a business license from the regulator, so it was found guilty of committing a banking crime. During the operation of the business activities, NL successfully recruited 16,155 customers and collected an amount of IDR414 billion (USD28.7 million). Once the funds collected from the MT Financial Credit Institution customers amounted around IDR7 billion to IDR10 billion (USD485,380 to USD693,400), it was then deposited by NL into several bank accounts belonging to the defendant, then it was withdrawn. Furthermore, the money was deposited back into the bank accounts in the name of NL, his wife, his child, and employees with project payment or business purposes as the underlying transactions. NL also purchased three plots of land, two plots of land with residential buildings, one hotel building, three cars, one dump truck and three insurance policies.

Japan

A Boryokudan boss and accomplices sent health food products through a cash-on-delivery service to victims who had not ordered these products. These victims were then forced to pay for these products. These funds were then transferred to an account opened in the name of a third party through staff of the cash-on-delivery service provider.

Macao, China

Suspect B was previously sentenced to imprisonment at the court of Jurisdiction N after being convicted of fraud, attempted fraud and conspiracy to steal. To disguise and conceal the origin of criminal proceeds, Suspect B laundered the fraud-related funds in an obscure and indirect way. He used Jurisdiction N's remittance agents to transfer the illicit proceeds into third persons' bank accounts in a nearby jurisdiction he purchased earlier. Subsequently, he swiped the bank cards of those accounts at stores in Macao for cashing out, withdrawing a total of approximately HKD7 million (USD903,140). A small amount of the money was spent on gambling, while the rest was brought out of Macao.

The Public Prosecutions Office charged Suspect B for ML in 2019. In the course of the investigation, apart from evidence gathering by the Public Prosecutions Office, they sent an MLA request to Jurisdiction N through the court for assistance in investigation and taking of evidence. The judicial assistance rendered by the requested party helped support the existence of the predicate offenses and the movement of proceeds thereof. Suspect B was eventually convicted of ML at the Primary Court of Macao in the same year and sentenced to three years and three months imprisonment. The sentence is now res judicata.

Pakistan

The management of the XYZ Trust opened a PKR account in XYZ Trust's name in ABC Bank in the category of NPO for charity purposes. The aforementioned trust was run by well-known business group. The account was opened for charitable purposes however, numerous high value cash withdrawal transactions were conducted in the account which were not commensurate with XYZ Trust's disclosed profile. On analysis of the statement of account, it was noted that high value outward clearing cheques were credited in the account. The funds were then withdrawn through high value inward clearing cheques on the same or the very next day. This trend was followed for a long period. In addition to the above mentioned account, more accounts maintained by XYZ Trust with other banks, were also identified during the search in the FMU's internal database wherein high volumes of funds had been routed over a period of time.

CNIC numbers of the signatories were searched in FMU's internal database wherein a large number of CTRs, mostly from the accounts maintained in the name of business entities, were found reported on their CNICs from different banks and exchange companies but on the other hand these business entities paid very nominal amount of income taxes.

Signatories of XYZ Trust were involved with multiple businesses. Seemingly they had been running the aforementioned trust for the purpose of charity, however, the high turnover and large number of high value currency transactions suggested that they were evading income taxes. The financial intelligence was shared with income tax authorities under the provision of AML Act.

Singapore

Two foreign nationals charged for recruiting Singaporeans to receive and transfer criminal proceeds

Two foreign nationals, believed to be part of a transnational internet love scam syndicate, recruited two Singaporean women as money mules to receive criminal proceeds of at least S$85,700 (USD61,430) between 2017 and 2018. The money mules withdrew the proceeds in cash and handed over the proceeds to the syndicate members in Jurisdiction M in person. This syndicate was dismantled through Singapore's joint investigation with Jurisdiction M. Close collaboration and timely sharing of information between the law enforcement agencies of both jurisdictions lead to the identification of key syndicate members. Two of the syndicate members were arrested in Jurisdiction M and extradited to Singapore to face charges of abetting others to retain benefits from criminal conduct. The two money mules were charged in court for failing to make a cash movement report when they entered/left Singapore with more than S$20,000 (USD14,330) in cash.

Court proceedings are ongoing.

Chinese Taipei

Mr Z was the owner of Company A and Company B, with Company B established in Hong Kong, China and wholly owned by Company A. Mr Z colluded with his girlfriend, Ms G, to apply for an export loan by falsely trading with other companies based on a triangular trade business structure for the purpose of investing in a United States hotel. Ms G introduced Mr L, owner of Company G registered in China, to Mr Z and they established Company P to act as the supplier. Ms G arranged for Company G to place an order with Company B, which subsequently allowed her to place an order with Company P. After the trade documents were finalised, Mr L presented a letter of credit from Company G and the commercial invoices of Company P to successfully obtain loans in excess of USD89 million from several banks.

After receiving these loans, Mr Z withdrew USD3 million and remitted Company H, a US company controlled by Ms G. Ms G used these funds to purchase a hotel in the United States which was then sold in April 2018 with USD3 million being returned to Mr Z after the liquidation. Mr Z then concealed these funds in the accounts of his daughter and girlfriend. After the investigation by MJIB, the case was referred to the Prosecutors' Office in May 2019 for violations of the Banking and Money Laundering Control Acts.

5.14 Gambling Activities (Casinos, Horse Racing, Internet Gambling Etc.)

Hong Kong, China

In mid-2017, a bookmaking syndicate engaging in online casinos, horseracing and soccer bookmaking activities in HKC expanded its illegal bookmaking network to Jurisdiction X through two HKC brokers who travelled frequently to Jurisdiction X. In mid-2018, 45 people including the mastermind were arrested for bookmaking and/or ML. Approximately HKD2 million (USD258,060) in cash was seized at scene and over HKD1 million (USD129,030) was withheld in their bank accounts. The investigation is ongoing.

Singapore

Conversion of criminal proceeds through gambling activities

While investigating a Singapore bunkering firm, that had been conducting short-supply and buy-back transactions of bunker fuel, for conspiracy to cheat vessel owners into paying for the extra bunker that was not delivered, a parallel financial investigation was initiated to pursue possible ML offences. Investigations revealed that staff of the bunkering firm would receive commissions from their firm based on their transactions. One of the staff members, a programmer, was found to have converted most of his proceeds of crime amounting to around S$1.9 million (USD1.36 million) to casino chips at a local casino. After gambling away some, the remaining chips were encashed and used for payment of housing loans, car loans and insurance premiums. Investigations are ongoing in relation to the ML charges.

5.15 Casino Value Instruments (Casino Chips / Ticket In-Out/Gaming Machine Credits/Cashier's Orders/Casino Cheques/Gift Certificates/Casino Reward Cards, etc.)

Brunei Darussalam

Person B was charged for two counts of cheating under section 420 Penal Code Cap 22 and two counts of ML under section 3(1)(b) of the Criminal Asset Recovery Order 2012. On two separate occasions, Person B cheated two victims into paying him BND50 (USD35) and BND40 (USD28) respectively for the sale of items which he never intended to sell off. Those proceeds of crimes were then converted by Person B into tokens used for gambling using online platforms. He was sentenced to 10 months' imprisonment for each of the cheating offences and 12 months' imprisonment for each of the ML offences. In total, he was sentenced to 2 years' imprisonment.

5.16 Purchase of Valuable Assets (Art Works, Antiquities, Race Horses, Vehicles, Etc.)

Brunei Darussalam

Two judicial officers faced 40 charges for offences of criminal breach of trust by a public servant under section 409 of the Penal Code Cap 22; ML under section 3 of the Criminal Asset Recovery Order 2012; and possession of unexplained property under section 12(1)(b) of the

Prevention of Corruption Act, Cap 131. Initially arrested on 21 July 2018, the investigation into the matter found that the married couple used their authority to unlawfully obtain funds from 255 Judgement Debtors' Official Receiver (OR) accounts between 2004 and 2017. More than BND15.7 million (USD11.2 million) were embezzled and used to fund their lavish lifestyle which included purchases of at least 21 luxury cars and at least 456 high-value assets such as watches, handbags, accessories and shoes. Their funds as well as luxury items were seized.

Intelligence exchange between the FIU and the investigators to determine that a large portion of the funds withdrawn from these OR accounts were deposited in their personal savings accounts. Some of these funds were withdrawn using BND10,000 (USD7,160) notes. Authorities were able to trace the movement of cash using the unique serial numbers of these notes that were recorded by banks when transactions took place. The FIU has implemented these additional reporting requirements towards banks since August 2011, as a measure to mitigate the risks associated with high denomination currency notes. Serial number tracing also proved useful in determining that the two judicial officers used the BND10,000 (USD7,160) notes withdrawn from the OR accounts to purchase luxury vehicles at several car dealers in the jurisdiction. Specifically, currency notes withdrawn by the two suspects were eventually deposited at a bank by car dealers. Additional investigation at the car dealer confirm the transfer of the currency notes between the two suspects to them, based on car purchase records.

Intelligence cooperation with several key partners overseas, specifically with four regional and international FIUs as well as the law enforcement counterparts, also confirmed that some of the proceeds of crime that were transferred to overseas accounts were used to pay rental fees on luxury accommodations and vehicles while the two judicial officers and their family were out of the jurisdiction. In February 2019, charges against the two suspects were finalized in the High Court as follows:

- Fifteen charges of criminal breach of trust by a public servant contrary to section 409 of Penal Code (PCA), Cap 22 against Person E.
- Ten charges of ML contrary to section 3(1) of Criminal Asset Recovery Order 2012 against Person E.
- Charges of ML contrary to section 3(1) of Criminal Asset Recovery Order 2012 against Person F.
- Three charges for possession of unexplained property contrary to section 12(1)(b) of the Prevention of Corruption Act, Chapter 131 against Person E.
- Charges for possession of unexplained property contrary to section 12(1)(b) of the Prevention of Corruption Act, Chapter 131 against Person F.

The two suspects claimed trial to all the charges against them. The trial was heard in September to November 2019. At prima facie stage, the Court ordered for the charges under section 12(1)(b) of the Prevention of Corruption Act, Cap 131 to be stayed. At the conclusion of the trial, the Court found Person E guilty of all charges under section 409 of the Penal Code and section 3(1) of the Criminal Asset Recovery Order 2012. Person F was found guilty of 6 out of 8 charges under section 3(1) of the Criminal Asset Recovery Order 2012. Person E was sentenced to a total of 10 years' imprisonment and Person F to 5 years' imprisonment.

Notice for an application of restraint order under the Criminal Asset Recovery Order 2012 on all seized property has been filed to the High Court with a view that they will be confiscated

under section 60 (conviction-based). Person E and F have indicated that an appeal will be made against conviction and sentence.

5.17 Investment in Capital Markets, Use of Brokers

THE PHILIPPINES

K Inc. is registered before the SEC as a non-stock, non-profit religious organization. K Inc. is said to be collecting investments from the public in the guise of a 'donation'. These donations, according to the founder, shall be used to achieve K Inc.'s mission for the "propagation of the religious faith, establishment of livelihood programs for the benefits of its members." In exchange, donors are promised a 30% monthly return, called "love gifts" or "monthly blessings", in perpetuity. The founder of K Inc. is Mr. J, a former DJ at a radio station in B City in the southern part of the Philippines. Mr. J's wife, Mrs. J, a former public school teacher was the one who administered the so-called donations.

K Inc. was not granted a secondary license by the SEC. Its acts of soliciting investments, therefore, constituted violation of the Securities Regulation Code. An estimated five million people were defrauded by the religious company. Considering that the minimum amount of donation to K Inc. is Php10,000 (USD202) and K Inc. claims that it has five million members, it can be concluded that it amassed an estimated minimum amount of Php50 billion (USD1 billion). Mrs. J administered and transacted the funds by using banks and insurance companies, and by putting up business fronts in various industries to give the investment scam the appearance of legitimacy. These business fronts included K Trading, J Firm, R Corp and JL Inc. In addition, AMLCS investigation revealed that Mrs. J committed layering. She opened several bank accounts which facilitated the inter-account transfers and acquired insurance policies. She transferred significant amounts to different persons and entities with the intention of distancing the hundreds of millions they derived from their Ponzi scheme.

The ML activity of the spouses becomes more evident with the establishment of numerous entities. They used the same to justify the large amounts they have transacted. Moreover, the spouses obtained real properties, motor vehicles and sea vessel, which is part of the subsequent investigation being conducted on K Inc. Several individuals namely H, R, L and the responsible officers of H Corp. and HT Corp. also participated in the ML scheme that Mr. and Mrs. J planned. They directly received millions of pesos either from RLA herself or from the business fronts she has organized as evidenced by the bank documents. Other persons, BT and SD, also benefitted from the unlawful activity manifested in their financial transactions. SD's cryptocurrency accounts were related to the unlawful activity considering the large amount involved and the clear-cut association of SD with K Inc. The investments, amounting to millions of pesos, were mostly done in cash, and were conducted during the commission of the investment scam. The financial investigation revealed the link between the illegal investments and H Corp, HK, RD and HT Corp., through fund movements originating from Mrs. J's accounts to their accounts.

At present, there is an ongoing civil forfeiture case on the subject bank accounts amounting to at least Php110 million (USD2.2 million).

Chinese Taipei

Financier and stock market investor, Mr C, invested in Company Y and took over control of the company in December 2017. In 2017, with the intention of manipulating stock prices, Mr C used capital from Company Y to invest in Companies E, F and G, and borrowed a large amount of money from another financier to facilitate this margin trading. In February 2018, the stock prices of Companies E, F and G dropped sharply and resulted in Mr C's in-debt status. Mr C conspired with Mr D, the owner of Company Y, to embezzle capital from Company Y. In March 2018, Mr T, the representative in Chinese Taipei selling X fund, assisted Mr C to disguise Company Y's investments capital as fake foreign capital and transferred the money to the foreign accounts under Mr C's control in Banks A and B. Mr C then transferred these funds into his own accounts. Mr C instructed Mr T to establish Company S, from which Company Y purchased the X fund and transferred the money into Company S's account in Hong Kong, China. It was estimated that in excess of NTD191 million (USD6.48 million) was purchased from Company S by Company Y between March and May 2018.

After the investigation by the MJIB, the case was transferred to the Prosecutors' Office in June 2019 for violations of the *Securities and Exchange Act*.

Thailand

AMLO in collaboration with the Department of Special Investigation seized assets from the perpetrators who were accused of masterminding online foreign exchange trading scheme. Mr. A. and accomplices took members' money to invest in foreign exchange trading in other jurisdictions with a promise to split the profits, with members/investors getting 60 per cent while the forex company gets 40 per cent, but many victims didn't get those high returns. A total of 11,565 people claimed to have lost approximately 1.585 billion Baht (USD50.68 million) to the scheme and filed complaints to the police. The Transaction Committee issued order to seize assets worth 90.9 million Baht (USD2.9 million).

5.18 Mingling (Business Investment) and Investment Fraud

Indonesia

The convicted company, namely PT. BBU, was appointed as a supplier of goods/services for the City Government, in the fiscal year 2014, of which the contract value amounted to IDR9 billion (USD623,500). The actions of the defendant PT. BBU as a supplier of goods/services in the project had enriched the defendant himself as a company and caused state losses in the amount of IDR3,7 billion (USD256,340). The money obtained from such criminal acts of corruption had been transferred/incorporated by the goods/services user to the account of the defendant PT. BBU in Bank A, so that the funds were mixed with money that had already saved in the account with the aim of concealing and disguising the origin of the assets originating from the corruption crime. The work carried out by the defendant PT. BBU based on the review results of the civil engineering expert were not in accordance with the contract, however the defendant received payments as though the work had been successfully completed.

Such actions of transferring and disguise of the funds into Bank A owned by defendant PT. BBU resulted in the funds obtained from the conduct of criminal act of corruption in the

implementation of the project amounting to IDR3.7 billion (USD256,340) unable to be separated from any other funds obtained from other sources.

Japan

A foreign company was deceived by a fraudulent commercial email and transferred money into the bank account of a legal person managed by Suspect A. Suspect A was able to facilitate the transfer of these funds into the account by way of false explanation to the bank teller and disguising the funds as legitimate business proceeds.

Vietnam

Intelligence gathered from the FIU and other relevant authorities identified that individuals X and Y established Company B to operate an import and export business. Company B was used to smuggle mobile phones and other telecommunications equipment with proceeds from these smuggling activities mixed with the business turnover of Software Company A, which was also owned by individuals X and Y. Individuals X and Y were investigated and prosecuted for smuggling and ML under Vietnam's *2015 Criminal Code*.

5.19 Shell Companies/Corporations

Hong Kong, China

Company A was a garment manufacturing company listed in the HKC Stock Exchange with factories in Jurisdiction X and Jurisdiction Y. In 2006, Mr. B, the chairman and director of Company A, dealt with a total of HKD885 million (USD114.2 million) in a time deposit bank account in HKC held by a shell company registered in Jurisdiction Z. Part of the proceeds was generated from the share option scam and fraudulent sale of Company A's subsidiary company orchestrated by Mr. B. Fund flow analysis was conducted on multiple layers of bank accounts. Mr. B was identified as the beneficial owner who had exercised control over the bank accounts. It was also found that Mr. B had used a stooge to set up a shell company and to open corporate bank accounts to launder the crime proceeds of HKD885 million (USD114.2 million). Mr. B was subsequently arrested and convicted of 'Conspiracy to Defraud', 'Theft' and 'ML'. In mid-2017, Mr. B was sentenced to 11 years' imprisonment and disqualified from being a company director.

Indonesia

Two companies, XYZ Company and MNO Company, conducted bribery by transferring funds totalling EUR6.2 million (USD6.9 million) and USD873,000 through the shell companies of CI Company and SP Company, owned by Mr. B Agent/ Marketing Consultant of XYZ and MNO Company in Indonesia. Some of the funds were transferred to a shell company, WI Company, which was owned by Mr. A (the Indonesian CEO). There were also funds transferred to Mr. C and Mr. D, who were both directors of the Executive Boards of the Company.

Based on further searches it was found that the funds obtained by Mr. A through its shell company were transferred to an account held by Mrs. E in Jurisdiction B (Mr. A's in-laws). Afterward, Mrs. E transferred the funds to several accounts belong to Mrs. F (Mr. A's wife) and Mrs. E in Indonesia. This information also corroborates information that Mr. A is the

beneficial owner of the PWX shell company established in Jurisdiction B. Mr. C (former Director of the Company) received funds from abroad totalling S$514,927 (USD368,950) (in one transaction) and USD1.65million (in 11 transactions) within the period of 2010 to 2016, from foreign parties on behalf of himself and other parties including a law firm called KLM (alleged gatekeeper), and OPQ (shell company). On January 5, 2011 there were transfers from OPQ Company to Mr. I's account (child of Mr. C) and Mrs. L (child of Mr. C) each amounting USD999,980. The incoming funds were then transferred to another account on his own behalf, investment in deposits and securities was carried out, which was then disbursed and transferred to another account on his own behalf and to account that was not yet known to the owner and made cash withdrawals.

Macao, China

Suspect A and other individuals formed a criminal syndicate involved in fraud and ML. To receive the proceeds of the overseas frauds, Suspect A established a Shell Company, Company X, in Macao. Company X had no business activities with any other employee except Suspect A. Suspect A opened several bank accounts in Macao in the name of Company X and received over MOP5 million (USD626,170) of remittances in total. Later, the banks in Macao were notified that the above transfers were derived from frauds; some transactions were reversed while some were lost as they had been withdrawn by Suspect A's accomplices. Suspect A used Company X's bank accounts in Macao to conceal the illegal source of funds and the BOs. Arrested by Macao police in 2019, Suspect A was charged in the same year by the Public Prosecutions Office (MP) for offences of criminal association and ML.

Singapore

Singapore director of shell company prosecuted for failing to exercise reasonable diligence in discharge of director duties

In April 2014, Company M received a wire transfer of EUR339,880 (USD383,500) that was linked to a criminal offence committed overseas. These funds were transferred out of Singapore on the same day. Investigations revealed that Company M had no legitimate business operations in Singapore and was used only to facilitate the laundering of criminal proceeds through Singapore. Investigations also revealed that Company M was incorporated through a Corporate Service Provider (CSP) owned by Person P to fulfil the statutory requirement of having a director ordinarily resident in Singapore. Person P recruited his friend to serve as the Singapore based director of Company M.

In October 2019, the Singapore director of Company M was charged with failing to exercise reasonable diligence in the discharge of his duties as a company director. Person P, as a director of the CSP, also faced the rigour of the law and was charged with abetting the said offence. They were both sentenced to the maximum fine of S$5,000 (USD3,580).

Foreign professional facilitator prosecuted for registering shell companies and opening bank accounts in Singapore to launder criminal proceeds

A foreign professional facilitator was prosecuted for facilitating a complex ML scheme in Singapore through the use of shell companies. He is part of an overseas crime syndicate that was found to have cheated victims of more than US$600,000. He recruited and arranged for foreign nationals to enter Singapore and serve as the registered directors of 13 shell companies

incorporated in Singapore. He also accompanied them to interviews with bank officers to set up bank accounts in the name of these 13 shell companies. The professional facilitator would hand over control of the internet banking tokens for these bank accounts to an overseas resident, Person A. In turn, he would receive remuneration of between US$1,500 and US$5,000 for each Shell Company and bank account he took control over. The bank accounts of these shell companies were subsequently used to launder foreign illicit proceeds through Singapore. The accused was also found to have knowingly provided forged documents such as invoices and bank statements under the name of the foreign directors to the banks to support the accounts' opening. For his conduct, the foreign professional facilitator was sentenced to 88 months of imprisonment for forgery and ML offences. Proceeds amounting to more than USD800,000 and SGD 460,256.94 (USD329,750) were seized from the shell companies during the course of investigations.

Chinese Taipei

Case Study 1

Ms C was the owner in charge of Company S which conducted a triangular trade business by purchasing timber from an Australian company and selling it to China. From November 2016 to April 2017, Ms C established three offshore paper companies A, B and C and instructed employees of Company A to forge documents to sell goods to Companies B and C. Forged bills and invoices were then provided by Ms C to several banks for export negotiations. These transactions were enabled and USD891,823 was provided to Company S. Ms C purchased goods from Companies A and C in the name of Company S and provided forged pro forma invoices and credit to Bank H. A loan to the value of USD1.49 million was authorised by Bank H to Companies A and C.

After the investigation by MJIB, the case was referred to the Prosecutors' Office in May 2019 for fraud and forgery offences.

Case Study 2

Mr L, chairman of Company G, borrowed USD3.2 million from Mr X, owner of Company Z, for his own private use in July 2018. In order to pay off the debt, Mr L conspired with Mr F, owner of Companies A, B and C, to drain funds over NTD115 million (USD3.9 million) from Companies G and D. This was achieved by using the name of Company D to pretend to purchase stocks in Companies A, B and C. Mr L asked Mr F to transfer NTD4.85 million (USD164,700) from Company D to the account of Company B in Bank H. Company B also deposited NTD4.89 million (USD166,050) from Company D and NTD3.8 million (USD129,040) borrowed from a friend. These funds were then transferred to the account of Company Z to pay off Mr L's personal debt. The NTD17.85 million (USD606,140) received from Company D for stocks in Company C was also transferred by Mr L to the account of Company W, also under the control of Mr F. These funds were then distributed into three separate accounts and used to pay off debts and invest in the stock market.

After the investigation by MJIB, the case was referred to the Prosecutors' Office in May 2019 for violations of the *Securities and Exchange Act* and the Money *Laundering Control Act*.

5.20 Currency Exchanges/Cash Conversion

Australia

AUSTRAC links Australian assets to suspects wanted for crimes in China

Following requests for information from AUSTRAC's Chinese counterpart, and law enforcement agencies in Australia and China, AUSTRAC identified a complex international ML scheme run by individuals who were wanted by Chinese authorities on bribery and corruption charges. AUSTRAC financial intelligence analysts discovered that the suspects had put in place complex ML schemes involving structuring of funds through multiple third-party accounts and tax havens, some of which had been placed into the accounts of wealth management and investment companies. The suspects had also received a series of international funds transfer instructions that did not list a jurisdiction of origin. AUSTRAC was able to show that the funds were domestic transfers sent to the suspects from a remittance service provider based in Australia via an offsetting arrangement with a partner remittance service provider in China. The arrangement appeared to be designed to avoid the USD50,000 per annum foreign exchange cap placed on individuals in China. The Australian Federal Police confiscated the suspects' Australia-based assets.

Pakistan

Multiple STRs/CTRs were reported on the individual Mr. ABC, who was the chairman of a well-known pharmaceutical and healthcare products manufacturing company in Pakistan. The individual was engaged in currency exchange transactions and deliberately avoided the SBP threshold of USD50,000 to purchase foreign currency in a single day, through structuring and utilizing different exchange companies. The individual purchased high volume of foreign currencies i.e. USD2 million and AED5 million (USD1.36 million) in a short span of time. During further analysis, it was found that the individual was maintaining multiple local currency and foreign currency accounts at Alpha Bank. High volume of funds were credited to the local currency accounts via clearing of cheques and internal transfers in a short period, which were immediately withdrawn through clearing of cheques and cash in tranches, followed by purchase of USD from open market. The amounts of foreign currencies were deposited into foreign currency accounts in same bank, afterwards the funds were remitted out of jurisdiction to his personal accounts in UAE, Singapore and Canada. Further, the tax history of the individual and associated companies reveals declining trend and apparently do not commensurate the level of transactional activity in the accounts. On the basis of above findings, it was suspected that the subject was involved in unauthorized capital flight and tax evasion. Therefore, the financial intelligence was shared with tax authorities under the *AML Act 2010*.

5.21 Currency Smuggling

Singapore

Money mule smuggled more than S$560,000 of criminal proceeds out of Singapore

Person A acted as an intermediary who provided laundering services. She had allowed her Singapore bank accounts to be used to receive criminal proceeds linked to foreign fraud

offences in exchange for a fee. From December 2012, Person A started to receive significant sums of money in her bank accounts. She transported more than S$560,000 (USD401,240) in cash out of Singapore to another money mule in Jurisdiction M on 4 occasions in January and February 2013. Despite being called up by the Police for investigations, Person A continued to assist to receive criminal proceeds in Singapore, including from other money mules, and subsequently handed over such proceeds to third parties. In total, Person A received at least S$1.6 million (USD1.14 million) of criminal proceeds. In November 2018, Person A was convicted and sentenced to 36 months' imprisonment and a fine of S$8,000 (USD5,730) for the offences of ML and failing to declare the movement of cash out of Singapore.

5.22 Credit Cards, Cheques, Promissory Notes, etc.

Indonesia

LA was a People's Representative Council member. She had a meeting with Director of OAR, Ltd (a Jurisdiction X company engaged in mining and has two mine development projects in Indonesia) to discuss the settlement of the issue of a joint venture (cooperation) of OAR, Ltd with the KUD (Village Unit Cooperative) DTM as the owner of the Mining Business Permit for the development of a gold mining project. Based on the letter of termination of cooperation, both parties agreed to issue funds. LA communicated with the Director and CEO of OAR, Ltd, stating that the OAR Board of Directors agreed to grant funds amounting to USD1.78 million which will be given, in order to overcome the termination of the joint venture contract, where some funds would be used to bribe some regional officials and members of the Council. It would be used so that LA could be chosen as the head of the KUD DTM.

The ML process carried out by LA from the bribe from OAR, Ltd was by placing the proceeds by borrowing the amount from the company's account as a means of holding corruption funds from the OAR, Ltd's company account in Jurisdiction X to an account in the name of MAP Company. Transactions were carried out 5 times from Jurisdiction X to Indonesia through interbank transfers with a total value of USD1.78 million. Furthermore, LA ordered BPA as the representative of OAR, Ltd to break up the funds received into personal accounts in the name of LA through interbank transfers and checks with a total value of Rp15.5 billion (USD1.07 million) and in cash with total amount to Rp20.4 billion (USD1.4 million). The remaining Rp4.63 billion (USD321,650) was managed by BPA on orders, requests and approvals from LA for operational and bribery needs to other parties such as notaries, managers of the KUD and NGOs.

5.23 Structuring (Smurfing)

Australia

International crime-fighting effort smashes global money laundering network

An investigation into a complex international ML operation led to arrests in Australia, India and the UK, and the deregistration of several Australian remittance service providers who were laundering money by substituting legitimate international transfers with the proceeds of crime. A law enforcement investigation identified an extensive international network of remittance service providers laundering millions of dollars out of Australia on behalf of organised crime syndicates.

Australia-based crime syndicate members used the remittance network to exchange funds obtained through criminal activities for legitimate, or 'clean', funds held overseas. The network, which operated mainly out of India but also had connections to the UK and the US, used Australian bank accounts, corporate structures and complicit remitting agents in Australia and overseas to launder the funds. The investigation identified Australian bank accounts that were receiving multiple cash deposits, structured to avoid triggering any threshold transaction reports (TTR) by the banks. Further investigation connected the account holders with property purchases, and large amounts of cash suspected to be the proceeds of crime. The funds in the accounts were also shown to be inconsistent with the income tax declarations of the account holders. Law enforcement in Australia, India, the US and the UK made a number of arrests. Two offenders in Australia were arrested and charged with offences relating to dealing in the proceeds of crime, while three offenders in India were charged on drug trafficking and ML offences. Authorities seized around AUD10 million (USD6.9 million) in assets.

Joint-agency effort disrupts international crime syndicate

AUSTRAC's financial intelligence helped identify the syndicate members involved in ML, which led to their arrest and imprisonment. Trident Task Force – a joint-agency task force involving AUSTRAC, Australian Federal Police, Australian Border Force, Victoria Police, Australian Criminal Intelligence Commission and the Australian Taxation Office – was set up to identify, deter and disrupt serious and organised crime on Victoria's waterfront. During the investigation, AUSTRAC worked within the task force to identify suspicious activities including bulk cash collections and drop-offs, remittances and other transactions. These activities were analysed in conjunction with other information from the task force for indicators consistent with ML associated with drug importation and trafficking. AUSTRAC investigated and identified bulk cash collections, use of multiple third parties (namely students) to conduct multiple same-day 'structured' cash deposits at various financial institutions and use of offsetting to facilitate the movement of proceeds of crime.

As part of an investigation into an international crime syndicate suspected of shipping illegal drugs into Victoria, Trident members discovered almost 100kg of cocaine hidden inside a container that arrived on a cargo ship from Panama. Law enforcement arrested seven people for drug and ML offences, including dealing with property reasonably suspected of being proceeds of crime being more than AUD100,000 (USD69,400) (under the *Criminal Code Act 1995*) and conducting transactions to avoid reporting requirements (under the *Anti-Money Laundering and Counter Terrorism Financing Act 2006*). Law enforcement also seized AUD1.2 million (USD832,700) in cash and property worth AUD800,000 (USD555,130). In May 2018, the primary ML syndicate members were found guilty and sentenced to periods between one and four years' imprisonment.

5.24 Wire Transfers/Foreign Bank Accounts

Brunei Darussalam

Case Study 1

Person C was employed at Company A as a barcode operator. Part of Person C's responsibility included holding on to cash sales money which they were entrusted to deposit into the company's bank account. Sometime between December 2018 and January 2019, Person C had

received the cash sales monies in the sum of BND60,390.80 (USD43,250). Person C did not subsequently deposit the monies to the bank but instead spent the money on their family in the Philippines and for their own personal use. Person C was charged with an offence of criminal breach of trust.

Investigations revealed that between December 2018 and January 2019, Person C remitted BND1,451 (USD1,040) through remittance companies over 10 occasions to their family in the Philippines. Person C was charged for offences of ML under section 3(1) (b) of the *Criminal Asset Recovery Order 2012* in respect of these 10 transactions. Person C was sentenced to a total of 5 years and 4 months' imprisonment for all the offences. Pertaining to the ML charges, Person C was sentenced to 2 years and 8 months' imprisonment for each charge but were ordered to run concurrently to each other.

Case Study 2

Person D was a station manager at Petrol Station B. Person D was entrusted with calculating the sales money which was kept in a deposit box. Person D was then responsible to hand over the money to the security company who would then deposit the sales money into Petrol Station B's bank account. In October 2015, the cash shortage was discovered by the accountant at the said petrol station and was reported to the police. As a result of investigations, it was discovered that between January 2015 and September 2015, Person D in their capacity as a station manager had misappropriated a sum of BND163,800.11 (USD117,300) which were from the proceeds of sales.

Police investigations further revealed that between the months of April 2015 and June 2015, Person D admitted to have remitted the monies through two different remittance service providers in the jurisdiction. Person D pleaded guilty to one charge of criminal breach of trust by clerk under section 408 and 14 charges of ML under section 3(1)(b) of the *Criminal Asset Recovery Order 2012* for the various occasions of money remitted. Person D was sentenced to 40 months' imprisonment for the predicate offence and 16 months' imprisonment for each of the ML offence. In total, Person D was sentenced to 4 years and 8 months' imprisonment.

Indonesia

NA as a Governor has the authority to issue approval for Mining Business Permits. In relation to this authority, NA ordered his colleagues and political consultants to look for a mining company that would be used to obtain the regional reserves, namely AHB Company. It is known that AHB Company was taken over by BI Company, owned by NA's colleague. In the shareholders' general meeting (SGM), it was agreed that the PT AHB was 95% owned by BI Company. After the takeover of AHB Company by BI Company was completed, Nickel mining / production activities were carried out until 2014 producing Nickel 7,161,090 Wet Metric Ton (WMT). Then AHB Company sold the Nickel to RI, Ltd and WVI, Ltd in Jurisdiction X. NA has been proven to have gratified or given bribes from Jurisdiction X entrepreneurs. The forms of gratuity and ML carried out by NA were in the form of insurance policy worth IDR20 billion (USD1.38 million) paid from the ABC Bank on behalf of RI, Ltd in Jurisdiction X through 3 separate transfers to bank accounts with a total value of USD2.5 million.

The modus operandi of the gratuities was by overestimating the insurance policy payment funds, and the excess fund was then placed the in NA's personal account of IDR2,329,106,800 (USD161,400). Furthermore, RI, Ltd transferred funds to the Insurance Policy Account in the

name of NA in the amount of USD2 million. Then, NA's account was used to open two insurance policies, with total value of IDR10 billion (USD693,000), while the rest is transferred to NA's account in instalments totalling IDR7.9 billion (USD550,200). Then, the entire insurance policy was cancelled and disbursed to the personal account in the name of NA and STMA Company accounts in instalments. The form of separation of funds or layering carried out by NA was by opening a company account on behalf of STMA Company and then signing 74 blank deposit slips and 90 blank withdrawal slips. Then, STMA Company's account was used by NA to receive the third disbursement of insurance policies totalling IDR28.6 billion (USD1.98 million) through 72 cash deposit transactions and amounting to IDR1.87 billion (USD129,670) through five cash deposit transactions. The number of gratuities obtained by NA was IDR40.27 billion (USD2.79 million).

The Philippines

Mr. X was arrested in a buy-bust illegal drug operation which led to the confiscation of illegal drugs worth USD1 million. Based on the investigation, the house where he was arrested was bought in cash just a few months before. As revealed, the proceeds of illegal drug trafficking were shown to have been extensively sent through remittance companies, as payment to Mr. X. The latter greatly depended on MSBs, and not banks, in receiving and sending of funds. Further, Mr. X's cohorts in his illegal drug dealing activities, as well as in purchasing real properties using the proceeds thereof, were his close relatives. Records revealed that Mr. X and his relatives were not gainfully employed nor had any registered business to support their purchases of property and substantial transactions with remittance companies. It was also established that several of the remitters of Mr. X were previously arrested for selling illegal drugs.

Singapore

Foreign Scammer imprisoned 12 months in a transnational money laundering case

Person P is a foreign scammer who cheated a victim in the United Kingdom of £350,000 (USD439,400), and thereafter deliberately laundered part of his criminal proceeds through the Singapore banking system. In July 2014, Person P convinced his victim to transfer £350,000 (USD439,400) to a bank account in the United Kingdom for investment. After the funds were received, Person P instructed his accomplice in the United Kingdom to transfer the funds to various overseas bank accounts, including an account maintained by company B in Singapore. Notably, Person P had directed the commission of the ML offences in Singapore whilst overseas. CAD worked closely with its foreign counterparts to obtain evidence that Person P was the actual scammer and prime mover behind this ML scheme. In April 2018, Person P was sentenced to 12 months' imprisonment for abetting the dishonest receipt of stolen property and abetting the transfer of his benefits from criminal conduct.

5.25 False Identification and Documents

Hong Kong, China

In mid-2015, a cross-border ML syndicate made large cash deposits via ATMs into bank accounts which were opened with false identity documents in Jurisdiction X and remitted the funds to HKC in structured sums. Two males (Mr. A and Mr. B) were subsequently arrested

for ML in Jurisdiction X when the duo was depositing cash at an ATM. Cash of over HKD1 million (USD129,030) and several bank cards of different account holders associated with those bank accounts were found in their possession. HKP identified the bank accounts which were used to receive the remittances of over HKD100 million (USD12.9 million) from Jurisdiction X from late 2014 to mid-2015. Several millions in HKD were withheld in one bank account. The investigation is ongoing.

Indonesia

CJK was imprisoned in a correctional institution between June 2017 and March 2018 over a narcotics case. CC is an entrepreneur engaged in the vinegar production business and S is an employee of CC's company. CC was ordered by CJK to open four bank accounts using the names of employees in CC's company, including in the name of S. Initially CC and S did not know that the four accounts would serve as a means of buying and selling narcotics. After three months CC asked CJK about the transfers of large amounts of money and was informed by CJK that as long as he didn't retain the narcotics there were no concerns, indicating that CC was aware that the account was used for drug sales transactions.

To run the narcotics business, CC helped CJK to operate S-owned accounts by transferring to a number of accounts on CJK's orders sent via electronic messages. Furthermore, CJK ordered CC to purchase a number of valuable assets in the form of gold weighing 500.06 grams and gold weighing 850,210 grams.

5.26 Cases from Suspicious or Threshold Transaction Reports

Australia

Timely access to financial intelligence for ML investigations

AUSTRAC assisted Australian law enforcement agencies with a ML investigation involving several Romanian-born Australian citizens who were suspected of trafficking and distributing drugs, and dealing with the illicit proceeds of these activities. AUSTRAC's analysis of the outgoing IFTIs reports submitted by the banking and remittance sector helped identify that the syndicate members remitted more than AUD1 million (USD693,850) offshore over the previous two years. AUSTRAC's analysis of the suspicious matter reports looking at IFTIs to Romania linked this financial activity to the syndicate.
As a result of AUSTRAC's analysis, authorities were able to identify the key member of the ML and drug trafficking syndicate. The main offender was charged with ML and failing to declare physical currency in excess of AUD10,000 (USD6,940) when leaving Australia. The individual pleaded guilty to the charges and was subsequently sentenced to more than seven years' imprisonment.

Joint Commonwealth / State ML investigation

In July 2019, a 36-year-old Sydney man was arrested following an investigation into a ML syndicate based out of Sydney. Officers from the AFP, along with members of the WA Joint Organised Crime Taskforce (JOCTF), arrested the man following warrants executed in Perth, Western Australia. The WA JOCTF is a multi-agency taskforce comprised of the AFP, Western Australia Police Force, ABF, AUSTRAC, the Department of Home Affairs and the ACIC.

It is alleged that the man travelled between Sydney and Perth multiple times to deposit funds totalling AUD7.7 million (USD5.3 million) into bank accounts controlled by a New South Wales man. The 36-year-old man has been charged under the *Criminal Code Act 1995* with one count of dealing in money reasonably suspected of being the proceeds of crime and one count of committing an offence at the direction of an organisation. The maximum penalty for these offences are three and seven years' imprisonment respectively. Further charges are anticipated as the investigation continues. AUSTRAC provided financial intelligence throughout the operation which enabled the criminal's financial activities to be exposed.

Brunei Darussalam

Brunei Darussalam imposed specific measures to mitigate risks associated with the use of BND10,000 (USD7,160) denomination notes in August 2011 to all banks in the jurisdiction. These additional reporting instructions have come to great use in an investigation for Criminal Breach of Trust and ML from 2017 to 2019 whereby the case was successful in securing convictions in January 2020. These additional reporting requirements enabled investigators to link funds withdrawn from a third-party account at one bank to another bank under the suspects' personal bank accounts, as well as to link funds withdrawn from the third-party account at a bank, to a car purchase and subsequent deposit of the cash by car dealers to the car dealers' bank accounts.

Malaysia

Fraud – Business Email Compromise

Around June 2019, the FIU received a suspicious transaction report (STR) on Subject X that an amount of USD220,328.80 had been fraudulently transferred from Victim A in Jurisdiction Y to a bank account belonging to Subject X in Malaysia. Subject X was impersonating an established professional large scale manufacturer of apparel in Jurisdiction Z. The imposters, using fake email addresses, had deceived Victim A into initiating a wire transfer of USD220,328.80 to Subject X's bank account at Bank C in Malaysia. Arising from the STR, the FIU immediately contacted Bank C to block the account from performing any withdrawals. However, Subject X had partially withdrawn the funds via fund transfers to three local counterparties leaving the account with a balance of approximately MYR1,362.38 (USD318). Bank C also managed to block one of the counterparties, Subject Y's bank account with a balance of approximately MYR713,371.68 (USD166,750). 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 established around the same time in early and middle 2019. 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.
- 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.

The case was forwarded to the relevant law enforcement authorities which resulted in accounts of Subject X and Y being frozen and the subjects being investigated.

Singapore

Accountant prosecuted in an embezzlement and laundering case developed directly from STR
In 2017, Singapore's FIU (STRO) received an STR on Person A, who was an accountant of a Singapore-registered company, Company B. STRO's analysis revealed that Person A had deposited multiple cash cheques issued by Company B into his Singapore bank account. Subsequently, the funds were drawn down via cash withdrawals. The cash cheques issued by Company B were each below S$10,000 (USD7,160) and were sequentially numbered. Acting on the STR, CAD initiated an investigation into Person A. Investigations revealed that Person A was authorised to sign singly for Company B cheques of up to S$10,000 (USD7,160). Between April 2013 and June 2017, Person A misappropriated nearly S$4 million (USD2.86 million) from Company B by issuing cash cheques to himself and depositing most of them into his bank accounts in Singapore. Thereafter, he withdrew the cash from his bank accounts and remitted approximately S$3 million (USD2.15 million) to overseas bank accounts in his name and the name of his family and friends on 835 occasions across 241 days, via various remittance agencies.

Person A was sentenced to nine and a half years' imprisonment for offences, including criminal breach of trust and transferring benefits of criminal conduct. CAD seized a total of S$22,008.11 (USD15,760). The rest of the proceeds were either expensed or transferred out of jurisdiction. CAD has sent out a MLA request to follow up on the transferred proceeds.

Thailand

In 2019, AMLO received an STR from a bank regarding a company, Company E, that there were several transactions conducted through internet banking and business cash management system in amount ranged from thousands to million baht. Additionally, transactions through internet banking were more than 30 transactions per day. There were also groups of customers coming to open accounts, a total of 89. And when the bank asked for purposes of account opening, they said the accounts were to receive dividends and product reviewing payment from Company N which has a linkage to Company E. The bank thus suspected that there is an involvement in public fraud and filed an STR.

AMLO conducted a financial investigation and found that there were a large amount of funds flow and at high frequency, and the persons involved were subjects in legal proceedings by the Department of Special Investigation in public fraud cases. Company N was also criticized in social media that their action resembled a Ponzi scheme. Later in November 2019, the police reports to AMLO that Company E involved in the Ponzi scheme. As a result, the AMLO Transaction Committee issued an order on 26 December 2019 to freeze and seize assets of Company E. In total, an amount of over 174 million baht (USD5.6 million) was frozen to further damages to the general public were prevented.

6. EFFECTS OF AML/CFT COUNTER-MEASURES

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

6.1 Impact of Legislative and Regulatory Developments in Detecting and/or Preventing Particular Methods

Afghanistan

Reconciliation of Hawala Reporting

Since MSPs are required to report their large cash transactions (LCTRs) within the specific dates to FinTRACA, the responsible section within FinTRACA established the reconciliation process for Hawala reporting. This was established in the central office and regional offices of FinTRACA. The reconciliation process focuses on the cross reporting of transactions from both sides of the MSP branches to ensure both parties have reported the transaction details of their customer in the specific period under reconciliation.

Since the establishment of the process in 2018, FinTRACA has concluded 28 reconciliation reports, as a result of which 28 MSPs were identified as violators and financial penalties equivalent to 1.4 million AFN (USD18,160) imposed.

FinTRACA Measures in Da Afghanistan Bank (DAB) f auction process

The Center has always played an active role in achieving and maintaining the highest level of integrity and transparency in the Afghanistan financial sector. Remaining steadfast to its commitments to protect the financial integrity of the financial sector, the Center engages itself in the DAB USD auctions process. To promote transparency, FinTRACA has established the following procedures:

- DAB USD Auction Reports Receipt - MSPs and foreign exchange dealers (FXDs) are reporting entities to FinTRACA as per legislation. These sectors are required to report their LCTRs related to DAB USD auctions to FinTRACA via the FX Portal regardless of the amount.
- Enforcement measures of FinTRACA in DAB USD auction Process - As per the enforcement action matrix specific for DAB USD auctions and relevant laws and regulations, FinTRACA takes enforcement measures for non-compliance with auction terms and conditions and minor regulatory violations. These enforcement actions include six permanent exclusions and 54 temporary exclusions for violations of the DAB auction process.
- Enforcement measures concerning discrepancies in auction reporting - FinTRACA notifies the Financial Supervision Department of DAB of any discrepancies observed in the online reporting of USD auctions between the amount purchased from DAB and the amount reported to FinTRACA.
- Watch-list - All entities on the FinTRACA watch-list are prohibited from participating in the DAB USD auction process.

FX Portal

All reporting entities of FinTRACA have electronic reporting systems in place to ensure transparency in reporting and enable reporting entities to report in a timely manner. MSPs and FXDs have recently been provided with an electronic reporting portal called the 'FX Portal'. All MSPs and FXDs are required to register themselves on this portal. The portal is provided in three languages (Dari, Pashto and English) and is easily accessible across the jurisdiction via computers and mobile devices. The FX Portal enables both MSP/FXD sectors and relevant government authorities to further analyse the transactions as prescribed in the AML/CFT laws of Afghanistan. This may assist in identifying and mitigating ML and the use of the sectors by entities designated on UN Sanctions lists. Since the establishment of the FX Portal in 2019, 3,015 entities comprising of 1,610 FXDs, 1,402 MSPs and 3 MSBs have been registered on the portal. In addition, 128,696 reports have been received via the portal. During the implementation of the FX Portal almost 200 training sessions were conducted across 34 provinces by the FinTRACA Regional Operations Team.

To ensure compliance with the registration requirement, FinTRACA instructed all banks to terminate their business relation with unregistered FXDs and MSPs. Non-compliance with the FX Portal requirements has resulted in the revocation of seven licences and the suspension of 16 licences.

Australia

Proposed amendments to Chapter 11 of the AML/CTF Rules

In October 2019, AUSTRAC released proposed amendments to the *Anti-Money Laundering and* Counter-Terrorism Financing Rules Instrument 2007 (No. 1) (AML/CTF Rules) for public consultation. These amendments adjust certain reporting periods and obligations under the AML/CTF Rules. A Bill to amend the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 is currently before Australian Parliament. Relevant amendments include:

- New provisions strengthening correspondent banking protections by prohibiting CBRs with financial institutions that permit their accounts to be used by shell banks, and requiring due diligence assessments before and during all CBRs.
- New Cross-Border Movement provisions consolidating existing reporting requirements for physical currency and BNIs to provide for a single reporting framework.
- New Secrecy and Access provisions to provide a simplified and flexible framework for the use and disclosure of AUSTRAC information to better align with existing operational practice.
- Expansion of exceptions to prohibitions on 'tipping-off' to permit reporting entities to share SMRs and related information with external auditors, foreign members of corporate and designated business groups.

Brunei Darussalam

A number of regulatory developments can be seen since the establishment of Brunei Darussalam's AML/CFT Supervision in 2017. A range of remedial actions and sanctions were imposed in 2019 including issuance of supervisory letters, directions and fines. The most common non-compliance observed was related to failure to submit Cash Transaction Reports,

which has resulted in the issuance of two directions and one fine. Other non-compliance involved deficiencies in AML/CFT framework and transaction monitoring system, and failure to submit STRs. The supervisory actions taken has resulted in improvements in the reporting entities, such as:

- Increased number of STRs submitted.
- Timely submission of CTRs.
- Overall increased investment into AML/CFT compliance including restructuring and expansion of compliance functions, appointment of experts and consultants to review and improve AML/CFT systems and processes.

To demonstrate, Brunei Darussalam previously recorded 403 STR submissions in 2018. This increased to 2,081 submissions in 2019. The STRs submitted are increasingly better quality and have shown improvement in the private sector's detection of suspicious activities. Furthermore, some of these STRs have resulted in several disseminations of intelligence packages to relevant law enforcement agencies, some of which have resulted in assisting ongoing investigations. In addition, Brunei Darussalam saw its first conviction for third-party money laundering under section 3(1)(b) of the *Criminal Asset Recovery Order, 2012* in a 2019 case relating to the sale of a vehicle. In this case, Person A sold a vehicle that was still under financing agreement with a bank to Person B through Person C in order to evade payments to a bank. Person C sold the car to Person B and gave a share of the proceeds to Person A. Person C then proceeded to attempt to remove the vehicle across the border to a foreign jurisdiction. Once convicted, Person C was sentenced to 12 months' imprisonment.

This case paved the way for another conviction in early 2020 relating to a case of corruption, criminal breach of trust and ML where one of the defendants was similarly charged and convicted for third-party ML under section 3(1)(b) of the *Criminal Asset Recovery Order 2012*.

Indonesia

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 VAs in payments and payment systems. However, for investment and/or trading purposes, VAs are still allowed. The regulations requires the Crypto Assets and Digital Gold Traders in the Futures Trading Market to comply with AML/CFT regulations.

Lao PDR

Lao PDR has issued 38 legislative instruments related to AML/CFT with a further four currently being drafted. These legislative amendments have seen three new ML cases investigated.

Macao, China

In order to make AML/CFT guidelines applicable to different sectors in line with the revised FATF Standards, the following guidelines have been revised:

Sector	Effective Date
Notaries and registrars	15 November 2018
Gaming Sector	29 January 2019
Dealers of high unitary value goods; Auctioneers; Company service providers	31 January 2019
Auditors; Accountants; Tax advisers	31 January 2019
Commercial and auxiliary offshore services institutions	1 April 2018
Financial institutions	30 January 2019
Insurance companies; Private pension fund management companies; reinsurance companies, captive insurance companies and insurance intermediaries	31 January 2019
Solicitors	28 November 2018
Lawyers	10 January 2019
Real estate intermediaries	31 January 2019

In regards to the above mentioned revised guidelines, the affected supervisory agencies will engage with the private sectors under their supervision to ensure an effective implementation of the revised guidelines in 2020. Apart from the above, an industry guidance on AML/CFT controls on "gaming-related" customers has been issued by the Monetary Authority of Macao to set out the expected EDD measures that should be applied to these types of high-risk customers. The Gaming Inspection and Coordination Bureau also issued two practical guidance, one which is aimed at prohibiting the attempt to abuse Macao SAR for any ARS operations within junkets and the other aimed at further enhancing the record keeping of junkets as a result of past junket financial accounting reviews conducted.

AML/CFT training sessions covering the revised AML/CFT legal framework, competence of the Financial Intelligence Unit, role of the AML/CFT Working Group as well as explanation of the law "Asset Freezing Regime" and the law "Control of Cross-Border Transportation of Cash and Bearer Negotiable Instruments" have been conducted to raise the awareness of the private sector and the supervisory agencies.

Malaysia

Issuance of Revised AML/CFT Guidelines

Bank Negara Malaysia (Central Bank of Malaysia) revised its AML/CFT Guidelines for financial institutions and DNFBPs which came into effect on 1 January 2020, to increase the requirements on higher risk situation as follows:

Application of full customer due diligence (CDD) requirements for government-linked companies (GLCs) and state-owned companies (SOCs) given the higher potential for involvement in ML risk, particularly corruption, as evidenced by major cases of corruption and abuse of power involving senior and key officers of GLCs and SOCs. Enhanced measures for provision of nominee services by gatekeepers, in which clients requesting nominee services are

automatically subjected to enhanced CDD or enhanced on-going due diligence requirements. This is in view of the higher ML/TF risks associated with the nominee services, which allows criminals to obscure the ultimate control and ownership of legal persons.

Introduction of obligations on casino to impose control measures on junkets in view of the inherent ML/TF risk emanating from the junkets' activities that provide layers of obscurity and less regulation imposed on junkets in Malaysia. The new requirements are introduced to increase preventive control by the reporting institutions as well as to provide better information for LEAs, in the case of investigation. As the new requirements came into effect on 1 January 2020, the assessment of impact could not be ascertain at the material time.

Cash Transactions

Cash transactions remain to be the preferred method by criminals to move illicit proceeds. Recognising the risk of cash, Malaysia has reduced the cash transaction reporting threshold from MYR50,000 (USD11,690) to MYR25,000 (approx. USD5,845) in January 2019, resulting in an increase of almost two fold in the submission of cash threshold reports for that particular year. The National Coordination Committee to Counter ML (NCC) proposes for CTL to be introduced to complement existing financial integrity measures such as the suspicious transaction report (STR) and the cash threshold report (CTR) which will potentially serve as an additional deterrent to further mitigate the abuse of cash for illicit activities, by providing the competent authorities with the requisite tools to further strengthen financial integrity.

Singapore

Legislative and regulatory developments on AML/CFT regime for precious stones and metal dealers (PSMDs)

The Precious Stones and Precious Metals (Prevention of Money Laundering and Terrorism Financing) Act (PSPMA) came into effect on 10 April 2019. The PSPMA led to the appointment of the Registrar of Regulated Dealers within the Ministry of Law (MinLaw) and empowers MinLaw to supervise the PSMD sector for AML/CFT purposes through monitoring, investigation and enforcement. The PSPMA introduces countermeasures against ML/TF by subjecting the PSMD sector in Singapore to a full suite of AML/CFT requirements, including but not limited to:

- Registration with the Registrar.
- Performing customer due diligence (CDD) for relevant transactions, keeping records of relevant transactions and documents, ongoing monitoring of transactions by reviewing information and documents obtained through CDD, and filing cash transaction reports (CTR) and suspicious transaction reports (STR) where appropriate.
- Performing ML/TF risk assessments in relation to the PSMD's business, and developing and implementing controls to manage and effectively mitigate the ML/TF risks identified.

The requirements of the PSPMA were developed in consultation with PSMDs and industry associations, raising AML/CFT awareness within the sector. These engagements, along with various outreach efforts to encourage registration, resulted in the registration of PSMDs in

Singapore by October 2019. In addition, MinLaw conducted extensive outreach through "on-boarding" conferences and provided guidance materials to the PSMD sector, which PSMDs found helpful. Going forward, MinLaw will continue to introduce initiatives to better educate the PSMD sector on their ML/TF risks and their AML/CFT obligations and continue with on-site supervision, with the adoption of a risk-based approach to supervision.
These legislative and regulatory developments will mitigate the vulnerability which the PSMD sector faces in terms of ML/TF threats.

Legislative development to enhance intelligence sharing with FIUs

With effect from 1 April 2019, Singapore has amended Section 41 of the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act* (Chapter 65A) (CDSA) which enables STRO to exchange financial intelligence with FIUs in the Egmont Group without the need for a MOU/LOU, if the following conditions are fulfilled:

- The financial intelligence may be relevant to an investigation into a drug dealing offence or a serious offence in the foreign jurisdiction.
- The foreign FIU is able to provide STRO with financial intelligence upon our request.
- The foreign FIU has given appropriate undertakings for protecting the confidentiality and controlling the use of the financial intelligence.

This will strengthen collaboration among FIUs, to aid in detection of ML activities, its predicates, and TF activities.

Amendment of the CDSA to enhance law enforcement agencies' ability to enforce and prosecute money laundering and terrorism financing offences

On 1 April 2019, the following changes to the CDSA and TSOFA came into force:

- A new ML offence was introduced in the CDSA to criminalise the possession or use of property reasonably suspected of being criminal proceeds, if the accused cannot satisfactorily account for it.
- For ML cases involving overseas crimes, the Courts will now be able to decide on the basis of evidence presented by the Prosecution that a drug dealing or serious offence had indeed been committed in the overseas jurisdiction, without having to rely on foreign governments or experts.
- The scope of prohibited activities under the TSOFA was expanded to include the financing of the overseas travel of an individual to any place to provide or receive any training in facilitating or carrying out any terrorist act.
- Higher maximum fines for ML and terrorism financing offences committed by entities.

These changes strengthen Singapore's anti-ML and counter-terrorism financing frameworks to more effectively tackle such offences, ensuring that our laws remain relevant to the current operating landscape, and provides the necessary legislative powers to quickly detect and neutralise criminal and terrorist operations, and deprive perpetrators of illicit funds.

Amendment of ACRA (Filing Agents and Qualified Individuals) (FA&QI) Regulations 2015 to require mandatory AML/CFT training and proficiency tests for CSPs seeking to be registered

Accounting and Corporate Regulatory Authority (ACRA) has amended the ACRA (FA&QI) Regulations 2015 on 11 May 2018 to require CSPs seeking to be registered from 15 November 2018 onwards to undergo mandatory AML/CFT training and pass a proficiency test before registering or renewing their registration. The training programme encourages CSPs (or 'registered filing agents' as they are also referred to in Singapore) to stay up to date with AML/CFT measures and implement them robustly. Since the introduction of the mandatory training program, more than 2,700 individuals have since completed the training programme. About 2,000 of them had gone on to take the AML/CFT proficiency test and about 82% of them had passed the test and had their registrations renewed. All registered filing agents must sit for and pass the AML/CFT proficiency test before they are allowed to register or renew their firm's registrations.

Regulatory developments with respect to Virtual Assets Service Providers

The *Payment Services Act* (PS Act), which introduces a regulatory regime for VASPs or digital payment token service providers (DPTSPs) as used in the PS Act, came into force on 28 January 2020. DPTSPs licensed under the PS Act are subject to AML/CFT requirements consistent with the revised FATF Standards (i.e. R.15). Entities dealing in virtual assets for investment purposes (i.e. capital market products) are already required to be regulated under the *Securities and Futures Act* (SFA) and to comply with AML/CFT requirements.

The Monetary Authority of Singapore (MAS) had adopted a risk-focused approach in implementing our AML/CFT requirements. ML/TF risks have been identified as the primary risk concerns posed by virtual assets, given the anonymity, speed and cross-border nature of transactions facilitated by VASPs.

Under the PS Act, intermediaries that buy, sell or exchange digital payment tokens (DPTs) in Singapore (or solicit customers in Singapore) are required to be licensed and regulated for AML/CFT. DPTSPs must understand the ML/TF risks they face, and apply appropriate mitigating measures. They are also required to conduct CDD, including the identification and verification of BOs, and implement transaction monitoring measures, as well as report suspicious transactions to the authorities. Given the potential ML/TF risks and nascent regime, Singapore has adopted a stricter zero-dollar CDD threshold (as opposed to the USD/EUR1,000 allowed for occasional transactions under the FATF Standards) for all DPT transactions. DPTSPs also have to comply with the value-transfer requirements for DPT transfers in line with the revised FATF Standards ("travel rule"). In addition, they are required to screen their customers (and beneficial owners) for ML/TF risks and sanctions compliance, as well as screen and submit information on their customers when transferring DPTs to one another on behalf of their customers, and make this information available on request to relevant authorities in Singapore.

Separately, offers or issues of VAs are already regulated by MAS where the VAs are capital market products under the SFA. This includes the financial activities surrounding the issuance of a VA. MAS has clarified its regulatory position on VAs that are capital market products through the issuance of "A Guide to Digital Token Offerings" to provide further guidance on the application of securities laws to offers of VAs in Singapore. MAS also applies a risk-based approach to supervising VASPs in Singapore, which includes a combination of on-site inspections and off-site monitoring and surveillance. MAS' off-site surveillance of higher risk areas in the virtual assets space includes reviewing virtual asset transactions and networks to detect unusual behaviours or suspicious transactions, and to proactively detect entities that may

be operating illegally without a licence. MAS also works closely with law enforcement authorities in Singapore to identify and detect ML/TF typologies and risks relating to the VASP space.

To be aligned with the revised FATF standards for VAs adopted in June 2019, MAS will be expanding the scope of legislation, including the PS Act, to cover additional activities of virtual assets service providers. To this end, MAS will also regulate entities incorporated in Singapore providing virtual assets services (i.e. those relating to payments and/or investments), solely outside of Singapore. As VA activities and its ML/TF/PF risks continue to evolve with new business models emerging, Singapore authorities, including MAS, are closely monitoring the risks posed and will continue to take necessary steps to mitigate these risks.

Chinese Taipei

In 2019, the FSC revised the AML/CFT questionnaire to integrate the information mentioned in Chinese Taipei's NRA, and updated the risk rating and risk profile of financial institutions in early 2020.

Regarding the enhanced cooperation between law enforcement and private sectors, the FSC has asked relevant financial industry associations to hold compliance forums periodically and invited law enforcement and tax authorities to share ML typologies of tax crime and illegal remittance, types of sanction evasion, and financial investigation cases in 2019. These measures could make financial institutions better understand risk and threat and effectively assist law enforcement authorities to trace proceeds of crime. The FSC will continue to implement its AML/CFT Strategy Map, review the related regulations to conform to international standards, and supervise the financial institutions to comply with AML related regulations and implement AML/CFT works.

Recently, Chinese Taipei passed the *Amendments to the Money Laundering Control Act (MLCA)* and *Counter-Terrorism Financing Act (CTF Act)* on November 7, 2018. The amendments to MLCA mainly includes enterprises handling virtual currency platform or transaction to AML/CFT regime. Besides, based on the newly released amendments, financial institutions and the DNFBPs should establish the AML/CFT 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.

Thailand

In order to strengthen preventive measures at the initial stage of conducting transactions, the Bank of Thailand issued notification no.19/2562 on KYC for opening deposit accounts of in FIs, enacted on 3 September 2019. AMLO has developed "AMLO Person Screening System" or APS which is available on AMLO website and mobile application. The APS aims to promote more compliance with AML/CFT requirements for REs and the public by facilitating the implementation of sanction screening requirement in relation to terrorism and proliferation of WMD.

7. 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
APG	Asia/Pacific Group on Money Laundering
ATM	Automatic Teller Machine
AUSTRAC	Australian Transaction Reports and Analysis Centre
C&ED	Customs and Excise Department (Hong Kong, China)
CDD	Customer Due Diligence
CFT	Countering the Financing of Terrorism
CTR	Cash/ Currency Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group
FATF	Financial Action Task Force
FINTRAC	Financial Transactions Reports Analysis Centre (Canada)
FIU	Financial Intelligence Unit
FMU	Financial Monitoring Unit (Pakistan)
FPTBTS	Fictitious tax invoices (Indonesia)
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
MJIB	Ministry of Justice Investigation Bureau
ML	Money Laundering
MR	Money Remitter
MSP	Money Service Provider
NCC	National Coordination Committee to Counter Money Laundering (Malaysia)
NGO	Non-Government Organisation
NPO	Non-Profit Organisations
NRA	National Risk Assessment
PS	People Smuggling
PEP	Politically Exposed Person
PKR	Pakistan Rupee
POI	Person of Interest
RI	Reporting Institutions
SAR	Suspicious Activity Report
SEC	Securities and Exchange Commission (Philippines)
STR	Suspicious Transactions Report
SVF	Stored Value Facilities
TF	Terrorist Financing
VAT	Value Added Tax