APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2021

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

July 2021

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

Tel: +61 2 5126 9100
Email: mail@apgml.org
Web: www.apgml.org

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 to 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 Each year APG members and observers provide case studies, observations on trends, research, information on regulatory enforcement action, and examples of international cooperation. The information collected provides a basis for further study of particular and high priority topics.

3 The case studies featured in this report are a small part of the work by law enforcement and intelligence agencies 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.

4 This report includes a brief chapter on understanding risks associated with proliferation financing in light of the amendments to Recommendation 1 and its Interpretive Note (INR.1) adopted by the FATF on 23 October 2020.

5 The APG Operations Committee has oversight of the typologies research programme and is Co-Chaired by Samoa and New Zealand (2020-2021).

1. PROLIFERATION FINANCING RISK

1.1 Risk Assessments and Proliferation Financing

Until recently, the FATF framework used a foundation of risk to assess responses to ML and TF This expectation did not extend to proliferation financing (PF). On 23 October 2020, the FATF adopted amendments to Recommendations 1 and 2 (R.1 and R.2) to require jurisdictions, financial institutions (FIs), designated non-financial businesses and professions (DNFBPs) and virtual asset service providers (VASPs) to identify and assess the risks of potential breaches, non-implementation or evasion of the targeted financial sanctions (TFS) related to PF, as contained in FATF Recommendation 7 (R.7), and to take action to mitigate these risks. In this context, the typologies related to PF TFS have attracted renewed interest.

Obligations aimed at countering the financing of proliferation of weapons of mass destruction (WMD) under R.7 focus on jurisdictions'' implementation of two jurisdiction-specific regimes created by United Nations Security Council Resolutions (UNSCRs): the Democratic People's Republic of Korea (DPRK)[1] and Iran.[2] Broadly, R.7 requires jurisdictions to freeze, without delay, the funds or other assets of, and ensure that no funds and other assets are made available, directly or indirectly to, or for the benefit of (a) any person or entity designated by the United Nations Security Council (UNSC), (b) persons and entities acting on their behalf or at their directions and/or (c) those owned or controlled by them.

PF risks as set out in R.1 include:

- The risk of a potential breach or non-implementation of TFS: this risk may materialise when designated entities and individuals access financial services, and/or funds or other assets, as a result, for example, of a delay in communication of designations at the national level, lack of clear obligations on FIs and DNFBPs, failure on the part of FIs and DNFBPs to adopt adequate policies and procedures to address their PF risks (e.g. weak customer on boarding procedures and ongoing monitoring processes, lack of staff training, ineffective risk management procedures, lack of a proper sanctions screening system or irregular or inflexible screening procedures and a general lack of compliance culture);

- Risk of evasion of TFS: this risk may materialise due to concerted efforts of designated persons and entities to circumvent TFS (e.g. by using shell or front companies, joint ventures, dummy accounts, middlemen and other fraudulent intermediaries).

This chapter provides a brief introduction to the new obligations and an overview of typological and risk assessment work being undertaken in our region or relevant for our region. In particular, the APG has collaborated with the Royal United Services Institute (RUSI) to showcase some research on PF typologies and PF TFS implementation.

[1] *See* UNSCR 1718 (2006)
[2] *See* UNSCR 2231 (2015)

1.2 Amendments to the Standards

The new elements of R.1 require governments to identify, assess, and understand the PF risks for the jurisdiction, in addition to existing requirements under R.7 in relation to TFS frameworks. The amendments also require jurisdictions to place obligations on FIs, and DNFBPs and VASPs to identify and assess the risks of potential breach, non-implementation or evasion of TFS when dealing with their customers, and taking appropriate mitigating measures in line with the level of risks identified.[3] Importantly, in the context of R.1, 'PF risk' refers strictly and only to the potential breach, non-implementation or evasion of the targeted financial obligations referred to in R.7.

The FATF published its 'Guidance on proliferation financing risk assessment and mitigation'[4] on 29 June 2021 to assist the public and private sectors in implementing the new requirements to identify, assess and mitigate PF as defined in R.1 and INR.1.[5] Notably, this 2021 Guidance provides an updated list of key indicators relevant to identifying instances of PF.[6]

The changes to the FATF Recommendations will come into effect for the purposes of the 4th round of APG mutual evaluations.[7]

1.3 UN Panel of Experts Reports

As noted above, the obligations in the FATF under R.7 relate to UNSCRs that focus on two specific jurisdictions: DPRK (UNSCR 1718) and Iran (UNSCR 2231). In endorsing the Joint Comprehensive Plan of Action, UNSCR 2231 terminates previous provisions of resolutions relating to Iran and WMD proliferation, including UNSCRs 1737 (2006), 1747 (2007), 1803 (2008) and 1929 (2010), but retained TFS on a number of individuals and entities designated pursuant to these resolutions and also established new specific restrictions, including a number of other measures. However, the obligations in relation to DPRK remain broad.

The UN Security Council 1718 Sanctions Committee is tasked with oversight of the sanctions measures designed to prevent the DPRK from accessing materials and items for their WMD programmes. The Committee is supported by a Panel of Experts responsible for gathering information from member states and other sources on the implementation of the 1718 sanctions and where there have been examples of non-compliance.

---

[3] https://www.fatf-gafi.org/publications/financingofproliferation/documents/statement-proliferation-financing-2020.html

[4] https://www.fatf-gafi.org/publications/fatfrecommendations/documents/proliferation-financing-risk-assessment-mitigation.html

[5] https://www.fatf-gafi.org/publications/fatfgeneral/documents/public-consultation-proliferation-financing-risk.html

[6] *See also*, FATF's 2008 Typologies Report on Proliferation Financing (accessible at https://www.fatf-gafi.org/publications/methodsandtrends/documents/typologiesreportonproliferationfinancing.html), and the FATF's 2018 Guidance on Counter Proliferation Financing - The Implementation of Financial Provisions of United Nations Security Council Resolutions to Counter the Proliferation of Weapons of Mass Destruction (accessible at https://www.fatf-gafi.org/publications/financingofproliferation/documents/guidance-counter-proliferation-financing.html)

[7] As part of a phased approach, FATF will begin assessing jurisdictions for implementation of these requirements at the next (5th) round of mutual evaluations, to allow time for governments to take the necessary domestic measures.

The Panel of Experts produce a report, which is generally issued as a mid-term and final report,[8] detailing the trends and methodologies by which DPRK has sought to obtain the resources required to further their nuclear, ballistic and other WMD programmes. These reports have observed the activities DPRK employs to obtain both the materials (including dual-use goods) and the technology (including the intellectual property of foreign experts) to support and expand the proliferation of WMD. Importantly, these reports have a section, typically titled 'Finance', specifically dedicated to the manner in which DPRK is able to access international financial systems. Funds raised from sanctions evasion activities and laundered through these networks support the DPRK's nuclear, ballistic and other WMD programmes.

The Panel of Experts Report gathers, examines and analyses open source material, information from proactive and reactive submissions of UN member states, relevant UN bodies and other interested parties regarding the implementation of the measures, and in particular, on incidents of non-compliance to identify the methods by which DPRK accesses these materials. Where the Panel of Experts investigation reveals the suspected involvement of an entity or person in a member state, it will make a request to the member state for further information or action. The Panel of Experts also receives information and data proactively from member states to assist in its investigations.[9]

In recent years, the reports have identified emerging and changing trends and typologies utilised by DPRK to facilitate its PF including some of note to the APG membership. DPRK continues to utilise complex corporate vehicles, including joint ventures, offshore accounts, shell companies, and overseas banking representatives to disguise its ongoing **access to international finance systems** in order to raise funds and further its PF activities. Lastly, the increasing use by DPRK of **cyber activities against FIs** targeting virtual assets (VAs) and virtual asset service providers (VASPs) and exchanges including the theft and laundering of cryptocurrencies into fiat currencies is becoming a significant PF typology.

[8] https://www.un.org/securitycouncil/sanctions/1718/panel_experts/reports
[9] https://www.un.org/securitycouncil/sanctions/1718/panel_experts/work_mandate

RUSI: CRYPTOCURRENCY AND PF

The use of cryptocurrency to evade sanctions and raise revenue is a feature of modern day PF. In 2019, RUSI published a landmark study on DPRK's cryptocurrency activities in Southeast Asia.[10] This study set out the various steps in PF where cryptocurrencies can be abused:

- Acquisition: Cybercrime is unquestionably the most prevalent method of sanctioned actors obtaining cryptocurrencies, especially by hacking cryptocurrency exchanges in East Asia. DPRK has also been involved in ransomware campaigns, such as WannaCry,[11] and has been particularly interested in phishing and online fraud in the last few years.[12]
- Movement typologies: Like traditional money laundering, large-scale cryptocurrency launderers such as DPRK use layering as a technique.[13] Attackers create thousands of transactions in real time through one-time use cryptocurrency wallets.[14] They are then able to muddy their tracks and break the transaction path.
- Exchanges: It has become increasingly clear that DPRK relies heavily on unregulated[15] or noncompliant[16] exchanges to launder funds, as well as peer-to-peer exchanges. Lack of regulation in many jurisdictions makes this pursuit relatively easy.
- Liquidation speed: DPRK generally cashes their cryptocurrency into fiat currency or another cryptocurrency relatively quickly,[17] with liquidation speed increasing recently. There appears to be little interest in stockpiling cryptocurrency for future use.
- Scale: According to the most recent analysis,[18] DPRK hackers are estimated to have stolen at least $1.75 billion from cryptocurrency exchanges.

[10] https://rusi.org/publication/occasional-papers/closing-crypto-gap-guidance-countering-north-korean-cryptocurrency
[11] https://www.washingtonpost.com/world/national-security/us-set-to-declare-north-korea-carried-out-massive-wannacry-cyber-attack/2017/12/18/509deb1c-e446-11e7-a65d-1ac0fd7f097e_story.html?utm_term=.cd703dfb03a2
[12] https://www.justice.gov/usao-cdca/pr/3-north-korean-military-hackers-indicted-wide-ranging-scheme-commit-cyberattacks-and
[13] https://www.swift.com/sites/default/files/files/swift_bae_report_Follow-The%20Money.pdf
[14] https://www.justice.gov/opa/press-release/file/1253491/download
[15] https://www.elliptic.co/blog/following-money-from-bithumb-hack
[16] https://www.justice.gov/opa/pr/two-chinese-nationals-charged-laundering-over-100-million-cryptocurrency-exchange-hack
[17] https://go.chainalysis.com/2021-Crypto-Crime-Report.html
[18] https://www.forbes.com/sites/thomasbrewster/2021/02/09/north-korean-hackers-accused-of-biggest-cryptocurrency-theft-of-2020-their-heists-are-now-worth-175-billion/?sh=691163865b0b

The reports also flag the continued exploitation of the shipping industry through ship-to-ship transfers, laundering of ship identification, manipulating flags and vessel identifiers, and technological methods of deceiving automatic identification system tracks. In clarifying the ambit of 'financing' as covered by UNSCRs, UNSCR 2270 affirms that the term 'economic resources'[19] include assets of every kind, which potentially may be used to obtain funds, goods, or services and specifies that this includes maritime vessels.

RUSI: Shipping and PF

RUSI's Project Sandstone uses open source data-mining and data-fusion techniques to spot DPRK sanction evasion activities, particularly in the maritime space. The project aims to provide open-source intelligence and actionable evidence to those engaged in enforcement and the policy community in general. Investigations in Project Sandstone include research into DPRK's oil procurement networks, typologies for the movement of DPRK funds through the international finance system, and the significance of the city of Dandong in trading companies associated with PF.[20]

In the APG region, the MERs of China and Singapore were able to draw on the work done by the Panel of Experts report to understand the level of effectiveness under IO 11. For example the Panel of Experts reports have been mentioned in MERs to the extent that they contained examples of accounts, funds or assets held by designated entities in the assessed jurisdiction, and (front) companies run by designated entities in that jurisdiction.[21] Further, requests by the Panel of Experts for information about alleged links with designated entities have led to authorities taking compliance action domestically.[22]

1.4 PF Risk Assessments in the Asia Pacific[23]

Indonesia

In 2020, Indonesia initiated a PF risk assessment and a subsequent update of the existing ML/TF risk assessment. The methodology on Indonesia's PF risk assessment is similar to Indonesia's ML/TF risk assessment that identifies the risk based on vulnerability level, threat level, and impact level through quantitative and qualitative information. This methodology is also similar to the FATF methodology for conducting national risk assessments (NRAs). The development of the PF risk assessment involves the following stakeholders: the Indonesian National Police (Special Detachment 88 Anti-Terror, State Intelligence and Security Agency of the Indonesian National Police), BIN (State Intelligence Agency), Ministry of Foreign

[19] The term is clarified specifically for the purposes of paragraph 8(d) of UNSCR 1718 which, in broad terms, places a freezing obligation on Member States in relation to funds, other financial assets and economic resources connected to PF by DPRK.
[20] https://rusi.org/project/project-sandstone
[21] China MER paragraph 274: http://apgml.org/includes/handlers/get-document.ashx?d=5b27e83d-c28b-4e87-9549-20839d4bd92c
[22] Singapore MER paragraph 288: http://apgml.org/includes/handlers/get-document.ashx?d=1280e446-2110-430c-b709-3a777b85a020
[23] This section includes contributions from APG members on their work to implement the amendments in R.1 and R.2. The APG has not reviewed or assessed the work on PF risk summarised by members here.

Affairs, Directorate General on Customs and Excise (Ministry of Finance) and regulators of financial services providers and DNFBPs as reporting entities (Bank Indonesia/Central Bank, Financial Services Authority, PPATK, etc.), and representatives from FIs and DNFBPs.

Indonesia identified 3 levels of PF risk that consist of 9 quadrants which are, low level (score 3-5), medium level (score 5-7), and high level (score 7-9). The scope of Indonesia's PF risk assessment is limited to the effectiveness of TFS related to PF, as required by R.7. The PF risk assessment excludes the wide scope of PF risk as mentioned in UNSCR 1540 and its successor. Nevertheless, Indonesia considered the volume and materiality of dual use goods trading, specifically to Iran and DPRK as designated jurisdictions based on customs and excise information. In conducting the PF risk assessment, Indonesia also utilised cross-border cash courier (CBCC) information, specifically related to individuals or entities associated with Iran and DPRK.

Overall, Indonesia identified a medium level of PF risk, considering existing diplomatic and economic relationships with Iran and DPRK, and the jurisdiction's geographic proximity to DPRK. Indonesia also identified a potential threat arising from the accounts of former foreign diplomats who are no longer serving in Indonesia and have subsequently been misused by other parties. Nevertheless, some PF risk mitigation has been conducted, such as issuing the Joint Regulation (enacted 31 May 2017) that designated persons or entities based on UN lists (both for Iran and DPRK, concerning PF) and freezing without delay the funds of persons and entities listed. Implementation of the Joint Regulation was expanded to require FIs to identify and freeze the assets of individuals or entities, including those affiliated with UN designated persons and entities. Moreover, in order to mitigate PF risk, some of Indonesia's FIs limit international funds transactions related to Iran and DPRK, including wire transfers. A few FIs will not open any business relationship with Iran and DPRK. Indonesia also established a WMD Task Force in 2017 which consists of the following agencies: PPATK, State Intelligence Agency, Indonesian National Police, Ministry of Foreign Affairs, and NERA (Nuclear Supervision Authority). The main role of the WMD Task Force is to identify and monitor activities and financial flow of individuals or entities, including those affiliated with UN designated persons and entities, through integrating spontaneous exchange information.

Malaysia

Malaysia's National Coordination Committee to Counter Money Laundering (NCC) has recently approved and endorsed the work on a risk assessment on proliferation financing (PFRA), undertaken at the beginning of 2019, in collaboration with export control authorities in Malaysia. The PFRA intends to achieve the following objectives:

- Provide base-line assessment to enhance understanding of Malaysia's risk exposure to PF;
- Identify and address key vulnerabilities in the financial and DNFBP sectors that may be exploited to finance activities relating to proliferation of WMD or to evade UNSC sanctions; and
- Support development of appropriate strategies and recommend measures in mitigating the risks and vulnerabilities identified to strengthen Malaysia's overall countering proliferation financing (CPF) framework.

The assessment has grown in importance and in line with the recent adoption of the revised FATF Recommendations 1 and 2. The completion of PFRA will serve as a key step to ensure effective implementation of the recommendations from the following four different clusters:

- Legislative, policy and coordination framework;
- Regulatory and supervisory initiatives;
- Implementation and guidance; and
- Enforcement actions.

Upon endorsement by the NCC, the sanitised version of the report is expected to be published to the public tentatively in the third or fourth quarter of 2021.

Philippines

On 4 March 2021, the Bangko Sentral Ng Pilipinas (BSP) completed its sectoral risk assessment for banks and other BSP-supervised financial institutions (BSFIs) which highlights the ML/TF/PF threats and vulnerabilities of banks and other BSFIs and the consequences of criminal activities, as well as the overall ML/TF/PF risks associated with other priority areas such as trade-based ML/TF/PF and the implementation of the TFS regime.

RUSI: THE PRIVATE SECTOR AND PF IMPLEMENTATION

In 2020, RUSI conducted a global survey on PF compliance, in partnership with the Association of Certified Anti-Money Laundering Specialists (ACAMS). Key findings include:

- International banks (with operations in several regions of the world) appear most likely to have a compliance function that incorporates PF (76%), in comparison to national banks (63%) and non-banking institutions (46%). This finding tracks with RUSI's own experience delivering training and technical assistance around the world, as well as several mutual evaluation reports, which confirm that banks are generally more aware of their PF obligations, whereas DNFBPs have not considered PF as a discrete financial crime risk.
- Respondents working in international banks are also more likely than other types of institutions to consult red flags, typologies and other PF resources. Some resources, such as the UN Panel of Expert reports on DPRK, are rarely consulted. The survey also found that a higher number of respondents in international banks consult the UN Panel of Experts reports (25%) compared to national banks (3%). Additionally, advisories issued by the US government are mostly consulted by respondents in international banks (39%), and less in other types of institutions (16-17%).
- There are also key regional differences in PF awareness, with Asia having the highest proportion of respondents that say they stay up to date on the latest DPRK sanctions evasion activities through news reporting.
- Over three-fifths agree it is challenging to incorporate lists of dual-use goods into transaction monitoring programmes, and a majority of respondents also agreed that the industry should prioritise strict end-user checks rather than identifying specific goods in transactions.
- On DPRK-specific sanctions concerns, respondents were most concerned about effectively implementing UN obligations on DPRK joint ventures, and detect and stop the sale of fuel to DPRK.

Thailand

Thailand's Financial Intelligence Unit (FIU), the Anti-Money Laundering Office (AMLO), is currently updating its NRA to capture PF, and other crimes and entities not yet covered by Anti-Money Laundering Act (AMLA). The scope of the PF risk assessment is on the potential breach, non-implementation or evasion of the TFS obligations in R.7. The updated NRA is expected to be finalised by the end of 2021.

Through this exercise, AMLO aims to understand Thailand's ML/TF/PF threats, vulnerabilities, risks and consequences. The exercise is intended to serve as a guideline in formulating policies, strategies and measures to mitigate ML/TF/ PF risks.

Thailand's PF update to its NRA will include public and private partners, competent authorities such as AMLO, security and intelligence agencies, regulators and self-regulatory bodies,

company registries, tax authorities, finance agencies, foreign affairs agencies, law enforcement agencies (LEAs) including customs and border agencies, import and export control agencies, and justice agencies. With respect to the private sector, reporting entities (FIs and DNFBPs), non-profit sectors (NPOs) and other legal persons will be included. Lastly, the risk assessment will consult with international partners such as relevant police liaison officers in Thailand.

Progress thus far includes collection and analysis of data, including agency risk assessment data, and data from questionnaires and interviews/focus groups. AMLO will analyse data collected to assess threats, vulnerabilities and consequences.

AMLO will disseminate the NRA to all relevant public and private partners to further strengthen their policies, plans, measures, and procedures to ensure that ML/TF/PF risks will be effectively mitigated, and Thailand's financial system will be well protected from being abused for ML/TF/PF.

Usefully, AMLO have been able to give an insight into the challenges that come with conducting a PF risk assessment. The lack of PF understanding, especially within the private sector, leads to a low of level of awareness with respect to PF risk and an inappropriate level of mitigation. In response, Thailand has identified the need for outreach on PF obligations and associated risks of sanctions evasion.

Co-mingling of legitimate business with illicit transactions in the international financial system also poses difficulty in identifying and mitigating PF risk. Therefore, PF risk, including the amount of PF, might be assessed based on perception rather than statistical data. This challenge requires enhanced co-operation and coordination, and information sharing both at a national and international level.

1.5 Guidance and training provided to FIs and DNFBPs

Case provided by Chinese Taipei

On 2 February 2021, the Financial Supervisory Commission forwarded to FIs, the 'Implementation Handbook for UN Sanctions on North Korea', published by Compliance and Capacity Skills International in partnership with CRDF Global in March 2019.[24]

Case provided by Singapore

The Monetary Authority of Singapore (MAS) published the 'Guidelines to MAS Notice 626 on prevention of money laundering and countering the financing of terrorism' in April 2015.[25] This guidance includes information regarding the potential indicators of PF, as well as the requirements of banks and FIs in relation to PF and freezing funds, customer due diligence and internal controls.

[24] https://www.amlo.moj.gov.tw/media/15269/dprk-un-sanctions-implementation-handbook_english-version.pdf?mediaDL=true

[25] https://www.mas.gov.sg/-/media/MAS/Regulations-and-Financial-Stability/Regulations-Guidance-and-Licensing/Commercial-Banks/Regulations-Guidance-and-Licensing/Guidelines/MAS-Notice-626-Amendments-Nov-15/Guidelines-to-MAS-Notice-626--November-2015.pdf

MAS has also been working with FIs to assist them in the countering of PF risks. Following a series of supervisory visits to banks, MAS published a paper in August 2018 entitled 'Sound Practices to Counter Proliferation Financing' which provides a summary of the key findings and discusses the sound practices observed during their thematic supervisory visits. This paper can be used by banks and FIs to enhance their existing controls and practices in relation to PF.[26]

In addition, MAS has worked in conjunction with the Association of Banks in Singapore (ABS) to make PF a standing agenda item at the ABS annual Financial Crime Seminar, which is one of Singapore's key AML/CFT industry outreach events and is attended by over 500 delegates from Singapore and the region.

Case provided by Thailand

AMLO, in collaboration with foreign counterparts such as the United Nations Office on Drugs and Crime (UNODC) and RUSI, organised training and workshops regarding understanding PF risk and PF risk assessments, for competent authorities and other relevant partners such as AMLO (FIU), security and intelligence agencies, regulators, finance agencies, foreign affairs agencies, LEAs including customs, justice agencies, and finally reporting entities (FIs and DNFBPs).

The scope of the training and workshops included:

- Identifying the risks posed by both state and non-state actors which seek to acquire or facilitate the acquisition of WMD;
- Taking measures to mitigate PF risks which include detecting, investigating and disrupting PF; and
- Raising awareness of ways to ensure the national implementation of UNSCR against PF and related FATF standards.

[26] https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing

2. UPDATE ON COVID-19 IMPACT ON ML/TF TYPOLOGIES

Chapter 1 of the 2020 APG Yearly Typologies Report focused on COVID-19's impact on ML/TF typologies given not only its relevance to the APG membership but also globally. The chapter provided an overview of how the global pandemic prompted criminal groups to 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.

As the pandemic continues into 2021, APG members were asked to provide an update on ML and TF typologies associated with predicate activities linked to COVID-19 (e.g. welfare fraud, scams, counterfeit medicines, corruption, drugs, smuggling, etc).[27]

A number of case studies were provided by members that indicate how the pandemic continues to change the ML/TF landscape, including an increase in online scams and fraud in relation to the sale of personal protective equipment (PPE) and pharmaceutical products. Fraud has also been identified through the use of fake charities to receive pandemic-related donations as well as individuals pretending to be affiliated with governments in order to solicit donations. Members continue to report fraud claims for COVID-19 related government subsidies.

Given the pandemic-related border closures there has also been a reported increase in the detection of smuggling related to illicit drugs, alcohol and tobacco. An increase in the number of suspicious transaction reports related to online gambling is believed to be a result of COVID-19 quarantine measures.

[27] See section 9

3. APG WORKSHOPS AND PROJECTS 2020 - 2021

This section of the report provides a brief overview of typologies-related work undertaken by the APG between July 2020 and June 2021.

3.1 Typologies Projects

Digital Know Your Customer (KYC) Workshop

At the APG's 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 approved project is to support the implementation of digital KYC and ID 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 was postponed and was held virtually on 2-5 February 2021, within the 22nd APG typologies workshop.
- Phase two of the project is currently underway and 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 in Southeast Asia

The APG secretariat worked with the Global Center on Cooperative Security over the course of 2020-2021 to finalise the typology report on Financing and Facilitation of Foreign Terrorist Fighters and Returnees in Southeast Asia. This report is expected to be adopted in July 2021 at the APG Annual Meeting, which will finalise the secretariat's work on this project.

The draft report was shared with APG members for their feedback and review in advance of the 22nd APG typologies workshop, where Financial Profiles of Foreign Terrorist Fighters (in collaboration with Global Center on Cooperative Security) formed a workshop stream.

The APG hosted a Private Sector Roundtable to gather insights and feedback from the private sector on Financial Profiles of Foreign Terrorist Fighters.

FATF Project on TF Risks Related to Illicit Arms Trafficking

The APG participated in the FATF project on Illicit Arms Trafficking and Terrorist Financing.

Human trafficking and people smuggling project (Phase two)

Due to COVID-19 travel-related restrictions, the final workshop of the Human Trafficking and People Smuggling Project (Phase two), due to be completed in June 2020, did not proceed and the programme will be considered finalised.

3.2 22nd Typologies and Capacity Building Workshop

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

The 22nd APG typologies workshop was held in a virtual format on 2-5 February 2021 due to restrictions on travel during the COVID-19 pandemic. The four day workshop involved approximately 325 delegates from 36 APG members, 10 APG observers, and 29 private sector or non-government organisations.

The workshop included a plenary session (first and last day) and two streams, running in parallel, on: (i) Digital KYC (in collaboration with AFS-IT and (ii) Financial Profiles of Foreign Terrorist Fighters (in collaboration with Global Center on Cooperative Security). Expert presentations, panel discussions and other contributions were made in both streams by APG members, observers and other from the global network.

4. 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 2020 and June 2021.

4.1 FATF Typology Projects

Virtual Assets Red Flag Indicators of ML and TF (September 2020)

This FATF report complements the FATF 'Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers (2019)'[28]. It contains ML/TF red flag indicators associated with VAs to assist reporting entities, including FIs DNFBPs, and VASPs. The red flag indicators included are based on more than one hundred case studies contributed by jurisdictions from 2017-2020.

Key indicators in this report focus on:

- Technological features that increase anonymity - such as the use of peer-to-peer exchanges websites, mixing or tumbling services or anonymity-enhanced cryptocurrencies;
- Geographical risks - criminals can exploit jurisdictions with weak, or absent, national measures for VAs;
- Transaction patterns - that are irregular, unusual or uncommon which can suggest criminal activity;
- Transaction size – if the amount and frequency has no logical business explanation;
- Sender or recipient profiles - unusual behaviour can suggest criminal activity; and
- Source of funds or wealth - which can relate to criminal activity.

The report is available on the FATF website at:
https://www.fatf-gafi.org/media/fatf/documents/recommendations/Virtual-Assets-Red-Flag-Indicators.pdf

Trade-Based Money Laundering: Trends and Developments (December 2020)

The publication of this report[29] marked the completion of a joint project between FATF and the Egmont Group on trade based ML. Using numerous case studies from around the FATF global network, the report examines criminal methods of exploiting trade transactions to move money, rather than goods.

The report contains recommendations to address the trade-based ML risks targeted at both the public and private sectors, including the use of NRAs and other risk-focused material to raise awareness entities involved in international trade. The report also recommends improving information sharing of financial and trade data, and cooperation between public and private sectors, including public-private partnerships.

[28] https://www.fatf-gafi.org/media/fatf/documents/recommendations/RBA-VA-VASPs.pdf
[29] https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

The report is available on the FATF website at:
https://www.fatf-gafi.org/media/fatf/content/Trade-Based-Money-Laundering-Trends-and-Developments.pdf

Trade-Based Money Laundering: Risk Indicators (March 2021)

The FATF and Egmont Group published these risk indicators in March 2021 to help public and private entities identify suspicious activity associate with trade based ML.

The report includes risk indicators on:

- The structure of the business;
- Trade activity;
- Trade documents and commodities; and
- Account and transaction activity.

The report is available on the FATF website at:
https://www.fatf-gafi.org/media/fatf/content/images/Trade-Based-Money-Laundering-Risk-Indicators.pdf

Update: COVID-19-Related Money Laundering and Terrorist Financing Risks (December 2020)

This paper updates work published by the FATF in May 2020, highlighting COVID-19-related ML and TF risks and policy responses. Using input from the FATF global network, and from private and public sector webinars in July and September 2020, the paper details how criminals continue to exploit the crisis. A selection of case studies illustrates how the risks have evolved as the pandemic has progressed, and how authorities have dealt with them. These include the counterfeiting of medical goods, cybercrime, investment fraud, charity fraud and abuse of economic stimulus measures.

The paper confirms the FATF concerns expressed in May 2020, including:

- Changing financial behaviours - especially significant increases in online purchases due to widespread lockdowns and temporary closures of most physical bank branches, with services transitioning online; and
- Increased financial volatility and economic contraction - largely caused by the losses of millions of jobs, closures of thousands of companies and a looming global economic crisis.

The paper recommends authorities and the private sector take a risk-based approach (RBA) responding to these evolving risks, as required by the FATF Standards, by mitigating the ML and TF risks without disrupting essential and legitimate financial services and without driving financial activities towards unregulated service providers.

The report is available on the FATF website at:
https://www.fatf-gafi.org/media/fatf/documents/Update-COVID-19-Related-Money-Laundering-and-Terrorist-Financing-Risks.pdf

Guidance on TF Investigations and Prosecutions (2021)

This confidential guidance provides best practices to national authorities to improve the effectiveness of their legal actions against TF. It covers detection, investigative strategies for common types of TF activity, proving intent and knowledge, and confiscation of assets as a tool to disrupt TF. The final version of this confidential report has been disseminated to operational authorities. Authorities should get in contact with their FATF national contacts should they want a copy of the report.

TF Risks Related to Illicit Arms Trafficking (2021)

This confidential report on the links between illicit arms trafficking and TF aims to raise awareness across the FATF global network, particularly in the context of NRAs, and help jurisdictions develop effective operational responses.

The final version of this confidential report has been disseminated to operational authorities. Authorities should get in contact with their FATF national contacts should they want a copy of the report.

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

This non-public update to the FATF comprehensive report on the Financing of the Islamic State in Iraq and the Levant (ISIL)[30] published in February 2015, is based on information provided by the FATF global network and covers Al-Qaeda, and ISIL and Al-Qaeda affiliates. Authorities should get in contact with their FATF national contacts should they want a copy of the latest ISIL update.

Joint Experts' Meeting (November 2020)

In November 2020, the FATF held the annual Joint Experts' Meeting (JEM) in a virtual format for the first time. Approximately 400 participants representing 95 jurisdictions from across the FATF global network, FSRBs and international organisations attended the meeting.

The meeting started with a high-level session to discuss evolving ML/TF risks faced by members across the FATF global network and had a concluding session to discuss the need for stronger co-operation when pursuing ML cases in a multilateral context. Four other sessions were held to advance ongoing and upcoming priority projects under the FATF German Presidency. These sessions covered: (1) ML and environmental crime; (2) the financing of ethnically or racially motivated terrorism; (3) illicit arms trafficking and TF; and (4) digital transformation of AML/CFT for operational agencies. The discussions at the JEM also covered high level issues including, emerging money laundering and terrorist financing risks, and co-operation in multi-jurisdictional money laundering cases. The meeting provided invaluable inputs into FATF's ongoing work.

Additional details on the outcomes are available on the FATF website at:
https://www.fatf-gafi.org/publications/methodsandtrends/documents/jem-2020.html

Money Laundering from Environmental Crime (July 2021)

[30] https://www.fatf-gafi.org/media/fatf/documents/reports/Financing-of-the-terrorist-organisation-ISIL.pdf

This report aims to strengthen awareness of the scale and nature of criminal gains and laundering techniques for environmental crimes. The report brings together expertise from across the FATF's Global Network to identify good practices that governments and the private sector can take to disrupt the profitability of environmental crimes. The findings for this report are based on case studies and good practices provided by over 40 jurisdictions, alongside expertise from civil society and the private sector.

Key findings of the report include:

- Estimates of the scale of financial flows from environmental crimes vary considerably, but evidence suggests that proceeds account for hundreds of billions of dollars annually impacting all regions. With the exception of waste trafficking, environmental crimes generally occur in resource-rich developing and middle-income jurisdictions, with proceeds coming from larger, developed economies.
- Criminals often rely on cash intensive sectors (frequently linked to the export sector) and trade-based fraud to launder proceeds from environmental crimes.
- The significant role of trade-based fraud and misuse of shell and front companies to launder gains from illegal logging, illegal mining, and waste trafficking.
- Criminals frequently comingle legal and illegal goods early in the resource supply chains to conceal their illicit source.
- Actors, enabled by corruption, rely on corporate structures, third party transfers and offshore jurisdictions to obfuscate the beneficial owners.
- Jurisdictions face a range of challenges in identifying and disrupting environmental crimes. These include gaps in effective understanding and awareness of financial flows connected to environmental crimes; internal and inter-agency co-ordination gaps; low levels of international co-operation on the financial flows; insufficient awareness of risk-indicators to develop red-flags; and inadequate private sector capacity to implement successful preventive measures.
- Jurisdictions highlighted a number of good practices including coordinated risk assessments involving environmental and AML agencies, clear and coherent legal frameworks (including criminalisation of ML for environmental crimes that occurred abroad), guides for domestic co-operation, joint taskforces and information exchange to follow and repatriate the money for environmental crimes from overseas, and consultation with the private sector to develop red-flags.

The report identifies the following key priorities for Members of the FATF Global Network:

- All Members of the FATF Global Network should consider whether criminals may be misusing their financial and non-financial sector to conceal and launder gains from environmental crimes. This includes jurisdictions without domestic natural resources.
- Members must also strengthen their operational capacity to detect and pursue financial investigations into environmental crimes. This includes working with foreign counterparts to share information, facilitate prosecutions and the effective recovery of assets that are moved and held abroad.
- Jurisdictions should fully implement the FATF standards as an effective tool to combat money laundering from environmental crime. This includes ensuring AML outreach to relevant intermediaries covered by the FATF Standards, such as dealers in precious metals and stones and trust and company service providers.
- Jurisdictions should consider establishing and strengthening public-private sector dialogue to share risk information, and organisation of industry-led initiatives to strengthen due

diligence of supply chains and their financial flows. These initiatives can play a significant role in raising awareness about suspicious financial activity and addressing comingling by finding means to demonstrate the legitimate source of goods.

The report is available on the FATF website at:
https://www.fatf-gafi.org/publications/environmentalcrime/documents/money-laundering-from-environmental-crime.html?hf=10&b=0&s=desc(fatf_releasedate)

Ethnically or Racially Motivated Terrorism Financing (June 2021)

The report brings together expertise from jurisdictions and institutions which have had experience in tackling ethnically or racially motivated terrorism (EoRMT) with an aim to increase the understanding of TF risks related to extreme right wing (ERW) actors more broadly among competent authorities, non-governmental bodies, the private sector, and the broader public. The findings in the report are based on inputs from around 30 jurisdictions across the FATF Global Network, as well as expertise from the private sector and international bodies partnered with the FATF. The report provides an outline of key ways in which ERW actors raise, move and use funds, as well as practical examples of this.

Key findings of the report include:

- While extreme right wing terrorist attacks are mainly perpetrated by self-funded lone actors, extreme right wing (ERW) groups employ an array of fundraising techniques. These include donations (through both crowdfunding and private contributions), membership fees, commercial activities (including organisation of concerts, sales of merchandise and real estate ventures), and criminal activities. Notably, most of the funding for ERW groups appears to come from licit sources.
- ERW groups appear to be less concerned with concealing their transactions than in other forms of TF. Many jurisdictions also reported that ERW actors are becoming increasingly operationally sophisticated in how they move their funds.
- Funds appear to be used for varying activities, ranging from financing of attacks, to purchasing equipment, training, creating and dispersing propaganda, recruitment, networking, legal fees, and even purchasing and maintaining real estate assets.
- The report highlights several challenges in tackling the financing of ERW-motivated groups and attacks including different legal regimes in place for combatting ERW terrorism in different jurisdictions; few national designations of groups; growing transnational links between groups (and, in some instances, individuals who have perpetrated terrorist attacks); the fact that most ERW attacks are carried out by self-funded lone actors; and, the limited public-private partnerships in place for exchanging financial information.

Recommendations contained within the report include:

- Jurisdictions are encouraged to continue to develop their understanding of EoRMTF, especially through including this threat in their NRAs, working with relevant public and private partners on threat detection, and exchanging best practices with relevant international partners to tackle the increasingly transnational characteristics of EoRMTF.
- Jurisdictions should maintain their focus on the evolving threat posed by EoRMTF, particularly in the context of the COVID-19 crisis which has provided a recruitment opportunity for violent extremist groups.

The report is available on the FATF website at:
https://www.fatf-gafi.org/publications/methodsandtrends/documents/ethnically-racially-motivated-terrorism-financing.html

4.2 Middle East and North Africa Financial Action Task Force

A Study on: Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in the Middle East and North Africa Region (August 2020)

This report documents responses to a questionnaire disseminated by MENAFATF to its members requesting information and case studies on the effects of the pandemic on AML/CFT systems in the region and the most important methods and trends used in committing related crimes.

The report explores the measures taken by jurisdictions in the region with regard to their AML/CFT systems in response to developments as a result of the pandemic. Several jurisdictions indicated that there had been a significant decrease in the number of suspicious transaction reports (STR) as a result of economic decline and quarantine conditions. The report explores the most prominent challenges facing AML/CFT systems in the region including technological difficulties with regard to remote working, reduced cooperation between domestic authorities as well as reduced international cooperation, the redirection of resources towards combating the pandemic and effects on onsite inspections by supervisory bodies.

The report also documents best practices taken by jurisdictions in the region to mitigate the effects of the pandemic including using technology to conduct virtual onsite inspections and to fulfil KYC requirements.

The report also outlines key typologies identified in the region during the pandemic including cybercrime, corruption, cross-border smuggling of cash and fraud including with regard to donations and counterfeiting of medical goods.

The report recommended that competent authorities take several key actions, including:

- Not only attempt to restore the level of compliance to what it was before the COVID-19 pandemic, but also strengthen AML/CFT systems continuously and sustainably even in times of crisis;
- Develop a unified risks map associated with ML and TF related to the pandemic and work to find measures to mitigate it and similar crises.
- Review the adequacy of AML/CFT regulations and their ability to meet critical and crisis conditions.
- Activate international cooperation channels and respond accurately to requests for information in a timely manner.

The report is available on the MENAFATF website at:
http://www.menafatf.org/information-center/menafatf-publications/coronavirus-pandemic-covid-19-and-its-impact-amlcft-systems

4.3 Eurasian Group on combating money laundering and financing of terrorism

Typologies of the use of preventive measures of financial institutions for crime detection and risk assessment (2021)

The report summarises the approaches and best practices of jurisdictions related to the use of STRs and includes information on preventive measures applied by FIs for identifying offences and assessing risks. The report includes case studies from Eurasian Group (EAG) members on best practices related to the use of STRs and preventive measures. The report also outlines the specificities of supervision and implementation by reporting entities of preventive measures amid the COVID-19 pandemic.

Key findings of the report include:

- The main preventive measures, that have proved their effectiveness in mitigating ML/TF risks in practice, are refusal to carry out transactions for customers and refusal to enter into bank accounts (deposit) agreements with customers, also known as denial of services;
- In some EAG members, the STR form includes information on beneficial owners of customers and IP and MAC addresses of devices used by customers for accessing online banking services. Such information enables the FIUs to identify additional links and make thematic collections of the incoming STRs;
- There have been changes in financial behaviour during the COVID-19 pandemic due to the rapid growth of online services and development of e-commerce;
- There has been an increase in cybercrime, online fraud and the misuse of public funds during the pandemic;
- There has also been an increase in fraud related to personal protective equipment, medicines and in the area of charities;
- There has been an increase in cross-border online gambling;
- Some jurisdictions experienced increases in the number of STRs during the pandemic attributed to a surge in digital transactions and an increase in cybercrime, while others experienced decreases in the number of STRs attributed to a decline in economic activity; and
- In a number of the EAG member states in the first half of 2020, scheduled inspections in a number of sectors of FIs were cancelled and on-site inspections were replaced with remote ones.

Recommendations contained within the report for EAG members include:

- Analyse the practices of financial institutions in applying the right to refuse to conduct transactions and the right to refuse to enter into an account (deposit) agreement as risk mitigation measures and, if necessary, take measures to optimise them;
- Consider including in the format of the electronic message about a suspicious transaction information about the customer's beneficial owner, as well as the IP and Mac addresses of the devices used by customers in remote banking, as well as a special marking to highlight important STRs that require an urgent response;

- Competent authorities of the EAG members are invited to review, in collaboration with the private sector, current pandemic trends and risks and, if necessary, to update relevant recommendations and guidance documents on identifying high-risk transactions; and
- Competent authorities of the EAG members are invited to consider expanding the formats of using IT tools for remote interaction with reporting entities for implementation of non-contact supervision and for prompt collection of information about risks and vulnerabilities among a wide range of respondents.

The report is available on the EAG website at:
https://eurasiangroup.org/files/uploads/files/Preventive_measures_final_report_eng.pdf

4.4 Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism

Money laundering and terrorism financing trends in MONEYVAL jurisdictions during the COVID-19 crisis (September 2020)

This report used responses to a questionnaire sent out to all MONEYVAL jurisdictions to ascertain emerging ML cases, practical challenges, typologies and trends surfacing during the pandemic.

Key findings of the report include:

- The overall level of criminality remained stable or slightly decreased and suspicious transactions reporting remained steady;
- Jurisdictions reported a surge in certain crimes, especially transnational crimes, such as fraud (through electronic means) and cybercrime, creating new sources of proceeds for ML purposes;
- No reported increase in crimes related to drug trafficking, TF, abuse of NPOs and insider trading. Several jurisdictions reported growth in medicrime, cybercrime and corruption;
- Opportunities for abuse of government emergency economic relief measures (such as financial aid and tax incentives) to support businesses and the population were identified.
- Vulnerability for fraud and corruption has been created by the temporary suspension of complex controls in public procurement procedures for medical equipment and supplies in some jurisdictions.
- Cooperation between FIUs has not been affected and has proven to be particularly relevant on exchanging information on cross-border cases related to fraudulent offerings of medical and sanitary equipment, counterfeited products, non-delivery scams and illegal over-pricing.

Three main types of fraud related to COVID-19 were identified: medical equipment fraud, economic relief measures fraud, and fraud/embezzlement related to public procurement contracts.

Recommendations contained within the report include:

- Law enforcement should place sufficient focus on investigating frauds and cybercrimes committed during the pandemic crisis.

- Border police and customs authorities should pay special attention to the cross-border movement of cash which might be related to "late demand" to move illicit funds. Cross border cash movements are used by criminals to finance their operations and it is said that now criminal organisations face a "late demand" for cross border transportation of cash given the temporary closing of national borders due to the pandemic.
- Authorities should closely monitor the situation of public procurement, to detect possible cases of abuse and corruption, especially where controls have been relaxed.

The report is available on the MONEYVAL website at:
https://rm.coe.int/moneyval-2020-18rev-covid19/16809f66c3

4.5 Egmont Group

Public Bulletin on Money Laundering of Serious Tax Crimes (July 2020)

This bulletin aims to present key lessons, best practices, and representative case examples to help enhance the fight against ML of serious tax crimes both at the national and international levels. The bulletin relies on a questionnaire and survey on case examples distributed to the Egmont Group's FIUs.

Key lessons from the bulletin include that effective national capabilities of authorities to receive, access, analyse and share relevant tax-related information, including on related ML, are key to the ability of jurisdictions to effectively tackle serious tax-related crimes. In addition, national legal frameworks that grant high levels of tax secrecy complicate reciprocity in the exchange of information. Furthermore, low level/no taxation policies do not only increase the attractiveness of the concerned jurisdiction for investors, but also for criminals, which can create vulnerability in other jurisdictions as a lack of beneficial ownership transparency hinders transnational investigations.

The bulletin recommends best practices in the fight against ML of serious tax crimes including to facilitate effective cooperation between FIUs and tax authorities at the national level and international cooperation between FIUs. The bulletin provides a series of case examples to illustrate best practices including effective cooperation between FIUs.

The bulletin is available on the Egmont Group website at:
https://egmontgroup.org/en/filedepot_download/1661/117

COVID-19 Best Practices for Financial Intelligence Units (March 2021)

This report is informed by a series of virtual roundtables conducted by the Egmont Centre of FIU Excellence and Leadership (ECOFEL) in order to strengthen the capabilities of FIUs during the COVID-19 crisis, together with a stocktaking exercise of open source material published by Egmont Group members, observers and other international organisations. The report documents a variety of typologies that have emerged as a result of the COVID-19 pandemic.

The report finds that suspicious activity report numbers have not decreased significantly during the pandemic, with FIUs only noting a reduction where there has been economic decline or reporting entities have limited capacity.

Importantly, the report also notes that most FIUs have identified some new emerging risks as a result of the pandemic, particularly relating to fraud (concerning medical equipment and PPE), corruption linked to the relaxation of public procurement rules and cybercrime including phishing. FIUs have noted increases in fraud, phishing, other online scams and increases in the misuse of public funds. Other emerging risks include child pornography and child exploitation, counterfeit currency and the emergence of wildlife crime. FIUs are also aware of new emerging risks, such as those relating to the development of COVID-19 vaccines.

The report provides examples of action taken by FIUs against COVID-19 related crime and lists recommendations for FIUs to respond to the changing COVID-19 risk landscape.

The report is available on the Egmont Group website at:
https://egmontgroup.org/en/filedepot_download/1661/123

ECOFEL - Financial Investigations into Wildlife Crime (January 2021)

This report aims to provide FIUs with an enhanced understanding of wildlife crime and presents the trends and patterns associated with wildlife crime financial flows. The report also explores the links between wildlife crime and other forms of criminal activity such as drug offences, corruption, TF and the illegal weapons trade. It notes that historically, there have been very few financial investigations into wildlife crime globally and the resulting lack of financial scrutiny and low penalties make wildlife crime a highly profitable, low-risk enterprise for perpetrators.

The report emphasises the benefits of investigations into the financial flows of the illegal wildlife trade and explains how FIUs can get involved in supporting financial investigations into wildlife crime. The report lists recommended practices to increase the effectiveness of FIU efforts including properly assessing the risks of wildlife crime in the jurisdiction's NRA, filtering and analysing STRs based on strategic assessments of wildlife crime within the jurisdiction and enhancing inter-agency cooperation and information exchange. International organisations and non-government organisations (NGOs) active in the fight against wildlife crime are also suggested as good partners for FIUs.

The report is available on the Egmont Group website at:
https://egmontgroup.org/en/filedpot_download/1661/122

Public Bulletin on Combatting Online Child Sexual Abuse and Exploitation through Financial Intelligence (July 2020)

This bulletin focuses on the strategic intelligence picture associated with payments identified as relating to online streaming of child sexual abuse and exploitation (CSAE). The bulletin notes that the criminal business models specifically established for online streaming bring a financial dimension to the activity that is not always prevalent in the other forms of CSAE. The bulletin then explains the financial dimension of online streaming of CSAE including the payment patterns for online-streamed material and the associated business models. It also emphasises how the analysis of reports submitted by private sector entities, including suspicious activity reports and STRs, enables FIUs to provide LEAs with actionable intelligence relating to the movement of funds and the identification of both offenders and facilitators.

The bulletin is available on the Egmont Group website at:
https://egmontgroup.org/en/filedepot_download/1661/119

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

Illegal Wildlife Trade and Financial Investigations in West Africa (April 2021)

This paper was published by RUSI with the support of the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA). The paper relies on 89 interviews with key stakeholders in West and Central Africa, as well as a survey of 12 out of 17 GIABA member FIUs to assess the extent to which the financial dimensions of the Illegal Wildlife Trade (IWT) are investigated in the region.

The paper analyses IWT trends in West Africa, with a focus on high-grossing trafficking in elephant ivory, pangolin scales and rosewood. It also identifies key challenges that currently prevent the use of financial investigations in IWT cases.

The paper's key findings include:

- 86% of respondents considered IWT a 'serious issue', but only 58% made reference to environmental crime or IWT in their national ML/TF risk assessments;
- Only one FIU considered itself to be regularly involved in the investigation of IWT cases;
- Only 25% (three) of the FIUs reported ever having conducted IWT financial investigations, no jurisdiction had completed more than one and none led to a prosecution for ML or another financial crime;
- FIUs have very minimal knowledge about the methods used to generate, transfer and launder the proceeds of IWT in West Africa;
- Most GIABA member states criminalise environmental crime as a predicate offence to ML, but most FIUs identified a 'lack of awareness of IWT as a predicate offence' as the most important reason why financial investigations do not currently occur in wildlife cases;
- Most FIUs identified the need for greater training, knowledge and financial resources to pursue IWT cases as a capacity-building priority; and
- The paper affirms that global enforcement action remains disproportionately focused on low-level, easily replaced poachers, leaving the controllers and ultimate beneficiaries of IWT virtually untouched.

Key recommendations of the paper include:

- The establishment of a financial crime working group in the West Africa network to combat wildlife crime that will be responsible for coordinating the implementation of the West Africa Strategy on Combating Wildlife Crime at the regional level.
- The inclusion of FIUs and anti-corruption agencies in all national level domestic taskforces created to address wildlife crime.
- Policymakers charged with developing national counter-wildlife crime strategies and action plans should include the requirement to initiate parallel financial investigations in all suitable IWT cases.

- Proposals for improving domestic and international cooperation and information sharing.

The report is available on the GIABA website at:
https://www.giaba.org/media/f/1131_IWT_west_africa_Report_2021.pdf

5. CURRENT MONEY LAUNDERING AND TERRORISM FINANCING METHODS AND TRENDS

5.1 Use of offshore banks, international business companies, and offshore trusts, including trust company service providers.

Fiji

Offshore Profit Shifting and Tax Evasion

Person B, a dual citizen of Fiji and jurisdiction X was reported for claiming a false VAT refund from the local taxation authority on the pretext of a legitimate business expense. Checks by the Fiji FIU revealed that Person B started a sole proprietor business in Fiji with a trading activity of real estate and is a director of two other companies in Fiji, which were both related to the construction industry. However, it was established that there was no corresponding trading activity in relation to the VAT claim since one of his companies had no significant trading activities while the other company was incurring losses for the same period. The Fiji FIU established that more than $110,000 (USD 53,981) was claimed and refunded as VAT from the taxation authority by Person B. Person B also sent large remittances to Fiji from jurisdiction X to himself, his companies and Person C who was his associate amounting to more than $750,000 (USD 368,893) within five years. The remitted funds were used to acquire three properties in Fiji with a total value of more than $1.8m (USD 885,359) which were partly financed by a loan. A case dissemination report was provided to the taxation authority in Fiji and the relevant FIU in jurisdiction X.

New Zealand

Abuse of New Zealand Trust or Company Service Provider and related structures for ML of offshore corruption proceeds

At the instruction of an offshore-based individual, a New Zealand (NZ) Trust or Company Service Provider (TCSP) established two foreign trust structures using NZ limited liability companies as the trustees and as the partners (limited and general) of multiple NZ limited partnerships which were also incorporated into the structures and used to open NZ bank accounts. The TCSP was the director for all of the entities and had authority to operate the bank accounts. The offshore-based individual and his wife were beneficial owners of the above structures, however, they had no identifiable links to any of the above structures in NZ publicly available databases.

The offshore-based individual was subsequently indicted for conspiracy to commit wire fraud as part of a violation of anti-kickback laws in jurisdiction A, using a company based in jurisdiction B. Authorities alleged the offshore-based individual was part of a wider conspiracy relating to a sham marketing agreement used to disguise kickback and bribe payments relating to provision of medical supplies. It was suspected the proceeds of this scheme were laundered via an international web of trust and company structures – including the NZ foreign trust

structures in whose name overseas assets were purchased and whose NZ bank accounts were known to have facilitated the movement of more than USD 1.5 million.

Proceeds from offshore political corruption and bribery laundered through NZ

A political official and head of a state-owned energy company in overseas jurisdiction A was indicted in jurisdiction B on charges of bribery, corruption and conspiracy to commit money laundering, in relation to bribes he received from company officials in the jurisdiction B to corruptly secure energy contracts and payment priority on outstanding invoices. The official had been living in jurisdiction C for the past seven years along with his wife.

The official admitted to authorities that between 2011 and 2014, he conspired with officials in jurisdictions A and B to solicit and direct bribes to a range of associates, and to launder the bribes through a series of financial transactions, including to bank accounts in jurisdictions D and E owned or controlled by the official or associates.

A NZD 17.4 million (USD12,564,408) transfer was made into a NZ account from a bank account held in jurisdiction E registered in the name of the wife of the indicted official. The funds were received into the NZ account of an NZ accountancy firm specialising in the creation and administration of offshore structures on behalf of international 'high net worth' clients. The accountancy firm's employees featured prominently in Panama Papers reporting where they were listed as officers and/or nominees of numerous NZ and overseas companies which formed part of the Mossack Fonseca network of entities.

The fund transfers were conducted under order of the wife of the indicted official. As part of ECDD, the bank requested further information from the accountancy firm, which stated that due in part to political issues, the bank moved to close all accounts for jurisdiction A nationals operating in jurisdiction E and the portfolio was liquidated to enable funds to be transferred to NZ for investment purposes. The accountancy firm stated it was expecting the wife to visit NZ in the near future and it had set up the 'required structures' on her behalf in the meantime.

Singapore

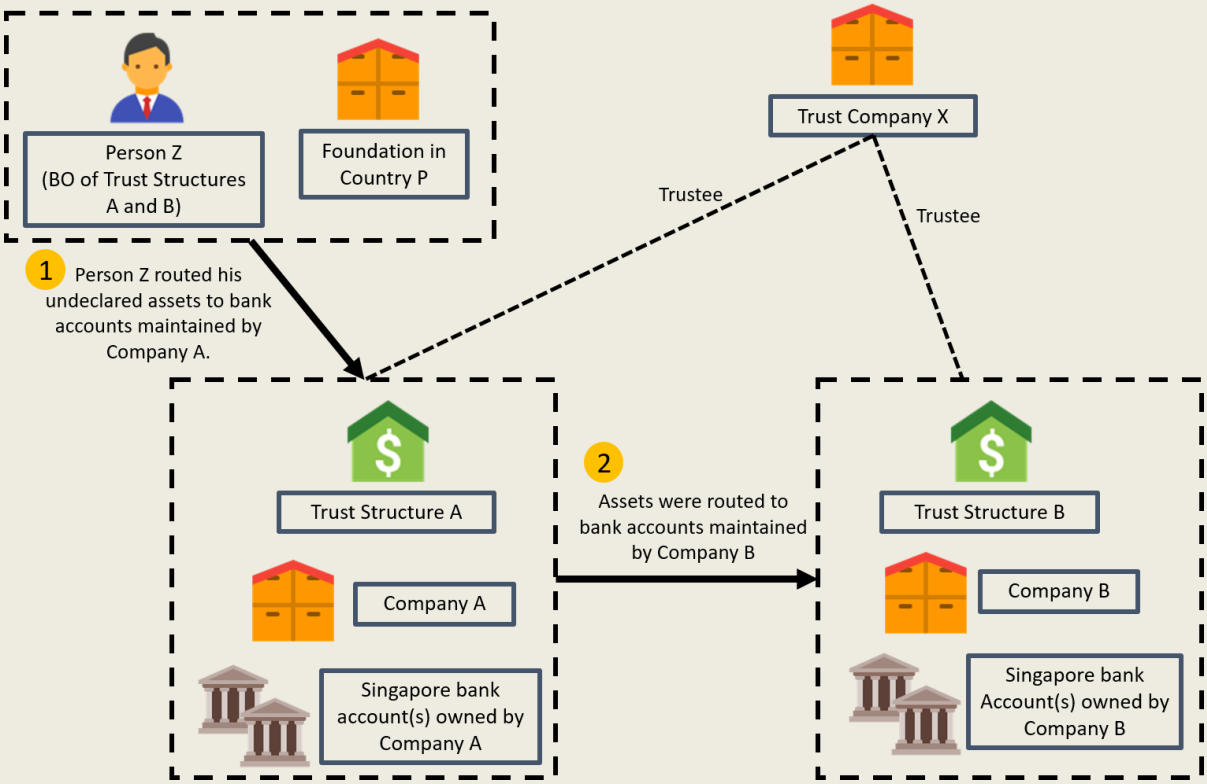
The Commercial Affairs Department of the Singapore Police Force (CAD) investigated allegations against a licenced professional intermediary for concealing beneficial ownership using trust structures.

A Singapore-incorporated trust company ("Trust Company X"), allegedly conspired with asset managers based in jurisdiction S to set up complex trust structures in Singapore with the aim of concealing the beneficial ownership of financial assets belonging to a Jurisdiction A national, Person Z. This investigation arose from a MLA request from Jurisdiction A which commenced civil forfeiture proceedings against Person Z. Person Z faced a tax evasion charge under Jurisdiction A laws for failing to declare assets in undisclosed and untaxed offshore bank accounts held outside of Jurisdiction A.

Trust Company X facilitated the set up and administration of two trust structures, and was registered as the trustee of the assets under them. The beneficial owner of the trust structures was Person Z. The trust structures comprised companies (Companies A and B) incorporated in

jurisdiction B, and these companies in turn maintained corporate bank accounts in Singapore. From 2012 to 2017, Person Z routed his undeclared financial assets from a foundation in jurisdiction P to the corporate bank accounts in Singapore of the said companies incorporated in jurisdiction B.

Working closely with Jurisdiction A authorities during investigations, Singapore seized the funds in bank accounts amounting to approximately SGD 3.5 million (USD 2.6 million). Pursuant to a settlement agreement between Jurisdiction A authorities and the accused person Z, the proceeds of the Jurisdiction A tax evasion offences were recovered and eventually restituted to Jurisdiction A's government. Investigations are currently ongoing for money laundering offences against Trust Company X.



5.2 Use of virtual assets (cryptocurrencies)[31].

Australia

In June 2020, the Australian Federal Police (AFP) commenced an investigation into an unknown person using the details of victims of identity theft to register for multiple accounts with Digital Currency Exchanges (DCEs) and subsequently using these accounts to launder proceeds of crime. Working in conjunction with the DCEs the AFP identified in excess of AUD $40,000 (USD 31,100) being deposited into cryptocurrency ATMs and transferred via nine

[31] A virtual asset, as defined by FATF, is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations (https://www.fatf-gafi.org/glossary/u-z/)

separate accounts registered with the DCE. Further investigations identified the unknown person responsible who was subsequently arrested and charged with the following offences:

- Receiving a designated service using a false customer name, contrary to the Anti Money Laundering and Counter Terrorism Financing Act 2006 (Cth) s140(1); and
- Possession of identification information, contrary to Criminal Code (Cth) s372.2(1).

New Zealand

Bitcoin trader facilitates fraud

A peer-to-peer bitcoin trader operating on localbitcoins.com facilitated the conversion of fraudulently obtained fiat currency into bitcoin on behalf of international fraudsters operating offshore. The overseas fraudsters would contact NZ-based victims and engage in deceptive practices (primarily romance and 'advance fee' scams) to convince the victims to provide them with money. The scammers instructed their victims to meet with their local 'associate' (the bitcoin trader) to conduct a cash handover, providing the victims with a time and place to meet the associate. Meanwhile, the scammers also contacted the bitcoin trader advising they wished to purchase bitcoin with NZD, instructing the trader to meet with their 'associate' (who was actually the scam victim) at a specific time and place to conduct the handover. The scammers provided the trader with their bitcoin wallet address to which he was to credit bitcoin to the value of the cash handed to him by the victim. The bitcoin trader did not undertake any forms of CDD when facilitating these trades, accepting the cash from the victim, and crediting the value in bitcoin to the fraudster on a 'no questions asked' basis.

Pakistan

Drug Trafficking and unauthorised dealings in Virtual Assets

An STR was reported by XYZ Bank on the account of Mr. AM upon suspicion of his involvement in unauthorised dealings in virtual assets. Activity on a Virtual Asset trading platform revealed that Mr. AM was involved in the sale/purchase of Bitcoins, which is not legal in Pakistan as per the Central Bank's instructions.

The bank investigated the account of Mr. AM because transactional activity was reportedly unusual due to high turnovers in the account and transactions with unrelated counterparties. During the analysis of transactional activity, it became clear that the individual was involved in the trading of virtual assets.

Further, Mr. AM was conducting high value transactions with various unrelated counterparties, most of whom were suspected of being involved in Hawala or other criminal activity. As per the Pakistan FIU's databases, one of Mr. AM's counterparties, Mr. BA, a proprietor of M/s AA was found during an investigation by the Anti-Narcotic Force to have acquired proceeds from the sale of drugs**.** The account of Mr. BA was credited with a substantial volume of funds from the account of Mr. AM with no clear purpose.

The financial intelligence was shared with law enforcement agencies and the central bank as it was suspected that Mr. AM is involved in virtual asset transactions and possibly facilitating others to route the proceeds of crimes using virtual assets.

Ponzi scheme & Crypto currency

An STR was raised by XYZ bank on an entity, namely ABC, as complaints were received by the bank through the Prime Minister's Delivery Units (PMDU) and the complaint portal of the Company Registry (SECP) that the entity ABC Trading was involved in the unlawful activities of soliciting unauthorised deposits from a public offering promising unrealistically hefty returns on investments. As per the website of ABC trading, it was dealing in the sale/purchase and investment in cryptocurrencies and also offered wallet facilities and ATM facilities for cryptocurrencies in different jurisdictions.

ABC Trading was not found to be registered with the Securities & Exchange Commission of Pakistan (SECP). It was identified through complaints that the entity was working in the jurisdiction presumably through multiple different incorporated companies while their affairs are run by three individuals including Mr. SR, his wife Mrs. ZK and his son Mr. AW.

Furthermore, multiple STRs were also reported by different banks on Mr. SR and his family members based on their involvement in Ponzi schemes and cryptocurrencies on a large scale.

Mr. SR had opened 70 bank accounts during the period 2011 to 2020 where the funds were mainly credited through online cash coming from different cities of the jurisdiction and debits to the accounts were made through clearing transactions. 59 out of 70 accounts were opened during the period 2018 to 2020. A huge turnover was observed in the accounts. Most of the funds were credited through online cash and debited through centralised inward clearing, pay orders and cash.

The same business address was provided in the account opening forms for diversified businesses run by these individuals under different business names. Upon a search in Inland Revenue's database of taxpayers, it was discovered that a nominal amount of tax was paid by the businesses. The financial intelligence was shared with relevant law enforcement agencies and the Central Bank in order to investigate the matter.

Philippines

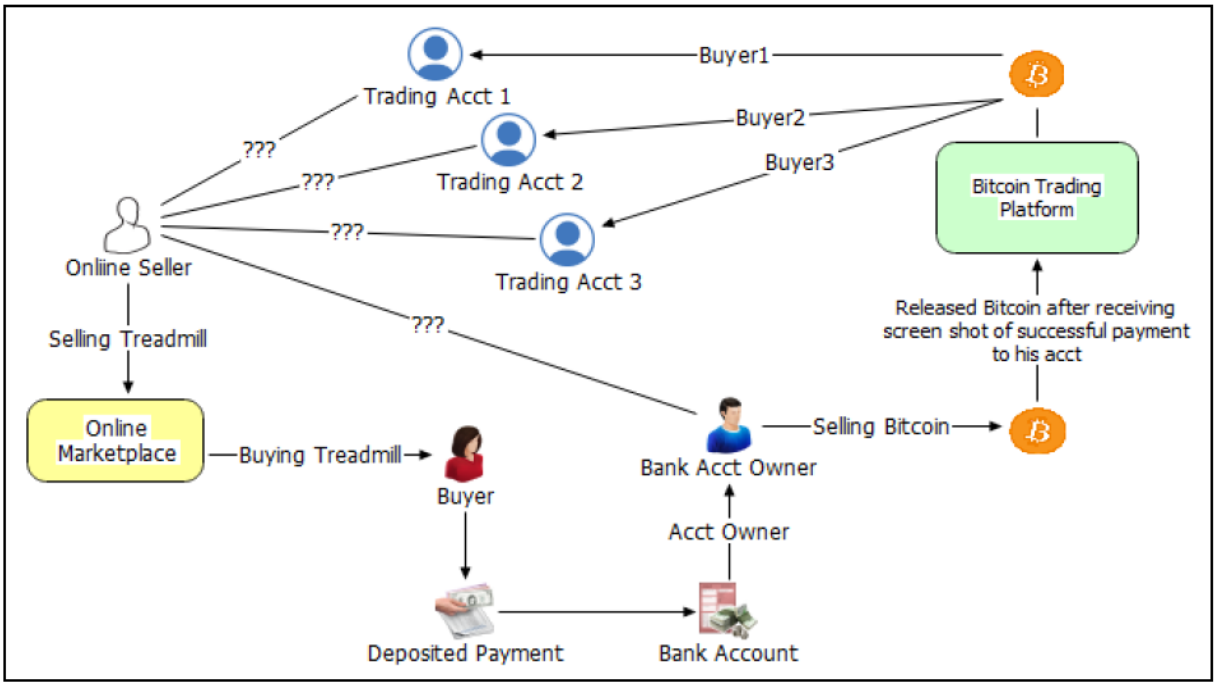
Receipt of deposit/fund transfer with no underlying legal transaction involving bitcoin

The subject opened a passbook with ATM access account in a bank in the Southern Tagalog Region, Philippines, in January 2020. Based on the completed customer information sheet, the subject earned a monthly income of PHP 70,000 (USD 1,461) as the business owner of a general store. However, the bank's monitoring system triggered an alert due to an inward remittance from a single sender amounting to PHP 55,400 (USD 1,156) in March 2020. The bank attempted to contact the subject to request supporting documents for the alerted transaction. The subject was contacted on 13 May 2020, and he disclosed that the transaction was payment from a customer who ordered 5,000 facemasks. However, the bank ascertained that the inward remittance was from a verified Bitcoin company. The subject was advised to visit the branch to provide supporting documents, but the client failed to do so due to the imposition of enhanced community quarantine (ECQ). The branch asked the subject to e-mail a copy of the voucher and delivery receipt or any proof of the transaction. The subject submitted a delivery receipt and a voucher but upon checking, the documents were deemed unacceptable. The bank also requested that the subject provide a copy of the delivery/courier receipt and screen shots of conversations regarding the transaction since the subject claimed that the transaction was the result of an online sale. The bank called the subject almost every day between 13 and 27 May 2020 to seek further documents, but to no avail. The subject is now

rejecting the bank's calls, and funds from the subject's account have gone below the maintaining balance.

Online shopping bitcoin scam

A buyer bought a treadmill from an online marketplace and the online seller instructed the buyer to deposit the payment in a certain bank account. On 1 June 2020, the buyer made five fund transfers, totalling PHP 22,000 (USD 459), but the ordered item was never delivered. The beneficiary bank account owner (Mr. BBAC) denied any relation to the online scammer/seller, emphasising that he has never sold gadgets/equipment. Mr. BBAC mentioned that at the start of the COVID-19 crisis, he started engaging in Bitcoin trading in a legitimate online peer-to-peer finance platform, where individuals are registered under a username or alias. On 31 May 2020, Mr. BBAC traded Bitcoins with three users. Upon receipt of the screenshots of successful payment transfers to his bank account, Mr. BBAC released the Bitcoins to the traders not knowing that the transferred funds were from the buyer. Mr. BBAC submitted all the supporting documents, including screenshots from the trades. Details of the ultimate beneficiary/suspect remain unknown.



Singapore

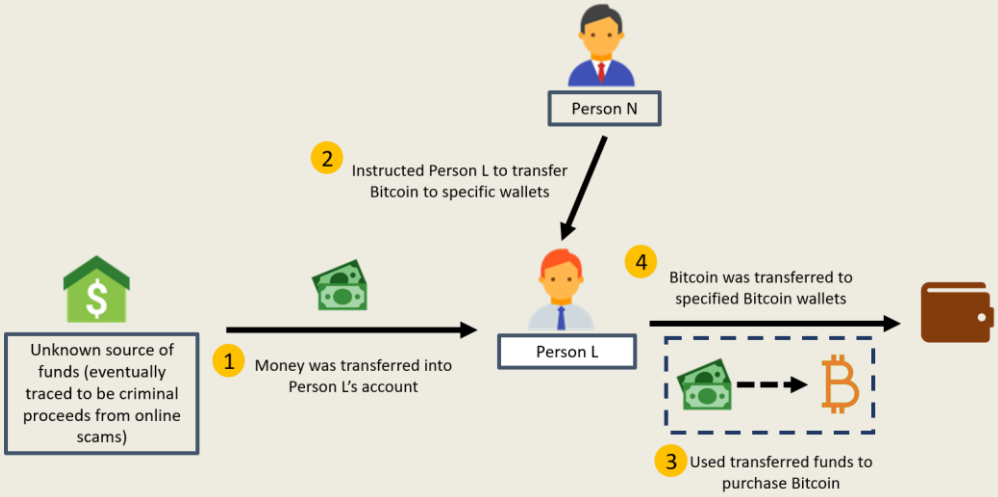
Person L was sentenced on 28 January 2021 to four weeks' imprisonment for providing digital payment token services without a licence. This is Singapore's first conviction under the Payment Services Act (PS Act) which came into force in January 2020. The PS Act criminalises individuals who carry on a business of providing payment services without a requisite license under the said Act.

Sometime in late February 2020, Person L came across a job advertisement listed on a social media platform by an online persona named "Person N". The job required Person L to receive monies in his own bank account, and use them to purchase Bitcoins for a commission set at 10% of the transaction amount.

Person L accepted the job, receiving 13 inward transfers into her bank accounts and withdrawing close to SGD 2,800 (approximately USD 2110) to make multiple purchases of Bitcoin at a Bitcoin machine. At Person N's direction, Person L transferred the Bitcoins to

specified Bitcoin wallets, and deleted the WhatsApp conversation history between them from her phone after every Bitcoin purchase she made.

Although the monies were traced to be criminal proceeds from online scams, investigations did not reveal that Person L knowingly laundered criminal proceeds. Nonetheless, Person L was culpable for an offence through her actions in providing the digital payment token services without a licence.



5.3 Use of professional services (lawyers, notaries, accountants).

Malaysia

Involvement of Law Firm in Siphoning Company Funds

The suspect was appointed by a government agency to oversee the purchase of a landbank for the planting of rubber trees. Deposits for the purchase of the landbank were paid into a law firm's client account which was subsequently transferred to a company before it was swindled by the suspect and his associates, with the collaboration of the lawyer. The purchase of the landbanks never materialised and was aborted by the government agency. The law firm allowed the use of its client accounts to receive the proceeds of illegal activities before the subsequent transfers to the company and ultimately the withdrawal of funds via cash cheques.

Philippines

Use of designated non-financial businesses and professions in setting up entities alleged to have received funds from illicit activities

In 2018, a foreign government requested assistance from the Philippines in relation to an ongoing investigation of its nationals for alleged drug trafficking and ML. The foreign nationals transferred large funds to several jurisdictions, involving the fictitious import of goods from the Philippines. The aforementioned subjects allegedly transferred PHP 1.53 billion (USD 30.6 million) worth of proceeds from drug trafficking to 21 Philippine-based entities and two individuals. Four domestically incorporated service providers were recipients of about PHP 189.3 million (USD 3.79 million) worth of proceeds. Financial records, however, showed PHP 386.42 million (USD 7.73 million) credited to the accounts of the said four service providers.

The 21 entities of the subject request were registered as service providers, trading companies, software solutions, consultancy firms, among others. A certain lawyer and law firm facilitated the incorporation of these companies including the four service providers.

Based on the typology, it was made clear that the lawyer and the law firm providing services are within the scope of the DNFBP Guidelines, e.g. acting as a formation agent, providing a correspondence address, and acting on behalf of juridical persons or arrangements, as defined in the DNFBP Guidelines. They are covered persons under the Anti-Money Laundering Act of 2001 (AMLA), as amended, and as such should be registered with the AMLC.

The existence of typologies and the increasing number of STRs may demonstrate a higher threat rating because these two expose the possible emergence of threats, involving legal persons in the jurisdiction.

5.4 Trade-based money laundering.

Australia

Use of high-end electronics in TBML

In 2017, the Australian Border Force (ABF) commenced examination of a TBML referral from another jurisdiction relating to the exploitation of trade in small portable electronics. Detailed examination through a range of analytical techniques, supplemented by financial and criminal intelligence, enabled ABF specialists to prepare a detailed criminal network assessment of associated entities. Piecing together an extensive network of ML facilitators, the ABF found more than AUD 500 million [EUR 319.8 million/ USD 388,806,522] had passed through Australian bank accounts since 2014.

Proceeds were generated by the sale of drugs in North America. The criminal proceeds were transmitted to bank accounts in South East Asia, before they were subsequently layered through a multitude of Australian bank accounts in Australian FIs. The proceeds were remitted to offshore bank accounts, or used to purchase small, high-end electronic devices for export to companies in South East Asia and the Middle East. The undervaluation of exported devices exaggerated the illicit value being transferred offshore.

In this case, the ABF was able to use a combination of automated and manual trade data discrepancy analysis techniques to better identify and assess suspected instances of TBML. Declarations of goods on export from jurisdiction A should match the corresponding import to jurisdiction B (because the consignment, in theory, is the same thing). When they did not match in this case, ABF officers had reason to believe that the discrepancies were an indicator of trade mis-invoicing, and therefore, potential TBML. Further investigation and collaboration with partner agencies have enabled the linking of the OCG with the transactions.

Daigou operations facilitating TBML:

Investigations have revealed a four-step methodology used in daigou operations to facilitate TBML. Daigou operations refer to persons in one jurisdiction making, often large scale, purchases for consumers in another jurisdiction.

Step One – Funds are generated from the sale of the illicit commodities (including Bitcoin Diamonds (BCDs)) in Australia.

Step Two– Illicitly generated funds are then ‘pooled’ by a money laundering organisation (MLO) and provided to multiple daigou coordinators. Encrypted communication platforms are used by MLOs to provide instructions to daigou coordinators.

Step Three - Daigou coordinators take responsibility for distributing the funds to daigou shoppers in Australia to fund purchases of consumer items. Daigou coordinators also partner with related entities to fund business operations using pooled money.

Step Four – Consumer items are packaged and shipped overseas to an affiliated daigou coordinator, which then sells the items and realises profits in the receiving jurisdiction.

Export indicators of TBML exploiting daigou networks:

- Key indicators of illicit or non-compliant behaviour exhibited include:
- Purchases by daigou shoppers are funded by pools of cash provided by coordinators;
- Pooled funds are held outside of the formal banking system;
- Shoppers receive payment for their activities in cash;
- An absence of legal documents evidencing the nature of the commercial relationship between coordinators and shoppers;
- Off-setting arrangements between Australian-based daigou coordinators and their offshore counterparts are documented in code and/or not declared to government officials.

Bangladesh

Two garments companies 'X Garments Ltd' and 'Y knitting Ltd' exported goods worth USD 5.09 million to business entity 'Z Ltd' against 33 export bills through four banks namely 'M' 'N' 'O' and 'P'. 33 export bills (EXP) were issued by four banks against a sales contract on an advance remittance basis. However, export proceeds amounting to USD 4.68 million out of USD 5.09 million had not been repatriated from business entity 'Z Ltd'.

Bank 'M' issued a Back to Back Letter of Credit (BTB LC) against a fake contract submitted by Company 'X Garments Ltd'. Bank 'M' issued two EXP and Bank 'P' issued 19 EXP against contract and discounted the bills. Bank 'N' issued six EXP and Bank 'O' also issued six EXP against contract on an advanced remittance basis.

The goods (FOB Value USD 429,000) exported through the letters of credit (LCs) issued by Bank M, N and P were found to be sold in a public auction at 'L' Port of the importer jurisdiction. The importer company 'Z Ltd' released goods of six EXP of Bank 'O' with copied documents although the original shipping documents were found to be held in the custody of Bank 'O'.

Both company 'X' and 'Y' are directly connected with business entity 'Z' as the Managing Director of company 'X' is also the owner of business entity 'Z' which is located in a jurisdiction in the Middle East. Thus, it was revealed that Mr. 'S' had exported goods from his Bangladeshi company to his own company located in a foreign jurisdiction and ultimately did not expatriate the export proceeds and thus laundered money from Bangladesh through trade. Based on the analysis, an Intelligence Report with supporting documents was disseminated to Customs intelligence and Investigation Directorate, National Board of Revenue and Criminal Investigation Department (CID), Bangladesh Police for further investigation and necessary legal actions under the provisions of the Money Laundering Prevention Act (MLPA), 2012.

Embezzlement of Bank funds

Mr. X, the proprietor of export-import and supplier company 'ABC Trading' established businesses abroad violating the provisions of the Foreign Exchange Regulation Act, 1947. An

open search revealed that 'ABC Trading' has 20 other sister companies out of which four companies (1. AB Ltd, 2. BC Ltd, 3. CD Ltd, and 4. DC Ltd) were conducting business abroad.

A suspicious transaction report and media report triggered an investigation into the exports of 'ABC Trading' and an export order was identified that was valued at about USD 50 million against 110 letters of credit (LCs), issued by four foreign banks, that had been sent to a Bangladeshi Bank called PQR Bank '(LC Acceptance Bank). The LCs were issued by four banks' in favour of three importer companies, L Ltd, M Ltd and N Ltd for importing tiles from the Bangladeshi company, 'ABC Trading'. Although a team including the branch manager of the LC accepting Bank, PQR Bank, visited the factory of ABC Trading, they did not provide any visit report. Such a gap raised a suspicion as to whether the exporting company had any production facility at all to export tiles.

On the other hand, analysing the credit reports of the tiles importing companies it was revealed that the nature of the business of those three importing companies were leather and wool products. The importation of different kinds of products in a substantial volume compared to their respective paid up capital seemed suspicious. Furthermore it was found that the owner of the three importing companies is a Bangladeshi Citizen Mr. Y.

Unconvinced about the export, further analysis was carried out by the FIU which revealed that all the four LC issuing banks were Shell Banks. Mr. X & Mr. Y in collaboration with PQR Bank's senior executives successfully smuggled about BDT 25 (USD 295,115) million by fraud, forgery and overvalued Export Bills. Later, the bank allowed the exporters to take another BDT 18 million (USD 212,486) in the name of purchasing a documentary bill. In doing so only 80 export bills out of 220 had been repatriated to Bangladesh in order to camouflage illicit business. BFIU analysis concluded that the exporter and importer, in collaboration with senior bank officials under the disguise of international trade had siphoned off money abroad.

Following the findings, an intelligence report was sent to the respective Law Enforcement Agency under the Money Laundering Prevention Act, 2012 for further investigation and legal action.

Fiji

Evasion and elusion

Company F was reported in a STR for making advance payments from Fiji to overseas suppliers and failing to produce customs import entries on a timely basis to its bank. Fiji FIU analysis showed movement of funds from the company loan bank account to the daily administration bank account of Company F. Profiling revealed that Company F had stopped importing in 2016 and began trading as another entity, Company B, since 2015. It was further established that Company B was classified as a hotelier and that Service Turnover Tax (STT) and Environment & Climate Adaptation Levy (ECAL) were also applicable to Company B. The Fiji FIU established that Company B did not lodge its Service Turnover Tax (STT) and Environment and Climate Adaptation Levy (ECAL) since 2015-2019. A case dissemination report was sent to the local taxation authority for further investigation.

Singapore

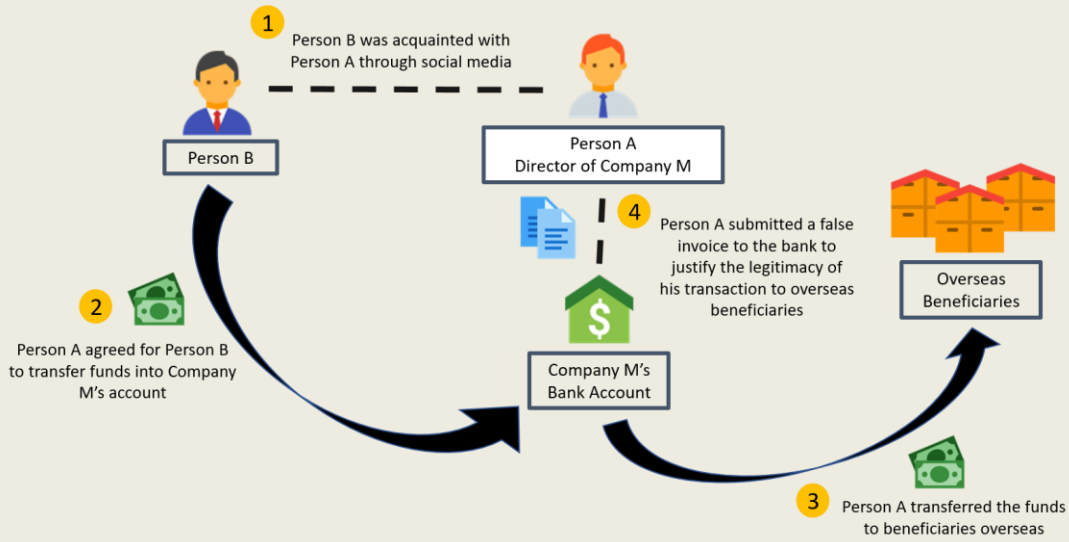
Person A, the sole director of Company M, has been prosecuted for falsifying invoices and money laundering offences.

Pursuant to intelligence received from Singapore's Financial Intelligence Unit, the Suspicious Transactions Reporting Office (STRO), the Commercial Affairs Department (CAD) of the

Singapore Police Force (SPF) commenced investigations into the matter. Sometime in early 2019, Person A became acquainted with an online persona, Person B, via social media, with the latter claiming to be an investor who was keen on investing into Person A's company. Subsequently in July 2019, Person B sought the assistance of Person A to receive and transfer funds to overseas beneficiaries for which Person A would receive a commission for the deposited amount. Person A agreed and allowed the use of Company M's bank account for this purpose.

Company M's bank account was eventually found to have received proceeds, amounting to approximately SGD 225,000 (approximately USD 169,546), arising from an alleged business email compromise fraud victim based in jurisdiction N. Pursuant to notifications received by the bank in relation to a funds recall request on this sum of money, Person A submitted a false invoice to the bank to justify the legitimacy of the transaction, stating that Company M had provided the stated services to a client when it did not. He further extended a copy of the false invoice to Person B to solidify the deception should further checks be made.

Singapore informed the authorities of jurisdiction N that their citizen had been a victim of fraud, which led to eventual exchanges of information. The successful cooperation between jurisdiction N and Singapore authorities was valuable towards the prosecution of money laundering offences, arising from a foreign predicate offence.



5.5 Underground banking / alternative remittance services / hawala.

China

Case on Underground banking

D, W and other suspects developed a website and a smart-phone based application to sell game cards and provide top-up services for both Chinese and foreign clients. They provided illegal cross-border currency exchange, payment and settlement services on third-party platforms for commission.

The public security agency and the AML department of the People's Bank of China established a joint task force to carry out an investigation. In 2020, the public security agency launched a crackdown on the criminal network and arrested more than 50 suspects.

Chinese Taipei

Mr. J was the owner in charge of S group company (S Group) and its subsidiary companies. Between January 2016 and August 2020, with the intention of making a profit by furnishing a place to gamble or assembling people in order for them to gamble, Mr. J convened with various members to establish W online gambling group company (W Group) and set up its branch companies to support the group's basic functions such as hardware maintenance, client services, database management, and financial management. In 2016, W Group began to attract the interest of site owners from other online gambling websites who wished to use the platform designed by W Group and its backstage management services. W Group allotted the profit with those site owners based on a monthly revenue. It was estimated that from the period up to the end of 2019, over 500 site owners had joined, while W Group received approximately NTD 59.5 billion (USD 2,121,308,344) profit during 2016 to 2020.

It was discovered that most of the gamblers were from Jurisdiction X. Those gamblers had transferred funds into the dummy accounts provided by W Group. W Group then moved the funds back to Chinese Taipei using an underground banking system. When Mr. J and his accomplices received the above gambling gains in the form of NTD, they then hid the proceeds in a safe deposit box placed in the subsidiary company filed under S Group and used some to pay personnel and equipment costs of S Group. Moreover, in order to launder the illegal gains through investment, Mr. J and his accomplices established an investment company D, then purchased the stocks of public companies under the names of D, Mr. J, and his accomplices. Furthermore, assisted by the group member, Mr. J purchased the plots of lands to facilitate further investment projects in Jurisdictions P, Q and R, as well as acquiring a public company T in jurisdiction S.

The Prosecutors' Office prosecuted Mr. J, along with his accomplices for violations of the Criminal Code and Money Laundering Control Acts in October 2020.

Hong Kong, China

Case 1

Frequent HKD and USD transactions amounting to HKD 1.6B (USD 206,023,727) and temporary repository of funds were observed in the bank account of an alleged technology company in Hong Kong, China. The pattern of transactions gave rise to a suspicion of activities of an unlicensed money services operator. A police investigation revealed that the company was indeed a shell company and action has been taken to strike it off from the Companies Registry. A police investigation is ongoing.

Case 2

Over HKD 300,000 (USD 38,628), mainly sourced from cash top-up at convenience stores or by peer-to-peer fund transfers via e-wallets, was deposited into stored value facility ('SVF') accounts of a domestic helper in Hong Kong, China and her employer. The funds were then credited to another SVF account under the name of the domestic helper. Investigation revealed that the domestic helper registered three SVF accounts using the identity card of her employer without consent for remitting monies to her home jurisdiction. The domestic helper was arrested and she admitted that she wired monies for her friends and charged them remittance fees. The domestic helper was charged with 'Fraud' and 'Operating Money Service Without Licence'.

New Zealand

Alternative remittance network laundering proceeds of illicit drug offending within NZ

A network of Auckland-based foreign-exchange and money transfer businesses are suspected to have knowingly facilitated the movement of millions of dollars' worth of criminal proceeds derived from illicit drugs, fraud, and other acquisitive crimes. The network used cash collectors to conduct cash pickups from clients wishing to remit funds internationally and deposit the funds into bank accounts of young, third-party mainly foreign nationals in NZ on student visas, where the funds would be consolidated and used to complete remittances from offshore parties seeking to move funds into NZ as NZD (an informal value transfer system). A significant proportion of the cash collected by the network's collectors is believed to have derived from serious illicit drug offending, along with fraud and other acquisitive offences. Neither the principals nor the collectors undertook sufficient (if any at all) CDD on their customers.

Pakistan

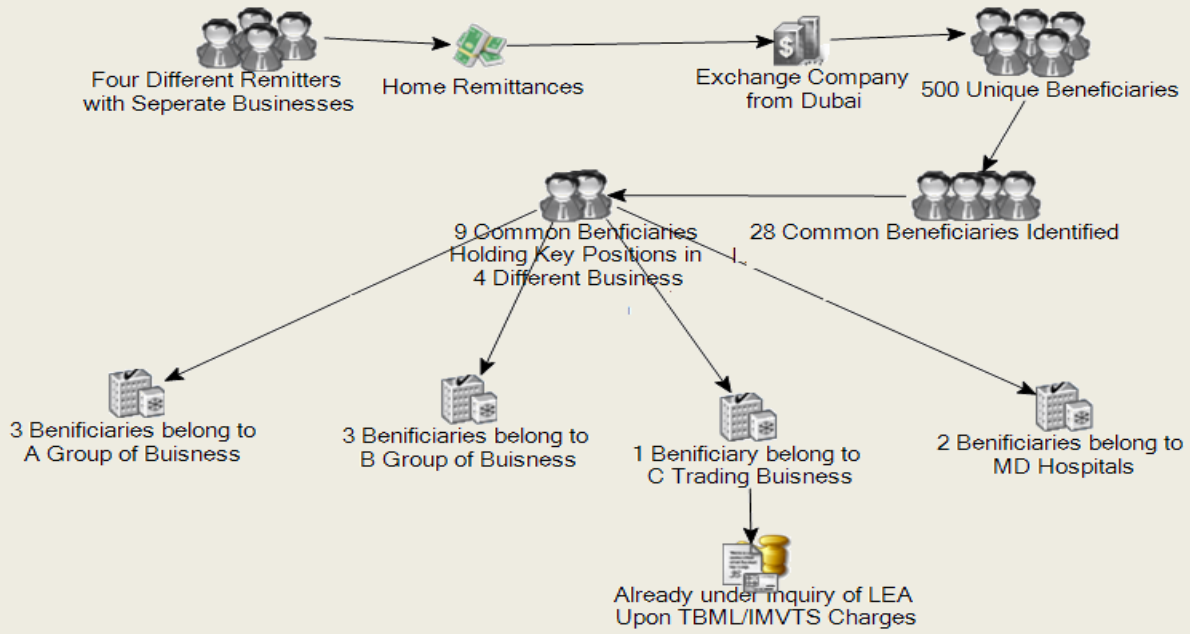
Tax Evasion/Illegal Money Value Transfers

A reporting entity raised STRs on four different individuals for remitting a substantial amount of funds from jurisdiction D to multiple persons in Pakistan. The remitters were Pakistani nationals residing in jurisdiction D, and were engaged in different occupations/businesses. Funds were remitted through an exchange company of jurisdiction D with the purpose of "Home Remittances". Such a substantial number of remittances sent with the sole purpose of home remittances created suspicion.

These four individuals remitted a considerable amount of funds through 1300 transactions to more than 500 individuals in Pakistan. Upon a detailed analysis, more than 28 common beneficiaries were found who were receiving funds from more than one remitter. Nine out of 28 beneficiaries belonged to four different business groups where they held key management positions and received remittances from more than one remitter. These nine beneficiaries paid a very low amount of personal and business income taxes during the last three financial years. During the analysis, it was also identified that a business entity namely XYZ Trading run by one of the beneficiaries was already under investigation by a law enforcement agency for Trade Based Money Laundering charges. The financial intelligence was shared with the relevant LEAs as the suspects were apparently involved in using the channels of IMVTS and home remittance for tax evasion.

International Cooperation Request:

An international cooperation request for information on all the four remitters was sent to jurisdiction D. The FIU of jurisdiction D responded in a timely manner with valuable financial information on the subject remitters which was shared by FMU with the relevant law enforcement agencies for analysis in their ongoing investigation.



Singapore

Person W has been prosecuted under the Payment Services Act for carrying out unlicenced remittance businesses for allegedly receiving illicit proceeds which he tried to remit overseas.

Person W is a Singaporean who is employed at a money-changing company to introduce customers to the company. However, Person W also provided money-changing and remittance services in his own capacity despite not being licensed to do so.

Person W assisted his customers to change or remit monies via net settlements with his overseas contacts. He would collect cash from his customers, and contact his overseas contacts to transfer the equivalent amount in foreign currency from casino accounts, to destination accounts designated by his customers. In one instance, Person W assisted his customer, Person T, to remit monies from Singapore to another jurisdiction, by collecting cash from third parties under Person T's instructions. It was eventually revealed that these monies which Person W collected were fraudulently obtained, having arisen from government official impersonation scams that targeted three individuals.

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

Hong Kong, China

A resident from Jurisdiction X found her online banking account being hacked, resulting in a loss of approximately HKD 16 million (USD 2,060,186) via 23 unauthorised transfers to other bank accounts worldwide, where over HKD 5 million (USD 643,808) was remitted into three bank accounts in Hong Kong, China. The funds were further dissipated to bank accounts held by five shell companies in Hong Kong, China under the directorship of five local persons from Jurisdiction Y. One HK individual was arrested and HKD 3.5 million (USD 450,660) was frozen in the bank accounts. An investigation is ongoing.

5.7 Use of new payment methods / systems.

Hong Kong, China

Case 1

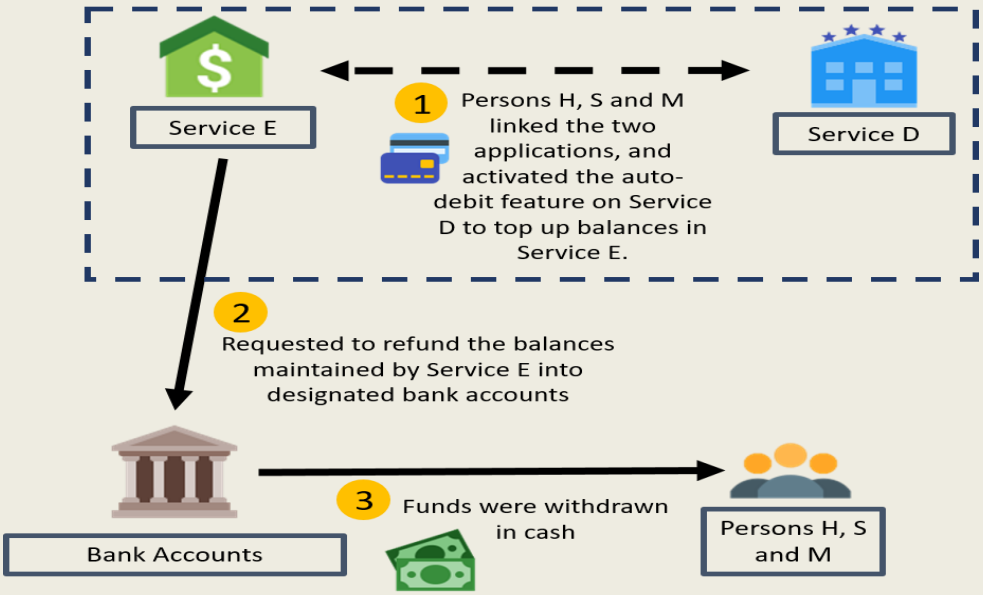
A bookmaking syndicate, with a view to receiving and laundering proceeds of illegal gambling, set up a number of stored value facility ('SVF') accounts in Hong Kong, China under names of their brokers and subordinates. Gamblers transferred monies to brokers for exchanging game points for gambling on the online website and redeemed the points for fiat currency through the brokers via SVF transactions. The syndicate further transferred the crime proceeds to the subordinates' SVF accounts and cashed out at money exchange operators. An investigation revealed that there were over 10,000 transactions amounting to HKD 4 million (USD 515,681) made within two years' time. 17 SVF account holders were arrested for the offence of Conspiracy to gambling and Money Laundering. An investigation is ongoing.

Case 2

Through analysis of a series of cases of online investment fraud and online extortion wherein victims were deceived to transfer monies to virtual bank accounts in Hong Kong, China, it was revealed that these accounts were opened by subordinates employed by a bookmaking syndicate. The syndicate was further found to have laundered crime proceeds totalling HKD 90 million (USD 11,588,125) with the assistance of the person-in-charge of a money service operator. 38 persons were arrested. An investigation is ongoing.

Singapore

This is a syndicate case where Police investigated money laundering offences and offences under the Computer Misuse Act, among others. In 2020, Person H, the mastermind, was sentenced to 27 months' imprisonment for money laundering offences and offences under the Computer Misuse Act. Persons S and M were sentenced to 24 months' supervised probation and fined SGD 5,000 (approximately USD 3767) respectively. Between January to February 2019, Persons H, S and M created accounts on mobile applications services "E" and "D" to facilitate a payment service fraud. Service E is a stored value card which could be used for payment of merchandise, and offers a cash refund service as one of its features. Service D offers virtual prepaid card services. After linking the two App accounts, the perpetrators took advantage of an automatic reload function of Service E with Service D when the former reached minimal balances. Under this arrangement, Service E allowed users to transact on the 'topped-up' balance while only settling the debt with Service D at a later stage. Users of the Service E App were also able to 'refund' the remaining balance in their accounts to a specified bank account. Thus, by deliberately maintaining an insufficient balance in their Service D accounts, the perpetrators were able to incur mounting debts with Service D, which they had no intention of paying off, whilst receiving 'refunds' into their personal bank accounts from which they withdrew cash from ATMs. By virtue of using Service E in the manner described, Person H had committed offences under the Computer Misuse Act. Under this scheme, Person H managed to obtain 'refunds' into his bank account amounting to a total of approximately SGD 36,000 (approximately USD 27,127), either directly using his own bank account or with the assistance of other parties involved in the scheme, such as Person S and Person M. Person H subsequently spent the illicit funds on himself.



5.8 Laundering of proceeds from tax offences.

Australia

In July 2020, AFP Operation BORDELON went to resolution, which resulted in the arrest of a number of Australian-nationals for their alleged involvement in a large-scale tax fraud conspiracy involving misappropriating 'Pay As You Go Withholding' (PAYGW) tax from the Commonwealth, through a structure of entities within the labour hire industry. The proceeds of this crime were subsequently laundered through separate entities both within Australia and overseas.

The alleged fraud involved the following three tier structure:

Tier One comprised two well-established labour hire companies, directed by trusted professional facilitators. These companies contracted services out to multinational construction entities (clients) to provide labour hire and payroll services. The clients, through an invoice financing arrangement, paid the Tier One companies for labour hire services. Upon receipt of these payments, the Tier One companies then transferred the gross wages, plus superannuation, into the payroll service companies (Tier Two).

Tier Two comprised one or more payroll entities, which were appointed with professional straw directors by the syndicate. These companies processed the payroll, transferring the net wages and superannuation to the nominated employee accounts. Financial analysis identified the syndicate's professional facilitators received part of the PAYGW tax as payment from this Tier in return for their services. The remaining PAYGW tax was then withheld from the ATO and transferred directly to the Tier Three companies.

Tier Three comprised multiple companies, operated and controlled by the syndicate. False invoices were allegedly used to disguise the true nature of the financial transfers to these entities (for example, to characterise them as payments for consultancy work, or loans). The proceeds of crime were then transferred on to the personal and corporate accounts of members of the wider criminal syndicate, for their financial benefit.

Fiji

Tax Evasion and Accumulation of Unexplained Wealth

The Fiji FIU received a STR on Person A for the misuse of their personal account for business related transactions, conducting large deposits and a possible case of tax evasion. Checks by the Fiji FIU revealed that Person A was a director of a company and had a sole proprietor business. The nature of business for the company and the sole proprietorship was the provision of freight services and both business entities had alleged to have incurred accumulative losses for the past four years. However, the Fiji FIU established that Person A received large sums of "salary" amounting to more than $450,000 (USD 221,904) within the four years from the company despite declaring losses for both business entities. Further analysis also revealed that Person A opened a term deposit of $130,000 (USD 64,105) subsequent to declaring the losses. A case dissemination report was provided to the local taxation authority.

Hong Kong, China

Two residents of Jurisdiction X were arrested in Jurisdiction X for smuggling cash out of the jurisdiction and luxurious goods from Hong Kong, China to Jurisdiction X without declaration. Fake invoices purporting that the value-added tax was settled in Jurisdictions X and Y were also found to have been presented for the purpose of tax evasion. An investigation by Hong Kong Police revealed that the suspected proceeds derived from the tax evasion were remitted to bank accounts in Hong Kong, China and HKD 11 million (USD 1,416,315) was withheld. An investigation is ongoing.

Indonesia

As stated in the Academic Paper on the Effectiveness Index of AML/CFT by the Indonesian FIU, the Financial Transaction Reports and Analysis Centre (PPATK) in 2020, the case of money laundering with predicate offences in the field of taxation was carried out by Mr. RAS by issuing tax invoices that were not based on actual transactions and the misuse or unauthorised use of a Taxpayer Identification Number or Taxable Entrepreneur Registration Number. The state losses arising from this crime amounted to IDR 577 billion (USD 39,903,910). The typology carried out by Mr. RAS in carrying out money laundering proceeds of crime is as follows:

a. Placing; placing the proceeds of tax crime by ordering agents or sellers and users of fictitious invoices to deposit funds into Mr. RAS' account and / or on behalf of the suspect's company for at least IDR 25,761,908,836 (USD 1,781,455).

b. Transferring; transferring the proceeds of tax crime by transferring money on behalf of the suspect either at the same bank or to another bank and transferring money from the suspect's company either at the same bank or at a different bank, and transferring money from the suspect / company belonging to the suspect's third party account. There were minimum incoming transfers of IDR 51,881,427,007 (USD 3,586,524) and USD 1,465,648, and minimum outgoing transfers of IDR 14,002,394,683 (USD 968,290) and USD 75,855.

c. Spending; to spend the proceeds of the tax crime by purchasing assets in the form of property and offices of at least IDR 15,200,000,000 (USD 1,050,728).

New Zealand

Laundering of tax evasion proceeds

A restauranteur concealed more than NZD 6.5 million (USD 4,660,912) in primarily cash sales conducted through the chain of 13 restaurants he owned, during a six-year period. As part of this plot, his companies filed 115 GST returns which contained false or misleading sales figures and a GST tax shortfall of more than NZD 700,000 (USD 501,953).

The proceeds of the offending was laundered via discrete activities which were undertaken with the express intention of concealing the source of funds. This included handing bags of cash to his accountant which was then sent around the world and laundered through foreign exchange transactions and forex trading.

Given the offending spanned many years, the absence of reliable records and the offender's persistent failure to ensure tax returns were filed by his restaurants, the precise scale and nature of the offending is unknown. The offender pled guilty to 34 tax evasion charges and nine charges of money laundering and was sentenced to three and a half years imprisonment and fined NZD 50,000 (USD 35,853).

Singapore

The Inland Revenue Authority of Singapore (IRAS), Commercial Affairs Department (CAD) of the Singapore Police Force and the Corrupt Practices Investigation Bureau of Singapore (CPIB) initiated a joint investigation against Person A. In June 2020, a foreign national, Person A, was convicted on tax evasion, corruption and money laundering offences, and sentenced to 18 months' imprisonment and a tax penalty of SGD 60,000 (approximately USD 45,212).

Person A made at least six fraudulent tourist refund claims under the Electronic Tourist Refund Scheme ("eTRS") in 2013, with the assistance of Person B who was a Singapore Customs officer responsible for approving the said claims. Investigation showed that Person A gave bribes to Person B for endorsing the fraudulent claims. Person A subsequently departed Singapore over several occasions with the GST refunds totalling cash of SGD 27,895 (approximately USD 21,020), which constituted the removing of criminal proceeds from Singapore.

Person A left Singapore prior to the commencement of investigations, but he was swiftly apprehended upon his re-entry to Singapore in October 2019. Person B was also convicted and sentenced for tax evasion and corruption offences and is no longer employed with Singapore Customs.

5.9 Real estate, including roles of real estate agents.

Chinese Taipei

In December 2018, Ms. C and her accomplices forged the contract which enabled the borrowing of Mr. W's name for real estate registration, and also engraved Mr. W's seal without his consent. The contract recorded that Ms. C purchased a plot of land A from Mr. X, and registered it under Mr. W's name.

According to this contract, Ms. C is allowed to ask Mr. W to return the land to her at any time. With the purpose of defrauding the other financiers, Ms. C then designed a fraud scheme, by which she first accused Mr. W of not returning land A to her after she formally made a legal request; then Ms. C made a civil writ mediation petition and brought it to court. In January 2019, Ms. C's accomplice faked his identity as Mr. W and appointed a lawyer to make an

agreement with Ms. C. Ms. C then acquired the legal ownership of land A. Ms. C subsequently hired the agent Ms. L to introduce to her people who could provide financial aids after reaching an agreement with Ms. C that Ms. C provided the land A and used it as collateral to the financiers under a maximum-amount mortgage.

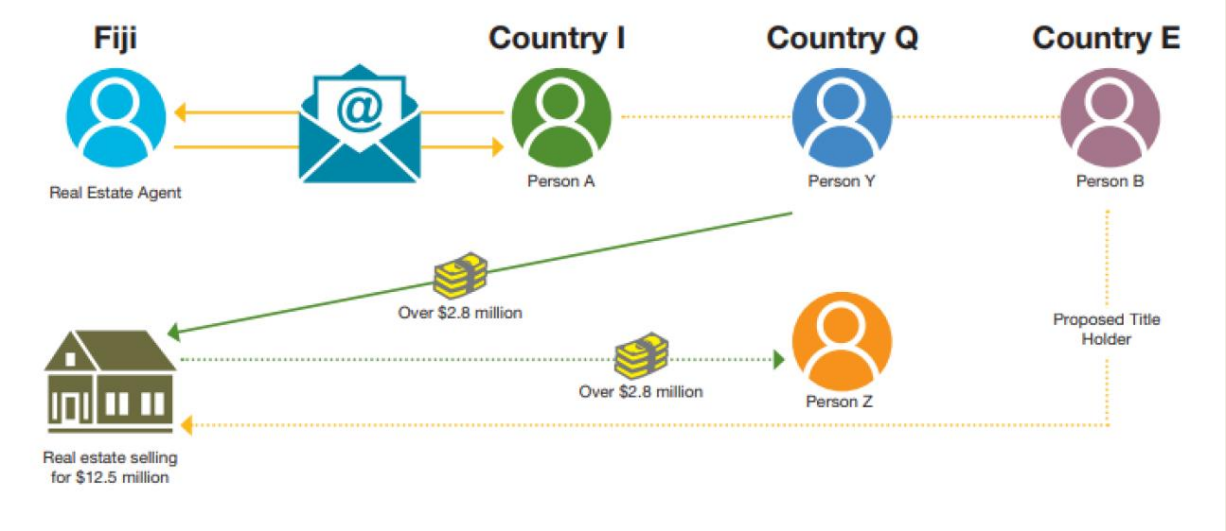
In order to conceal and transfer the illegal gains, Ms. C opened her personal accounts at Bank E and Bank F as well as her banking account opened at Bank G. After receiving the remittances from those aforementioned financiers, Ms. C went to those banks to make cash withdrawals in small amounts many times. In addition, she asked the above banks to issue cashier's cheques and subsequently borrowed other people's bank accounts to cash those cheques.

After investigation, the case was referred to the Prosecutors' Office in August 2019 for violations of the Criminal Code and Money Laundering Control Act.

Fiji

Money Laundering through Real Estate Transactions Persons

A, B, Y and Z, who are foreign nationals, were reported to the Fiji FIU in a STR for a possible case of money laundering involving a real estate transaction of over FJD 2.8 million (USD 1,380,713). In December 2019, Person A attempted to purchase a high-end luxury property for FJD 12.5 million (USD 6,163,944). Person A and another unknown individual met with the real estate agency regarding the property deal. In January 2020, Person A arranged funding through Person Y in jurisdiction Q, who remitted over FJD 2.8 million directly into the real estate agency's trust account as the deposit payment. Person A stated that Person B, who was his business partner in jurisdiction E, would be listed as the owner of the property in the sale and purchase (S&P) agreement. When the offer by Person A of FJD 10 million (USD 4,931,206) was not accepted by the vendors of the property, he instructed the real estate agency to refund the deposit amount to another individual, Person Z in jurisdiction Q. Fiji FIU analysis revealed that Person A was the only party communicating with the real estate agency through email and instant messaging applications, which did not include Persons B, Y and Z. It appeared that Person A was the main party in control of the real estate transaction. Interestingly, Persons A, B and Y had never travelled to Fiji and it was noted that Persons Y and Z had the same dates of birth. Further checks with national and international law enforcement agencies revealed that Person A was allegedly working with an organised crime syndicate involved in illicit importations of drugs in jurisdiction Y, and that Person B and Person Z are jurisdiction Q nationals issued with jurisdiction E citizenship through jurisdiction E Government Development Support Program. Additionally, it was established that Person B was a red notice fugitive in jurisdiction Q, who was using fake identification documents in Fiji. Person B was deported to jurisdiction Q in January 2020.



Hong Kong, China

Members of a syndicate purchased eight luxury real estate properties in Hong Kong, China and applied for mortgage loans with the banks. An investigation revealed that the proof of income in the mortgage loan applications was fictitious and artificially made up by the syndicate. Nine syndicate members were arrested with HKD 10 million (USD 1,287,484) in proceeds of crime temporarily frozen. An investigation is ongoing.

5.10 Trade in gems and precious metals.

Australia

In October 2020, the United States Office of Foreign Assets Control (OFAC) listed an Australia-based al-Qa'ida-associated facilitator person A for having materially assisted, sponsored, or provided financial, material, or technological support for, or goods or services to or in support of, Al-Qa'ida.

Person A has had financial dealings in a number of jurisdictions and is involved in dealing gemstones, which provide him with the ability to move funds internationally for the benefit of al-Qa'ida. Person A conducts business around the world.

Hong Kong, China

A person and two accomplices purchased 3,000 taels[32] of gold bars with HKD 60 million (USD 7,724,993) cash at a goldsmith shop in Hong Kong, China. The trio were arrested and an investigation revealed that they were paid to collect the cash from a money service operator for the purchase and deliver the gold to others. Further investigation revealed that the monies were remitted from Jurisdiction X and the gold would be delivered to a syndicate in Hong Kong, China. Three syndicate members were then arrested with a total of 600 pieces of 5-tael gold bars, cash and jewelleries amounting to HKD 78 million (USD 10,042,222) seized. An investigation is ongoing.

Singapore

[32] A Chinese unit of measurement. One tael is defined as 1+1⁄3 ounce and is approximated as 37.7994 g

In March 2020, three precious stones and precious metals dealers ("PSMDs") – Companies P and G and Person T – were charged in court with offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, Chapter 65A ("CDSA").This was in relation to a series of frauds perpetrated in 2019 by a criminal syndicate against a public agency, which resulted in total losses of SGD 40 million (approximately USD 30 million). In particular, two of the syndicate members were found to have used the criminal proceeds to purchase SGD 600,000 (approximately USD 452,123) worth of jewellery and gold bars from these three PSMDs using cash. These two syndicate members have been charged with money laundering offences, among others. In Singapore, PSMDs who enter into cash transactions exceeding SGD 20,000 (approximately USD 15,070) are obligated to submit a cash transaction report ("CTR") to a Suspicious Transaction Reporting Officer within 15 business days. The three PSMDs in this case had failed to do so for the said purchases. Furthermore, Person T also failed to perform the requisite customer due diligence which was a punishable offence under the CDSA. Between August and October 2020, Company P and G and Person T were sentenced to fines ranging from SGD 9,000 (approximately USD 6,781) to SGD 40,000 (approximately USD 30,141).

5.11 Association with human trafficking and people smuggling.

Hong Kong, China

Hong Kong Police neutralised a human smuggling syndicate, which arranged sea passage and entry of illegal immigrants from Jurisdiction X to other jurisdictions through Hong Kong, China, and resulted in the arrest of the ringleader and three active syndicate members. An investigation revealed that suspected crime proceeds of about HKD 3.4 million (USD 437,766) were laundered via the ringleader's two personal bank accounts in Hong Kong, China. The ringleader was convicted of 'Money Laundering' and sentenced to 3 years' imprisonment. A total of HKD 270,000 (USD 34,764) was also confiscated.

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

Hong Kong, China

Case 1

An investigation into the personal bank accounts of an arrested drug trafficker in Hong Kong, China and his close relatives revealed that the drug trafficker had been controlling his own and mother's bank accounts to launder over HKD 7 million (USD 901,293) in crime proceeds. The drug trafficker was charged with Money Laundering and a court proceeding is ongoing.

Case 2

A joint operation was launched between Hong Kong, Jurisdictions X and Y to combat against cross-jurisdictional drug trafficking activities where the syndicate ringleader had been arranging fishing vessels to transport dangerous drugs from Jurisdiction X to other jurisdictions and colluding with his associate in Jurisdiction Y to procure vessels and recruit crews for the transportation. An investigation revealed that the ringleader and his two family members had used 21 bank accounts in Hong Kong, China to launder HKD 113 million (USD 14,548,025)

in drug proceeds. One of the family members was convicted of 11 counts of Money Laundering and sentenced to 3 years of imprisonment. The remaining HKD 42 million (USD 5,407,255) in her bank accounts was confiscated.

Indonesia

Mr. NL is the President Director of the XYZ Financial Credit Institution (FCI) which aims to raise public funds without a business license from the regulator and then lend funds to the public with an interest rate of 10%. During the 5 years of operation, the FCI managed to raise funds amounting to IDR 413 billion (USD 28,533,176) from 16,155 customers. However, on the other hand, FCI XYZ did not actually obtain a business license from the management of Bank Indonesia.

For each fund that has been collected, an amount of around IDR 7 billion (USD 483,791) to IDR 10 billion (USD 691,120) in the FCI XYZ account, will be transferred by NL to a personal account which is then transferred back to many accounts, including accounts belonging to NL, NL's wife, NL's children and employees. In addition, NL also used the money to purchase assets in the form of land, buildings, project payments, cars and three insurance policies worth IDR 500 million (USD 34,555) each. For this act, NL has been sentenced to four years and a fine of IDR 1 billion (USD 69,084).

Macao, China

Suspects B and C, who are a couple, allegedly embezzled over USD 800,000 from jurisdiction N. In order to disguise and conceal the illicit origin of the funds, suspects B and C remitted their deposits in jurisdiction N to Macao, China and informed suspects D and E, who are suspect C’s parents, to collect the money. Suspects D and E repeatedly received the remitted funds at banks, applied for fixed deposits, bought insurance policies, purchased stocks and shares, and engaged in real estate property transactions in Macao, China to transfer and conceal illegal proceeds, by converting illegal proceeds into other forms of assets.

Suspects B and C were convicted of embezzlement and sentenced by the court of jurisdiction N afterwards. In 2020, suspects B, C, D and E were charged for money laundering by the Public Prosecutions Office. When jurisdiction N was investigating the embezzlement case against suspects B and C, a request for mutual legal assistance in criminal matters was issued to Macao, China for assistance in investigation and getting evidence.

Pakistan

Money Laundering/Tax Evasion

STRs were reported against multiple members of a family and their employees by two different reporting entities during 2019 and 2020 on the grounds that they were maintaining various bank accounts and giving the mandate of operating those accounts to two family members, Mr. A and Mr. B, who were related as father and son.

Upon analysis of multiple STRs raised by reporting entities on members of a family and their employees, it was found that they were all engaged in the timber business in a famous market of one of the biggest cities of the jurisdiction. Moreover, it was also revealed that alongside running sole proprietorship businesses, they were also holding the positions of directorship in a number of private limited companies and were maintaining individual, sole proprietorship

and company accounts. The same business addresses and contact numbers were provided in account opening forms of all the bank accounts. After an analysis of the statements of those accounts, it was observed that a substantial amount of funds were routed through various accounts being maintained by the family members and their employees at different banks. After receipt in the accounts, the funds were then immediately transferred to the accounts of other members of the family where Mr. A and Mr. B exercised effective control. Funds were also credited through transfers by the counter parties located in far flung areas of the jurisdiction who appeared to be involved in Hawala/Hundi. In addition to the accounts, of which there were 72 as reported in the STRs, 37 more accounts were identified in CTRs reported on the same family members wherein the mandate of operating these accounts was again held by both the individuals, Mr. A and Mr. B. Furthermore, a practice of opening new accounts and closing the old ones by the accountholders was observed. Based on the analysis, the financial intelligence was shared with an LEA to further investigate the matter for money laundering and tax evasion.

Philippines

Nationals from Jurisdiction X used and enticed Filipinos to register sole proprietorship businesses and open bank accounts for the said businesses. The Filipinos were only the owners on paper, while the Jurisdiction X nationals had full control of the business and the accounts.

Person Z (Jurisdiction X national) deposited millions of pesos into the accounts of Persons D (Jurisdiction X national) and F (Filipino). The recipients of funds declared Company H, a Philippine-registered business, as the source of funds.

The Anti-Money Laundering Council (AMLC), in coordination with the said law enforcement agency, was able to trace the accounts and froze the funds with an estimated value of PHP 78 million (USD 1,624,174).

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

Chinese Taipei

CIB received information concerning a fraudulent syndicate T, which specialised in setting up dummy accounts in Jurisdiction X and provided these accounts to others for illegal uses. After an investigation, it was discovered that the principal suspect of the syndicate T, person A recruited unspecified persons to open financial accounts in banks operated in Jurisdiction X, and used those accounts to launder money through illegal online gaming operators.

It was determined that all of the recruited accounts were collected and used by a same group working in the same building, which was deemed a laundering centre. It was estimated that the daily money laundering flow was about 10 million in Jurisdiction X currency (USD 1,544,823). On 8 June 2020, CIB searched the building and multiple locations and subsequently seized 19 computers, 87 telephones, 57 SIM cards, 23 application contracts, 323 USB keys from banks located in Jurisdiction X, 140 Union Pay cards and other money laundering exhibits, and arrested person A and another eight members who worked in the above laundering centre.

After a thorough investigation, CIB further found that the members working in the laundering centre were all employees of Y Company. On June 18, 2020, CIB searched the head office of Y Company and discovered another three online gambling platforms operated by Y Company. CIB immediately seized 10 computers, 16 mobile phones, and 7 Union Pay accounts and arrested the head of the company, person B, and his accomplices.

Hong Kong, China

Case 1

Hong Kong, China and Jurisdiction X jointly neutralised a cross boundary bookmaking syndicate with 23 persons arrested for 'Bookmaking' and 'Money Laundering' in Hong Kong, China and 33 persons arrested in Jurisdiction X during synchronised raids. An investigation revealed that more than HKD 216 million (USD 27,806,578) derived from bookmaking activities was laundered through 18 accounts in the names of four core syndicate members. Three of them were convicted of 'Money Laundering' and 'Bookmaking' and sentenced to 24 to 57 months of imprisonment and HKD 2 million (USD 257,467) was confiscated. A court proceeding is ongoing against the last mastermind who is facing a count of 'Money Laundering' and HKD 20 million (USD 2,574,701) worth of assets in both Hong Kong, China and Jurisdiction Y have been frozen.

Case 2

A financial investigation suggested that Mr. A had used his personal bank account and that of his family members and associates in Hong Kong, China to launder crime proceeds of about HKD 100 million (USD 12,873,244) in five years' time. The residence of Mr. A was raided with bookmaking paraphernalia such as betting slips and audio betting records seized. After investigation, Mr. A, his family members and associates were charged with and convicted of 'Engaging in Bookmaking' and 'Money Laundering'. Confiscation Orders were granted against three of the convicted persons, who were ordered to pay some HKD 4 million (USD 514,928) to the Government.

Mongolia

An STR was submitted by a bank with the suspicion that 'the amount, number and frequency of transactions on customer B's account did not correspond to the customer's employment and business. He may have been involved in organising illegal online gambling activities'.

FIU-Mongolia conducted an analysis on this STR collecting more information from reporting entities and found out that person B was using his two accounts to collect betting money and distribute winning money to players. During the period of analysis, person B received the total amount of MNT 1 billion (approximately USD 350,000) in about 500 transactions through ATM and domestic bank transfers to his first account. Moreover, he received MNT 5.7 billion (approximately USD 2 million) into the same account from five different individuals in 3,025 transactions with descriptions containing the same word. It is assumed that these five individuals were associates of person B. After receiving the funds, he transferred a large sum of money from his first account to his second account. Then he transferred and distributed money in small amounts to 6,000 different individuals from his second account through 70,000 transactions with descriptions containing random letters and numbers. In addition, the majority of the aforementioned transactions were made from 1 am to 5 am at intervals of 1-2 minutes.

As a result of the analysis, FIU-Mongolia disseminated this case to a law enforcement agency for further investigation.

During the investigation, it was established that these suspects organized illegal online gambling, laundered the proceeds gained from such gambling and bought movable and immovable properties worth MNT 4-5 billion (USD 1,404,201 to USD 1,755,251). The investigation of this case is ongoing.

5.14 Purchase of valuable assets (art works, antiquities, race horses, vehicles, etc).

New Zealand

Proceeds of multi-billion-dollar international fraud scheme used to purchase artwork, property and vehicles in name of NZ foreign trust

A network of overseas-based offenders misappropriated billions of dollars from a (non-NZ) government-owned investment company and laundered these funds via a complex network of trust and company structures. One of the principals of the network (individual A) established two NZ foreign trusts, naming himself and his close family members as beneficiaries, with a NZ limited liability company established by a NZ TCSP to act as the trustee of the trusts. The trusts owned assets in several overseas jurisdictions, including several pieces of artwork by an internationally renowned artist, a luxury yacht, and luxury properties. The ownership structure involved the creation of special purpose (non-NZ) companies which owned the assets; the shares of these companies were owned by holding companies in another (non-NZ) jurisdiction, whose shares in turn were owned by the NZ foreign trusts, the beneficiaries of which were individual A and his family members.

5.15 Investment in capital markets, use of brokers.

Chinese Taipei

Mr. S was the owner in charge of T company, while Ms. Z was T company's accountant as well as cashier. During the period from 2016 to 2019, with the intention of embezzling the company's property for her own personal use, Ms. Z took Mr. S' passbook and his seal of the account opened at A bank, which Mr. S provided only for T company's use, to withdraw a total of NTD 7,615,420 (USD 272,306).

In order to conceal these illegal gains, during the period between 2018 and 2019, Ms. Z made three separate withdrawals, extracting a combined sum totalling NTD 1,080,000 (USD 38,621) from Mr. S' aforementioned account, subsequently transferring this money into her son's settlement account to buy the stocks of C company.

After the investigation by MJIB, the case was referred to the Prosecutors' Office in October 2020 for violations of the Criminal Code and Money Laundering Control Act.

Hong Kong, China

Two cannabis plant cultivation centres were raided, resulting in the arrest of four persons including the mastermind Mr. X and his family member Ms. Y in Hong Kong, China. The 11 bank and securities accounts of Mr. X recorded total deposits of more than HKD 7 million (USD 901,142) in 3,500 transactions, over half of which was deposited by cash from unknown sources while the remaining portion was transferred from various counterparties. Ms. Y was found to have controlled more than 15 bank and securities accounts and the total deposits amounted to HKD 15 million (USD 1,931,008) in 7,500 transactions, which were inconsistent with her financial background. Mr. X and another two persons were convicted and sentenced to five years and 10 months' imprisonment and over HKD 5 million (USD 643,657) was confiscated. Ms. Y was charged with 'Money Laundering' and over HKD 7 million (USD 901,142) worth of assets were restrained. A court proceeding is ongoing.

Indonesia

Market Manipulation

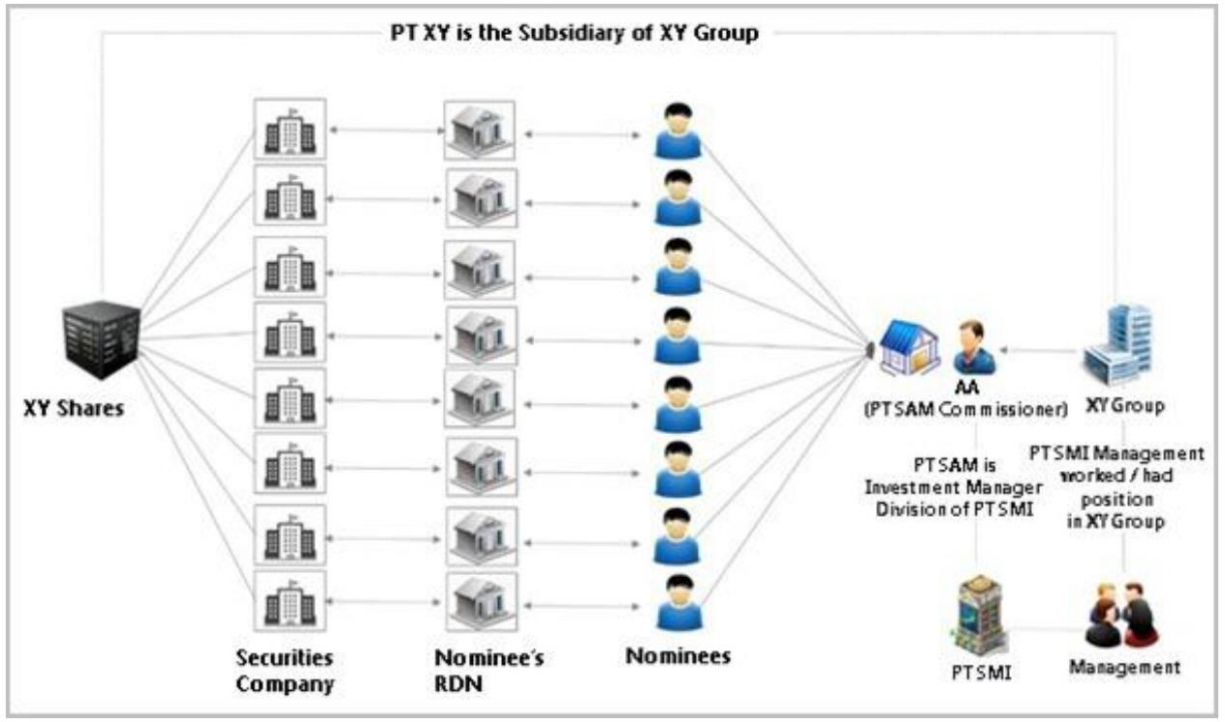
Mr. AA is a Commissioner at Company A which is engaged in Investment Management as a result of the separation of the Investment Manager Company division of SMI Company. Company A itself has a license as an Investment Manager from the regulator.

Mr. AA uses parties as nominees to conduct stock transactions through 13 different securities companies. Based on the identification of the Customer Securities Account of the nominee parties, the account opening was carried out at the same bank, namely Bank XX and within the same period or close.

The job profiles of nominee parties that are used vary widely, including private employees and self-employed workers who have different income and age profiles and even have an income of less than IDR 2 million (USD 138) per month.

Then, Mr. AA transfers to the accounts of nominees, which are then used to purchase one type of the same share, namely XY shares. During 2016, Mr. AA's account had a total transaction volume of IDR 7 trillion (USD 484,940,661).

Based on the analysis of financial transactions, there is a flow of funds in the form of "U Turn Transactions" from the nominee party's account to Mr. AA's account. A comparative analysis was conducted on the transactions of Mr. AA through the nominees. When the XY stock value reached the highest value, the total transaction volume of the nominees reached more than 40 percent of the transaction volume of XY shares in the market. This shows the significance of the sale and purchase transaction of XY shares by Mr. AA through the nominees. In addition, the funds sent from Mr. AA to the nominees were only used to transact in XY shares. There is an alleged affiliation between Mr. AA with XY Group because Mr. AA worked at XY Group and there is a flow of funds in Mr. AA's account from several XY Group subsidiaries.



RDN: Securities account

PT: Company

5.16 Mingling (business investment).

Indonesia

Fraud and Illegal Bank

B Cooperative was a cooperative operating in the transportation and other businesses in Indonesia. Its management consisted of Mr. AND as the chief, Mr. CEK as the Secretary along with Mr. JUL and Mr. YUL as the administrators. Meanwhile, Company A which was also led by Mr. AND was faced with a financial obligation that prevented Mr. AND from listing it as a public company. It was stated that Company A was constrained by Bapepam's (Indonesia's Securities and Exchange Commission) regulations so that the Company cannot go public if it has obligations to more than 50 parties.

There was a partnership agreement between Company A and its investors (called partners). However, Mr. AND made an agreement with Mr. CEK and the partnership was transferred to Cooperative B without the partners' knowledge. The partnership also transferred Company A's debts to B Cooperative, clearing the way for listing of Company A on the stock exchange. However, B Cooperative was not licensed to accept deposits from public fundraising.

Partner funds of Company A that have been collected from 2007 to 2014 amounted to IDR 4,779,976,704,333 (USD 333,823,791) and around IDR 3,264,688,621,100 (USD 227,924,779) could not be retrieved by partners.

The investment money from the community/partners was placed by the defendants in accounts in the name of the B Cooperative and was then withdrawn in cash by cheque and giro transfer form. The funds were placed back through banking instruments by means of cheques, giro transfer form and RTGS into the personal accounts of the defendants and companies owned by the defendants, which amounted to around IDR 319,456,000,000 (USD 22,309,663). The funds were used to pay employee salaries, pay vehicle tax and purchase land and building assets and lend to Company A amounting to IDR 200,000,000,000 (USD 13,967,582).

5.17 Use of shell companies/corporations.

Hong Kong, China

A drug trafficker was arrested in Jurisdiction X and an investigation revealed that the drug trafficker had laundered HKD 540 million (USD 69,524,478) through four corporate accounts of two shell companies in Hong Kong, China, out of which HKD 138 million (USD 17,767,240) was remitted through remittance agents in Jurisdiction X. The directors of the two companies were convicted of 'Conspiracy to Money Laundering' and sentenced to 38 months' imprisonment.

New Zealand

NZ registered shell company used as part of international ML network

A NZ limited liability company (Company A) was incorporated and used to open bank accounts in an overseas Jurisdiction (Jurisdiction A). Funds were sent to Company A's accounts in jurisdiction A from company B's accounts in another overseas jurisdiction (Jurisdiction B). Overseas inquiries established that Company A was likely being used as part of a wider network of companies to move illicit funds from Jurisdiction B to Jurisdiction A.

Company A was listed as a 'manufacturer or wholesaler' but in reality it had no substantive business operations either in NZ or the overseas jurisdictions. The payments made in Company

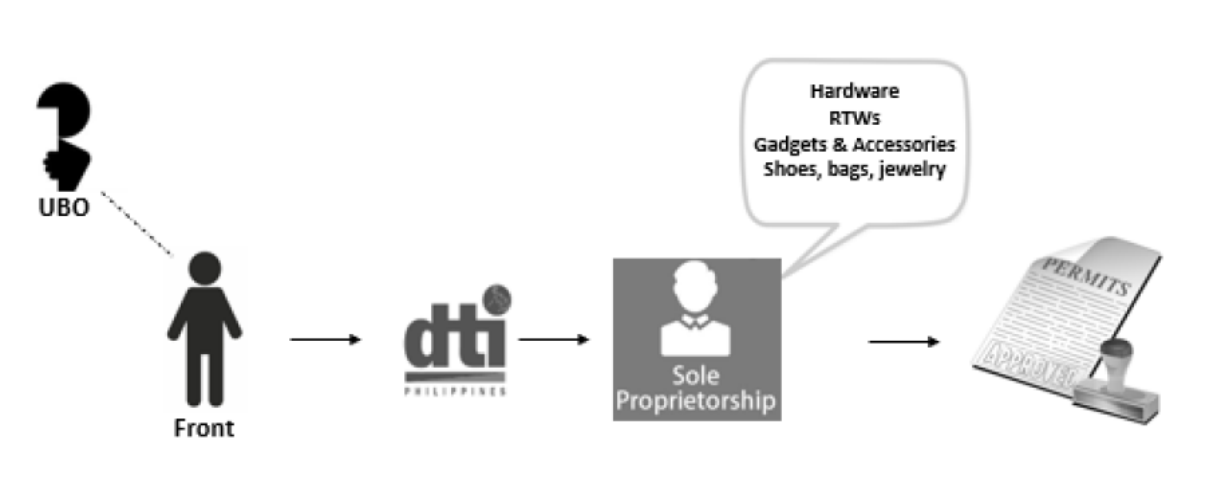
A's name were accompanied by false invoices referencing textile products, with fake logos, stamps and signatures that had been superimposed over electronic documents. Further inquiries by offshore agencies established no goods were actually being shipped – they were 'phantom shipments'. Company A had been incorporated by a NZ TCSP whose website advertises 'offshore asset protection and tax minimisation… with professional directorship services provided on request.' It had no substantive NZ footprint, no NZ bank accounts, and the directors and shareholders were nominees appointed by the NZ TCSP.

Philippines

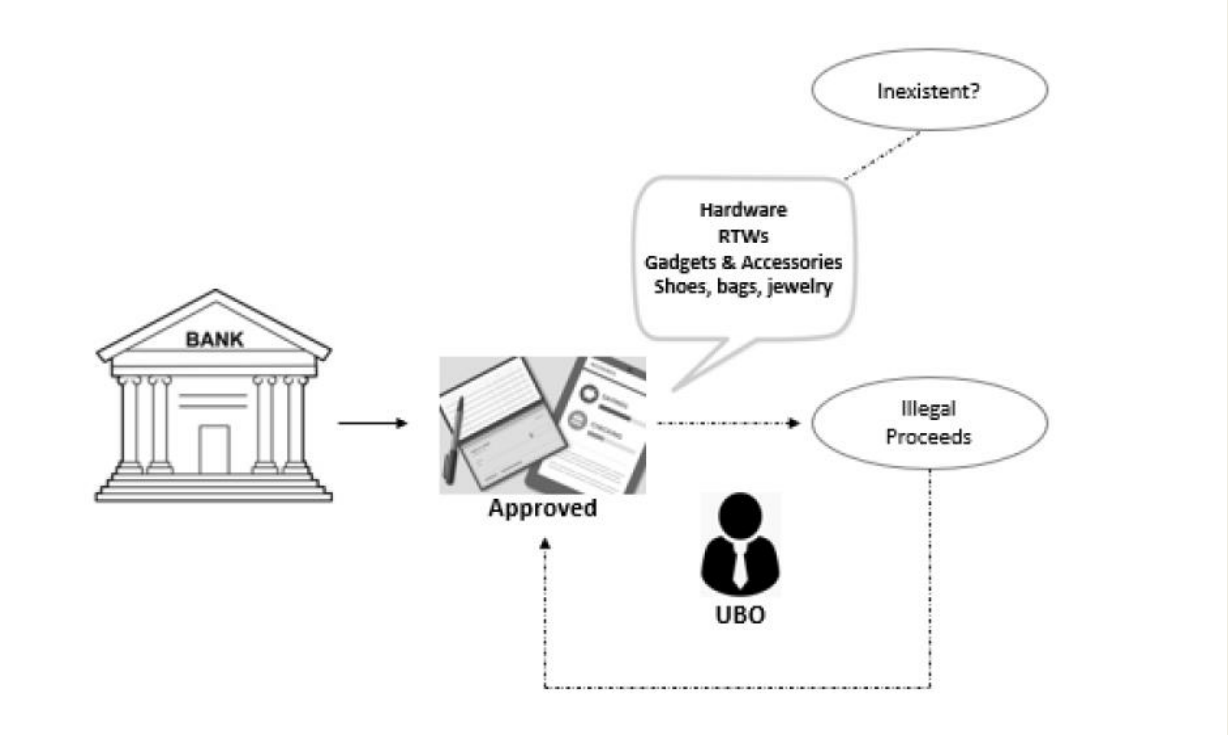
Use of business entities to facilitate drug trafficking

In August 2020, the AMLC published a typology on the use of Filipino nationals and their businesses by foreign nationals in illegal drug activities.

The identified modus operandi involves Filipino nationals ("the front"), who register sole proprietorship retail businesses with the Department of Trade and Industry (DTI) on behalf of certain foreign nationals, who are the actual and ultimate beneficial owners (UBOs) of the said businesses. The said businesses likewise operate without the capitalisation required by law for foreign owners. These companies are under the complete control and operation of these foreign nationals.



After registration with the DTI, the front goes to the bank (mostly commercial and universal banks) with the newly acquired DTI registration permit to open an account in the name of the newly registered business.



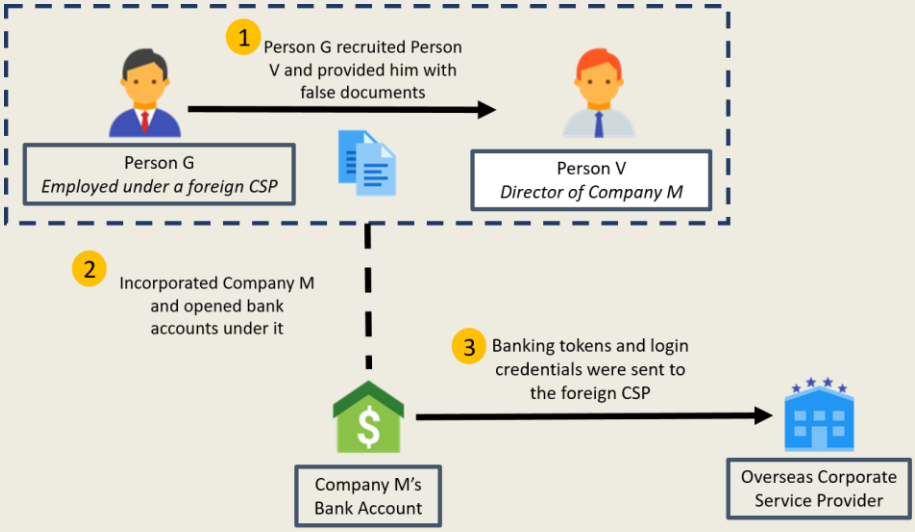
The said bank account will then be managed and controlled by the foreign nationals—the UBOs—for the purpose of receiving funds from illegal proceeds. Moreover, the majority of the registered sole proprietary businesses, as identified in this modus operandi, are discovered to be "shell companies" or inexistent companies.

Singapore

Case one

Person G was sentenced to 10 months' imprisonment in January 2020 for money laundering offences. The co-accused, Person V was sentenced to five months' imprisonment for using a false document to dishonestly induce a local bank into approving his corporate bank account application. Person G worked for an overseas corporate service provider and one of his responsibilities included recruiting individuals to become nominee company directors and set up corporate bank accounts in the company's name. These nominee directors would then cede control of the company and its bank accounts for a fee. Person G was aware that his employer was in the business of selling shell companies and their corporate bank accounts, often for criminals to launder money. In this particular case, Person G recruited Person V, and the two persons visited Singapore in December 2018 to incorporate Company M and open corporate bank accounts. Pursuant to this, Person G handed Person V a false document that portrayed the latter as a successful businessman to assure the bank that the company was operated by someone with sound financial standing. The Internet banking access token, together with Internet login credentials, were then couriered to the overseas corporate service provider after the bank account was opened.

In April 2019, CAD received a report that Company M had received USD 50,000 in criminal proceeds in its bank account. CAD swiftly established the identities of the persons involved and arrested Person G and Person V when they entered Singapore. CAD recovered around USD 7,600 of criminal proceeds during investigations.



Case two

In August 2020, Person B was convicted in court for an offence under Section 157(1) of the Companies Act, for his failure to exercise reasonable due diligence as a director. He was sentenced to a fine of SGD 5,000 (USD 3,758) and disqualified from being a director for one year. Two other charges under the Companies Act were taken into consideration for sentencing. Between 2012 and 2015, the Commercial Affairs Department (CAD) of the Singapore Police Force undertook money laundering investigations against six local companies for allegedly receiving fraudulent funds amounting to approximately USD 2.25 million from jurisdictions across three different continents. The predicate offences committed included boiler room investment ruses and business email compromise frauds. Investigations revealed that all six companies had no legitimate business operations in Singapore, and were in fact shell companies. All of them were found to be incorporated with the assistance of the same corporate service provider, Person B, who also appointed himself as a nominee director for each company to fulfil the legal requirement of a local resident director under Section 145(1) of the Companies Act. However, Person B made little effort to inform himself of the affairs of the companies, including having little oversight over the corporate bank accounts maintained by these companies. CAD managed to seize approximately SGD 45,000 (approximately USD 33,909) which was returned to the victim, despite the fact that most of the alleged criminal proceeds had been quickly dissipated prior to investigations.

5.18 Association with environmental crimes (illegal logging, extraction, wildlife trafficking, etc.).

Australia

Joint Parallel Financial Investigation in Australia to Dismantle Reptile Smuggling Network

In 2016, the Australian Border Force (ABF) intercepted several outgoing international mail parcels containing native wildlife. Together with several intercepted inbound packages containing exotic wildlife they were linked to an Australian person of interest (POI). To further investigate, the Department of the Environment and Energy (DoEE) undertook a joint investigation with the AFP, and coordinated significantly with the ABF, the FIU (AUSTRAC), the Department of Agriculture and Water Resources, and various state and territory wildlife authorities.

The AFP confirmed that the POI coordinated an IWT criminal network to export Australian native reptiles. Many of the POI's exports were destined for associates in Jurisdiction X. The investigation involved sharing intelligence with Jurisdiction X Police authorities on the activities of POIs with Jurisdiction X nationality. A search was conducted on the POI's residence resulting in their arrest. During the search two Burmese pythons were discovered on the property, along with approximately USD 30,000 in cash.

Financial intelligence helped identify the broader criminal networks. Bank transaction information obtained from the FIU linked the primary POI directly to a number of Jurisdiction X wildlife traffickers, supporting the criminal investigation. Likewise, FIU analysis showed that the same Jurisdiction X entities had been sending funds to another Australian reptile trader.

The payment methods used were: cash; bank transfers; payments through a large Money or Value Transfer Service (MVTS) provider; "in-kind" transactions (exchange of wildlife of equal value); and transactions to associates and family members of wildlife traffickers. The volume of financial flows is difficult to quantify; however, estimates indicate that the primary POI stood to gain over half a million Australian dollars (USD 389,014) from an intercepted import of fish, stingrays, reptiles and turtles from Jurisdiction Y.

The POI was convicted of six charges including: attempting to export regulated native specimens (Environment Protection and Biodiversity Conservation Act 1999 (EPBC Act) 303DD); importing of regulated live specimens (EPBC Act 303EK); possession of illegally imported specimens (EPBC Act 303GN); and money laundering (Criminal Code Act 1995). The individual was sentenced to four years' imprisonment, with a non-parole period of two and a half years. During the investigation, authorities confiscated approximately USD 30,000 in cash as proceeds of crime, along with USD 340,000 (estimated value of the wildlife).

China

Case on illegal wildlife trafficking

In 2020, the China Customs seized 1.1 million Japanese eel fry smuggled and exported by means of a fabricated declaration. As the Japanese eel fry cannot be artificially bred, it is a wild animal protected by China's wildlife conservation laws and regulations. By cooperating with the China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC), the China Customs quickly identified the fund chain linking sellers, customs clearance service providers and overseas receivers, and identified the gang members and their trading modes. The law enforcement agency cracked down on the eel fry smugglers and arrested 16 suspects. The value of funds involved in the case reached 150 million yuan (USD 23,213,713), among which more than 30 million yuan (USD 4,642,859) was frozen.

Hong Kong, China

An investigation into a crime syndicate in Jurisdiction X which has been engaging in cross boundary bookmaking and illegal wildlife trading activities revealed that the mastermind had been using bank accounts of his company and accomplices in Hong Kong, China to launder over HKD 550 million (USD 70,814,566) and dissipated the crime proceeds for purchasing bonds, securities and real estate. The two accomplices in Hong Kong, China were arrested with over HKD 260 million (USD 33,475,035) frozen. An investigation is ongoing.

Indonesia

Based on the results of the Forest Products Circulation operation by a joint team carried out by the Ministry of Environment and Forestry, the Indonesian Navy, Bareskrim (Criminal Investigation Department) of Indonesian National Police Headquarters, Customs and Excise, the Port Head has checked and secured 199 containers containing processed wood that are suspected of being illegally logged.

The case relates to the transportation of wood from forest products without a certificate of legality of forest products. Based on the results of document checking and inspection, only 12 transport documents were found in the form of Certificates of Legality of Processed Timber Forest Products totalling 57 containers owned by Company A. 27 Containers owned by Company B were confiscated because they were transported using a document in the form of a Timber Transportation Note by the Company which did not match its designation. The Illegal Timber Products are transported using a ship owned by Company C at the Port of Teluk Lamong Terminal Co. Surabaya, East Java. The same thing was also done by Company D which intentionally misused the timber forest product transport document issued by the authorised official. The estimated value of the crime is in the hundreds of billions of rupiah.

It is known that based on the flow of funds, Company A has received incoming funds from abroad amounting to IDR 5 billion (USD 349,766) as well as several cash financial transactions in the billions of Rupiah. In addition, cash financial transactions received by DG as Director of Company A amounted to more than IDR 13 billion (USD 908,558). Furthermore, the majority of cash flows to DT, as the Director of Company A, were in the form of cash withdrawal transactions reaching IDR 2 billion (USD 139,965). Meanwhile, TS (the director of Company D) placed funds in insurance policies for individuals, children and wives in the amount of more than IDR 3 billion (USD 209,948).

5.19 Currency exchanges / cash conversion.

Macao, China

A phone scam victim deposited cash into a designated Macao, China bank account multiple times, as instructed by the perpetrator who was impersonating a police officer, with the incurred loss being around MOP 200,000 (USD 25,000) in total. In order to receive part of the scam proceeds, suspect A provided a bank account in Macao, China as required by the crime syndicate. However, this bank account was held by suspect K, whose business was to provide mobile application top-up and money transfer services. Upon receiving the funds in MOP, suspect K exchanged the said illicit proceeds from MOP to another foreign currency, with forex service charges deducted first, and then transferred the money in foreign currency into suspect A's mobile application or overseas bank account. Suspect A then remitted the money to another overseas bank account designated by the crime syndicate. In the aforementioned case, despite knowing that the transferred funds were derived from criminal activities, suspect A still disguised the illicit origin of the funds and concealed his/her involvement in the scam by using a third party bank account held by suspect K. In 2020, suspect A was charged with fraud and money laundering by the Public Prosecutions Office and suspect K was charged for receiving stolen goods.

Pakistan

Laundering of proceeds through illegal currency exchange and hawala/hundi business

STRs were raised against an individual, Mr. XX, on the suspicion that high value structured currency exchange transactions were conducted by him which were not consistent with his declared profile as a wage earner.

After an analysis it was identified that in addition to the STRs, the suspect was identified in a large number of CTRs (cash transactions above the threshold of PKR 2 million- USD 13,078) involving substantial amounts of funds with different reporting entities including banks and exchange companies during the period 2016 to 2020.

70% of the CTRs were reported by different exchange companies during the period 2018 to 2020 whereas the remaining 30% were reported by different banks on the reported individual, Mr. XX.

An analysis of the bank accounts of Mr. XX showed very minimal activity indicating that Mr. XX was conducting transactions in other accounts. In order to determine the ultimate beneficial owner of the transactions, the analysis was further extended to those accounts where Mr. XX had conducted transactions. It was found that Mr. XX had been frequently conducting transactions as an operator of the account of an individual named Mr. YY during 2020.

The Computerised National Identity Card (CNIC) number of Mr. YY was searched in FMU's database wherein it was found that financial intelligence on Mr. YY was already shared with an LEA and was under investigation with the Law Enforcement Agency on account of his possible involvement in illegal currency exchange and Hawala/Hundi business.

Based on the above information, it was suspected that Mr. XX was *benami* of Mr. YY and was working as a conductor of transactions in Mr. YY's accounts. The financial intelligence was forwarded to an LEA to further expand the ongoing investigation against Mr. YY.

Singapore

Person L was an employee of a bank, whose duties involved facilitating the hedging of forex exposure for customers. In this regard, he was allowed to enter foreign exchange ("forex") trades only after he received instructions from customers and had checked with the bank's treasury desk for prevailing quotes.

Between 2011 and 2013, Person L executed a scheme to conduct unauthorised forex trades in his clients' accounts, using the accounts maintained by two sole proprietorships controlled by him as counterparties to these trades. Person L then made additional unauthorised trades in other clients' accounts to close the forex positions of earlier customers. Through this scheme, Person L accumulated benefits amounting to approximately SGD 1.2 million (approximately USD 0.9 million). Person L used these criminal proceeds to repay his outstanding credit lines, and loans and exchanged the rest into foreign currencies for his own investments.

In 2019, Person L was sentenced to imprisonment of eight years and four months for offences relating to the unauthorised modification of computer material, instigating others to commit cheating by personation, and the laundering of proceeds of criminal conduct.

5.20 Use of credit facilities, credit cards, cheques, promissory notes etc.

Indonesia

Case one:

The defendant Mr. HT made modifications to credit cards issued by Bank X on behalf of Mr. KS and Mr. RH by transferring data from the original credit card chip to a smart chip using X2 software so that the credit card can be used without going through the Bank X host system and can be used on the Bank X EDC machine. Using a credit card on the EDC machine will issue proof of the transaction so that the merchant thought that the transaction is legitimate and registered with the host Bank X.

Furthermore, the defendant Mr. HT met the defendant Mr. BS and Mr. MFN to explain the use of the modified credit card before use. The way it works is that after selecting the item to be purchased, the buyer will be asked to enter a PIN so the defendant can enter a 6-digit PIN randomly and the transaction will be successful. For the first time the defendant Mr. HT invited the defendant Mr. BS and Mr. MFN conducted a trial using the card to purchase gold weighing approximately 8 grams for IDR 3,200,000 (USD 224). After the defendant Mr. BS and Mr. MFN knew how to use the modified card, they were ordered by the defendant Mr. HT to buy goods such as gold, cell phones and electronic goods as priority items. The use of cards is carried out in various shops from various regions on the islands of Sumatra and Java.

All proceeds from the purchase of goods were handed over to the defendant Mr. HT to be converted into money / sold with the aim of disguising the proceeds of crime. The total loss suffered by Bank X due to the use of credit cards is IDR 2,553,840,268 (USD 179,292). The defendant Mr. HT distributed IDR 32,000,000 (USD 2,251) to Mr. BS and IDR 31,000,000 (USD 2,177) to Mr. MFN. The defendant Mr. HT used the money to pay debts, the cost of living for his wife and children, to pay for rotating savings and credit association (Arisan in Bahasa Indonesia), rent an apartment, and money amounting to IDR 175,298,871 (USD 12,329) was deposited into Mr. HT's colleague's account. While the defendant Mr. BS used the money for a clothing manufacturing business and the defendant Mr. MFN used the money for business capital.

Case two:

Person A as Head of Corporate Banking at Bank Z takes advantage of his position to facilitate the credit application process of Company A for IDR 150 billion (USD 10,494,664). It is known that the Beneficial Owner of Company A, namely Mr. HS, manipulated seven other banks. Person A uses his authority to change the proposal for submitting a credit application for Company A which was previously rejected by the Corporate Credit Risk Division. One of the collateral or credit guarantees used by Company A as the underlying form of Company A to Company B turned out to be fictitious in that Company C never had a debt to Company A.

In connection with this, the defendant received IDR 1.5 billion (USD 105,030) transferred from Company A to person A for the purpose of "office operations". Person A then transferred the funds to five accounts, one in his name and four accounts in the names of other parties. It is also used to pay for hospital medical expenses, car purchases, credit card bills for overseas trips, purchases of foreign currency in USD and SGD and house rentals.

New Zealand

Fraud/ML scheme using stolen cheques

A criminal network used stolen cheques to defraud NZ victims of more than $1.4 million (USD 1,003,447). The network used stolen chequebooks as payment for orders placed online. Once the online order was placed the offenders asked for a bank account number to make a ‘bank deposit’ as payment for the online orders. The offenders then deposited the fraudulent cheques into the victims’ accounts via ATM deposit. When the victims looked at their account it looked

like they had been paid and they therefore began to make arrangements to have the goods shipped. Several days later the deposit is identified as fraudulent, however, by this time some goods had already been dispatched to the offenders. The network deposited stolen cheques to a wide range of retailers across NZ, sourcing items such as gold bullion, jewellery, cameras, computer goods, thermal imaging gear, off-road motor bikes and blank firearms.

Pakistan

Fraud/ Ponzi scheme

STRs were reported against Mr. AB and Mr. MA. Both individuals were involved in illegal auto leasing businesses. They were using a social media platform to offer the public a number of investment schemes at an unrealistically high rate of profit. FMU initiated the case for analysis of STRs against both of the individuals.

FMU analysed the accounts of both individuals. It was revealed during the analysis that all the reported 10 accounts of Mr. AB and his company were opened during the period of the last three years. None of the automobile business related transactions were noted in his bank accounts despite the fact that he had declared himself as an auto leasing dealer in the account opening documents of the bank. Likewise, an analysis of the bank accounts of Mr. MA revealed that the accounts were opened during the period of the last year and a half.

Both the individuals lured the public by offering financing at a rate lower than the market rate. They offered a financing facility for automobile and housing at the rates of four and six percent, respectively. Moreover, the individuals also clarified on their website that the financing facility was not available to the media and members of law enforcement agencies.

Moreover, one of the companies run by the aforementioned individuals, was already issued with sanctions by the Securities & Exchange Commission of Pakistan (SECP) for its involvement in unlawfully running businesses related to the leasing of vehicles, houses, electronics etc. However, the reported individuals ultimately managed to continue running the businesses.

The above financial intelligence was shared with a Law Enforcement Agency whereupon action was taken against the individuals. The offices of Mr. AB were raided and sealed while arrests were also made. Further investigations are underway.

5.21 Wire transfers / Use of foreign bank accounts.

Chinese Taipei

Mr. H is a scammer with several criminal conviction records. Ms. L is the owner of a foreign company (Jurisdiction A) named YK. In 2019, with the intention of executing a fraud scheme on Ms. L, Mr. H impersonated a member of G Bank Group in Chinese Taipei and a lawyer practicing in Jurisdiction B, and claimed that he could assist Ms. L to obtain VVIP membership of G Bank Group, to deal with her family's contract lawsuit, and to invest together in real estate. Ms. L was deceived out of more than 4 million USD by the scheme, and transferred the funds from her personal savings into Mr. H's designated dummy accounts, including a company account registered in Jurisdiction B.

The Prosecutors' Office prosecuted Mr. H and his associates for violations of Criminal Code and Money Laundering Control Acts in August, 2020.

Hong Kong, China

The bank-to-bank messaging system of a bank in Jurisdiction X was attacked and 11 unauthorised transactions totalling HKD 108 million (USD 13,905,561) were made to various banks around the globe. A total of HKD 52 million (USD 6,695,234) was credited to bank accounts in Hong Kong, China and some of the funds were further dissipated through wire transfers on the same day. Upon receiving the report, the Hong Kong Police Force swiftly withheld HKD 27 million (USD 3,476,411) in the beneficiary accounts. A total of 11 account holders were arrested. Three of them were convicted and sentenced to imprisonment for 26 to 30 months. Two defendants have absconded and are yet to be located.

Singapore

In 2018, the Commercial Affairs Department (CAD) of Singapore Police Force received information from authorities in Jurisdiction X that several bank accounts in Singapore were used by Person R from Jurisdiction N to launder proceeds of crime.

Person R was the Chief Executive Officer of a company based in Jurisdiction N, which allegedly produced and sold encrypted hand-held devices designed to provide a secure means to communicate openly about criminal activity without fear of detection by law enforcement. Pursuant to investigations conducted by Jurisdiction X authorities, Person R eventually pleaded guilty to offences involving conspiracy to commit racketeering acts and to distribute cocaine. As part of his guilty plea, Person R agreed for a sum of his assets to be forfeited, including money that was held in bank accounts in Singapore.

Acting expediently on information provided by foreign authorities, CAD commenced a domestic money laundering investigation and in the process seized over SGD 5 million (USD 3,759,238) of proceeds held in the bank accounts of Company C, a Singapore-registered company for which Person R was a director and sole shareholder. Upon the conclusion of investigations, CAD worked with the Attorney-General's Chambers to invoke our judicial process to lift the seizure and successfully repatriated the seized assets of USD 3,971,468.40 to Jurisdiction X authorities in 2020.

Additionally, the corporate service provider which had assisted in incorporating Company C may have committed offences under the Companies Act, including the failure to exercise reasonable due diligence as a director of Company C. Court proceedings are in progress.

5.22 Use of false identification.

Brunei Darussalam

On 9 March 2020, a victim filed a police report stating that BND 67,800 (USD 50,943) had been transferred out of her joint account with her husband and suspected a third party (their daughter) to be involved in the theft. The Royal Brunei Police Force (RBPF) initiated the predicate offence investigation and arrested Person A and Person B.

Investigations revealed that Person A, the daughter of the victim, with the help of her cousin Person B used deceitful means to transfer the funds from the victims' account to Person A's

account. They gained access to the victim's account and, using the bank's online banking application, proceeded to conduct the transfers.

As part of RBPF's investigations, the police seized a large number of items which they had believed were bought using the proceeds of her theft. This included monies amounting to BND 8,200 (USD 6,160) and IDR 16 million (USD 1,118). Both Person A and Person B used the money for their own personal expenses as well as luxury trips to overseas.

On submission of the investigation papers from the RBPF, the Attorney General's Chambers (AGC) advised to carry out the further investigations on Person A to obtain the relevant evidence that could support money laundering charges such as the value of the seized items, where they were purchased, when they were purchased and whether they were purchased with the stolen money.

The RBPF was able to obtain sufficient evidence and on 30 April 2020, Person A was prosecuted and convicted for theft and money laundering offences. She was sentenced to 32 months' imprisonment, however, this was increased to 40 months after a successful appeal made by the public prosecutors. Person B was sentenced to eight months' imprisonment.

Hong Kong, China

In a property fraud case in Hong Kong, China, Mr. X used a forged identity card and appointed a property agent and legal representatives to sell a property on behalf of the property owner. Mr. Y changed his name officially to that of the house owner and opened a bank account. A buyer paid about HKD 3M (USD 386,272) as deposits to Mr. Y who later withdrew all the money in cash and changed back to his original name. The case surfaced when the genuine property owner received a letter from a law firm informing of the change of ownership. Mr. Y was convicted of 'Using a False Document', 'Money Laundering' and sentenced to imprisonment for 48 months while Mr. X was convicted of 'Fraud' and 'Conspiracy to Defraud' and was sentenced to imprisonment for 42 months.

Indonesia

There were 52 debtors related to indications of fraud committed by CRR as Branch Manager (BM) with Branch Officers (Credit Officers) at Bank X. CRR committed fraud by borrowing debtor identity data to apply for a loan, including fictitious businesses as one of the requirements possessed by the debtor, falsification of the debtor's identity documents, engineering the sale and purchase of collateral assets for loan applications from banks and mark-up on the results of business income and the value of the debtor's collateral, so that the loan can be approved. Then, CRR gave an amount of money to the party whose identity was borrowed from IDR 2.5 million (USD 175) to IDR 5 million (USD 351) as a fee for using that party's identity to apply for a credit loan to Bank X.

CRR received money from banking crimes amounting to IDR 931,300,000 (USD 65,511). The money laundering was carried out through the purchase of assets in the form of land using someone else's identity.

For this act, CRR was sentenced to imprisonment for eight years and a fine of IDR 200 million (USD 14,075).

New Zealand

Organised Crime Group engaged in bank loan fraud

A group of NZ citizens defrauded several NZ banks by taking out bank loans, changing their names by deed-poll to avoid authorities and then defaulting on the loan repayments. The activity was aided by use of a NZ construction company which provided payslips and fake wage payments in support of the loan applications. Financial intelligence identified a number of individuals receiving payments from the NZ company labelled 'wages'. The individuals used these statements as part of a wider suite of documents (wage statements, payslips, employment agreements) from the company, to obtain loans from several NZ banks. It is estimated the group obtained several-hundred thousand dollars' worth of loans from multiple banks. Once they had obtained the loans, the offenders legally changed their names, enabling them to better-avoid follow up inquiries by the bank and law enforcement. Fraudulently obtained funds were largely withdrawn as cash or funnelled through a network of third-party accounts.

5.23 Association with corruption/bribery

Bangladesh

Laundering of Illegally Earned Money to Several Jurisdictions by a Government Official

Mr. 'A' is a government official and his wife Mrs. 'R' is the proprietor of a business entity named 'Company A, a contracting firm supplying surgical equipment to government hospitals and institutions. More than BDT 5202.2 million (USD 61,286,951) was transacted in the bank accounts of Mr. 'A', his wife Mrs. 'R', and their concerned entities. About BDT 4300 million (USD 50,657,108) was transacted in the bank accounts of Company A of which BDT 1020 million (USD 12,016,424) was deposited in this account for the purpose of bidding for a government tender (as per declaration in the deposit slips).

Money was transferred from the bank accounts of Company A to the account of another entity named Company B whose proprietor's name was published in the Panama Papers. Furthermore, a substantial amount of money was transferred to several accounts from this account very frequently. Analysis revealed that Mr. 'A' was the ultimate controller and beneficiary of his wife's company, Company A. Open source information revealed that he used to prepare fake papers of supplying goods and controlled government tenders in favour of his wife's company and even managed to obtain a tender without minimum capital/security money.

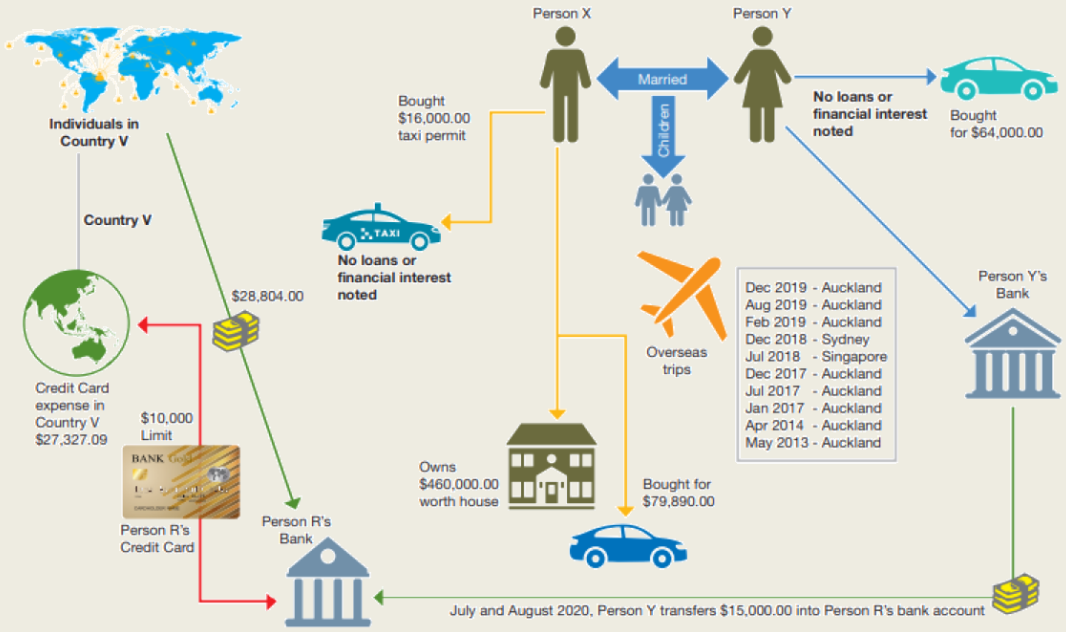
In addition, Bangladesh Financial Intelligence Unit (BFIU) obtained information of accounts being maintained by Mr. A and his wife in four foreign jurisdictions, namely jurisdiction Wx, Xy, Yz and Zx. There was information of numerous cash transaction reports, large transaction reports and electronic fund transfer reports amounting to a total of USD 13.45 million against the accounts of Mr. 'A' and his wife in those jurisdictions. Furthermore, in one of those jurisdictions, suspicious transactions made between December 2014 and June 2020, were reported. Additionally, a business entity in a foreign jurisdiction in the name of Mr. 'A' was detected even though a Bangladeshi cannot invest in a foreign jurisdiction without approval from the appropriate authority.

After the analysis, it appeared that Mr. 'A' with the assistance of his wife amassed a considerable amount of illegitimate wealth and had tried to conceal his illegally earned money by establishing a contracting company in his wife's name and ultimately funnelled the amount to foreign jurisdictions through illegal channels. Based on the findings BFIU prepared an intelligence report and disseminated the same to the Anti Corruption Commission for further investigation and necessary legal actions as per the Money Laundering Prevention Act (MLPA) 2012.

Fiji

Corruption, bribery, kickback and unexplained wealth

Person R, employed by a local statutory body, was brought to the attention of Fiji FIU for a possible case of bribery, corruption and unexplained wealth. Analysis revealed that Person R received deposits totalling approximately $28,804 (USD 14,107) into his bank account between July 2018 and September 2020 from various individuals in Jurisdiction V and Fiji. It was also noted that Person R, his unemployed spouse (Person Y), and their children frequently travelled to jurisdiction V. In August 2019, Person R acquired a taxi permit, however, there was no corresponding transaction showing that Person R had paid for the taxi permit. Person R and Y collectively own four high value vehicles that were purchased without any financing. Further analysis revealed that Person R acquired a freehold property in the central division and has made significant improvements to the property in the last few years. Further analysis revealed that patterns in Person R's transactions and accumulation of wealth were not consistent with the annual income declared. It was also established that person R and his family frequently travelled abroad, however, funding for tickets and travel expenses could not be traced to credit card or bank account transactions. A case dissemination report was provided to the Fiji Independent Commission Against Corruption (FICAC) to examine the case for possible unexplained wealth as a result of corruption and bribery.



Indonesia

Case one:

Mr. ZAI is a Regent of the South Lampung region for the period 2016-2021. From 2016 to 2018, Mr. ZAI through Mr. AGU (Head of Sub Division of Finance at PUPR (Ministry of Construction and Housing) Office from 2015 to January 2017) and Mr. ANJ (Head of the PUPR South Lampung Office from December 2017 to July 2018) received money (termed 'commitment fees') for the allocation of infrastructure work.

Mr. ZAI with Mr. AGU, Mr. ANJ, Mr. HER and Mr. SYA received cash in stages from 2016 to 2018 amounting to a total of IDR 72,742,792,145 (USD 5,116,854) from entities who were awarded projects by the PUPR Office.

Under the commitment fee arrangement, Mr. HER formed a team coordinated by Mr. SYA. Mr. HER then provided a list of jobs to Mr. SYA and ordered Mr. SYA to collect commitment fee money from entities that were to be awarded the jobs (infrastructure work) according to project plotting. The commitment fee was then submitted to Mr. AGU. The task of the team coordinated by Mr. SYA was to prepare bid documents for the companies that paid the commitment fee and upload them into the Electronic Procurement Service (LPSE) system. The commitment fee could amount to approximately 21% of the project value.

Case two:

Mr. SLM, Mr. BS and Mr. AN are civil servants in a government agency. Mr. SLM is the Head in charge of expenditure with regard to the Supply Fund (SF) and Additional Supply Fund (ASF). However, it was discovered that the SF and ASF were not entirely used to finance operational, non-operational, supplies, services, and maintenance expenditures in accordance with the agency's activity plan that has been determined, but were also used for the personal interests of Mr. SLM, Mr. BS, Mr. AN, and other parties. Funds that were used contrary to normal expenditure guidelines amounted to IDR 5,018,121,329 (USD 347,816). The funds used for the personal interests of Mr. SLM, Mr. BS and other parties amounted to IDR 4,685,971,329 (USD 327,794), while the remaining IDR 332,150,000 (USD 23,022) was controlled by Mr. AN. The funds that had been received by these parties were then divided between several of the defendants' associates.

Case three:

a. On two instances, Mr. NZ placed or transferred the proceeds from corruption in procurement activity using the accounts of companies part of the PMI Group and accounts in the names of others amounting to IDR 70.018 billion (USD 4,903,635) and SGD 1,034 (USD 774 - around IDR 9.3 million); ownership is transferred in the form of shares of a company under the control of the PMI Group, namely ETU co. and PNH co. is worth IDR 50,425 billion (USD 3,529,984).

b. Furthermore Mr. NZ transferred ownership of land and buildings worth IDR 18.447 billion (USD 1,291,476); to spend or pay for the purchase of land and buildings IDR 111,117 billion (USD 7,779,327); to spend or pay for the purchase of motorised vehicles amounting to IDR 1.007 billion (USD 70,500); spent or paid for an insurance policy of IDR 2.092 billion (USD 146,525).

c. Mr. NZ spends or pays for the purchase of shares which are then resold using companies that are members of the PMI Group or the names of other people on the Indonesia Stock Exchange, namely shares of GRD co., shares of Bank MDR, shares of Bank ABC, shares of GG co., shares of KS co., shares of JAW co., shares of BCE co. (using the name of Mr. NZ's wife), shares of PRW co., shares of CA co., shares of DMK co., shares of ETU co. and shares of PPM co.. Besides that, Mr. NZ bought bonds worth a total of IDR 374,747 billion (USD 26,211,738). Thus Mr. NZ’s total assets in the capital market is IDR 627.86 billion (USD 43,915,767).

d. To hide or disguise the origin of the proceeds of the crime, the proceeds from the sale of shares of GRD co. was transferred by Mr. NZ through the PMI Group Finance Director, which was done by transferring money from the Jurisdiction X Dollar Giro account at SCT Bank[33] on behalf of PPM co. amounting to around 6 million Jurisdiction X dollars (USD 4,494,743) to Mr. LKS's account as if it were for payment for the purchase of a Tug Boat in Jurisdiction X. Furthermore, this occurred through Mr. GL’s instructions as the President Director of a

[33] A type of securities account intended for foreign companies that open securities accounts in Indonesia.

recruitment agency named PT. TCL in Jurisdiction X to cross the shares of PT. GRD in the negotiation market of four companies, namely PT. PRW, PT. CA, PT. MK and PT. ETU to PT. TCL for the amount of IDR 163 billion (USD 11,414,212).

e. In addition, there are also transactions where the sale of shares of BCE co. was transferred by Mr. NZ's wife to the account of a company called WII, Pte Ltd. in Jurisdiction X for an amount of IDR 26 billion (USD 1,820,517).

New Zealand

Proceeds of offshore corruption scheme laundered via NZ property market

NZFIU received three Suspicious Activity Reports (SARs) regarding a NZ-registered company (Company A). The SARs related to the sale of a property in Auckland for NZD 23 million (USD 16,663,730) owned by Company A, to an undisclosed owner. The SARs identified that the beneficial owner of Company A was an overseas jurisdiction government official (Person A), who was subject to investigation by another jurisdiction's anti-corruption agency due to alleged corruption involving the other jurisdiction's natural resources, and had been subject to 'numerous' corruption allegations since the 1980s. As part of the SARs the reporting entity supplied beneficial ownership information for Company A which showed Person A to be the settlor of a trust (based in an EU jurisdiction) which owned 60% of Company A, which in turn was the sole owner of the NZ property valued at NZD 23 million (USD 16,663,730). This information also showed Person A to be the protector of a second (offshore-based) trust which owned a 20% share of Company A – effectively giving him an 80% ownership share of the company.

Proceeds of abuse of official position in offshore jurisdiction laundered through NZ bank accounts

NZFIU received a SAR regarding a New Zealand citizen living in overseas jurisdiction A who had come to the attention of the reporting entity via open source information alleging he had abused his position as a public official in Jurisdiction A for personal gain. The allegations included clocking up expenses and time off for which he was not entitled, and using his influence to obtain preferential treatment for key staff members. The suspect had previously been interviewed by jurisdiction A's anti-corruption agency and inquiries were ongoing.

SAR reporting on the suspect showed he received more than NZD 200,000 (USD 144,823) credited to his NZ accounts from his bank accounts in Jurisdiction A. These funds were then forwarded to third party accounts within NZ and also used to fund personal expenses

Proceeds of overseas bribery scheme laundered via NZ foreign trust structure

NZFIU received a spontaneous dissemination from an overseas partner regarding a foreign national (Subject X) who was subject to an international investigation regarding a 'notebook of bribes' where a group of overseas businessmen located in Jurisdiction A were accused of paying bribes to keep public works contracts administered by a government body in jurisdiction A. The partner FIU indicated that Subject X was the settlor and beneficiary of a trust (Trust Z) which was transferred to a New Zealand company (Company Z) in 2016, which held assets totalling USD 8.6 million in an offshore bank account.

Inquiries conducted by NZFIU identified Trust Z was indeed transferred to NZ in 2016, being set up as a NZ foreign trust with Company Z as the trustee. Company Z was associated with a group of companies which provide trust and company services in New Zealand and internationally, which had previously come to the attention of NZFIU for suspected

involvement in complex international money laundering schemes. The shareholder of Company Z was another overseas based company.

NZFIU inquiries revealed Trust Z did not hold banking facilities in New Zealand, but multiple payments referencing the name of Trust Z were credited into the NZ account of Company Z, which NZFIU assessed were likely payments for administration of the structures by the NZ TCSP and a portion of which was likely earmarked for forwarding to overseas bank accounts owned / controlled by Subject X.

Pakistan
Corruption & Bribery

The transactional activity in the account of Mrs. AA was suspicious as high value funds were transacted from the account which apparently were not consistent with her profile as a housewife. Furthermore, the source of funds and the true beneficiary of the funds was also unclear.

During the analysis, it was found that Mrs. AA was maintaining multiple PKR and foreign currency accounts at different banks where a high volume of transactional activity was noted. Furthermore, Mrs. AA received substantial funds in her local currency account from her father's account purportedly as a gift. The amount of the gift was then transferred to her own account maintained with another Bank, but the mandate to operate this account was held by her husband, Mr. AK. Afterwards, these funds were withdrawn through cash and clearing of cheques. As per KYC documents, Mr. AK was a high-level government official.

Through Computerised National Identity Card (CNIC) searches in FMU's database, it was found that Mr. AK and Mrs. AA conducted currency exchange transactions and remitted a considerable amount of funds abroad.

Suspecting Mr. AK as the ultimate beneficiary of the funds, the financial Intelligence was shared with an LEA on suspicion of corruption and bribery.

Singapore

In 2019, the Corrupt Practices Investigation Bureau of Singapore (CPIB) conducted investigations against a former senior management executive of a sports association for cheating offences, relating to the wrongful award of contracts due to concealment of interest with related vendors. Investigations revealed that between 2016 to 2018, the total proceeds of cheating amounted to SGD 647,180 (approximately USD 487,766). The said former Deputy Director and three other co-accused persons were prosecuted for cheating offences under the Penal Code, Chapter 224 on 9 December 2020. CPIB commenced parallel financial investigations to trace the illicit proceeds. Investigations revealed that the funds were channelled to two companies which the former deputy director had an interest in, by means of contracts awarded to the two companies. A substantial portion of the criminal proceeds were subsequently withdrawn from the companies' accounts and deposited into the former deputy director's wife's personal bank account. The illicit proceeds were co-mingled with her personal funds. In July 2017, she withdrew about SGD 573,000 (approximately USD 431,778) to finance the down-payment of a private property. In view of the findings, CPIB lodged a caveat against the property. CPIB also seized about SGD 156,000 (approximately USD 117,552) of

cash in possession of the former deputy director and his wife. Investigations are currently ongoing.

5.24 Abuse of non-profit organisations (NPOs).

Singapore

Three individuals, Persons A, B and C were convicted in February and March 2020 under the Terrorism (Suppression of Financing) Act for collecting and/or providing funds to benefit a terror group in jurisdiction J with ties to ISIL, Entity X, and were sentenced to imprisonment terms ranging from 18 months to 45 months.

These three individuals worked as foreign domestic workers ("FDWs") in Singapore. Between September 2018 and July 2019, they had collected and/or remitted monies amounting to SGD 1486 (approximately USD 1118) to two purported religious charities in the belief that these funds would be used to support militant causes of Entity X and the families of its members who had been detained or killed. All the monies were raised through self-funding, and sent to persons in jurisdiction I through the same licensed remittance agent. Accordingly, the trio had reasonable grounds to believe that the funds collected and remitted would be used to facilitate terrorist acts overseas, resulting in the terrorism financing charges against them.

6. PROLIFERATION FINANCING METHODS & TRENDS

6.1 Case studies of breaches, non-implementation or evasion of targeted financial sanctions related to proliferation financing.

Chinese Taipei

Law enforcement (MJIB) searched the residence and company of Mr W after an investigation in October 2018, known as the 'Vessel S case', which involved an illicit ship to ship transfer with DPRK. The MJIB analysed the evidence from the Vessel S case and found that Mr W established an offshore company to purchase petroleum from a Jurisdiction X company, known as Company S, which was then stored in an oil tank located at the Taichung Port. In May 2018, Mr W proceeded to charter a vessel, known as Vessel G, to carry 1,350 metric tonnes of petroleum from the Taichung Port to the high sea where it conducted a ship to ship transfer with Vessel S. Vessel S then moved to a different location and conducted a ship to ship transfer with DPRK Vessel P, which was designated by the UN Sanctions List and Chinese Taipei. Mr W also used Vessel G to conduct a further petroleum ship to ship transfer with DPRK Vessel A. Mr W then sold Vessel G to DPRK which violated Chinese Taipei law as well as the UNSCR 1718. Investigations by MJIB found that Mr W provided financial resources to designated targets on the UN Sanctions List, which violated Article 9, Paragraph 1 and Subparagraph 1 of the Counter-Terrorism Financing Act 2018 (CFTA). This case was referred to the District Prosecutors Office in November 2020 for prosecution.

Malaysia

Between 2012 and 2017, two Malaysian private limited companies were identified to be fronts for a DPRK-linked company dealing with radio communications equipment for military and paramilitary organisations. Upon review of the companies' bank accounts in local financial institutions, it appeared that the front companies had received a total of 50 international transfers amounting to RM 7.5 million (USD 1,819,806) from various foreign entities, which included later designated entities under the UNSC, entities under Panel of Experts investigations and other companies which appear suspicious or inconsistent with the business activity of the sending party. Upon receipt, the funds were then immediately transferred to several other entities, which have since been alleged by the Panel of Experts to be serving as front companies for UNSC-sanctioned persons.

It was observed that these companies frequently moved money between their accounts to avoid detection, before transferring to foreign front companies and subsequent transfers to the final recipient in Pyongyang.

New Zealand

A New Zealand charitable society which was established to promote relations between New Zealand and DPRK was implicated in a possible breach of UN sanctions in relation to a NZD 2,000 (USD 1,440) donation it made to the Red Cross Society of DPRK. Due to the UN sanctions in place, the New Zealand society was unable to send funds directly to DPRK, so it instead sent the funds to a contact in Jurisdiction X who then passed the funds on in cash to the

DPRK Embassy. Authorities identified concerns that the activity may have been in breach of the UN sanctions against DPRK.

Philippines

Case one:

In May 2020, the AMLC was approached by the Panel of Experts, through a letter from the Department of Home Affairs, for assistance in relation to the Panel's investigation involving Vessel A and Subject X, who is a Filipino national.

On 24 April 2019, Entity B was registered in the Jurisdiction X and Subject X became Entity B's director, shareholder and beneficial owner. In June 2019, Vessel A was sold and its name was changed to Vessel B and ownership of the vessel was changed to Entity C. In August 2019, Vessel B travelled from Jurisdiction Y to DPRK and returned to Jurisdiction Y in November 2019 carrying coal originating from DPRK.

Investigations into Subject X found that the date of birth and address provided by the Panel of Experts matched the information provided by Subject X in her KYC documents. It was also discovered that Subject X had made 103 large transactions between the period of July 2005 and February 2020 in amounts ranging from PHP 400,000 (USD 8,000) to PHP 4,000,000 (USD 80,000). There were also 10 confidential reports covering the same period on a joint bank account of Subject X and her husband, Subject Y, which stated that the transactions made in the joint account appear to have no underlying legal or trade obligation, purpose or economic justification. It was also noted that there was a high volume of cash deposits and cheque clearing transactions during the same period as the purchase of Vessel A and the registration of Entity B. Subject X was asked to provide information regarding the source of the funds, however she gave inconsistent and conflicting responses such as the money was from businesses and/or an allowance from her husband. Further investigations found that no businesses were registered with the Department of Trade and Industry and Subject X was unable to provide information about the businesses or how they were able to generate the funds in the account.

Investigations into Subject Y, Subject X's spouse, found that Subject Y owned a garments business, Entity D, in Manila. Subject Y had also made 49 large transactions from the period July 2009 to December 2015 in amounts ranging from PHP 400,000 (USD 8,000) to PHP 4,000,000 (USD 80,000) and the bulk of the transactions are in joint bank accounts with Subject X. Investigations are ongoing.

Case two:

An investigation conducted by the Panel of Experts concerned a case of a suspected sanctions violation involving a Jurisdiction Z-flagged vessel, Vessel C, and the delivery of refined petroleum products to DPRK in April 2020. The International Maritime Organisation's website lists an overseas company, Company YYY, as Vessel C's registered owner, ship manager and operator since November 2019. Information obtained from the Panel of Experts and publically available sources showed that the director of Company YYY was Mr G, a Filipino national. Investigations into Mr G found that he had made 130 transactions from November 2005 to April 2019. Mr. G also made cash deposits totalling PHP 254.36 million (USD 5.32 million), which did not appear to be in proportion to his business earnings. Moreover, he also had an

aggregate debit of PHP 223.77 million (USD 4,578,228) which approximates the aggregate cash deposit.

The delivery of refined petroleum products to DPRK occurred in 2020, however, there was no transaction report on behalf of Mr G during this time. It may be that the transaction did not pass the financial system or smaller transactions were made below the reporting threshold. It was also discovered by the Securities and Exchange Commission (SEC) that Company YYY was not a registered corporation and did not appear on the SEC database, however, the SEC did find that Mr G was associated with several other corporations. The Department of Trade and Industry certified that there was no existing business registration under the name of Mr G. An investigation is still ongoing.

Singapore

In September 2020, Person C was convicted of assisting Company S, C and D which were registered under Person C's control, to supply designated luxury items worth in excess of SGD 500,000 (USD 676,769) to DPRK on 40 separate occasions between December 2010 and November 2016. Investigations revealed that Person C had registered various companies since the 1980s in order to conduct trade with the DPRK for profit. Company S, C and D had supplied goods to four different entities in DPRK, one of which had grown into a distributor and wholesaler supplying various goods to other shops in DPRK.

In 2010, regulations were enacted under the United Nations Act prohibiting the supply of designated luxury goods to DPRK, however Person C did not cease their trading activities with DPRK despite being aware of the risks of trading with DPRK and actively took measures to avoid detection by the authorities. Person C would supply the luxury goods to DPRK by transporting them by air and sea shipments through a neighbouring jurisdiction or by hand via airport check in. Payments by DPRK for the luxury goods were made to Company S, C and D's bank accounts through front companies which were incorporated overseas. Investigations also revealed that Person C ran a low-key operation to avoid detection, by not displaying the names of the companies on the floor guides or outside the unit of their registered address, which was the same for all three companies.

Person C was sentenced to three weeks' imprisonment and company S, C and D were also fined a total of SGD 130,000 (USD 97,966). These sentences are pending appeal before the High Court, including an appeal by the prosecutor for a harsher sentence.

7. MONEY LAUNDERING & TERRORISM FINANCING 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.

7.1 Recent research or studies on ML/TF methods and trends.

Australia

ML/TF Risk Assessment: Junket Tour Operations in Australia

AUSTRAC published its risk assessment of junket tour operations in December 2020[34]. This assessment was developed as part of a targeted programme of work, focusing on Australia's largest financial services sectors – namely, the banking, remittance and gambling sectors.

AUSTRAC assessed the overall ML and TF risk associated with junket tour operations in Australia to be high.

Fintel Alliance Trade-Based Money Laundering Working Group

In early 2020, Australia's public private partnership, Fintel Alliance, established a dedicated TBML working group aimed at building resilience, sharing knowledge, and developing coherent strategies to combat and disrupt TBML in Australia. The working group, which meets on a monthly basis, comprises subject matter experts from government, law enforcement, and financial industry partners. One of the objectives of the working group is to identify and document how financial facilities and products are exploited for TBML purposes. The working group also aims to consider and review the adequacy of the controls to mitigate TBML. The working group will cultivate domestic and international partnerships, and develop typologies and indicators to establish best practices that enable an enhanced and collaborative response to combating TBML. In the short period of time since its establishment, the working group has launched a number of initiatives, including:

- The development of a TBML indicators paper comprising feedback from public and private partners.
- The establishment of an information-sharing framework for public and private collaboration under the guidance of the Australian Border Force, for the purposes of identifying and reporting suspicious activities in selected high-risk industry sectors.
  The creation and delivery of a dedicated training programme on trade financing by a financial institution.

Brunei Darussalam

Brunei Darussalam sees a continuing trend of activity that alludes to possible money lending without a license, an offence under Section 8 of the Moneylenders Act Cap.62 and ML, an offence under Section 3 of the Criminal Asset Recovery Order, 2012.

On 7 December 2020, the FIU issued a typology to all FIs and DNFBPs, described as follows:

Modus Operandi:

[34] https://www.austrac.gov.au/sites/default/files/2020-12/JTO_2020_FINAL.pdf

a. Person X (moneylender) searches and identifies potential customers using social media, particularly Facebook. Person X may prey on other persons who have a need to purchase assets through obtaining a loan but are not able to, due to exceeding their Total Debt Service Ratio (TDSR) limit,

b. Person Y (customer) seeks Person X's help to settle their debt in order to obtain a larger financing or loan amount for any unspecific personal purposes.

c. Person X provides Person Y with the money needed to settle their debt with the condition that Person Y obtain a new loan of an amount sufficient to repay Person X with commission fee (read: interest payment).

d. Person X may give the money to Person Y in the form of cash or electronic funds transfer.

e. Person X may use another third party to perform the electronic funds transfer on their behalf.

f. Person Y uses the funds to settle their loan in full.

g. Soon after that, Person Y applies for a new loan of an amount larger than previously settled. The difference in amount includes the 'commission' to be paid to Person X.

Red Flag Indicators to look out for:

a. A customer that applied for a loan, but was rejected due to exceeding their TDSR limit. This includes any attempts (i.e. consultations with any bank/finance company staff).

b. A customer whose previous attempt to obtain a loan was rejected, but is suddenly able to complete an early settlement of their existing loan(s).

c. A customer that applies for a new loan soon after an early settlement of a previous loan.

d. Early settlement of a loan for an amount that may not be possible with that customer's level of income.

e. Early settlement of a loan using funds from unknown sources or sources that the customer is not able to justify or where the justification provided does not make sense.

f. A customer receiving large amounts in their personal accounts from persons seemingly unrelated.

g. A customer receiving large amounts in their personal accounts and then immediately using it to settle their loan(s).

Indonesia

The Preliminary Report Document of Indonesia's Risk Assessment on Money Laundering in 2020, includes the following findings:

- Predicate crimes with high ML risk include corruption and narcotics. Furthermore, predicates with medium risk are banking, environmental, forestry, fraud and taxation crimes.

- The industrial sector reporting entities at high risk of involvement in ML are motor vehicle companies and property companies/property agents.
- Legal entities have a high ML risk, while business entities that have high ML risk are limited liability companies (PT) and government agencies such as ministries.
- Individual job profiles that have a high ML risk are legislative and government officials and employees of state-owned or regional government-owned enterprises (including retirees).
- A risk assessment was conducted based on typologies that have a high level of risk, including the use of false identities, transfer to property assets and the use of nominees or loan names, smurfing, structuring, use of professional services, use of new payment methods/systems, use of corporations (legal persons) and utilisation of sectors which are not well regulated.

The Preliminary Report on Indonesia's Risk Assessment on TF and PF of WMD in 2020, includes the following:

a. Terrorism Financing Methods

- At the fundraising stage: personal sponsors (terrorist financiers/fundraisers), the collection of donations through mass organisations and legitimate business ventures.
- During the fund transfer stage: through a financial service provider, carrying cash across borders, and using a new payment methods.
- During the use of funds: manufacturing of weapons and explosives, travel of foreign terrorist fighters, and the use of weapons and explosives.

b. High-risk profile of TF perpetrators

The profiles of high risk perpetrators of TF are: entrepreneurs/small and medium business owners, private employees, and traders.

The 2020 Research Report from the Indonesian Financial Transaction Reports and Analysis Centre (PPATK), compiling ML court decisions from 2019, identifies:

- 50 ML court decisions and 50 convictions.
- Five convictions linked to reports by DNFBPs (goods and services providers (GSPs)), accounting for 10% of the convictions.
- The convictions were related to 8 GSPs reports in relation to the purchase of property.

Macao, China

Common ML methods detected from STRs received are as follows:

- Irregular large cash withdrawals;
- Significant cash deposits with non-verifiable source of funds;
- Use of ATM, phone banking, cash deposit machines;

- Currency exchange/cash conversion;
- Chips conversion without/with minimal gambling activities;
- Foreign exchange transactions with unidentified source of funds;
- Suspected to be engaged in illegal financial activities;
- Use of cheques/account transfer etc. to transfer funds;
- Suspicious wire transfers.

Malaysia

The Malaysian FIU issued a report on Red Flags and Typologies for Tax Evasion in 2020. This report was issued with restricted circulation to reporting institutions (RIs), with the aim to:

- Provide insights and create awareness on tax evasion including its trends, techniques, methods and channels;
- Enhance and facilitate RIs' knowledge and understanding on tax evasion typologies;
- Assist RIs in identification of tax evasion offences from red flags/indicators exhibited by their customers and financial transactions involved;
- Enable early detection by RIs in order to disrupt activities related to tax evasion; and
- Further improve the quality of STRs.

Philippines

From the 2021 Money Service Business ML/TF Sector Risk Assessment

The money service business (MSB) sector has been a target of criminals to move and, at times, facilitate proceeds of criminal activities. In the Philippines' Second NRA, the MSB sector was rated high in relation to the threat to ML/TF, particularly citing the involvement of 17 remittance companies and foreign exchange dealers in drug trafficking and illegal sex trade. One of the biggest bank heist cases in 2016 also affected the sector. In the case, three remittance companies and foreign exchange dealers facilitated the transfer of PHP 3.8 billion (USD 75,721,308) from fictitious bank accounts to casinos, junket operators, and unidentified individuals.

Measures include amendments in the BSP manual of regulations and the extensive registration process, which resulted in a significant restructure and consolidation of the sector. While the MSB sector's level of understanding of ML/TF risks and AML/CTF obligations is developing, the newly structured MSB sector is seen to provide a strong framework for AML/CTF compliance.

To monitor and identify emerging risks associated with the sector, the AMLC, with the assistance of a foreign FIU and support of the BSP, undertook a risk assessment, using data from transaction reports, responses from the BSP, and survey results from relevant industries and other Philippine government agencies. This risk assessment shall serve as guidance for supervising agencies, FIs, and LEAs as regards policy issuances and risk-based strategies.

In the analysis of transactions and investigations of cases, certain services or products catered by MSBs are being used by criminals for their illegal activities. Remittance services and cash transactions, including money changing facilities, were the primary means of moving illegal proceeds.

From the STRs filed by MSBs from 2017 to 2020, child exploitation, child pornography, trafficking in persons, swindling/fraud, Securities Regulations Code violations rank among the most number of suspicious transactions reported.

In relation to ML Cases, in 2020 alone, the AMLC caused the filing of petitions for freeze order on seven cases predicated on illegal drugs (4 cases), violations of the Electronic Commerce Act of 2000 (1 case), violations of Customs Modernization and Tariff Act (1 case), and violations of the Securities Regulation Code (1 case). Sixteen (16) MSBs were identified in the said 10 cases. Twelve (12) of the 16 MSBs were impleaded as parties in the said cases. Three (3) MSBs were also involved in at least two cases. The value of proceeds from the ML cases amounted to PHP 258.69 million (USD 5.2 million).

Terrorism Financing

Anecdotal intelligence and reports have previously identified MSBs for terrorism and TF. From 2017 to 2020, MSBs reported 2,007 STRs with an estimated STR value of PHP 20 million (USD 400 thousand). There is also an increase in MSBs' suspicious transaction reporting on terrorism and TF with over 350% growth in 2020 compared with 2019.

The common range of TF-related funds is between PHP 500 and PHP 5,000 (below USD 100). In the AMLC terrorism and TF risk assessment study,[35] over 6,000 STRs were reported by stand-alone MSBs, electronic-money issuers, and pawnshops that are possibly related to terrorism and TF from 2018 to 2020.

Domestic locations of beneficiaries of terrorism- and TF-related STRs involving international remittance, include Basilan, Zamboanga, Metro Manila, and Sulu.

The extent of threat and emerging risks, inherent risk and availability of mitigating controls show that MSBs are used extensively by criminals to move illicit funds, and warrant an overall medium high ML/TF threat rating for the sector.

While there were alleged and anecdotal intelligence reports on the use of crypto currency, local or domestic terrorist groups still primarily use the MSBs, and in some cases, communist terrorist groups use the banking system to move and facilitate TF-related funds.

Possible terrorism financing (TF) activities linked to the use of cryptocurrency

From the 2021 Terrorism and Terrorism Financing Risk Assessment (T/TF RA) conducted by the Anti-Money Laundering Council (AMLC)

A report[36] in May 2020 stated that the Philippine Institute for Peace, Violence and Terrorism Research noted that Islamic State-linked terror groups conducted their first transactions using cryptocurrencies in the Philippines, which were then allegedly used to finance the activities of terror networks operating in Mindanao like the Jemaah Ansharut Dalauh and the Mujahideen Eastern Timur[37].

[35]http://www.amlc.gov.ph/images/PDFs/2021%20JAN%20TF%20RA%20EXECUTIVE%20SUMMARY%20(WEBSITE).pdf
[36] https://thediplomat.com/2020/06/how-terrorists-use-cryptocurrency-in-southeast-asia/
[37] https://cointelegraph.com/news/researchers-in-philippines-track-crypto-use-by-terrorists

The report further detailed the use of cryptocurrencies consisting of two phases:

1) Channeling of cryptocurrency of suspicious origin through unidentified exchanges; and

2) Exchange of cryptocurrency into fiat currency and returning the funds to the legal money cycle.

The report also stated that terror groups in Southeast Asia can trade cryptocurrency outside the supervision of regulatory institutions. This is seen as a concern due to the loose legal framework relative to cryptocurrencies. The report specifically cited the Marawi Siege in 2017 wherein there were unconfirmed reports of private remittances and cash couriers with cryptocurrency helping to finance the terrorist groups involved in the said siege.

While blockchain analysis techniques have been employed to decrypt and trace transactions, services to increase encryption of the currencies have also been used to obscure traces of both the sender and receiver of the transaction. Moreover, blockchain analysis is unable to pinpoint the users involved in a transaction because individuals registering for a digital wallet could use pseudonyms or change the wallet's crypto address to maintain anonymity.

The Philippines, however, has allowed cryptocurrencies to be used as legal tender. The conversion of cryptocurrency to fiat currency could easily be done via ATMs and other registered remittance and transfer companies. While the conversion of cryptocurrency to fiat currency is regulated by Bangko Sentral ng Pilipinas (BSP), authorities may find it difficult to pinpoint individuals involved in the transaction as the PhilSys, the Philippine Identification System, has not yet been completely implemented. Taken together, these factors provide terrorists with enough room to exploit cryptocurrencies for TF purposes. As of 30 November 2020, there are 17 remittance and transfer companies with virtual currency exchange services registered with the BSP.[38]

The T/TF RA identified covered persons engaged in digital currency exchange that reported eight STRs in 2019 and 106 in 2020 with an estimated value of PHP 1.77 million (USD 37,027). The reported suspicious transactions indicate emerging use of cryptocurrencies.

Singapore

Singapore Terrorism Financing National Risk Assessment (TF NRA)

Singapore updated the Terrorism Financing National Risk Assessment (TF NRA) in 2020.

The TF NRA is the collation of experience and observations from all relevant competent authorities over the past few years, and includes inputs from the private sector and academia. It seeks to further deepen the understanding by LEAs, supervisors/regulators and the private sector of Singapore's key TF threats and vulnerabilities, so that appropriate prevention and mitigation measures may be taken.

The TF NRA has found that:

- Singapore continues to be exposed to TF threats posed by terrorist groups, both regionally and internationally, in particular the propensity for individuals in Singapore to be radicalised and influenced to carry out TF activities.

[38] https://www.bsp.gov.ph/Lists/Directories/Attachments/16/MSB.pdf

- Certain sectors, notably money remittance (or payment service providers carrying out cross-border money transfer services) and banks, are more inherently vulnerable to TF threats, given the relative ease of access to their services, coupled with Singapore's status as a financial and transport hub and proximity to jurisdictions exposed to terrorism activities.

7.2 Association of types of ML or TF with particular predicate activities (eg terrorist organisations, terrorist training, corruption, drugs, fraud, smuggling, etc).

Bangladesh

Remote Gambling Scenario in Bangladesh

This study was published in the Annual Report of the Bangladesh Financial Intelligence Unit (BFIU).

BFIU received 20 spontaneous intelligence reports from a foreign FIU. Each report described the involvement of Bangladeshi nationals in online remote gambling. These 20 Bangladeshi nationals registered remote gaming accounts with Maltese-registered remote gaming companies. They deposited and withdrew gaming accounts funds through Neteller, Skrill, Moneybookers etc. The FIU also informed BFIU that due to the lack of information on source of funds and high velocity deposits by those individuals, the gaming company had closed their accounts.

It has been found in the analysis that some of the gamblers provided false identity information during account opening and hence could not be traced. Every player's IP address was traced back to many different jurisdictions of the world. It appears likely that they used Virtual Private Networks so that their identities could not be traced. Before the accounts were closed, the players operated their accounts for one to four years. The players mainly placed bets on sports books and played casino games. The sum of the funds deposited by the 20 players was- USD 39,77,141 and the total withdrawal was USD 27, 09,154. In some cases, it was found that the gamblers were maintaining bank accounts in Bangladesh. These cases were disseminated to the Bangladesh Police Criminal Investigation Department (CID) for further inquiry. In several cases, CID provided feedback that no concrete proof was found against the gamblers.

Gambling is a prohibited activity in Bangladesh. There are also strict legal sanctions against gambling in the Public Gaming Act of 1867. Despite a ban on gambling, large numbers of Bangladeshis are using online gambling sites. Still others pay to play games online. These games have given rise to cybercrime through identity theft and theft of gaming accounts, fraud and even fronts for ML and TF (since they depend on the user paying to play in the gaming ecosystem). Therefore, it is important that ML & TF authorities trace how individuals are investing their money into online gaming and gambling. Legally, online gambling account cannot be loaded with funds through banking channels. Further, operation of Neteller, Skrill, Moneybookers, Paysafe or such types of e-wallets (e-money service providers) is not legal in Bangladesh. On the other hand, gamblers/players have to deposit funds to their gambling accounts to play. So, they use an alternative channels, hawala/hundi to feed into their accounts and most of the gamblers use Neteller, Skrill, Moneybookers, Paysafe that operates in multiple currencies.

A person who wants to gamble online sets up an account with Neteller, Skrill or one of the other companies or gets someone to do it for him or her. Then they get in touch with someone who has dollars, say a freelancer who works for a foreign client. He pays in local currency to the freelancer who then asks his client to pay part of his service fees into a Neteller or Skrill account which belongs to the gambler. This is how a digital/e-money wallet is loaded and used to make payments for gambling. There are agents/intermediaries who collect money from different would-be gamblers/gamers (often through Digital Financial Services like Bkash) and use multiple individuals to funnel money into these e-money accounts. Further, a search on Facebook found that several websites such as PaymentBD.com advertise loading up Neteller, Skrill and other similar e-wallet accounts. As per PaymentBD.com, they can load dollars in Neteller account.

The intelligence reports related to the remote online gambling were received only when the related accounts were closed. It is easily assumed that there are many more gamblers still operating. Since funds are siphoned off abroad from Bangladesh through hawala/hundi for this purpose, initiatives have been taken to communicate with foreign FIUs to collect information on gamblers who are still operating as well as to work closely with law enforcement agencies to identity the suspects.

Chinese Taipei

Case one:

Mr. W was the chairman of S Company, and since June 2017, he hired a number of employees to run a string of online casino websites which included G1, G2 and G3. In order to launder the gambling funds, Mr. W used a large amount of mule accounts which were opened in Jurisdiction X from an unknown company nicknamed KT, and layered the money into three different accounts. The first-layer accounts directly received the gaming funds from gamblers. When the money in the accounts accumulated to a certain level of funds, Mr. W then removed this money to second-layer accounts, and so forth to third-layer accounts. For the purpose of concealing illegal gains, Mr. W subsequently borrowed some of his friends' personal accounts in order to receive the above money. It was estimated that between 2017 and 2020, those accounts received a total of 0.6 billion foreign currency (USD 93,190,941).

In the interests of earning more profits from the gambling business, Mr. W also hired engineers to develop a "Fourth Party Payment" system, which integrated the services with third party payment providers and benefited from receiving the service fees. For instance, a third party payment provider received a 3.2% service fee of the total stake, and if there was a certain casino website which was willing to pay 3.5%, Mr. W's system would match both parties and take the 0.3% as the margin profit.

The Prosecutors' Office prosecuted Mr. W, along with his accomplices for violations of the Criminal Code and Money Laundering Control Acts in August 2020.

Case two:

Person A had established "Century Dynasty", "Winning Century" and other short companies since 2010, and engaged in illegal money solicitation in Jurisdiction X, Jurisdiction Y, Jurisdiction Z and other places. The amount of fraud exceeded 100 million yuan (USD 15,532,009). There have been a large number of victims from Jurisdiction X, Jurisdiction Y,

and Jurisdiction A. Due to multiple investment fraud cases, the Central Bureau of Interpol in Jurisdiction Z issued a red notice on 15 May 2018, and the Central Bureau of Interpol in Jurisdiction X issued a blue notice on 25 July of the same year. Person A entered Chinese Taipei on 31 December 2019. He had not left the jurisdiction due to the outbreak of the Corona virus. During his stay in Taichung, he was seized by the police on 14 May 2020. With the joint cooperation of the police, NIA and Jurisdiction X authorities, person A was repatriated to Jurisdiction X on May 16.

According to Jurisdiction X's information, person A was suspected of having been involved in commercial crimes amounting to USD 672,000 in Jurisdiction Z since 2015. In addition, he has also been involved in several investment frauds in Jurisdiction X. The initial estimated amount is more than 1.35 million in foreign currency (USD 209,663), and the total amount is converted to more than 30 million NTD (USD 1,068,154). Person A was stranded overseas after committing the crime and travelled to and from Chinese Taipei, jurisdictions in the region and other places. In June 2019, Person A's spouse came from Jurisdiction X to Chinese Taipei to meet person A briefly. The Jurisdiction X authorities cancelled Person A's passport on 24 February 2020, in order to arrest him and requested the assistance of neighboring jurisdictions. Person A was separately wanted by Jurisdiction Z and Jurisdiction X for investment fraud. They feared that he would start a new business during the period of detention in Chinese Taipei, endangering the economic order and damaging people's property. After locating person A, the CIB immediately found him in Taichung City on 14 May 2020.

Indonesia

In the context of the crime of ML in Indonesia from 2016 to 2020, law enforcement officers gave their perceptions regarding the risks of various typologies of money laundering offences. The full typology of ML offences is assessed based on the experience of law enforcement officials in handling ML-related cases.

The five methods with the highest frequency in descending order are:

- using a false identity;
- transfers to property assets/real estate;
- use of nominees or loan names as in the names of family members, people who work for the perpetrators, or other trusted people;
- smurfing; and
- structuring.

a. Using a false identity

In many cases the use of false identities is due to the ineffectiveness of the single identity number for citizens, making it is possible to make an identity card (ID card) of the same person in different areas or also with a false identity. The invalid ID card is then used to open an account to launder criminal proceeds. The next vulnerability is the integrity of sub-district or village officials as officers who record data on citizens who apply for ID cards. If the sub-district or village officials make administrative errors in making the ID cards, it can be assumed that the data entered as material for making the identity card is also invalid.

For example, person A, an individual convicted of corruption who had fled abroad and had already changed their citizenship, wanted to return to Indonesia and falsified his ID card by

colluding with the head of the sub-district. This resulted in the removal of the head of the sub-district.

b. Using property company or property agents

The high rate of ML through property is due to tighter banking regulations and conversely weak ML supervision in the property sector. The tighter regulations in the banking sector have made criminals look for other places to store their criminal funds, one of which is property. For this reason, Indonesia has strengthened its regulations to prevent ML in the property sector, namely Law Number 8 of 2010 concerning the Prevention and Eradication of Money Laundering (TPPU Law) and Government Regulation Number 43 of 2015 concerning Reporting Parties in the Prevention and Eradication of the Crime of Money Laundering (second regulation). The TPPU Law requires property companies or property agents to submit STRs for transactions conducted in any currency with a value equivalent to IDR 500,000,000 (USD 35,020) or greater to the Indonesian Financial Transaction Reports and Analysis Centre (PPATK). The second regulation requires the land deed authorization officer (PPAT) to also report suspicious financial transactions to PPATK regarding the purchase and sale of property.

c. Use of nominee (borrowed name), trusts, family members or other third parties

Based on PPATK's research, in 2019 out of 174 ML cases currently undergoing legal proceedings, 50 of them used a nominee usage typology, while in 2020, the figure was 58 of the 86 ML cases. This shows an increasing trend in the use of nominees for ML. This typology tends to occur frequently and it involves not only family members, but also associates of the perpetrator. Nuclear family members are easily traced by law enforcement officials because they are listed in the KK (family card), but if the person is outside the nuclear family, the investigation is more difficult. Criminals usually do this by using the identities of the people who work for them such as drivers, helpers, and other employees. Basically, the use of a nominee is an attempt to remove traces of the proceeds of a criminal act by using the name of another person who is trusted by the perpetrator of the crime. It is also possible to use nominees to obscure the beneficial ownership of a legal business entity.

d. smurfing

Smurfing is the disguising of illegitimate transactions by breaking it up into multiple transactions using multiple accounts with different names. This typology can still relate to the use of nominees to collect proceeds from crime. The perpetrator uses many accounts with different names to carry out his transactions in a certain period of time. Usually the owner of these smurf accounts will be rewarded for lending their account services and the account owner does not necessarily know where and for what reason transactions occur in the account.

e. structuring

Structuring is a transaction that is carried out in relatively small amounts, but with a high frequency to disguise a larger transaction. This typology is commonly used to avoid the suspicious transaction limit that is set at or below the cash transaction reporting threshold. Usually the perpetrator will split the transaction with a nominal value below that limit so that it does not appear as a transaction that is considered suspicious. Sometimes structuring is done in the purchase of luxury goods, in this case a luxury car. The perpetrator of this crime utilises financial services in purchasing a car then the perpetrator will deposit money monthly as instalments for the credit for purchasing the luxury vehicle.

f. Use of professional services

ML is increasingly widespread in various sectors, not only in the financial sector or within financial service providers or goods providers, but also in the professional sector. The modus operandi that is usually used is to treat the professional person or body as an intermediary for the purpose of ML. Professional services here include advocates, notaries, land deed authorisation officers (PPATs), accountants, public accountants, and financial planners. The professional services mentioned are a means for ML perpetrators to hide or disguise the origin of assets that are the result of a criminal act, by taking cover behind the provisions on confidentiality of professional relations with service users as regulated in accordance with the provisions of laws and regulations.

In many cases, professional service providers are involved in the criminal acts of ML offenders, such as the case of Person A, where lawyers were also arrested by the police for violations of anti-corruption legislation and the criminal code. At the first and appeal court stages, the lawyer, Person B, was found guilty of obstructing the investigation of the e-KTP (ID Card) project corruption case with the suspect, former DPR (People Representative Council) Speaker Person A. Person A himself also violated anti-corruption legislation and the criminal code. Even other professional services, namely doctors, were also charged with the same charges as the lawyers because they were deemed to have obstructed an investigation. Although in this case the lawyer was not proven to be related to the crime of money laundering, at least it appears that professional services are very vulnerable to being involved in the context of the main case.

g. New payment methods

Rapid technological advances have changed many things, including the world of financial services. The market is no longer a physical market, but it has transformed into an online market. Not only goods, but various kinds of services have also been marketed online. Consequently, online payments also complement the online market. Transactions become easier, people do not need to physically walk to the market nor do they need to pay physically either. Online payment applications, both as part of banking service products such as mobile banking and internet banking, as well as payments through online payment services such as e-money and e-wallets offered by many financial technology companies (fintech) have become increasingly popular in the last five years. Their use has also succeeded in advancing very quickly to the small and medium enterprises sector. The banking world is one of the highly regulated sectors while this is in contrast to the fintech world which is still new and of course the regulations are not as comprehensive. In fact, many fintech companies offer the convenience of opening accounts, making payments, and even investing.

In general, bank marketing still goes through the physical branch offices of each bank in person, while financial technology companies market online without physically meeting consumers meaning that supervision is weaker. The procedure for opening an e-wallet is simply to do it with a photo of yourself, KTP (ID card), and telephone number, without any physical verification or anything else. On the one hand, it makes it easier for consumers, but on the other hand there is a concern that it could be misused for ML. The violation of regulations in the world of financial technology and the ease of conducting transactions in it have ensured this typology is considered a high risk by law enforcement officials as a means of ML.

h. Use of corporation (legal entity)

“Official” companies are often used as fronts to be a vehicle for ML, whereby the company is used to conceal proceeds of crime as legitimate revenue for the company. It is said to be an “official” company because from a legal point of view this company stands officially and complies with regulations. Criminals usually have many companies which collect funds from the proceeds of crime or are prepared as a means of money laundering. This is done to obscure

the traces of the flow of money because the name that is officially listed on the board of directors or the owner of the company's shares is not the beneficial owner (BO). Weak BO data is also one of the main vulnerabilities in this typology. Even the banking sector cannot easily find out the real name of the BO, when only a legal, formal company certificate without any additional information is used when opening a company account.

One of the modes of corruption with the main perpetrator Person M that was revealed to the public during a trial at the Corruption Crime Court, Jakarta, on 17 January 2020 was the creation of a company called Company P, which uses the name of a person who actually works as a personal driver for a director of the company. This driver, person O, works for a person closely associated to Person M, namely person P, and he only borrowed his identity as a condition for establishing the company and for the signing of the contract. Person O did not know anything about the auction process carried out on behalf of the company of which he was a director. This typology also contains the nominee typology discussed earlier. The identity of this driver was borrowed to become a fake director of a company that did not actually belong to him, even though the activities of it were not known to him. Person O's position working for someone left him no choice, but to follow his employer's orders.

The TF NRA Document (updated 2019) maps domestic TF risks including:

a. Fund raising stage
   - donation to terrorist groups

Example case:

On MTR's orders, HZ provided logistical assistance by opening an account in his wife's name, namely RWI at Bank A, which was intended to accommodate donations from members of the MIT group led by Santoso alias Abu Wardah, to help Santoso's struggle in his escape in the mountains of Poso Regency in the form of food and tools used for training on the mountain, with a total of IDR 49,600,000 (around USD 3,480).

   - self-funding from legitimate sources

Example case:

NNG facilitated seven people including himself at his own expense by selling his house in East Jakarta for IDR 590,000,000 (around USD 41,000) which was paid by transfer from the buyer's Bank B account to NNG's Bank C account. Then the money was added to the money from the sale of home furnishings, motor vehicles, and the proceeds from selling women's clothing, for a total of IDR 33,200,000 (around USD 2,300). The total of all these funds were used to finance seven people including NNG in the form of tickets and e-visas.

   - donation through social media

Example case:

BA at the beginning of June 2016 had the idea to make a bomb that came from money from selling narcotics, which was conveyed through his Facebook account inbox under BA's name and person F's Facebook account to HB's Facebook account. Then BA raised funds of IDR 32,800,000 (around USD 2,300) from friends on Facebook as capital for the manufacture of methamphetamine to be used to fund the making of bombs for terrorist acts.

b. Fund transfer/moving Stage

- domestic and cross-border cash carrying

Example case:

AX received IDR 800,000 (USD 56) in cash from AG on the orders of BA, who is a member of the East Indonesia Mujahidin terrorist group (MIT) for the purpose of purchasing materials for making bombs to be detonated in the Pantangolemba area, Poso, Central Sulawesi. In addition, AX also collects money from members of the Makassar MIT group using their account at Bank D in the name of WW in the form of deposit funds of IDR 10,000,000, IDR 5,000,000 and IDR 3,000,000 (about USD 700, USD 350, and USD 200, respectively)

- money remittance

Example case:

In 2016, AP was asked by AJ to send money through a non-bank licensed money remittance to SM using the name of a Jurisdiction X citizen with a total amount of IDR 150,000,000 (USD 10,536) sent for the purchase of firearms to be used in the shooting and bombing incident in Thamrin, Jakarta.

- banking

Example case:

On the orders of BN, around March 2016 MK received the money transferred to the X Bank account belonging to MK's wife (PA) in the amount of IDR 6,000,000 (around USD 400) and was asked to send the money by transfer using the account to the AH's Y Bank account amounting to IDR 800,000 (around USD 53) in June, to DA's Y Bank account amounting to IDR 2,700,000 (around USD 180) at the end of June, and IDR 2,000,000 (around USD 140) and at the beginning of July. All the funds were used for the suicide bombing incident at the Surakarta Police Station.

c. Fund use stage

- purchase of weapons and explosives

Example case:

On S's orders, DN purchased weapons by sending money contributed by supporters of the MIT to Jurisdiction X using a non-bank licensed money remittance, namely: on 5 March 2015 amounting to IDR 5,000,000 (around USD 350) and on 26 March 2015 amounting to IDR 16,150,000 (around USD 1,130). DN then left for Jurisdiction X to pick up the weapons that had been purchased at a cost of IDR 2,000,000 (around USD 140).

- maintenance of terrorist networks

Example case:

On the orders of BS, HD made a small cell to carry out terrorist acts where the funds used were funds that had been received from sympathizers. These funds were used to finance the formation of new cells.

- mobility of terrorist group members and FTF travel

Example case:

AP facilitated the travel of foreign terrorist fighters 12 times, using the Z bank platinum ATM card belonging to each group representative whose ATM card was used to purchase flight tickets for departures to Jurisdiction Y and the Jurisdiction X as well as paying for electronic visas via transfer for a total of IDR 468,376,080 (around USD 32,910).

- military training

Example case:

Based on AT's instructions, SU made a fund transfer through WA's N Bank account to O Bank for IDR 2,000,000 (around USD 140) for the purposes of MD's military training and also a transfer to AZ's P bank several times for IDR 3,000,000 (around USD 200) each. In addition, at the direction of AT, SU was asked to send funds to MD and members in Tamanjeka Poso for the purpose of buying a video camera costing IDR 2,500,000 (around USD 175).

- terrorist family compensation

Example case:

Funds collected by terrorists or terrorist groups are distributed to the wives of members of terrorist groups, either those who died due to being shot by the police, who were imprisoned, who fled because they were included in the wanted list (DPO) by the Police and individuals who were on the move in Poso to join a terrorist group.

Macao, China

Couple from Macao, China arrested for involvement in fraud, forgery and ML

Several STRs received by the Financial Intelligence Office revealed that an education centre was related to a fraud case. The education centre was owned by a couple from Macao, China. After checking the account information of the company, the education centre's bank account received a government subsidy amounting to almost MOP 4,680,000 (around USD 585,000) for the "Continuing Education Development Program" in Macao, China in the period from August 2016 to August 2017. However, the funds were mainly withdrawn in cash and a small portion was transferred to the couple from Macao, China and a wedding planning company. Information showed that the wedding planning company was also owned by the same couple and their source of funds was mainly cash deposits by ATM or OTC with cashier orders then issued to other third parties.

By analysing the account transaction patterns, the Financial Intelligence Office discovered that the accounts of the company only conducted a small number of transactions before August 2016. Most of the transactions occurred in the period of August 2016 to August 2017 and the funds were mainly withdrawn in cash that was not in line with normal business practices. In addition, FIU discovered that the couple were related to fraudulent activities in the past. Therefore, the Financial Intelligence Office passed the cases to the Public Prosecutions Office.

The Public Prosecutions Office then requested the Judiciary Police to investigate the cases. It was discovered that the case was related to fraud in relation to wedding banquet deposits and the swindling of a subsidy under the "Continuing Education Development Program" in February 2017 and June 2019 in succession. The couple who ran the wedding planning company deceived over 40 customers by collecting their wedding banquet deposits amounting to a total of MOP 5 million (around USD 625,000) in two years. At the same period of time, they owned an education centre and received a government subsidy of MOP 140,000 (around

USD 17,500) but had not actually held any kind of education course and forged student attendance records.

After conducting follow-up investigations on the two cases, it was found out that the wife had remitted a total of HKD 3.3 million (around USD 424,936) of suspected fraudulent proceeds to a bank account held by the husband and his brother in a nearby jurisdiction, via the account of the wedding planning company on multiple occasions. The funds were further remitted to other banks, as well as used for the issuing of cheques and repayment of credit card loans so as to launder the criminal proceeds.

Additionally, during the financial investigation of the suspect's bank account transactions, the Judiciary Police found out that the suspect had submitted documents such as a forged proof of income and a falsified bankbook to a bank when applying for a mortgage loan of HKD 2.23 million (USD 287,160) in 2017.

In May 2020, the Judiciary Police mobilised personnel to the residence of the suspects and brought them back for investigation. The suspects denied having committed the crime. Yet, they failed to give reasonable explanations for the investigative findings of the Judiciary Police. Therefore, the Judiciary Police transferred them to the Public Prosecutions Office for three offences including fraud, forgery of documents and money laundering.

Malaysia

As identified in the 2017 National Risk Assessment (NRA), fraud, corruption, illicit drug trafficking, organised crime and smuggling remain as the prevailing crimes in the jurisdiction, mainly as attributable to the STR reporting and investigations conducted. Currently, Malaysia is in the midst of finalising its 2020 NRA covering the development of trends and patterns of ML and TF since the last round of NRA. The 2020 NRA aims to identify, assess and understand the ML/TF risks in the jurisdiction, including threat and sectoral inherent risk, control measures, relevant emerging trends and the interconnectedness between sectoral and threat assessments.

With regard to illicit drug trafficking, the Royal Malaysia Police (RMP), had in January 2020, seized RM 366 million (USD 88,812,328) worth of assets linked to its investigation into the opening of a company account used in the smuggling of 12 tonnes of cocaine worth RM 2.4 billion (USD 582,375,921) that was seized in September 2019. The cocaine was mixed with charcoal to avoid detection and was believed to be from an international drug syndicate using Malaysia as a transit jurisdiction. Eight individuals including six foreign nationals were subsequently charged for the trafficking of dangerous drugs.

The investigation revealed a large network of companies and the key involvement of a businessman who was the chairman of publicly listed companies. The businessman, a proxy of the main suspect who is still at large, was identified as owning several joint accounts with his associates. Between 2012 and 2020, these accounts received substantial cash deposits from various locations nationwide which were transacted on a daily basis and were conducted below the reporting threshold, as well as fund transfers from numerous companies including those related to one of his publicly listed companies. The funds circulated among the joint accounts, creating many layers of transactions before their subsequent withdrawal to various companies and individuals. The case revealed the significant utilisation of funds towards purchases of properties, shares and vehicles that were owned by the suspects, relatives and proxies.

Pakistan

Terrorism Financing- Proscribed person under UNSCR-1373

The transactional activity of an individual Mr. XYZ was suspicious as he was placed on Schedule-IV of the Anti-Terrorism Act, 1997 (UNSCR-1373) in October 2020 under Category A (Terrorism) due to his affiliation with a banned group.

Upon proscription under UNSCR-1373, STRs were filed by different banks on the personal and business accounts of Mr. XYZ. As per KYC documents, he was the sole proprietor engaged in a business involving dried fruit and a commission agency in the terrorism-hit area near the border of a neighbouring jurisdiction. As per the National Identification Card for Overseas Pakistanis (NICOP), the individual was an overseas Pakistani and had a permanent address in a terrorism affected area in the jurisdiction. FMU received multiple STRs from different banks upon proscription of the individual under UNSCR-1373.

After analysis, it was found that the suspect was maintaining multiple individual, business and joint accounts in different cities of the jurisdiction. Overall, 14 accounts were identified in eight different banks. Furthermore, a high volume of transactional activity was noted in the accounts before proscription over the last three years with rapid movement of funds. The transactional activity revealed that funds were transacted through cash and internal transfers with unrelated counterparties indicating the involvement of Mr. XYZ in a Hawala/Hundi business. The accounts were frozen by the banks upon proscription of the individual.

Upon analysis of the accounts of the counterparties of Mr. XYZ, it was identified that one of his counterparties Mr. A, the proprietor of MT Traders engaged in the business of scrap, cloth and dried fruit, was already referred by FMU to a LEA for investigation on suspicion of being involved in the Hawala business. One counterparty Mr. B, proprietor of HAC, engaged in the business of food grains and dried fruit, was also already under investigation by a LEA and listed in the Red Book of the Most Wanted Terrorists due to his association with a person designated under UNSCR-1267. Similarly, many other counterparties were suspected of being involved in Hawala.

Keeping in view the analysis, it was suspected that the individual might be involved in the illegal business of hawala/hundi or using this channel for moving funds. Furthermore, he was listed on the Schedule-IV of Anti-Terrorism Act, 1997, and therefore the possibility of him being involved in terrorism financing could not be discounted. The financial intelligence was shared with relevant LEAs for an investigation into the matter. The matter is under investigation.

7.3 Emerging trends; declining trends; continuing trends.

Fiji

Emerging Trend

The FIU noted an increase in individuals using alternative technology and channels to transfer funds to other individuals. This includes the use of Post Fiji telegraphic money orders (TMO) and Paypal. In some instances it was noted that the use of these alternative technologies and channels was to deliberately avoid detection.

Reported cases of illegal pyramid schemes have also increased in 2021.

Continuing Trend

The FIU observed a continued occurrence of individuals falling victim to various online scams in 2020. Cybercriminals have taken advantage of the current global Covid-19 situation and have offered fake loans, packages, and relationships to vulnerable sectors of the community that remitted hundreds of thousands of dollars to these cybercriminals.

Indonesia

An emerging threat is a new mode of money laundering that has not been mitigated by the relevant authorities. From several funding cases that have occurred recently, it was found that there were a number of funding modes that could become a new threat, including e-commerce transactions, especially start-ups that facilitate buying and selling accounts.

a. No strict regulations regarding punishment of sales and purchase and use of accounts on behalf of others

Fraudulent acts relating to sales and purchases online are increasingly occurring. There is a method involving online account trading. Sales and purchases made online through certain e-commerce/marketplaces are conducted as illegal acts of account takeover victimising the customer who actually owns the account. In the case of an account buyer as a victim, usually the seller targets a target buyer who does not understand the risks involved in buying this account. Most of the accounts sold were blocked accounts belonging to other people, or secondhand accounts. In the case of the buyer as a criminal, it is very likely that the account is bought for abuse or as a deposit for fraud. Logically, if customers really need accounts for personal needs and not for misuse, they will find it easier to open accounts in their own names. These are some facts related to the prevalence of sales and purchases and the use of other people's accounts.

b. Limited supervision regulations on e-commerce and fintech practices

The rapid growth and development of the financial technology industry has raised concerns. The simplicity and practicality contained in it seems to be a double-edged sword. This concern stems from the absence of clear regulations related to the implementation of the AML-CFT programmes from regulators.

Meanwhile, the current state of technological development, coupled with the increasingly encouraging efforts to prevent and eradicate TF, has caused terrorist groups to continue to look for new alternative routes to seek financing of terrorism in ways that tend to be difficult to detect and trace, including:

• Use or misuse of corporation/companies

Through a legal company, terrorist groups can use banking facilities and financial service providers for the purpose of collecting, transferring and using funds so that it looks as if it is an ordinary business transaction. Criminal acts of terrorism financing committed by person B that were successfully revealed by law enforcers show that terrorist groups own oil palm plantations to fund their activities.

• Illegal drugs

According to the United Nations Office on Drugs and Crime (UNODC), in raising funds to support terrorist acts, terrorist organisations can rely on traditional criminal activities, including the sale of illegal drugs, or commonly known as narcoterrorism. The UNODC report regarding the existence of narcoterrorism in Afghanistan shows a correlation with the development of terrorism financing through criminal channels in Indonesia and there is a potential new threat in terrorism financing through the sale of illegal drugs.

• Virtual currency

The development of technology 4.0 in fintech companies led to the emergence of a funding model using virtual currency as happened in the case of person E who used bitcoin in terrorism funding. Virtual currency has features including fast transaction processing, low transaction fees, and relative ease; however, they are vulnerable to being exploited by criminals because they allow transactions to occur without using their real names, do not have reporting obligations and some do not require third-person intermediaries to carry out the transactions.

• Online loans

The emergence of fintech in the form of online loans makes it easy to get the desired funds in a short timeframe and with an easy process. However, the ease of technology also influences the ease of online lending to customers and can therefore be exploited by terrorist groups.

• Fundraising through social media (crowdfunding)

Fundraising through social media or crowdfunding, especially during the pandemic, such as raising funds raised for the purchase of medical devices can be used by terrorist groups to finance terrorism. In addition, the ease of creating social media accounts by utilising anonymous/ fake/other people's accounts allows the use of social media to spread fundraising messages more and more frequently.

In the 2020 NRA ML preliminary document, there are a number of technical and strategic issues that are considered important in determining the effectiveness of the eradication and prevention of ML in the future, include the following:

a. There is still limited attention, awareness and partisanship of state and government elites on the importance of law enforcement of ML for all predicate crimes. The optimisation of ML can be directed as a step to "impoverish" criminal acts so that criminals think again, given the higher consequences of crime.

b. A number of law enforcement agencies have shown their commitment to support the AML regime by establishing a special unit or ML task force.

c. The limited number of ML investigators and the inadequate coordination pattern between institutions, especially related to cases in the forestry and environmental sectors, which often stop at actors in the field.

d. It is necessary to strengthen the institutional quality of the MLA central authority at the Ministry of Law and Human Rights to increase the effectiveness of coordination and cooperation, and to eliminate a reluctance to share information amongst competent authorities.

e. The absence of an integrated data system or some kind of big data analytics that can help law enforcement, supervisory and regulatory agencies, as well as reporting parties, to optimise their ability to identify, monitor, and mitigate risks to the ultimate beneficial owner and PEPs related to ML.

f. The absence of a system of "Integrated ML Analysis Data" that can be implemented by the stakeholders of the AML regime.

g. The need for optimising the whistleblowing system related to ML crimes committed by corporations and individuals based on corporate identification on the alleged occurrence of ML.

Macao, China

Continuing trends

Internet-related fraud

In the first half of 2020, the trend for internet-related fraud cases was still of concern. Fraud cases mainly happened via the internet in relation to investment fraud, romance scam, etc. Sometimes local banks received telegraph messages from the ordering bank or an email from the victim claiming the relevant remittances were related to fraudulent acts. Through the continuing promotional campaign from law enforcement agencies, front-line bank staff would also alert a suspected victim to think twice before remitting money to a third party's account and stay vigilant against deception, in order to avoid losing money to scams.

Malaysia

Continuing trends

Over the years between 2017 and 2020, criminals' use of mule accounts to facilitate financial fraud, notably telecommunication scams, remains prevalent in the jurisdiction. More recently, there are also signs of the exploitation of companies incorporated onshore and offshore by international fraud/ML syndicates in moving or layering the funds via various fraud schemes including business email compromise (BEC) scams, personal protective equipment (PPE) fraud, etc. The increase in fraud-related STRs received by the Malaysian FIU coupled with the public complaints last year indicated that fraud schemes have become more predominant as criminal groups resort to exploiting the financial misfortunes of the public due to the COVID-19 pandemic. The modus operandi of these fraud schemes continue to evolve with the use of corporate mules as well as individual mules utilising non-conventional methods such as non-bank remittance service providers, e-money issuers and virtual assets to launder the proceeds of these fraud schemes. More sophisticated scams involve networks across multiple jurisdictions and the use of advanced technologies e.g. spoofing technology such as VoIP and the use of mobile internet rather than WiFi to avoid a trace of an IP address is also emerging.

Vietnam

Currently, the 4.0 technology revolution has had a strong impact on all sectors of the economy, especially in the fields of banking and finance. Accordingly, many types of payment intermediaries, including e-wallets and virtual money, have appeared, creating favorable conditions for consumers in transactions and payment for goods purchase and sale. However, these forms of payment also pose potential risks of being used by criminals to conduct money laundering and terrorism financing activities; in which, Mobile Money is one of the services with many potential risks to be used by criminals to commit money laundering due to its characteristics such as anonymity, difficult to control and fast execution.

8. 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.

8.1 The impact of legislative or regulatory developments on detecting and/or preventing particular methods (eg tracing proceeds of crime, asset forfeiture etc).

Australia

Following the conviction of Christchurch, New Zealand, mosque shooter Person A in August 2020, the New Zealand government imposed targeted financial sanctions on Person A, with the Australian Department of Foreign Affairs and Trade imposing similar sanctions on him shortly afterwards.

Chinese Taipei

On 7 November 2018, Chinese Taipei passed the Amendments to Counter-Terrorism Financing Act (CTF Act). The amendments ensure that the scope of TFS applies to the agent of a designated individual, legal person or entity, or other entities acting on behalf of, or under the direction of, designated persons and entities, in order to comply with international regulations. On 31 March 2018, Chinese Taipei implemented TFS on a citizen person A and froze the assets of entities controlled by person A after the aforementioned amendments.

In addition, on 1 February 2019, Chinese Taipei passed the Regulations on Competent Authorities Governing Specific Foundations for Anti-Money Laundering and Counter-Terrorism Financing. As stated in these regulations, competent authorities shall take appropriate measures to supervise foundations under the definition of FATF, which engage in the pursuit of raising or disbursing funds for charitable, cultural, educational, social, fraternal or other similar types of purposes beneficial to the public and which have been listed as foundations with high risk by the competent authorities through the procedures of risk assessment, to avoid those foundations being subject to ML/TF abuse. In addition, the Prosecutors' Office prosecuted person B and his accomplices in September 2020 for violations of the CTF Act which involved the illegal sale of oil to DPRK. It was the first prosecution case of this kind made by Chinese Taipei.

Chinese Taipei

The FSC has required the Bankers Association to send "Suggested Best Practices for Banks to Identify Beneficial Owners" to financial institutions for reference on 24 March 2020.

Regarding the enhanced cooperation between law enforcement and private sectors, the FSC has asked relevant financial industry associations to hold compliance forums periodically. For example, the Bankers Association has invited law enforcement to share Fintech and emerging crime typologies and cases, and invited financial institutions to share their best practices for identifying beneficial owners and financial groups to share AML/CFT information in 2020.

These measures could make financial institutions better understand risks and threats and effectively assist law enforcement authorities to investigate the proceeds of crime.

In 2020, the FSC revised the AML/CFT questionnaire, and updated the risk rating and risk profile of financial institutions in early 2021.

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.

Chinese Taipei is currently working on a draft which will include third-party payment service providers as a DNFBP in Subparagraph 5, Paragraph 3, Article 5 of Money Laundering Control Act (MLCA) when handling specific businesses, and will issue regulations governing the internal control system, audit system, identity verification mechanism, record keeping on necessary services, STR filing and all reporting on designated sanctioned individuals and entities.

Fiji

In March 2019, following a Fiji Police Force search for possible illicit substances, Person B was found in possession of FJD 28,000 (USD 13,718) in cash. Person B is the wife of the drug suspect and stated that the cash was from the sale of a vehicle, however, there was no evidence of the sale of a vehicle and there was no evidence that she was able to initially purchase a vehicle with that residual value. The police suspected that the cash was from the proceeds of the sale of drugs. Person B continued to maintain that the cash was from the sale of a vehicle to Person X, however, Person X denied purchasing a vehicle from her and there was no evidence of a vehicle transfer from her during this time period. Person B failed to provide an adequate explanation for the cash, ultimately resulting in the funds being declared as unexplained wealth by the High Court of Fiji in 2020 and forfeited to State. This successful trial was Fiji's first unexplained wealth case since the introduction of unexplained wealth laws.

Macao, China

AML/CFT/CPF Strategic Plan (2021-2025)

To respond to the complex changes in the development of international trends of ML/ TF /PF, and to further protect the sustained healthy growth and the diverse development of the economy of Macao, China, the government formulated the first AML/CFT/CPF Strategic Plan for the year 2016 to 2020 based on the result of the 1st overall risk assessment project. With the expiration of the first AML/CFT/CPF Strategic Plan, the second was developed to set out the policies and goals for the period from year 2021 to 2025.

The AML/CFT/CPF Strategic Plan (2021–2025) of Macao, China outlines the strategic direction of the government in the relevant regime. These include the following ten strategic goals:

Goal 1:	Continuously maintain a comprehensive AML/CFT/CPF legal and institutional framework to cope with the evolving economic development of Macao, China and international standards
Goal 2:	Enhance overall Macao, China ML/TF/PF risk assessment
Goal 3:	Foster international cooperation in relation to AML/CFT/CPF and related predicate offences
Goal 4:	Further reinforce parallel financial investigations for all major predicate offences
Goal 5:	Continuously maintain the high transparency of legal persons and legal arrangements
Goal 6:	Enhance confiscation and asset recovery to deprive criminals of criminal instrumentalities and proceeds
Goal 7:	Prioritise terrorist financing investigations as higher policy level objectives in accordance with international standards
Goal 8:	Uphold a sound Risk-Based Approach in supervision for all sectors and in criminal investigation
Goal 9:	Strengthen the implementation of CFT and CPF freezing mechanisms in accordance with international standards
Goal 10:	Promote a compliance culture, awareness and understanding of ML/TF/PF risks to all regulated entities to enhance the level of AML/CFT/CPF compliance

More detailed sub-goals and action items were further developed under the framework of the ten strategic goals. This new five-year strategic plan, as in the past, was read and discussed by the Executive Council which was headed by the Chief Executive of Macao, China, thus showing the high level political commitment to address AML/CFT/CPF issues.

Other AML/CFT Legislative or Regulatory Developments in 2020

In order for the reporting entities to have a better understanding on the implementation of the law "Asset Freezing Regime", the supervisory agencies, the Monetary Authority of Macao, China and the Gaming Inspection and Coordination Bureau, issued Circulars and Practical Guidance to financial institutions and gaming concessionaires in March and June 2020 respectively. The Circulars and Practical Guidance aim to explain in more detail the requirements of the law "Asset Freezing Regime", assist the reporting entities to refine their SOPs, as well as establish an expedited coordination and reporting mechanism with industries.

Statistics

(i) In the first half of 2020, a total of 947 STRs have been received and 57 STRs were reported to the Public Prosecutions Office.

(ii) In the first half of 2020, the number of AML/CFT investigations, prosecutions and convictions are given as follows:

Activities	AML/CFT
Investigations by the Judiciary Police	25
Investigations by the Commission Against Corruption	2
Investigations by the Public Prosecutions Office	20

Prosecutions	6
Convictions	2*

` * 1 case is still under appeal.

For cases developed directly from STRs, please refer to Macao, China's Case, '*Couple from Macao, China arrested for involvement in fraud, forgery and ML*' in section 7.2.

Malaysia

To complement the principle-based requirements in the revised Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions Policy Documents for FIs, DNFBPs and non-bank FIs (AML/CFT Policy Documents) which came into effect on 1 January 2020, Bank Negara Malaysia (BNM) has issued two guidance documents on beneficial ownership and verification of individual customers. The documents aim to facilitate the operationalisation of the requirements under the AML/CFT Policy Documents and provide recommendations for reporting institutions to strengthen the appropriate controls that are commensurate with risk levels.

To support industry players in navigating the COVID-19 pandemic, BNM issued a Circular on Regulatory Expectation on AML/CFT Measures during the COVID-19 pandemic in April 2020. It outlined regulatory flexibilities already accorded within the revised AML/CFT Policy Documents, such as the implementation of a RBA to determine appropriate CDD measures that are commensurate with ML/TF risk levels.

In addressing rising cybercrimes, the Royal Malaysia Police also took the initiative to develop a mobile application, "Semak Mule", in addition to its existing website[39], to enable the public to authentically check bank accounts and telephone numbers which have been linked to criminal activities. The mobile application also lists the top 10 bank accounts and phone numbers used in scams to allow the public to make an early check wherever they are and to avoid becoming victims of cybercrime in Malaysia. As the public can access it anytime of the day, this initiative has yielded results with a total of 9 million people having accessed the web portal and 120,000 have downloaded the application as at October 2020.

Philippines

The Philippines has an existing legal framework addressing terrorism. In 2007, the Philippines enacted Republic Act (RA) No. 9372 titled "An Act to Secure the State and Protect our People from Terrorism, also known as the Human Security Act of 2007". In 2012, the Senate and House of Representatives of the Philippines in Congress also enacted RA No. 10168, otherwise known as "The Terrorism Financing Prevention and Suppression Act of 2012" (TFPSA). RA No. 9732 was repealed through the enactment of RA No. 11479, or the Anti-Terrorism Act of 2020 (ATA).

[39] http://ccid.rmp.gov.my/semakmule/

RA 11479, titled "An Act to Prevent, Prohibit and Penalize Terrorism, Thereby Repealing Republic Act No. 9372, otherwise known as the Human Security Act of 2007", was signed into law by the President on 3 July 2020 and took effect on 18 July 2020.

Section 25 allows the Anti-Terrorism Council[40](ATC) to:

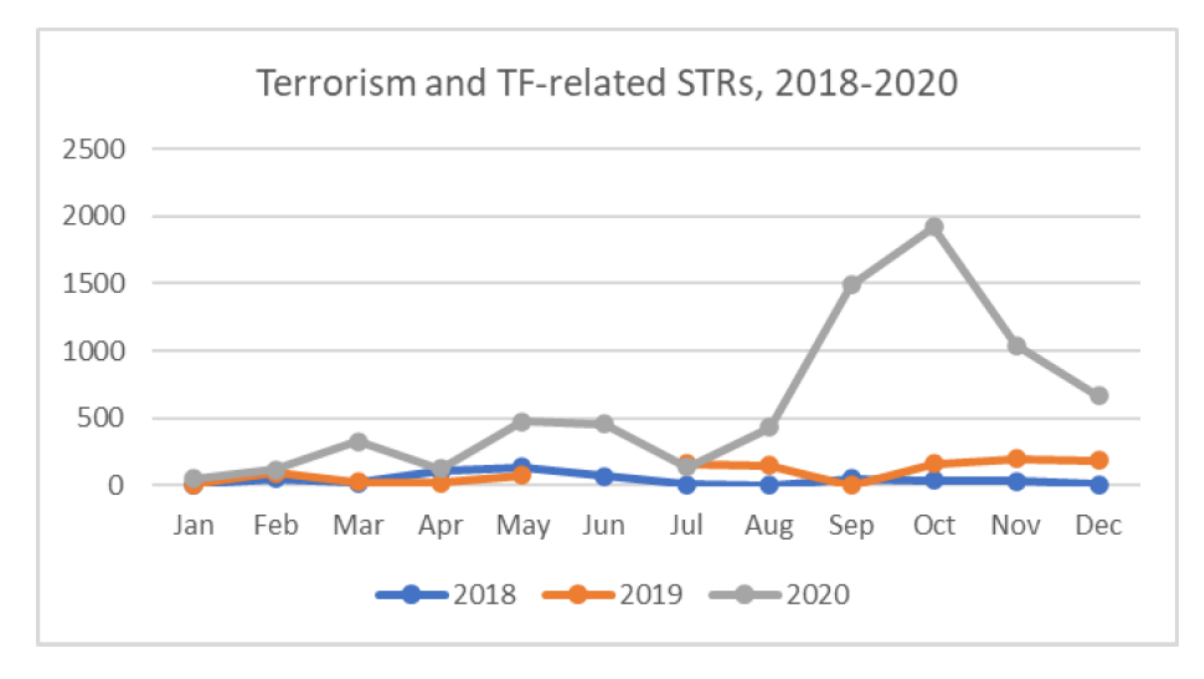
a) automatically adopt the UNSC Consolidated List of individuals, group of persons, organization or associations designated and/or identified as terrorists, financiers of terrorism;

b) adopt upon determination, requests for UNSCR 1373 designation of foreign states; and

c) designate domestic terrorists, upon determination of probable cause.

The passage of the ATA provides additional awareness to covered persons in identifying potential terrorists, and terrorism- and TF-related transactions. While the ATA is a welcome addition, LEAs in the Philippines can still use the TFPSA to prosecute TF.

An assessment of STRs showed a 580% increase in 2020 compared with the 2019 STRs. The monthly trend shows a surge in STRs from September to December 2020, in the months after the enactment of the ATA. There was also a surge of over 500% in STR reporting during the COVID-19 pandemic particularly from March to July during the imposition of the community quarantine.



STRs are reported through coordination between the AMLC and covered persons (CP) in the possible nexus of the accounts, with terrorism and TF. Other contributory factors are the regular

[40] Section 45 of the ATA provides for the creation of the Anti-Terrorism Council (ATC). The ATC is composed of nine (9) members of the Cabinet including the Executive Secretary, National Security Adviser, Secretary of Foreign Affairs, Secretary of National Defense, Secretary of Interior and Local Government, Secretary of Finance, Secretary of Justice, Secretary of Information and Communications Technology, and the Executive Director of the AMLC.

updating of risk understanding through regular engagement of the AMLC and other LEAs with CPs and industry associations; and the continuous and coordinated efforts of various agencies in the campaigns for AML/CFT.

Singapore

Legislative development to enhance intelligence sharing with FIUs

With effect from 1 April 2019, Singapore has amended Section 41 of our Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (Chapter 65A) ("CDSA") which enables the Suspicious Transaction Reporting Office (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; and

- the foreign FIU has given appropriate undertakings for protecting the confidentiality and controlling the use of the financial intelligence.

This legislative amendment allowed for collaboration with more FIUs to aid in detection of ML activities, its predicates as well as TF activities. In 2020, the numbers of requests for assistance that STRO sent out and received respectively from our foreign counterparts both saw an increase of approximately 10% each, as compared to 2019.

Legislative development of Payment Services Act

Under the Payment Services Act (PS Act), VASPs (or digital payment token service providers as referenced in the PS Act) that buy, sell or exchange digital payment tokens (DPTs) are required to be licensed and are subject to AML/CFT requirements. Service providers that deal in virtual assets for investment purposes are similarly required to be licensed under the Securities and Futures Act and comply with AML/CFT requirements.

To align Singapore's regulatory regime with the revised FATF standards for virtual assets, amendments to the PS Act were passed in Parliament in January 2021 to expand the scope of regulated DPT services to include the transfer of DPTs and the provision of custodial wallet services for DPTs. A DPT service provider that provides any of these services would similarly need to be licensed under the PS Act and be subject to MAS' AML/CFT requirements. This will include the need to conduct customer due diligence, monitor transactions and report suspicious transactions. MAS is also making legislative amendments to include entities incorporated in Singapore that are providing VA services (i.e. services relating to payments and/or investments) solely outside of Singapore within its regulatory ambit.

MAS applies a risk-based approach to supervising VASPs in Singapore. Robust AML/CFT-focused checks are conducted on licence applicants as part of the licensing process, to ensure that DPT service providers that intend to operate in Singapore have the relevant ML/TF risk awareness and appropriate AML/CFT controls in place. MAS also conducts risk-targeted inspections to examine the effectiveness of licensees' AML/CFT controls, including their monitoring and surveillance activities to detect unusual behaviours and suspicious transactions. MAS also leverages on its surveillance capabilities to proactively detect unlicensed DPT

activities for enforcement action, using both public and other data sources, such as corporate registry information and STRs.

As the VAs sector continues to evolve, Singapore authorities, including MAS and law enforcement agencies, work closely together to identify and detect ML/TF/PF risks and typologies, and take necessary steps to mitigate these risks.

Enhancing BO transparency in Singapore

Under the Companies Act and Limited Liability Partnerships Act, companies and LLPs are required since 31 March 2017 to obtain and maintain beneficial ownership information, and to make the information available to law enforcement authorities upon request.

As part of the Accounting and Corporate Regulatory Authority's (ACRA) ongoing efforts to uphold Singapore's reputation as a trusted financial hub, and to further enhance the transparency of ownership and control of corporate entities, the Companies Act and Limited Liability Partnerships Act were amended with effect from 30 July 2020 to require all companies and limited liability partnerships (LLPs) to file the information that they maintain in their Register of Registrable Controllers (RORC), with ACRA's Central Register of Controllers. The RORC information in ACRA's Central Register of Controllers is made available to law enforcement agencies for the purpose of administering or enforcing the laws under their purview.

8.2 Cases developed directly from suspicious or cash/threshold transaction reports.

Malaysia

Business email compromise (BEC) and involvement of a bank branch manager in facilitating the opening of mule accounts

The FIU received an STR from Bank X reporting on Entity A, a newly established sole proprietorship, which received a substantial amount of inward remittance funds from Jurisdiction S despite being in operation for only two weeks. Before the sender bank was able to alert Bank X that the inward funds were related to fraudulent transactions involving BEC, a small portion of the amount was immediately withdrawn over the counter. The remaining funds were transferred out to another account held by Entity B in a different financial institution.

Upon further checks, it was discovered that there was also an STR reported on Entity B's account on a similar basis of suspicion, in particular receiving a substantial amount of funds from a foreign entity and with an immediate outgoing transfer to another entity. The transactional behaviour of Entity B closely mirrored Entity A.

Further analysis by the FIU revealed that this BEC activity involved a group of sole proprietorships as mule account holders, with similar names of legitimate businesses established in foreign jurisdictions to deceive potential victims. These sole proprietorships were created to mask as these foreign businesses and employ the same modus operandi as Entities A and B.

In addition, after an internal investigation initiated by one of the financial institutions involved, it was discovered that the syndicate was facilitated by a bank branch manager to ease the process of account opening and withdrawal of funds.

The case was forwarded to the Royal Malaysia Police (RMP), which resulted in an investigation and the main suspects were charged under Section 420 of Penal Code while the seized funds were returned to the victim under section 60 of AMLA.

Filing of an incorrect return by a professional

A doctor served as a surgeon consultant in a private hospital and he also owned a clinic. Surveillance activities conducted by the Inland Revenue Board of Malaysia (IRBM) on the doctor's assets, liabilities, income and other related information showed that the doctor's reported income was understated. He had partially omitted earnings from his private practice and service at the private hospital.

Investigation by the IRBM revealed that the large total savings held in the doctor's accounts was not commensurate with his declared income. Inspections were conducted at the doctor's business premises and personal residences, and on various third parties related to or doing business with him. The doctor was charged under Section 114 (1)(a) of the Income Tax Act 1967 for wilful evasion of income tax for five years, which amounted to approximately RM 6.5 million (USD 1,577,096) in unpaid taxes. The case was subsequently withdrawn upon settlement of the payable tax and penalties through civil recovery.

An STR reported by a bank revealed that within a five month period, RM 8.2 million (USD 1,989,576) was deposited into a personal account jointly maintained by the doctor and his wife, who is a housewife. Some of the funds were from his fixed deposit accounts which had been closed, and he issued cheques for more new fixed deposit placements. According to the bank, he had a total of 12 fixed deposit facilities. In view of the large transactions in the account and his profession, the bank suspected that the doctor had used his personal account for business purposes, and he might be involved in tax evasion.

Tax Evasion Involving Illegal Income / Profit

A joint investigation was conducted by the IRBM with other LEAs on a group of 55 entities in a State in East Malaysia suspected to be involved in the smuggling of cigarettes and liquor from a neighbouring jurisdiction. The smuggled cigarettes and liquor were distributed to groceries and chain stores in the State.

Investigation by the IRBM revealed that the entities had a high turnover in their bank accounts with large transactions. The amount involved in transactions was not commensurate with income declared to the IRBM. The case was subsequently settled as a civil recovery under the Income Tax Act 1967. The total amount of tax evaded of RM 19.7 million (USD 4,779,828) has been paid.

Multiple STRs were reported on the two main subjects, Mr P and Mr T, who were involved in the wholesale and retail of food and groceries. A summary of suspicious transactions which indicate Mr P's and Mr T's possible involvement in illegal activities, ie. smuggling and tax evasion is as follows:

- Mr. P's personal accounts showed a high volume of deposit transactions via cash over the counter, cash deposit machine and cheques. The funds were withdrawn via cash cheques encashment.

- Mr. P informed the RIs that transactions conducted in his accounts were for business purposes. However, the source of funds and purpose of transactions performed by Mr P could not be determined/verified by the RIs.

- Mr. P had claimed one non-winning cheque from a casino despite no gaming activity at the casino, indicating that Mr P could have used channels other than banking institutions (e.g. casino) to receive business proceeds.
- Based on his declaration to the RIs, Mr P was related to Mr T, i.e. owning the same business or having the same employer.
- Mr. T had multiple roles, as director/shareholder and/or authorised signatory in various business entities involved in businesses such as transportation and hotel. Some of the entities had no clear nature of business.
- Mr. T was investigated previously by LEAs (an order under Section 48 of AMLA was issued against him).
- Mr. T appeared to be actively conducting transactions through a casino. He was reported to have conducted cash transactions in large amounts in a casino and claimed some non-winning cheques. Total amount of transactions which were not related to gambling was high.
- Mr T had also placed a large amount of funds in share investments.

Singapore

Person prosecuted in a tax evasion case developed directly from STR

STRO received a STR on Person A. Analysis revealed that there were numerous cash deposits of more than SGD 1 million (approximately USD 0.75 million) deposited into Person A's personal bank account over a period of four months. Person A had mentioned that the deposits were earnings from her pub businesses.

Acting on the STR, the Inland Revenue Authority of Singapore (IRAS) initiated an investigation into Person A. Using data analytics and advanced statistical tools, IRAS detected anomalies in the income tax declarations of two pub establishments. IRAS also noted that all the businesses registered in Person A's name had ceased before the time the deposits were made into Person A's personal bank account.

Investigations revealed that although Person A was not listed as a shareholder or director of the two pub establishments, Person A was actually the decision-maker for the businesses carried on by both companies and orchestrated an arrangement to omit cash sales. The companies had made false entries in their Income Tax Returns and had also understated output tax in their GST Returns.

Person A was convicted of assisting two pub establishments to evade Income Tax and Goods and Services Tax (GST). Person A was sentenced to 41 weeks' imprisonment and ordered to pay total taxes, penalties and fines amounting to SGD 2,318,452 (approximately USD 1,747,045).

STR supporting overseas investigation into possible fraud and embezzlement

STRO received intelligence on Person B's involvement in possible fraud and embezzlement of monies from a Savings and Cooperative Loan Fund based in a Southeast Asian jurisdiction

where repayments amounting to more than SGD 1 billion (USD 751,680,134) were defaulted from February 2020.

STRO conducted further analysis on the financial intelligence relating to Person B during the possible offence period. Our analysis uncovered that during this period, Person B had money flows of more than SGD 5.9 million (approximately USD 4.45 million) overseas through a mix of money changers and wire transfers via bank accounts. With the recent unravelling of Person B's alleged embezzlement, STRO had reasons to suspect that the money flows could potentially be related to the said Fund.

STRO expeditiously shared our analysis with our foreign FIU counterpart and received feedback from it that our analysis and information had provided insights for their ongoing investigations against Person B.

9. COVID-19 RELATED ML & TF TRENDS

9.1 Association of types of ML or TF with particular predicate activities linked to COVID-19 (e.g. welfare fraud, scams, counterfeit medicines, corruption, drugs, smuggling, etc).

Brunei Darussalam

On 16 March 2020, the Government of Brunei Darussalam implemented the closure of all borders and strictly monitored any persons claiming essential travel to arrive in the jurisdiction. Since then, there has been a steep increase in the discoveries of drug-related offences involving larger amounts of illegal narcotics.

Based on open source reports, it is estimated that a total of BND 5.9 million (USD 4,432,815) worth of drugs and BND 419,000 (USD 314,806) of cash suspected to be proceeds of crime (including foreign currency) as well as other assets such as cars, boats, jewellery and mobile phones was seized.

These discoveries also occurred in parallel to the increase in the smuggling of contraband goods such as alcohol and tobacco. This observation brings forth a correlation between border closure and the rise in the discovery of smuggling incidents and the amount of products being smuggled into Brunei Darussalam.

Drug smuggling offences cases

a. In September 2020, the Brunei Narcotics Control Bureau (NCB) recorded its largest ever confiscation of drugs, money and property. In an operation called 'Musang King', the NCB raided residential homes and arrested several individuals believed to be involved in a family drug business network suspected to be the largest supplier of methamphetamine in Brunei.

The operation saw the seizure of 19 kilograms of methamphetamine with an estimated market value of more than BND 3,700,000 (USD 2,779,833).

Other significant items seized included foreign currencies amounting to more than BND 250,000 (USD 187,828), various gold jewellery items, handbags and watches, gym and electronic equipment, home furniture, 13 cars, two boats and one motorcycle. Also found, were 202 cartons of various brands of cigarettes. The case is currently still under investigation.

b. In May 2020, the NCB conducted the seizure of 100 pills believed to be ecstasy, 155g of ketamine and cash from an individual attempting to smuggle it into the jurisdiction through a border control post. The suspect was driving a vehicle owned by a locally registered forwarding agency (parcel runner). The estimated value of the seized narcotics totals about BND 25,000 (USD 18,782).

Alcohol and tobacco smuggling cases

a. In December 2020, an Indonesian national was found to be guilty of the illegal possession of 12 boxes, 480 cartons and 10 packets of various brands of cigarettes. He was fined BND 460,000 (USD 345,626) or to serve 35 months' jail in default of payment. The cigarettes were found to be hidden in the person's house.

b. In November 2020, two men were ordered to settle fines well over BND 100,000 (USD 75,138) after pleading guilty for possessing large amounts of smuggled cigarettes.

A 29-year-old local man was fined BND 170,000 (USD 127,748) and would have to serve 23 months' jail in default of payment after he pleaded guilty to the charge. He was found to have kept 537 cartons and 107 packets of cigarettes in his car when the authorities inspected his house in March 2020.

A foreign national was ordered to settle a fine of BND 105,000 (USD 78,902) for possessing smuggled cigarettes and beer. He would have to serve 23 months' jail in default of payment of the fine after he pleaded guilty to the charge and admitted that he was caught red handed by the authorities while driving his vehicle in Pekan Bangar, Temburong District. He was found with 125 cartons of cigarettes in his vehicle and further inspection at his home in Kampong Subok revealed he had kept four cartons of beer without an import permit.

Chinese Taipei

Case One

Mr. C is a recidivist of fraud with several criminal convictions on his record. During the COVID-19 pandemic, he impersonated a foreign tycoon Mr. Y's secretary, and phoned the CEO of a Chinese Taipei mask manufacturing company M, claiming that he wanted to order 5,000 adult masks, 5,000 children masks, and 100 boxes of alcohol swabs as gifts for medical staff in U hospital. Besides this, in order to convince the CEO of M, Mr. C provided U hospital's address to company M as the shipping address. However, he gave his phone number to company M as a contact. When those masks and alcohol swabs arrived, Mr. C then intercepted the goods for his own private use. The Prosecutors' Office prosecuted Mr. C for violations of the Criminal Code in August 2020.

Case Two

The Telecommunications Investigation Corps of CIB received information about illegal sellers on the Internet who lied to consumers while selling medical-grade masks. Consumers found that the quality was different after purchasing, so they reported to the police. In order to prevent inferior medical masks from being sold in the market, the Telecommunications Investigation Corps of CIB and Lukang Branch of the Changhua County Police Department jointly organised a project and reported to the Prosecutor's Office.

The taskforce analysed the above-mentioned intelligence and relevant information then arrested an online seller person A in Yunlin County. According to the confession by the seller person A, the taskforce continued to trace its upstream shipping merchant person B, and searched his residence in Taichung City, and seized 20 boxes of fake and inferior masks on the spot. The taskforce continued to trace the source of the fake and inferior masks. It was discovered that the source of the goods was supplied by the suspect person C.

After the collection of evidence in this case was complete, the undertaking prosecutor commanded the taskforce to conduct a search on the suspect person C's factory. It is found that person C is a mask manufacturer. He used the opportunity of importing mask machine equipment from China to falsely claim to be a national team mask machine manufacturer, and using the reason of testing the yield rate of masks to produce a large number of masks which claimed to be medical masks. Then he sold them wholesale to online sellers for profit. The taskforce seized 440 boxes of finished masks and account books on the spot. In this case, a total of 1.15 million fake and inferior masks were seized. The whole case was transferred to the Prosecutor's Office on suspicion of violating the Special Act for Prevention, Relief and

Revitalization Measures for Severe Pneumonia with Novel Pathogens and special regulations for rescue and promotion, criminal law of fraud and pharmaceutical law.

Fiji

In March 2020, the Fiji FIU issued a press release advising members of the public to be aware of Covid-19 related online scams. Fiji FIU received a report of a product scam connected to COVID-19 whereby a local pharmaceutical company paid for an order of PPE it never received. The FIU also received a report of a fake foreign entity attempting to engage with a local accounting firm to facilitate payments for PPE. The local accounting firm was advised not to engage with the entity and cease all communications.

Hong Kong, China

With the support of the Hong Kong Monetary Authority, the Hong Kong Association of Banks (HKAB) held a sharing session on "Impact of COVID-19 Pandemic from AML and/or other Financial Crime Risk Perspective" in September 2020 to share financial crime trends observed and challenges encountered during COVID-19, and good practices of banks in managing and mitigating ML/TF risks. The information shared was based on member banks' responses to a questionnaire distributed by HKAB to collect the industry's observations and experiences amid the pandemic. Following the sharing session, a summary of the responses was circulated to the industry to help individual banks in identifying suspicious accounts and undertaking mitigating measures where appropriate. The summary includes, among others, key observations on financial crime trends as below:

Trends in Criminal Activities

Types of fraud

- COVID-19 related: Sales fraud on personal protective equipment / pharmaceutical products especially via online or via social media, fake charities set up to receive pandemic-related fundraising donations, fraud to take advantage of anti-pandemic fund.
- Others: Romance scam, telephone deception (e.g. impersonation of government officials/ bank staff), investment frauds, business email compromise (BEC) frauds.

Modus Operandi / Commonalities regarding the Opening / Usage of Mule Accounts

- Due to difficulties for non-HK residents to visit Hong Kong, China owing to travel restrictions and quarantine requirements worldwide, there was a shift in profile of accounts opened by suspected money mules from individuals of a particular nationality on short-term stays in Hong Kong to domestic helpers based in Hong Kong and Hong Kong residents with vulnerable background.
- Dormant accounts receiving surge in deposits marked as pandemic-related fundraising or donations.
- Surge in transaction volume during COVID-19 period, temporary repository, via cash / faster payment system (FPS) and online banking platform. The frequency and pattern of transactions were not in line with the customer’s stated purpose of account and/or nature of business.

- Some mule accounts with one beneficiary owner were opened within one year and the initial transactions were related to personal protective equipment sales to other jurisdictions, which were not consistent with the business areas provided in the CDD profiles.

Case 1

The government implemented subsidy schemes for businesses affected by the COVID-19 pandemic. Eighteen persons who had made fraudulent subsidy applications by submitting false information and forged documents purporting that the alleged businesses were in actual operation before the specified dates were arrested for 'Fraud' with over HKD 6 million (USD 772,444) involved. An investigation is ongoing.

Case 2

In response to online advertisements of the sale of surgical masks and medical equipment, an owner of a healthcare products trading company in Hong Kong, China was deceived to transfer HKD 450,000 (USD 57,936) into various accounts in Hong Kong and Jurisdiction X and bitcoin equivalent to HKD 4 million (USD 514,963) to virtual asset accounts held by the scammers. All of the scammers became out of reach after receiving the payment. An investigation is ongoing.

Indonesia

According to PPATK Research related to ML/TF Risks related to the COVID 19 Pandemic, there were cases of Business Email Compromise (BEC) fraud committed by Indonesian citizens by involving companies in the management and maintenance of medical equipment in Jurisdiction X. The company entered into a cooperation contract to purchase 1,500 lung ventilators and 5,000 multi-parameter monitors with companies in Jurisdiction Y with a total value of EUR 17,011,980 (USD 20,643,657). The method used by the perpetrators was to establish several companies with Indonesian legal entities that were engaged in trading laboratory, pharmaceutical and medical equipment with names similar to those of the Jurisdiction X company's business counterpart in Jurisdiction Y. The perpetrator also opened an account in the name of the company at a bank in Indonesia. Furthermore, by using a fake email domain similar to the corporate email domain in Jurisdiction Y, the perpetrator sent information on changes to payment bank accounts on the grounds of the COVID-19 situation, causing companies in Italy to send funds to fake company accounts in Indonesia totalling IDR 58.8 billion (USD 4,116,254) in three incoming SWIFT transactions.

In the adjacent period, the total incoming funds of IDR 2.7 billion (USD 189,105) were transferred to several company accounts where the funds were held and transferred to many individual parties in 72 transactions for further cash withdrawal transactions leaving only a minimal balance in the account. Meanwhile, the remaining funds of IDR 56.1 billion (USD 3,928,718) were successfully postponed by the financial services provider.

Macao, China

For the financial sector (excluding the insurance sector), a study was conducted to understand the impact of emerging risks related to COVID-19 from an AML/CFT perspective on the sector in July 2020. The result revealed that there was no material impact on the AML systems of the

financial institutions and they resumed normal operations swiftly since the pandemic in Macao, China was adequately controlled at its early stage. Financial institutions did not identify any emerging ML/TF trends or typologies specifically related to COVID-19, but were aware of an increase in the number of internet fraud cases. The Monetary Authority of Macao, China reminded financial institutions to remain vigilant to detect suspicious transactions and the related ML/TF risk trends and typologies in other jurisdictions.

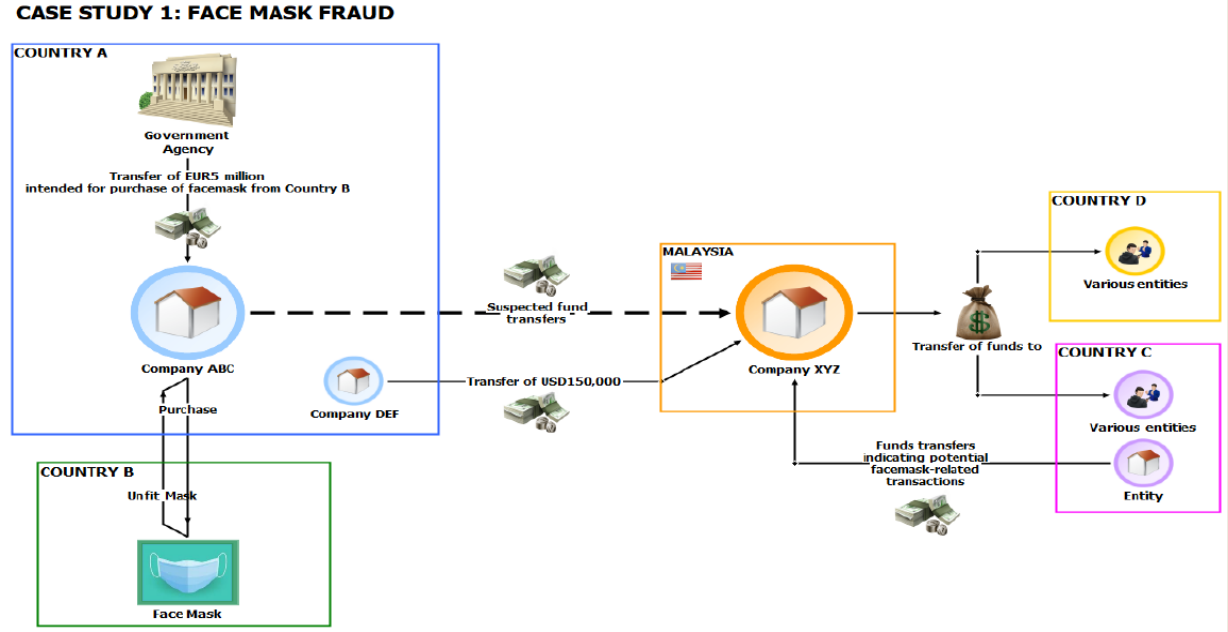
For the insurance sector, due to strict border-control during the COVID-19 pandemic, an insurance referral business was launched by insurers, of which non-resident customers were referred by brokers or third parties out of Macao, China. As the selling would be carried out by salesmen in Macao, China, the risk associated with such transactions would inevitably be increased. However, such ML risk was controllable as long as the required CDD/EDD procedures were well implemented. As for the potential risk on market conduct, a mechanism of close communication with and on-going monitoring of involved insurers had been established and a new declaration form has been adopted to ensure customers are well aware of potential associated risks. Further, insurers were requested to submit regular reporting of referral business status to the Monetary Authority of Macao, China for review of any irregularities.

Malaysia

Consistent with the change in the global threat landscape as a result of the COVID-19 pandemic, Malaysia also observed emerging crimes and/or an increase in fraud activities particularly linked to the counterfeiting of medical goods e.g. PPE and face masks, as well as cybercrime, illegal online gambling, the smuggling of cigarettes, illegal investment scheme's online promotional activities and drug trafficking. The growth in the amount of cybercrime is attributed to the increase in internet-related activities in the jurisdiction, with criminals increasingly leveraging on the uncertainties during the pandemic to exploit victims' financial insecurities.

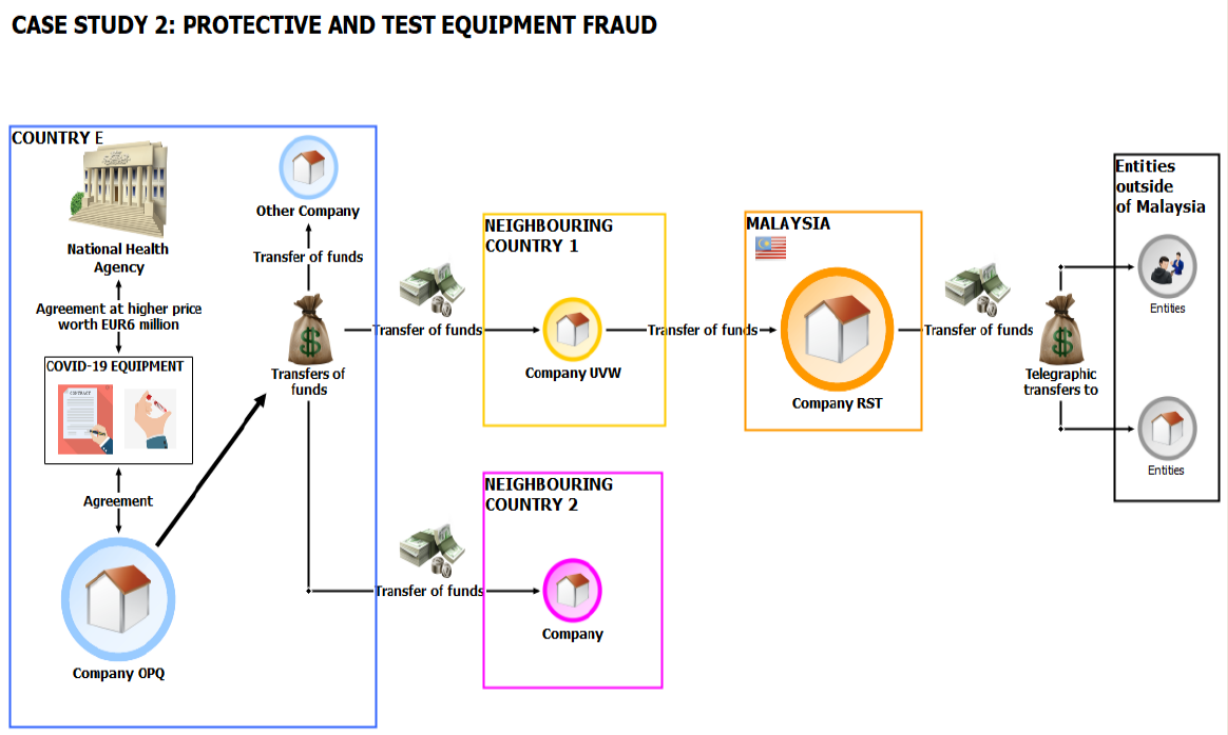
Case study 1: Counterfeiting of Medical Goods

FIU Malaysia received a request for information from a jurisdiction in Europe (Jurisdiction A) concerning a suspected facemask scam amid the COVID-19 pandemic. Approximately EUR 5 million (USD 6,088,976) was transferred by a government agency in Jurisdiction A to an entity in Jurisdiction A, namely Company ABC for the purchase of facemasks from Jurisdiction B. It was discovered that only a portion of the facemasks was delivered where all were found to be unfit for hospital use. Financial intelligence gathered by Jurisdiction A later revealed that Company ABC may have subsequently transferred a significant amount of money intended for facemask purchase to another entity, namely Company XYZ in Malaysia. Further transaction review of the company account also revealed an inward remittance received by Company XYZ from an entity located in Jurisdiction C with transaction remarks that may potentially indicate facemask related transactions. Within the same day, another large sum of monies amounting to approximately USD 150 000 was received from Company DEF, another entity in Jurisdiction A, believed to be engaging in sales of healthcare products including gloves, goggles and hearing protection. The funds received by company XYZ were observed to have been disbursed to various entities in Jurisdiction C and Jurisdiction D.



Case study 2: Counterfeiting of Medical Goods

FIU Malaysia received a request for information from a jurisdiction in Europe (Jurisdiction E) concerning suspected fraud with protective equipment for testing of COVID19. A national health agency in Jurisdiction E received a commercial proposal from Company OPQ in Jurisdiction E, to purchase protective equipment for testing of COVID-19 worth millions of euros. Company OPQ had defrauded the national health agency in Jurisdiction E into signing a contract for equipment of a higher price by providing false product information. Financial intelligence gathered by Jurisdiction E later revealed that Company OPQ may have subsequently transferred EUR 6.05 million (USD 7,367,814) intended for the purchase of protective equipment for testing of COVID-19 through networks of companies involving companies in Jurisdiction E and two neighbouring jurisdictions and eventually to another entity, namely Company RST in Malaysia. A transaction review of the company account revealed a pattern of rapid and high frequency of incoming and outgoing transactions involving multiple counterparties consisting of inward SWIFT and foreign wire transfers. Further review of the account revealed that Company RST received an inward remittance from Company UVW which was based in one of the neighbouring jurisdictions. Funds received were later transferred to entities outside Malaysia via wire transfers.



Mongolia

As per the observation and based on the statistics of STRs received by FIU-Mongolia from reporting entities in 2020, the number of suspicious transactions related to online gambling has escalated steadily. While the total number of STRs related to online gambling submitted by reporting entities was 42 in 2019, this number increased to 362 in 2020. It is presumed that this type of activity has been increasing on an unprecedented scale due to the impact of the pandemic and quarantine measures as some people are not being able to earn income as before and are willing to make money easily from home regardless of its illegal nature. "Organizing gambling" is considered as a crime under Article 20.17 of the Criminal Code of Mongolia.

New Zealand

Abuse of Covid-19 government stimulus measures

Between March and December 2020, the FIU received more than 450 SARs relating specifically to suspected abuse of government COVID-19 financial subsidies, detailing tens of millions of NZD worth of suspicious transactions. The predominant themes and trends within these SARs include:

- Individuals with either no known employment or who received unemployment benefits receiving wage subsidies credited to their accounts. A significant number of these individuals are adversely recorded in police systems for prior involvement in dishonesty offending, drugs, and in some cases organised crime.
- Businesses claiming wage subsidies for their employees but not passing the payments on to the employees, instead using the funds for personal or miscellaneous expenditure.

- Newly incorporated companies, with little to no identifiable trading profile, receiving wage subsidies.
- Individuals with no known employment or business links receiving multiple wage subsidies seemingly intended for multiple recipients, with these funds then withdrawn as cash, transferred to third party accounts, or sent offshore.
- Individuals with no known business associations receiving Inland Revenue (IR) 'small business loan' payments to their accounts; with the funds then withdrawn as cash, transferred to third party accounts or sent offshore.
- Individuals receiving IR small business loans when their only source of funds appears to be wages (i.e. they appear to be an employee rather than an employer and would therefore be ineligible for the loan)

Philippines

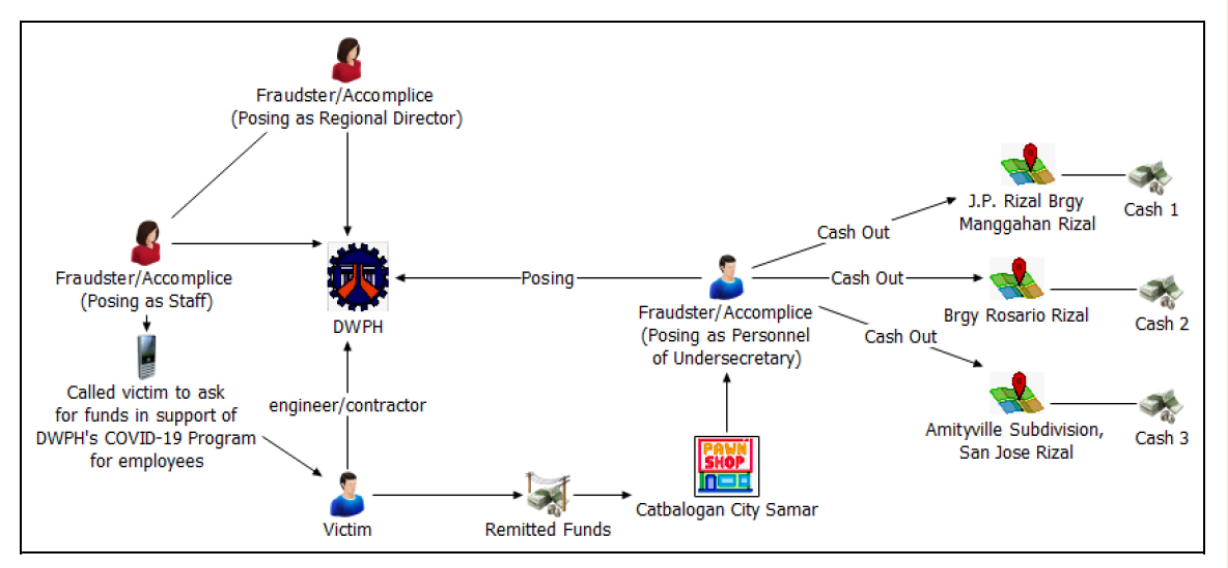
1. Fraudsters pretending to be affiliated with government units in soliciting Covid-19 donations from victims

Local Government Unit

A certain account, opened last 27 May 2020 under the name of an alleged fraudster, is purportedly being used to solicit donations or funds for COVID-19 using the name of the current governor of a certain province in Luzon. The solicited funds were deposited to the bank account of the fraudster. A review of the transactions shows that large cash deposits totalling PHP 622,000 (USD 13,004) were made into the account with subsequent same day withdrawals. It was also observed that frequent balance inquiries in one day were made by the alleged fraudster. Breakdown of material information is as follows: (1) review of documents gathered showed that the alleged fraudster is a TNVS[41] driver with gross monthly income between PHP 20,000 (USD 418) and PHP 50,000 (USD 1,045), which is the only source of funds as declared during the onboarding process. An open source search identified a social media post of another government agency regarding an advisory against a similarly named individual (alleged fraudster) who is using the name of the agency's Executive Director to solicit donations supposedly intended for Taal Volcano victims and that the donations were being deposited to another bank account of the fraudster.

[41] Transport Network Vehicle Service or TNVS is the term used to describe a Public Utility Vehicle accredited with a Transport Network Corporation (TNC), which is granted authority or franchise by the LTFRB to run a public transport service. A TNC is an organization that provides pre-arranged transportation services for compensation using an internet-based technology application or digital platform technology to connect passengers with drivers using their personal vehicle. Example of TNC are Grab Philippines and Angkas. Accessed from https://ltfrb.gov.ph/wp-content/uploads/2020/06/DO-2017-011-1.pdf on 8 October 2020.

Domestic Government Agency



Allegedly, the perpetrators are two females and one male, posing as employees of the Department of Public Works and Highways (DPWH), while the victim is an engineer/contractor in a regional office of DPWH. On 20 April 2020, the victim received a call from a female, who introduced herself as part of the staff of one of DPWH's regional offices. After telling the victim that the DWPH regional director (DRD) wanted to speak with the victim, the caller passed the phone to another woman, who pretended to be the DRD. The fake DRD informed the victim that the DPWH undersecretary was planning to give subsidies or relief packs to their employees relative to the COVID-19 pandemic. To augment this plan, the victim was told to raise funds, amounting to PHP 150,000 (USD 3,136), and to deposit the money directly into the undersecretary's bank account in Manila. Due to time constraints, the victim was advised to send the funds through an MSB instead of a bank. The fake DRD provided the name and the mobile number of the recipient of the funds—a male accomplice, who was introduced as the undersecretary's personnel. The victim sent PHP 150,000 (USD 3,136) through the MSB branch in Catbalogan City, Samar and texted the fake male personnel that the money was available for pickup. The victim then received text notifications that the remittances were claimed by the recipient in several branches in the province of Rizal.

2. Swindling/estafa (various product scams)

Confidential information indicates there has been overpricing and unauthorised selling of medical items, such as alcohol, medical masks, and thermal scanners. Moreover, other fake or bogus sellers took the crisis as an opportunity to scam victims into buying essential items. Most often, offenders will post items for sale in their social media account/s. After receiving the advanced payment from the buyer/victim, the seller/offender cuts off communication and blocks the buyer/victim in social media. The majority of these transactions involve local buyers and sellers. While violators were located in various cities and provinces in the jurisdiction, a substantial concentration of violators was observed in the National Capital Region (NCR).

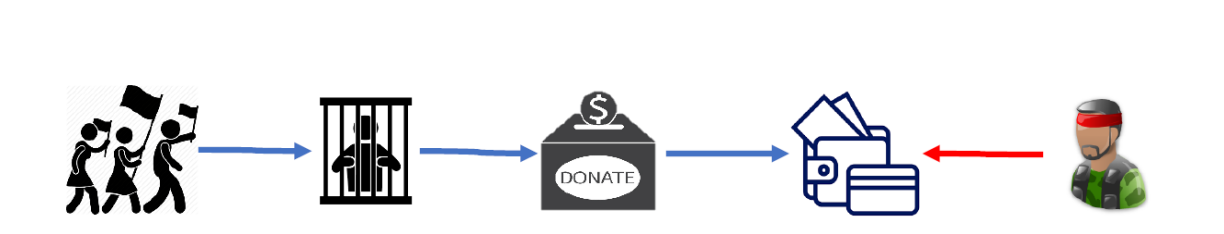
3. Donation scam (social media influencer)

Perpetrators set up a faux donation campaign in social media platforms to solicit funds from the public. During the enhanced community quarantine (ECQ), a purported social media influencer became popular for his social media challenge, where he posts his alleged donations

to COVID-19 relief efforts and encourages the upper class to donate. Based on information gathered from different sources, this person uses fictitious identities in order to deceive people and has been allegedly charged with various "swindling"/estafa cases over the years.

1. Possible terrorism financing activities linked to COVID-19

A group allegedly staged a protest rally demanding for the release of relief goods (food support) during the ECQ, as they claimed that they have not received any support from their local government unit (LGU). The said protest rally was purportedly organised and premeditated by two left-leaning organisations (LLOs) and other allied personalities to alienate the government from the marginalised community and agitate them to sow chaos and disorder in order to portray that the present government is incapable of governing during the COVID-19 crisis.



As the crowds became unruly, some protesters were arrested and charged with criminal offences, including violation of ECQ rules, and resistance and disobedience to lawful order. The accused were temporarily released from jail after posting bail bonds. Their legal counsel claimed that the money used to cover the cost of bail was sourced through online fundraising for legal assistance services. The said legal counsel claimed to have solicited money via social media and asked donors to deposit their donations in two bank accounts and through web-based donation/shopping platforms.

The LGU denied the allegation that there was no food support distributed to this group. Further, the arrested protesters appeared to be non-residents of the concerned LGU and were identified as members of the two LLOs associated with a communist group (CG) and its armed-wing group (AWG). The bank accounts used to solicit funds were also identified to be common depository bank accounts used by the allies and LLOs of CG and AWG for their fundraising activity.

1. Possible bulk cash smuggling using cruise ships

One notable attempted transaction was reported due to a deviation from the client's usual activity. The client requested the bank to pick up bulk foreign currency cash from a cruise ship docked at a Philippine port via a deposit pick up arrangement (DPA). The amount will then be deposited in the client's foreign currency account maintained in the local bank. This kind of transaction is usually done via telegraphic transfer from a bank abroad, but because of COVID-19 concerns, the client requested the funds to be picked up by the bank under the DPA. The amount involved, however, is above the average daily foreign currency volume of the client. Further, the client could not present any document as proof of source of funds.

2. Possible fraud - NPO to receive Covid-19 funds from suspected shell company

A non-profit organization (NPO) opened an account on 15 July 2020 for the purpose of accepting donations. The NPO stated that the account will also be used for their operating expenses, and funds relating to charitable works. As per the NPO's website, its advocacy is to

conduct Bible studies. Aside from account opening, the NPO also inquired about the documentary requirements if it is expecting to receive a donation of EUR 10 million (USD 12,143,443) from a company overseas. The NPO submitted a memorandum of agreement whereby it was stated that the company will be partnering with the NPO in a worldwide corporate social responsibility programme on the prevention of the COVID-19 pandemic and improvement of the quality of life and overall health situation in the Philippines, among others. While no actual credit has been made, it was noted that the documents provided are insufficient to support the large amount of funds expected to be received.

3. Continuous financial transactions despite business affected by lockdown

Fish Trading

A female client declared her fishing business as source of funds. Her account was noted to have 170 transactions from 15 November 2019 to 26 May 2020, ranging from PHP 50 (USD 1) to PHP 1,000,000 (USD 20,906) with a total value of PHP 41 million (USD 857,210). The client claimed that the transactions were related to the purchase of fingerlings as her business is fish trading. However, as noted by the bank, the transactions were mostly made during the ECQ, when all commercial flights and sea travels are prohibited. Moreover, the client was unable to present any document to support her claim.

Food court and restaurant

A corporate client is involved in the food court and restaurant business, and it was observed that between 21 January 2020 and 24 June 2020, there were 90 cash deposits into the client's account, ranging from PHP 183,103 (USD 3,828) to PHP 5,411,042 (USD 113,124), with a total value of PHP 140 million (USD 2,926,923). The bank requested for documents to support the substantial cash transactions. The client presented cash transmittal slips, but the branch confirmed that these were not enough to support the cash deposits. The bank also observed that the transactions were mostly made during the ECQ, when most restaurants are not allowed to operate.

4. Large transactions purportedly received from government units as payment for Covid-19 related products and services

Food pack

The subject is an owner of a construction and general merchandising business. On 30 July 2020, the subject's personal account received a fund transfer from a third-party account amounting to PHP 53 million (USD 1,106,822). According to the subject, this amount is inclusive of the PHP 21.8 million (USD 455,262), which the third-party claimed to be payment received from the Tagaytay City Government for food packs related to the 6th wave of COVID-19 ECQ assistance. It was further said that the entire PHP 53 million (USD 1,106,822) will be used to finance an alleged joint venture of the subject and the third-party for a real property acquisition.

Hotel Coordination on behalf of a Domestic Government Agency

The subject opened three bank accounts between August 2019 and June 2020 in different branches with declared source of funds as income from his real estate leasing business. Further, one of the accounts is a joint account with his wife. On 11 June 2020 and 10 July 2020, three cash deposits were made into the three different accounts of the subject with total amounts of PHP 1.2 million (USD 25,054) and PHP 1.05 million (USD 21,922), respectively. As per the bank's investigation, the subject said that they were coordinators for the Overseas Workers Welfare Administration (OWWA) and partner hotels, where Overseas Filipino Workers (OFW)

are being booked for quarantine. The subject further added that they also coordinate with the caterers and disinfection service providers. The subject disclosed that they have no signed contract with the OWWA and that the funds deposited were payment of the hotels, which would then be used to pay the service providers. Red flags included: (1) inability to provide acceptable supporting documents for the transactions with OWWA, (2) the nature of the transaction deviates from the declared source of funds during account opening, and (3) the amount of transactions appears to be structured.

5. Large cash deposit allegedly for COVID-19 donation for residents of a province in Mindanao

The subject opened a savings account in Iligan City on 25 November 2019 to serve as a settlement account for her insurance account. As per a declaration of the subject, she owns a jewelry shop, but her gross monthly income was not recorded in the system. The subject is the sibling of another bank client whose account was also opened on 25 November 2019 and who was also reported for suspicious transactions due to attempted significant cash deposits from unknown sources. On 7 May 2020, a certain blacklisted individual attempted to deposit PHP 4.5 million (USD 93,971) into the subject's account. The blacklisted individual is the same person who conducted the transactions in the account of the subject's sibling. The blacklisted individual claimed that the funds were donations accumulated due to the ECQ and the funds were intended for the people of Marawi City. The branch, however, denied the deposit for lack of supporting documents. Financial review of the subject's account from 25 November 2019 to 22 May 2020 showed 14 cash deposits ranging from PHP 2,000 (USD 41) to PHP 246,000 (USD 5,137), totalling PHP 1,473,000 (USD 30,756). According to the branch, these deposits are cash assistance from the subject's relatives intended for her living expenses. Funds withdrawn via ATM totaled PHP 471,000 (USD 9,833) and online payments and purchases via Express Payment System (EPS) totaled PHP 195,665 (USD 4,084). The subject's current account balance is PHP 406,782 (USD 8,493).

6. Unsubstantiated deposits based on declared business and source of funds

From ready-to-wear (RTW) business to lending

On 18 January 2019, the subject opened a savings account in Pampanga. The subject's declared source of funds was from a ready-to-wear (RTW) business. On 29 April 2020, a representative made a deposit of PHP 499,000 (USD 10,419) into the subject's account at Juan Luna Branch in Cebu City and another deposit on 14 May 2020 for PHP 500,000 (USD 10,440). The branch called the client to verify the source of funds, and based on the interview, the client disclosed that during the ECQ she engaged in a small lending business, which involved mostly cash and unsecured transactions since most of the malls are not open. She advised the branch that she will forward a copy of her Department of Trade and Industry (DTI) renewal certificate as a supporting document and other records to support the significant deposits. On 29 May 2020, her account was tagged as high risk due to the change in her nature of business and source of funds. Since then, the branch is unable to contact the client, and after several attempts, the client has yet to provide enough supporting documents to justify the source of funds.

From seafood trading to second-hand car trading

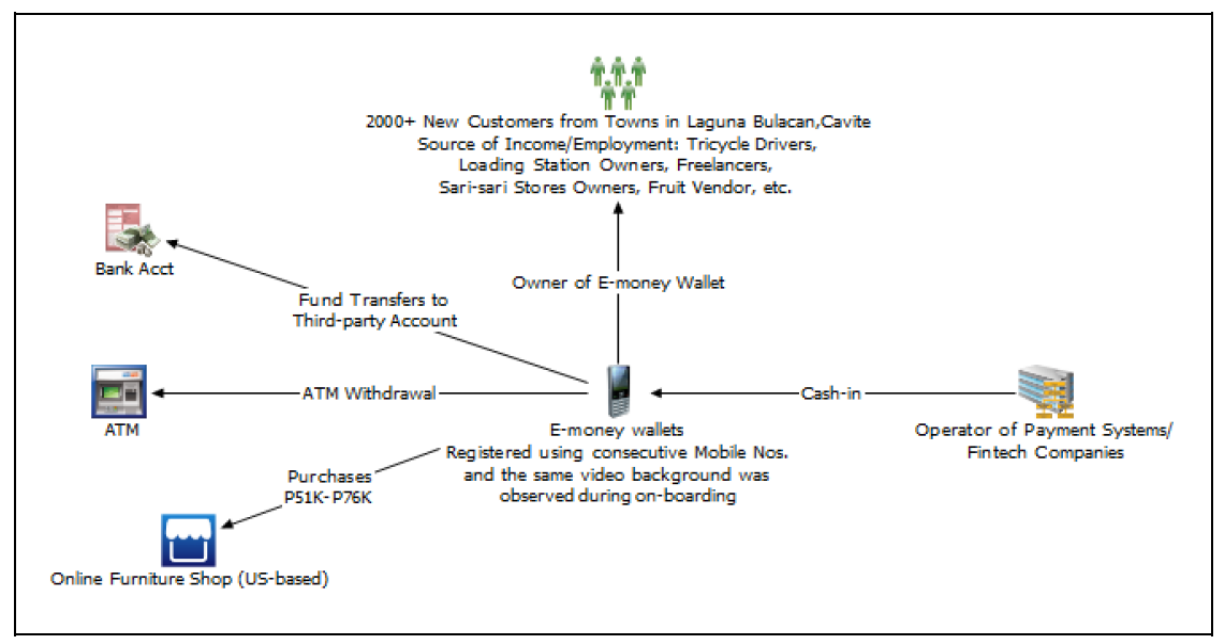
The subject opened a current account on 30 June 2020 with an initial deposit of PHP 25,000 (USD 521) and declared source of funds as income from a seafood trading business. However, due to the pandemic, the subject shifted to being a freelance agent of second-hand cars. As per the result of a transactional review covering 1 July to 13 August 2020, notable transactions on the account include: (1) 47 cash deposits ranging from PHP 500 (USD 10) to PHP 1.37 million

(USD 28,604), totalling PHP 9 million (USD 187,912); (2) 130 Instapay remittances, totalling PHP 2.47 million (USD 51,566); and (3) 11 local cheque deposits, totalling PHP 1.9 million (USD 39,641). As per the subject, the aforementioned deposits and remittances were payments from the selling of second-hand cars. Subsequently, the subject made cheque issuances totalling PHP 11 million (USD 229,572), payable to a certain company that accordingly owns the second-hand cars. The bank requested the subject to provide deed/s of sale or other proof of transaction, but the subject claimed that he was just a middleman/freelance agent of the aforementioned transactions and cannot provide any documents. As per open source, the aforementioned company, who allegedly owns the second-hand cars, was selling/leasing disinfection stations.

PEP engaging in second-hand car trading

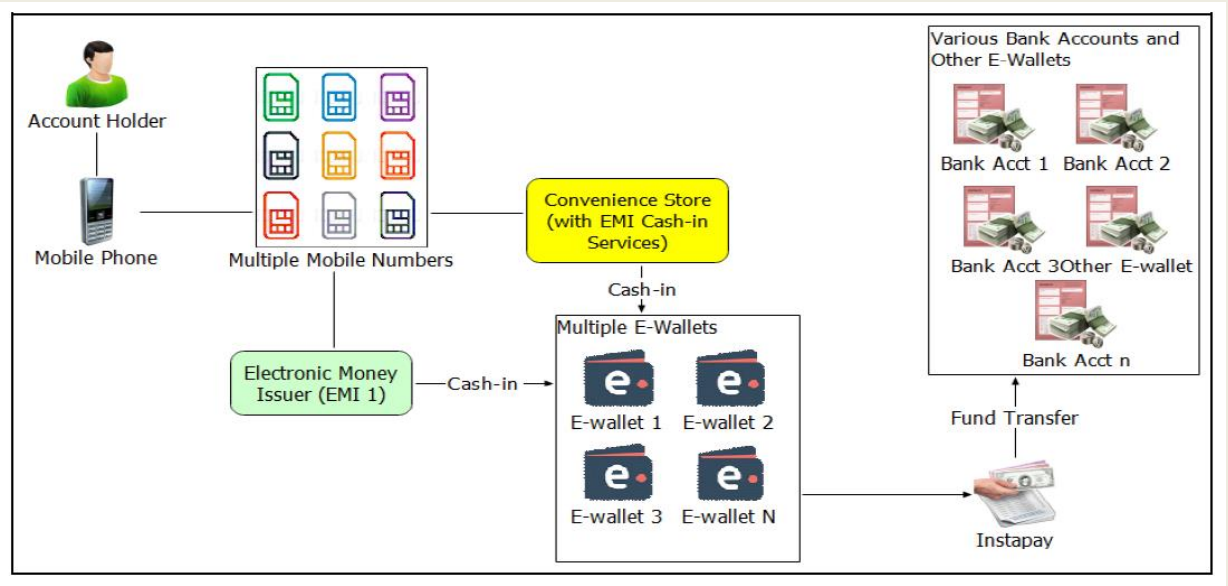
The subject opened a premium cheque account on 15 February 2010 with an initial deposit of PHP 400,000 (USD 8,345) and declared salary as municipal mayor of a northern province as source of funds. It has been noted that during the transactional review covering April to June 2020, the subject had total deposits of PHP 4.36 million (USD 90,957) in cash and PHP 3.4 million (USD 70,930) in cheques. Subsequently, these amounts were used to issue cheques payable to a certain third-party. As per the bank's telephone conversation with the subject, the deposits were from his buying and selling of used cars and construction business. However, the subject stated that both businesses have no business documents. Further, the subject allegedly referred to the third-party as a business partner. The subject presented copies of deeds of absolute sale for the two vehicles he recently purchased.

7. Abusing digital KYC/CDD to create suspected pass-through/money mule/smurfing accounts



More than 2,000 newly on-boarded e-money customers made multiple high value transfers, totalling PHP 180 million (USD 3,755,876), to third-party bank accounts. These transfers were transacted in a span of less than six months. Majority of the customers were on-boarded between July 2019 and February 2020. Most were identified to be residents of various provinces in Luzon. These account holders were profiled as tricycle drivers, loading station owners, freelancers, sari-sari store owners, fruit vendors, and private employees, who declared business

proceeds and salaries as source of funds. Suspicious indicators involving these accounts are as follows: (a) high value deposits from unidentified sources received in one day via certain financial technology (fintech) or payment system companies; (b) activities appear excessive considering the customers' profiles; (c) layering concerns as evidenced by the rapid movement of funds through subsequent cash withdrawals and transfers to a third party account; (d) majority of the customers' KYC videos have similar backgrounds; and (e) consecutive mobile numbers were registered in succession. Other notable activities seen are online purchases at an online furniture shop abroad.



In addition to the abovementioned case, between 1 March and 30 May 2020, an Electronic Money Issuer (EMI) reported 2,933 STRs related to suspected money mules or smurfers. These transactions have an estimated value of PHP 18.89 million (USD 393,956) transacted in less than four months. Individuals, usually using the same mobile phone, use different mobile numbers to create multiple e-wallet accounts. Once the e-wallet is created, individuals would cash-in via convenience stores on separate dates with only a few days apart. Another cash-in method is through another EMI, which is different from the EMI that issued the e-wallet. On the same day of credit to the e-wallets, the funds were subsequently transferred to several bank accounts and/or other e-wallets through Instapay. Transactions were also geographically concentrated in areas in Davao del Sur, Davao del Norte, Pangasinan, Ilocos Norte, Tarlac, Negros Occidental, Siquijor, Laguna, Zamboanga, Quezon City, and the City of Manila. Most account holders' declared occupation was student, while one was an employee of a convenience store.

Singapore

TBML from Purchase Order Scams

The Singapore Police Force have observed a re-emergence of purchase order scams, whereby scammers would pose as procurement officers from local universities or government agencies, and induce unsuspecting companies into delivering goods with false promises of payments at a later date. These illicit goods were then sent to foreign jurisdictions, which may then constitute as trade-based money laundering into these foreign jurisdictions.

The said companies would receive e-mails purportedly sent by a procurement officer from a local university or Government agency such as the Ministry of Health (MOH), asking for quotations for electronics, IT-related items or medical devices. The scammers would use e-mails bearing the template 'procurement@___ -sg.com' or 'purchasing@___,org' to convince the companies that they were genuine.

Once an agreement has been made, a purchase order (PO) would be sent to the company via email. Believing that they had received a genuine PO, the company would deliver the goods to the delivery address indicated in the PO. The delivery address indicated in the POs of such scams usually belonged to freight forwarding companies engaged by the scammers to ship the illicit goods overseas, including to the United Kingdom, Gambia, and Nigeria. No payments were eventually received.

For the second half of 2020, the Police have received at least thirteen reports of such scams, with total losses amounting to at least SGD 909,000 (approximately USD 684,970). Where timely information was provided to the Police, the Police managed to successfully intercept some goods before its intended shipment.

9.2 Displacement of ML or TF methodologies to established typologies (e.g. increase in reporting of the internet for ML/TF as use of cash decreases, impact of lockdowns and border closures on smuggling and trafficking, etc.).

Australia

The impact of hard international border closures on the counter terrorism space in Australian law enforcement has been significant, with POIs and potential POIs wishing to travel to conflict zones and neighbouring regions no longer possible. While this has the immediate effect of reducing the movement of physical currency which may have been used to finance terrorism, Australian authorities remain alert to wire transfers and remittances to jurisdictions of concern.

9.3 Any research or reports conducted on the impact of pandemics, natural disasters or economic crises on ML/TF trends and typologies.

Hong Kong, China

The Joint Financial Intelligence Unit of Hong Kong, China conducted in-depth thematic analyses and holistic reviews on selected STRs, FIU to FIU exchanged information and other information from various sources on prevalent crime trends with reference to the overall ML/TF threat and vulnerability in Hong Kong, China including crimes arose from the ML/TF trends linked to COVID-19.

Besides, the Fraud & Money Laundering Intelligence Taskforce (FMLIT) published alerts on COVID-19-related fraud and deception cases in 2020, which were shared with local institutions and overseas agencies. Anti-scam messages and publicity campaigns had also been published on various social media platforms to raise public awareness.

Malaysia

In 2020, Central Bank of Malaysia produced a series of advisories to selected industries on COVID-19 related crimes, ML/TF trends and red flags to assist in transaction monitoring and detection of suspicious transactions during the pandemic.

This includes the COVID-19 related scams published by the Securities Commission Malaysia in the form of videos/infographics to the public as well as the alerts issued by the Labuan Financial Services Authority to its reporting institutions on areas such as AML/CFT monitoring of emerging risks & threats arising from COVID-19, advice on CDD measures and reminder on STR lodgement obligations.

10. 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
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