APG Yearly Typologies Report

Asia/Pacific Group on Money Laundering

2022

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

July 2022

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

The Asia Pacific Group on Money Laundering (APG) is the FATF[1]-style regional body for the Asia/Pacific. One of the mandates of the APG is to publish regional money laundering (ML) and terrorism financing (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.

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.

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 due to ongoing investigative/judicial processes.

This report includes a brief chapter on the illicit financial flows from illegal, unreported and unregulated fishing (IUU) which seeks to draw attention to the urgent need for a response that targets the proceeds of IUU through associated financial and money laundering investigations.

The APG Operations Committee has oversight of the typologies research programme and is Co-Chaired by Samoa and New Zealand (2020-2022).

[1] Financial Action Taskforce

1. ILLICIT FINANCIAL FLOWS FROM ILLEGAL, UNREPORTED AND UNREGULATED FISHING

Illegal, unreported and unregulated fishing (IUU) is estimated to account for more than 15% of the world's total capture fisheries production, and is valued at USD 10–23.5 billion per year.[2] This scale makes it a contender for one of the most lucrative natural resource crimes, following timber and mining.[3] The combination of the unavoidable impact of IUU on global food security[4] and its connections with broader transnational criminal networks and activities[5] results in a complex and expansive threat for money laundering.[6]

While IUU constitutes a significant problem for jurisdictions around the world, the Asia/Pacific region is particularly affected due to the inclusion of jurisdictions with significant interests in the fishing industry and, on the other hand, small island jurisdictions with dependence on maintaining the sanctity of their exclusive economic zones.

On 7 December 2021, Financial Action Task Force (FATF) President Dr Pleyer called for a global push to take the illicit profits out of environmental crimes at a high-level FATF conference involving public, private, not-for-profit sectors and academia. In addition to the effects of the scale of illicit funds from IUU on the international financial system, IUU poses a serious threat to the environment and marine ecosystems in the context of rampant overfishing and depleted fish stocks.[7] The FATF Standards require jurisdictions to criminalise money laundering for a range of environmental crimes. Recently, the FATF added several examples of environmental crimes to the FATF Glossary to clarify for jurisdictions the types of offences that fall within this category.[8]

---

[2] Rivaz, C, Haenlein. C, Reid. A, Nouwens. V, Turning the Tide? Learning from Responses to Large-Scale Illegal, Unreported and Unregulated Fishing in Five Countries, RUSI Whitehall Report 3-19, November 2019, https://static.rusi.org/201911_whr_3-19_turning_the_tide_de_rivaz_web.pdf, p. 1.

[3] C4ADS, Strings Attached – Exploring the onshore networks behind illegal, unreported and unregulated fishing, 2019, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d7022301845f300016ee532/1567629912450/Strings+Attached.pdf , p.4.

[4] Phelps Bondaroff, Teale N., Reitano, Tuesday, van der Werf, Wietse, The Illegal Fishing and Organized Crime Nexus: Illegal Fishing as Transnational Organized Crime, The Global Initiative Against Transnational Organized Crime and The Black Fish, 2015, https://globalinitiative.net/wp-content/uploads/2015/04/the-illegal-fishing-and-organised-crime-nexus-1.pdf, p. 15.

[5] Burr. E, Concerning our coasts – money laundering and trafficking in global fishing, AMLRS Arachnys, 22 April 2021, https://www.arachnys.com/concerning-our-coasts-money-laundering-and-trafficking-in-global-fishing/

[6] United Nations Office on Drugs and Crime, "Rotten Fish. A guide on addressing corruption in the fisheries sector", 2019, https://www.unodc.org/documents/Rotten_Fish.pdf; United Nations Office on Drugs and Crime, "Fisheries Crime: transnational organized criminal activities in the context of the fisheries sector" https://www.unodc.org/documents/aboutunodc/Campaigns/Fisheries/focus_sheet_PRINT.pdf; United Nations Office on Drugs and Crime, "UNODC Approach to Crimes in the Fisheries Sector", https://www.unodc.org/res/piracy/index_html/UNODC_Approach_to_Crimes_in_the_Fisheries_Sector.pdf

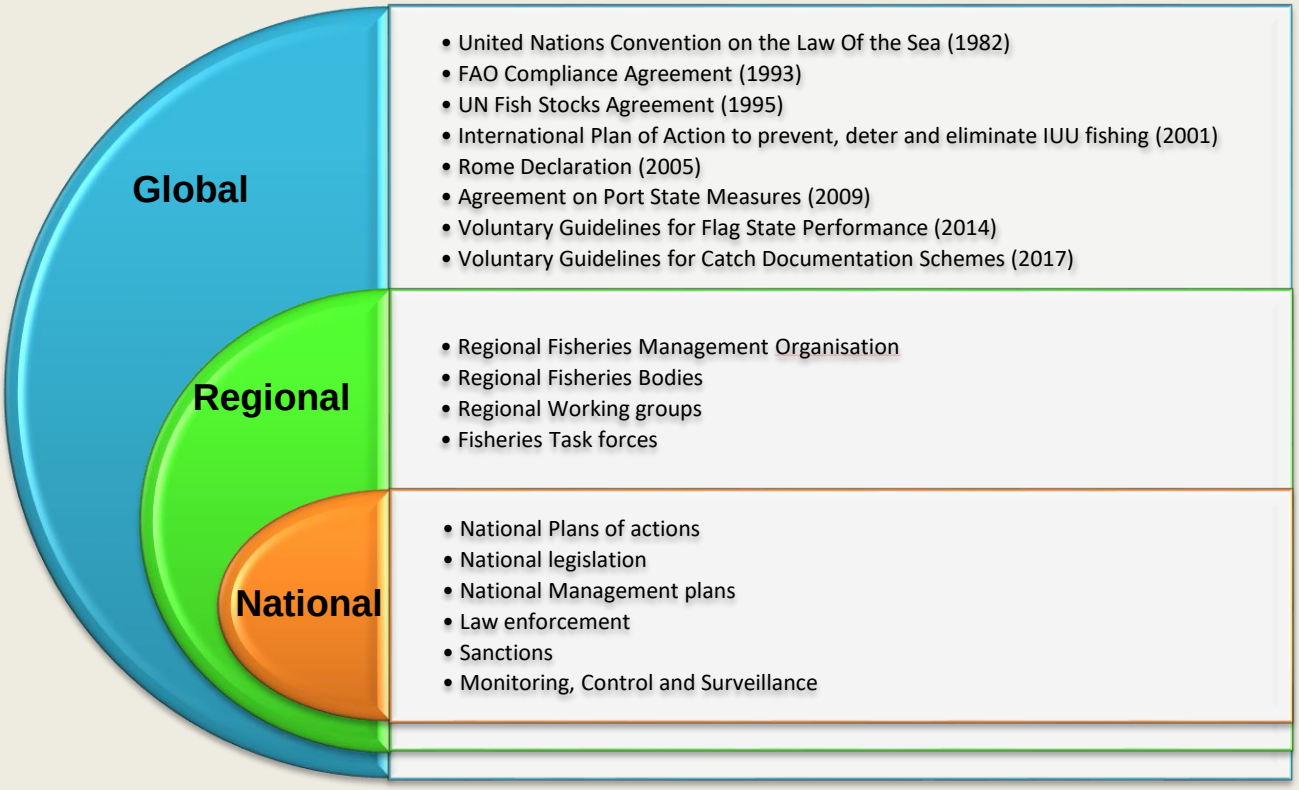
[7] Phelps Bondaroff, Teale N., Reitano, Tuesday, van der Werf, Wietse, The Illegal Fishing and Organized Crime Nexus: Illegal Fishing as Transnational Organized Crime, The Global Initiative Against Transnational Organized Crime and The Black Fish, 2015, https://globalinitiative.net/wp-content/uploads/2015/04/the-illegal-fishing-and-organised-crime-nexus-1.pdf, p. 17.

[8] Financial Action Task Force (FATF), International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, March 2022, FATF, Paris, France, https://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF%20Recommendations%202012.pdf, p. 121: "*environmental crime (for example, criminal harvesting, extraction or trafficking of protected species of wild fauna and flora, precious metals and stones, other natural resources, or waste)*."

This chapter explores the context of criminal activity related to IUU. In doing so, the APG seeks to draw attention to the urgent need for a response that targets the proceeds of IUU through associated financial and money laundering investigations as well as asset recovery and preventive measures in the financial sector.

1.1 Legality of fishing

The international framework for IUU originates from the United Nations Convention on the Law of the Sea (UNCLOS), established in 1982 to address fisheries governance at the global, regional and national level. Under this overarching framework, there continues to be developments in provisions, measures and treaties designed specifically to address IUU. These instruments are comprised of both binding and non-binding agreements. In conjunction with this framework enforcement conventions exist to address crimes associated to the fishers sector, strengthening international governance of IUU.[9]



This international framework is only effective at eliminating IUU when States fulfil and fully commit to their responsibilities at all levels and in cooperation with one another.[10]

According to the UN based frameworks, illegal fishing constitutes activities conducted by national or foreign vessels in waters under the jurisdiction of a State, without the permission of that State, or in contravention of its laws and regulations.[11] This includes fishing without a

[9] INTERPOL, International Law Enforcement Cooperation in the Fisheries Sector: A Guide for Law Enforcement Practitioners, 2018, https://www.interpol.int/en/Resources/Documents#Publications, p.28.
[10] Food and Agriculture Organization of the United Nations, IUU fishing - International framework, 2022, https://www.fao.org/iuu-fishing/international-framework/en/.
[11] Food and Agriculture Organization of the United Nations, International Plan of Action to Prevent, Deter, and Eliminate Illegal, Unreported and Unregulated Fishing, 2001, https://www.fao.org/3/y1224e/y1224e.pdf , p. 2.

licence, fishing in a closed area or marine protected area, fishing with prohibited gear, fishing over a quota or the fishing of prohibited species.[12]

The International Plan of Action to prevent, deter and eliminate IUU fishing (IPOA-IUU) also defines unreported fishing as fishing activities, which have not been reported, or have been misreported, to the relevant national authority, in contravention of national laws and regulations. Unregulated fishing is defined as fishing activities in the area of application of a relevant regional fisheries management organisation (RFMO) that are conducted by vessels without nationality, or by those flying the flag of a State not party to that organisation, or by a fishing entity, in a manner that is not consistent with or contravenes the conservation and management measures of that organisation.[13]

1.2 IUU and transnational organised crime

IUU operations are often conducted on an industrial scale by transnational organised criminal actors who are highly coordinated in their efforts to violate fishing laws.[14] IUU is frequently associated with other serious transnational crimes such as wildlife crime, human and drug trafficking, slavery and labour exploitation, arms trafficking, tax evasion, corruption, document fraud and customs fraud. IUU is also associated with trade-based ML.[15]

For example, two relatively recent cases in Papua New Guinean waters connect the drug trafficking trade with IUU operations. In one case, an unnamed vessel, suspected to be used in illegal fishing activities was linked to a major cocaine transhipment transported by another commercial fishing vessel in Australian waters.[16] In another case, a fishing vessel was associated with the illegal trafficking of cocaine valued at around AUD 50 million.[17]

International research highlights vulnerabilities throughout the supply chain, from the negotiation of access agreements to the bribery of fisheries and customs agents to evade enforcement action, that contribute to corruption and fraud.

[12] Phelps Bondaroff, Teale N., Reitano, Tuesday, van der Werf, Wietse, The Illegal Fishing and Organized Crime Nexus: Illegal Fishing as Transnational Organized Crime, The Global Initiative Against Transnational Organized Crime and The Black Fish, 2015, https://globalinitiative.net/wp-content/uploads/2015/04/the-illegal-fishing-and-organised-crime-nexus-1.pdf, p. 12.
[13] Food and Agriculture Organization of the United Nations, International Plan of Action to Prevent, Deter, and Eliminate Illegal, Unreported and Unregulated Fishing, 2001, https://www.fao.org/3/y1224e/y1224e.pdf , p. 2.
[14] Rivaz, C, Haenlein. C, Reid. A, Nouwens. V, Turning the Tide? Learning from Responses to Large-Scale Illegal, Unreported and Unregulated Fishing in Five Countries, RUSI Whitehall Report 3-19, November 2019, https://static.rusi.org/201911_whr_3-19_turning_the_tide_de_rivaz_web.pdf, p. 1.
[15] Burr. E, Concerning our coasts – money laundering and trafficking in global fishing, AMLRS Arachnys, 22 April 2021, https://www.arachnys.com/concerning-our-coasts-money-laundering-and-trafficking-in-global-fishing/
[16] Asia Pacific Report, PNG arrested 'black ship; believed to be linked to K1.47bn cocain haul, 28 August 2020, https://asiapacificreport.nz/2020/08/28/png-arrested-black-ship-believed-to-be-linked-to-k1-47bn-cocaine-haul/
[17] Lyons. K, The Guardian, Bust in Budi Budi: the day a fisherman hauled in $50m worth of cocainm 25 June 2019, https://www.theguardian.com/world/2019/jun/24/bust-in-budi-budi-the-day-a-fisherman-hauled-in-50m-worth-of-cocaine.

Case Study UNODC – Corruption and IUU[18]

Mr. SS operated an illegal enterprise with the purpose of poaching and selling abalone (*Haliotis midae*) from Jurisdiction X[19] to an APG member. A group of abalone divers worked under him supplying him with illegally harvested abalone. The accused allegedly bribed officials from Jurisdiction X Department of Agriculture, Forestry and Fisheries to prevent them from confiscating abalone and to buy back abalone already seized by the authorities. The officials are facing corruption charges in a separate trial.

In March 2018, the police searched the accused's house and found cash that the accused confessed to be proceeds of his illegal activities. In February 2021, Mr. SS pleaded guilty to 41 counts involving running an illegal enterprise, corruption, ML and possessing and transporting illegally harvested abalone. Factors aggravating the sentence included the seriousness of corrupting government officials, engagement in the illegal abalone trade on a commercial scale and financial greed.

The accused had been involved in similar crimes in the past and previously received prison sentences for his involvement with another illegal enterprise focusing on abalone poaching. In 2019, he was found responsible for operating an illegal abalone business in a different area and was handed a 14-year sentence. In the current trial, Mr. SS was sentenced to an effective 18-year sentence. Of those 18 years, 12 were determined to run concurrently to the previous sentence of 14 years.

The available data and observations suggest that the actors behind large-scale IUU operations consist of a limited number of players globally. This makes the identification of the beneficial owners connected to proceeds critical. For example, analysis from Oceana's Transparent Oceans Initiative in 2022 revealed that out of a database of 6,053 illegal fishing offences at least one-third of all recorded offences were associated with just 20 companies and 450 industrial fishing vessels.[20]

Case Study Fiji – Drug Trafficking and IUU

The Fiji Ministry of Fisheries and Fiji FIU were involved in an investigation into the association of legal persons and IUU. Person N, a foreign national and frequent traveller to Fiji was found in possession of 660kg of preserved, prohibited fish products at his residence. The prohibited fish products were estimated to have been purchased for FJD 33,050 (approx. USD 15,100).

The FIU established Person N travelled to Fiji on a visitors permit and did not have any financial transactions or bank accounts in Fiji. He was listed as a director of Company X and acquired and disposed of three vehicles in 18 months. There were no financial transactions associated with these purchases and consequent disposals. Two of the vehicles were transferred to two individuals from the same jurisdiction as Person N. Given Person N's frequent visits to Fiji, the FIU assessed he may be a mule used by a

[18] UNODC Sherloc, Case Law Database: Regina v Do Van Va, 14 July 2017, https://sherloc.unodc.org/cld//case-law-doc/wildlifecrimetype/zaf/2021/s_v_solomon_sauls.html?lng=en&tmpl=sherloc

[19] Not an APG member jurisdiction

[20] Dyhia Belhabib, Philippe Le Billon, 'Fish crime in the global oceans', March 2022, https://www.science.org/doi/10.1126/sciadv.abj1927

local network to carry the prohibited fish products out of the jurisdiction. He may also be carrying undeclared currency when he travels across the border.

Person N paid a FJD 20,000 (approx. USD 9,137) fine for possession of prohibited fish products under the Ministry of Fisheries Act.

Case Study Pakistan – Misuse of legal persons

During the period of 2019-2021, Pakistan's FIU (FMU) received four (4) STRs from ABC bank on four (4) individuals, Mr. SK, Mr. MH, Mr. HS (son of MH) and Mr. KZ. All individuals are associated with fishing and oil businesses, with Mr. SK and Mr. MH owning fishing boats and conducting business in the same locality. The four (4) STRs were reported to Pakistan FMU due to high turnover of funds and transactions to unrelated accounts belonging to teachers, oil lubricant distributors, scrap dealers, medical suppliers and wholesalers/ retailers for purchases associated with general items such as dry fruit, sugar and wheat.

The high turnover of funds was identified in the sole proprietorship accounts which did not match the profile of the account owner. Majority of funds were deposited by cheques and withdrawn daily in cash. The transactions to unrelated accounts recorded Mr. HS, declared as a seafood exporter, receiving large trade transactions into his sole proprietorship accounts. Mr. HS also received export payments from unrelated parties whose businesses involved trade in clothing, wholesale products, plastics, chemicals, fibre, wooden items, arts and crafts, resin and ceramics. The FMU also identified travel records associated with Mr. MH, Mr. HS and Mr. KZ.

Pakistan FMU's financial investigations and analysis on the suspicious activity associated with the four (4) individuals involved in the fishing and oil business was referred to an LEA for further investigation. The FMU's financial analysis indicates possible illegal activity is occurring between the four (4) individuals and their accounts such as smuggling, IUU fishing and hawala. The investigation by the LEA is ongoing.

The FATF and other AML/CFT bodies have published extensively on the importance of a ML perspective when dealing with predicate offences, like the global drug trade, where there is a strong transnational element and involvement of sophisticated transnational crime networks. However, the question of how proceeds of IUU are laundered is an area that remains under-researched.[21] A 2017 report from the Royal United Services Institute (RUSI), "*Below the surface – How illegal, unreported and unregulated fishing threatens our security*," indicates that the reason so few studies exist on offences committed in laundering the proceeds of IUU is due to the failure of investigators to adopt financial investigation tools to pursue the operators and owners of IUU vessels.[22] More effective implementation of the FATF standards to support targeted and coordinated financial investigations may contribute significantly to efforts to address this multi-layered and large-scale criminal activity.

For example, the Sri Lankan FIU has observed a large number of STRs in relation to IUU. According to the STR numbers, there is a slight increase in human smuggling related unlawful activities connected to IUU fishing activities (refer Table 1). Sri Lanka noted an observed

[21] Haenlein, C, Below the surface – How illegal, unreported and unregulated fishing threatens our security, RUSI occasional Paper, July 2017, https://static.rusi.org/201707_rusi_below_the_surface_haenlein.pdf, p. 22.
[22] Ibid, p. 23.

increase in drug smuggling related IUU activities. This is reinforced by open source media reporting on LEA drug raids on coastal fishing craft, with most of the fishing craft having a foreign origin.

Table 1: FIU Sri Lanka STRs involving unlawful activities in conjunction with IUU (2016-2021)

Activity	2016	2017	2018	2019	2020	2021*	Total
Drug trafficking in relation to IUU fishing	0	0	1	0	4	4	**8**
Human smuggling	8	2	4	1	4	10	**29**
Illegal fishing / unauthorized fishery related activities	0	0	0	0	0	0	0
Slavery and labour exploitation	0	0	0	0	0	0	0
Wildlife crime	0	0	0	0	0	0	0
Any other activity / naval related	0	0	0	0	0	0	0
Total	**8**	**2**	**5**	**1**	**8**	**14**	**37**

*Provisional

Sri Lanka reported that since the onset of the Covid-19 global pandemic, there has been an observed increase in IUU activity. In the month of July 2020, the Sri Lanka Navy reported 14 cases of IUU fishing that were all associated with illegal fishing using prohibited gear.

1.3 Law enforcement responses to addressing IUU fishing

A 2017 APG and UNODC research report, "*Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime*," identified that there are insufficient financial investigations conducted into wildlife crime and few attempts by jurisdictions to "follow the money" trail.[23] It is likely a lack of parallel financial investigations into the proceeds of IUU is attributable to the limited amount of information available on the nature and dynamics of illicit financial flows generated from IUU. AML legislation in many jurisdictions does not include IUU as a predicate offence for ML.[24] This likely contributes to a lack of financial investigations into the illicit financial flows generated from IUU.

Case studies, such as the one below, with a successful prosecution of the illegal fishing activities, but without proceeds being recovered, are commonplace. The challenges identified in this case study also apply across the region.

Case Study UNODC & Solomon Islands – IUU prosecution with no investigations on proceeds of crime

In 2017, three (3) "blue boats" from Jurisdiction A were apprehended by the Maritime Police of Solomon Islands. During the operation the defendants tried to escape with their fishing vessel, which resulted in the police using tear gas, rubber bullets and ramming the vessel to stop them from escaping. The "blue boats" had illegally entered

[23] APG and UNODC, Enhancing the Detection, Investigation and Disruption of Illicit Financial Flows from Wildlife Crime, 2017, http://www.apgml.org/methods-and-trends/documents/default.aspx , p. 21.
[24] Haenlein, C, Below the surface – How illegal, unreported and unregulated fishing threatens our security, RUSI occasional Paper, July 2017, https://static.rusi.org/201707_rusi_below_the_surface_haenlein.pdf, p. 23.

the exclusive economic zone of the Solomon Islands to illegally harvest marine resources, such as sea cucumber and giant clams, using prohibited fishing gear such as diving compressor hoses.

The court noted that financial prospects motivated the defendants to engage in illegal fishing in distant waters. The judge further remarked that this highlights the overfishing in their own national waters and emphasized the seriousness of harvesting vulnerable species. Other reports of similar activity by Jurisdiction A "blue boats" has been recorded in the region. Hence, the court also emphasised the need for a deterrent penalty as the Solomon Islands seem to be viewed as a soft target by those illegal fishing operators.

The defendants claimed they were the victims of human trafficking for the purpose of forced labour on the fishing vessels. The court determined there was not sufficient evidence to support this claim and the defendants pleaded guilty to four counts pertaining to violations of the Fisheries Management Act of 2015 and the Fisheries (Amendment) Regulations of 2009. On 14 July 2017, the defendants were sentenced to two years imprisonment and fines amounting to SBD 11,050,000 (approx. USD 1.4 million). The fines were payable within thirty days and another default period of two years imprisonment would run consecutively to the existing custodial sentence if payments would not occur. The three (3) vessels comprising the "Blue Boats" were forfeited to the Solomon Islands Government and have since been destroyed.

Authorities from the Solomon Islands noted that there are challenges in pursuing proceeds of crime investigations and filing for ML offences:

- Lack of experienced investigators to carry out investigations on Proceeds of Crime and ML offences;
- Limitations of technical knowledge to pursue ML investigations and prosecutions associated with environmental crimes in comparison to immigration, fisheries and penal code offences;
- Familiarity with relevant anti-money laundering legislation is low for judges and contributes to low numbers of parallel ML investigations associated fisheries crimes;
- High costs associated with detention of persons of interest while allowing ML and proceeds of crime investigations to take place.

RUSI's 2019 report, "*Turning the Tide? Learning from Responses to Large-Scale Illegal, Unreported and Unregulated Fishing in Five Countries,"* emphasised "dedicated research into the nature and dynamics of the illicit financial flows generated [from IUU], and the means used to launder them, is thus urgently needed."[25] Ultimately, jurisdictions need to prioritise research into how the illicit proceeds from IUU are integrated into the legitimate economy in order to effectively combat the ML threat of IUU.

In addition to increasing the application of financial investigative techniques, the complexity of contemporary IUU criminal actors means collaboration across government agencies is critical. Some jurisdictions have moved to better support cooperation and coordination in this

[25] Rivaz, C, Haenlein. C, Reid. A, Nouwens. V, Turning the Tide? Learning from Responses to Large-Scale Illegal, Unreported and Unregulated Fishing in Five Countries, RUSI Whitehall Report 3-19, November 2019, https://static.rusi.org/201911_whr_3-19_turning_the_tide_de_rivaz_web.pdf, p. 23.

regard. Thailand has prioritised a multi-agency approach to IUU in order to address the overlapping crime types involved.

Case study Thailand – collaboration across agencies

In February 2022, the Royal Thai Police established a special taskforce, 'IUU Hunter', responsible for investigating 22 coastal provinces' fishing industry business operations. IUU Hunter operations would seek to identify illegal business operations and labour exploitation or human trafficking syndicates. The taskforce collaborates with other relevant maritime authorities, such as the Department of Fisheries, Marine Department and Department of Labour Protection and Welfare to investigate cases related to working conditions on fishing boats.

Ban Don Bay in Surat Thani province is on Thailand's eastern sea border, with wide lanes of beaches, and is strategically important to Thailand's national security and marine ecosystem. As a result of Ban Don Bay's fertile condition and high return from culturing scallops, local fishermen and scallop farm operators illegally occupy the area and establish shell houses and buildings, locally known as Khanam, for their business operations. IUU Hunter operations identified 800 Khanams across an area of approximately 200, 000 rai (32,000 ha). AMLO in collaboration with the Royal Thai Police, Thai Maritime Enforcement Command Center, the Department of Fisheries and Maritime Department froze and seized proceeds of crime from seven (7) entities conducting illegal business operations from Khanams. The total amount of proceeds of crime was worth more than one million baht (approx. USD 29,011). All seven (7) entities had their Khanams demolished.

Existing research suggests the proceeds of crime from IUU may be invested in new fishing gear, fish processing facilities or vessels.[26] Illicit proceeds may also be laundered during the sale of fish at port or by paying crew members in cash.[27] It is thought that some criminal organisations involved in IUU protect themselves by laundering their profits through complex corporate ownership structures involving multiple front companies in different jurisdictions.[28] The use of shell or front companies, often in secrecy jurisdictions or tax havens, enables criminal organisations to hide the beneficial owners of vessels from authorities.[29] The use of complex financial transactions involving shell and front companies in secrecy jurisdictions allows criminal organisations to more effectively launder the proceeds from IUU and makes it more difficult for authorities to follow the money.[30] Further research is needed on the techniques used by criminal organisations involved in IUU to launder their profits, including through the use of shell and front companies, tax havens and secrecy jurisdictions.

[26] INTERPOL, Guide to International law enforcement cooperation in the fisheries sector, 2018, https://www.interpol.int/en/Crimes/Environmental-crime/Fisheries-crime, p. 10.
[27] Ibid.
[28] Phelps Bondaroff, Teale N., Reitano, Tuesday, van der Werf, Wietse, The Illegal Fishing and Organized Crime Nexus: Illegal Fishing as Transnational Organized Crime, The Global Initiative Against Transnational Organized Crime and The Black Fish, 2015, https://globalinitiative.net/wp-content/uploads/2015/04/the-illegal-fishing-and-organised-crime-nexus-1.pdf, p.46.
[29] C4ADS, Strings Attached – Exploring the onshore networks behind illegal, unreported and unregulated fishing, 2019, https://static1.squarespace.com/static/566ef8b4d8af107232d5358a/t/5d7022301845f300016ee532/1567629912450/Strings+Attached.pdf, pp.25-26.
[30] Haenlein, C, Below the surface – How illegal, unreported and unregulated fishing threatens our security, RUSI occasional Paper, July 2017, https://static.rusi.org/201707_rusi_below_the_surface_haenlein.pdf, p. 24.

Financial investigations and asset recovery tools should enable the discovery of evidence that will ultimately ensure the confiscation of both the proceeds and instruments used to commit IUU. Parallel financial investigations can identify criminal associates and corporate entities involved in the commission of IUU. These investigations can also help to uncover links with other crimes such as corruption and fraud.[31] Moreover, criminal organisations involved in IUU may launder illicit proceeds from other crimes or use their fishing activities as a front for smuggling drugs or people.[32] Ultimately, increased efforts to trace the illicit financial flows generated by IUU will ensure prosecutions occur and penalties are applied to act as a deterrent.

New Zealand
Tracing Illicit Financial Flows from IUU: A public-private partnership

One of the main five financial institutions in New Zealand produced its own thematic review of the IUU fishing risk. This was due to the financial institution baselining international trends on predicate crimes (including IUU fishing) and assessing where the monitoring and detection gaps lay for the institution.

The material in the document was used to brief all members of New Zealand's Financial Crime Prevention Network (FCPN) on IUU fishing in February 2022. The FCPN is a network with the membership of five private sector financial institutions and two government agencies (New Zealand Police – Financial Intelligence Unit and the New Zealand Customs Service). The purpose of the FCPN is to provide a platform for all members to openly discuss matters in a secure environment in a collaborative effort to tackle illicit financial flows derived from any nature of illicit activity.

Corporations operating in the fishing industry often face obligations to ensure the legality of supply chains, either through legislation or through voluntary codes. The driver for private sector concern appears to be that the scale of IUU seriously undermines the legitimate fishing industry while constituting a threat to national and regional security. The exercise of abiding by supply chain obligations can involve similar steps to those undertaken by LEAs such as tracing the proceeds associated with IUU, and mapping the actors involved. As such, these parallels are useful to consider.

1.4 Supply Chain Obligations on the Private Sector

Private fishing companies are subject to obligations related to supply chain transparency under both national government regulations as well as private sector transparency initiatives in which they voluntarily participate.[33] Examples of governments who have introduced transparency initiatives include Thailand and the United States.

[31] Rivaz, C, Haenlein. C, Reid. A, Nouwens. V, Turning the Tide? Learning from Responses to Large-Scale Illegal, Unreported and Unregulated Fishing in Five Countries, RUSI Whitehall Report 3-19, November 2019, https://static.rusi.org/201911_whr_3-19_turning_the_tide_de_rivaz_web.pdf, p. 58.
[32] Phelps Bondaroff, Teale N., Reitano, Tuesday, van der Werf, Wietse, The Illegal Fishing and Organized Crime Nexus: Illegal Fishing as Transnational Organized Crime, The Global Initiative Against Transnational Organized Crime and The Black Fish, 2015, https://globalinitiative.net/wp-content/uploads/2015/04/the-illegal-fishing-and-organised-crime-nexus-1.pdf, p. 43.
[33] John Virdin, Tibor Vegh, Blake Ratcliff, Elizabeth Havice, Jack Daly and Jack Stuart, *Combatting illegal fishing through transparency initiatives: Lessons learned from comparative analysis of transparency initiatives in seafood, apparel, extractive, and timber supply chains*, Marine Policy, Volume 138, April 2022, p.1.

Thailand has established a traceability system covering the whole supply chain from sea to plate to combat IUU fishing. The Thai Flagged Catch Certification Scheme and the Import Control Scheme ensure complete product traceability at each and every stage of production – from catch landing to offloading, processing and, ultimately, export. Cross-checking and surprise inspections are in place at all stages of the production process to ensure compliance. Consignments of processed fish that have received certificates permitting their export can be traced back to the vessel and specific batch of fish offloaded at Thai ports.

The United States Seafood Import Monitoring Program (SIMP), a risk-based traceability program, requires importers to provide and report key data from the point of harvest to entry into U.S. commerce on more than 1,100 unique species.[34] SIMP requires importers to document a product's chain of custody from the harvest location until arrival in the US.[35] Importers must then retain this information for two years and they may be subject to random government audits and inspections.

Private fishing companies also frequently voluntarily adhere to private sector transparency initiatives. For example, in order for fishing products from certified fisheries to use the Marine Stewardship Council (MSC) ecolabel, fishing companies must meet supply chain transparency requirements to receive a chain-of-custody certificate.[36] Other private sector transparency initiatives include the Seafood Business for Ocean Stewardship (SeaBOS) and Global Dialogue on Seafood Traceability (GDST) initiatives.

These initiatives present opportunities for collaboration between LEAs and private fishing companies as both are required to develop knowledge on the actors involved in IUU and where risks arise. There is also scope for financial gatekeepers (financial institutions and DNFBPs) to use the information available from transparency initiatives to identify risks of IUU, and improve the quality of reporting to FIUs.

1.5 Conclusion

The dynamics of the IUU fishing and related ML threat are varied across regions and individual jurisdictions. IUU has conventionally been treated as a fisheries management problem and is still prioritised as such. Asia Pacific jurisdictions largely commit to RFMOs and internationally binding measures of international organisations to promote sustainable fisheries governance. Despite this commitment, jurisdictions report challenges in mounting a sufficiently effective and proportionate law enforcement response to tackle IUU at its current scale. It is arguable that IUU is not yet prioritised as a criminal justice matter including a major source of proceeds of crime and loss of revenue to the state. A shift in characterising IUU as a predicate crime type for ML may trigger effective AML/CFT responses to tackle this complex and transnational threat.[37]

[34] NOAA Fisheries, *Seafood Import Monitoring Program*: Link: https://www.fisheries.noaa.gov/international/seafood-import-monitoring-program

[35] John Virdin, Tibor Vegh, Blake Ratcliff, Elizabeth Havice, Jack Daly and Jack Stuart, *Combatting illegal fishing through transparency initiatives: Lessons learned from comparative analysis of transparency initiatives in seafood, apparel, extractive, and timber supply chains*, Marine Policy, Volume 138, April 2022, pp. 3-4.

[36] Ibid, p.4.

[37] This chapter is part of a broader APG typologies project considering the illicit financial flows associated with illegal fishing (see section 3.1 below).

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

Since 2020, the APG Yearly Typologies Report has covered COVID-19's impact on ML/TF typologies. Chapter 1 of the 2020 APG Yearly Typologies Report 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.

In 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.).

In 2022, APG members were again asked to provide case studies documenting ML and TF typologies associated with predicate activities linked to COVID-19.

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 cybercrime and online fraud including business email compromise scams. Authorities have also detected the sale of forged vaccination records. Members continue to report fraudulent claims for COVID-19 related government subsidies. Corruption by government officials in relation to COVID-19 financial support programs has also been reported as well as a government official misappropriating a COVID-19 budget.

Criminal activity in relation to COVID-19 vaccines was also reported including criminals deceiving victims to pay for COVID-19 vaccines that were offered free by the government and instances where COVID-19 vaccines were illegally sold.

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. There has also been an increase in the discovery of large amounts of physical cash believed to be the proceeds of crime.

3. APG WORKSHOPS AND PROJECTS 2021 - 2022

This section of the report provides a brief overview of typologies-related work undertaken by the APG between July 2021 and June 2022.

3.1 Typologies Projects

Illicit financial flows generated from illegal fishing

In October 2021, the APG Operations Committee approved a typologies research project to understand and investigate the nature and dynamics of the illicit financial flows generated from illegal fishing. The project will rely on information collected from APG members, observers and select private sector bodies on efforts to identify proceeds generated from illegal fishing. The project will collect case studies from APG members concerning investigations and prosecutions related to the financial flows from illegal fishing.

The project aims to clarify how the illegal proceeds from illegal fishing are integrated into the legitimate economy and illuminate the channels and actors used to launder the proceeds. The project will produce a report that investigates the nature and dynamics of the illicit financial flows generated from illegal fishing; deliver a roundtable in the margins of APG's 2022 Annual Meeting between members, observers and the civil sector; and contribute to a focus stream at the next APG Annual Typologies Workshop.

Members and Observers of the project team include Germany, Ministry of Finance; Saudi Arabia, Islamic Development Bank Group; UNODC; Fiji, Offshore Fisheries Unit and Ministry of Fisheries; United States, United States Coast Guard Maritime Intelligence Fusion Centre Pacific and Department of Treasury; Australian Federal Police (AFP) advisor to the Pacific Transnational Crime Coordination Centre (PTCCC); Pakistan, Financial Monitoring Unit; Sri Lanka, State Ministry of Fisheries and Aquatic resources and Central Bank of Sri Lanka; New Zealand, Customs; Pacific Islands Forum Fisheries Agency; and Oceania Customs Organisation Secretariat.

Tax crimes

In October 2021, the APG Operations Committee approved a further typologies research project on tax crimes which aims to collate tax crime typologies observed by members, experiences of money laundering and taskforce investigations involving tax crimes and associated legal structures, and statistics on the seizure and confiscation of assets derived from tax crimes. The project will also explore the role of supervisors and risk-based supervision relating to complex legal structures and shell companies, secrecy jurisdictions, gatekeepers and facilitators in the laundering of proceeds of tax crimes.

The tax crimes typologies project will produce a report for APG members that identifies national tax crime frameworks, the risk context, and the use of corporate vehicles in laundering the proceeds of tax crimes as well as the roles of competent authorities and law enforcement agencies in the investigation and prosecution of the laundering of tax crimes.

Associated deliverables will also support Australian Whole of Government initiatives including the Australian Department of Foreign Affairs and Trade (DFAT)-led Mekong

Australia Partnership – Transnational Crime (MAP-TNC). In addition, these products will be valuable inputs and examples for tax crime investigation capability building as part of the OECD's efforts in the Asia-Pacific region such as the OECD Tax Crime Academy (located in Japan) and its Tax Inspectors Without Borders – Criminal Investigation pilot program.

Members and observers of the project team include Australia, Australian Taxation Office; Fiji, Fiji Revenue and Customs Service; Kiribati, Kiribati Police Service; Pakistan, State Bank of Pakistan, Securities and Exchange Commission and Financial Monitoring Unit; Singapore, Inland Revenue Authority and Singapore Police Force; Asian Development Bank; European Union; Islamic Development Bank and the Pacific Islands Tax Administrators Association.

Implementation of Recommendation 8 and Immediate Outcome 10 in the Asia Pacific Region

In October 2021, the APG Operations Committee approved a further APG typologies research project to be conducted in partnership with the Global Center on Cooperative Security. The project will involve a scoping exercise of APG members' implementation of the Financial Action Task Force (FATF) Recommendation 8 and Immediate Outcome 10 on preventing the abuse of non-profit organisations (NPOs) for terrorism financing. Through a horizontal review of mutual evaluation findings, APG member survey, consultations, and multi-stakeholder roundtable, the project will identify areas where further guidance is needed to enhance the implementation of FATF's Recommendation 8 and Immediate Outcome 10 across the APG membership while avoiding unintended consequences on civic space, human rights, and NPO operations and access to financial services.

The project will produce a report identifying strengths and implementation challenges related to FATF Recommendation 8 and Immediate Outcome 10 including case studies highlighting members and NPO's experiences and lessons learned. The report will offer recommendations to the APG and members on areas where further guidance, training or other support is needed to enhance implementation of the FATF standards. The report will also inform APG efforts to contextualize the work of the FATF unintended consequences project in line with the needs of the APG membership.

Members and observers of the project team include Australia, Australian Transaction Reports Analysis Centre; Bangladesh, Bangladesh Bank; India, Ministry of Home Affairs; Malaysia, Bank Negara Malaysia; Pakistan, Financial Monitoring Unit; Islamic Development Bank and United Nations Office on Drugs and Crime. The project team also includes civil society organisations who were consulted on the FATF's project to study and mitigate the unintended consequences resulting from the incorrect implementation of the FATF Standards.

3.2 APG Annual Typologies 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 23rd APG typologies workshop was held virtually from 9-11 November, and co-hosted by Malaysia (Bank Negara Malaysia). Over 190 representatives attended in a virtual format to

explore proliferation financing (PF) risk assessments and the use of public private partnerships (PPPs) in combating ML/TF and proliferation financing (PF). The event attracted experts in their fields, practitioners with hands-on experience and policy makers engaging in active discussions.

On PF, delegates discussed the foundations of PF risk assessments, FATF guidance and current trends and vulnerabilities. Delegates also explored the growth and evolution of PPPs, practical challenges faced in their implementation and operation, and future trends.

The presentations and panel discussions provided delegates with a range of views and unique insights from across the public and private sectors. Policy experts spoke on global trends and experiences whilst representatives from FIUs, financial institutions and LEAs highlighted the successes and challenges of countering PF and collaborating in PPPs to fight ML.

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 2021 and 2022.

4.1 FATF Typology Projects

FATF Work on ML, TF and PF Risks 2021-2022

Proliferation Financing (PF) Risk Assessment and Mitigation (Guidance and Webinar)

In June 2021, the FATF published Guidance on Proliferation Financing Risk Assessment and Mitigation to explain the latest FATF requirements in this area. This document provides information on how the public and private sectors should conduct risk assessments in the context of proliferation financing, and how they can mitigate the risks they identify. It also includes advice to supervisors and self-regulatory bodies in ensuring that proliferation financing risks are properly assessed and mitigated, and gives a focused explanation on how certain types of products, services, and sectors could be misused for potential breach, non-implementation or evasion of PF targeted financial sanctions (TFS). A list of updated risk indicators is included in the document.

Following the APG typologies workshop on PF in November 2021, the FATF held a webinar in December 2021. The webinar, which was joined by over three thousand participants across the FATF Global Network, included a panel discussion on the emerging trends on PF risks and techniques adopted by designated individuals and entities to evade PF TFS. Panellists also shared their experiences and lessons learnt in developing PF risk assessments and mitigation strategies.

The FATF will begin assessing jurisdictions for implementation of these requirements at the start of the next (fifth) round of mutual evaluations, i.e. from 2025/26, to allow time for the necessary domestic measures to be put in place.

The FATF Guidance can be found at the following link:

https://www.fatf-gafi.org/media/fatf/documents/reports/Guidance-Proliferation-Financing-Risk-Assessment-Mitigation.pdf

The webinar can be found at the following link:

https://www.youtube.com/watch?v=VQ-odSLnj7E

ML/TF Risks Arising from Migrant Smuggling

In March 2022, the FATF published a report on ML/TF and Migrant Smuggling. The report brought together key intelligence from competent authorities around the world on what is inherently a cross-border risk, also drawing on the findings of recent work by partner organisations Europol, INTERPOL, UN CTED, UNODC and FATF-style regional bodies CFATF and MENAFATF.

The object of the project is to help countries and the private sector to align their national and institutional controls and strategies through an enhanced understanding of ML/TF risks. The

target audience is both competent authorities - in particular financial investigators and experts responsible for assessing and monitoring national ML and TF risks - and the private sector.

Key findings of the report include:

- Migrant smuggling has grown in recent years, but the number of smugglers arrested remains very low. Many countries do not consider migrant smuggling a 'high risk' crime for ML and only very few investigations or prosecutions are initiated or concluded.
- An informal money transfer system, known as hawala, is the most common method of transferring funds generated from migrant smuggling between jurisdictions. Other methods include the physical transportation of funds via cash couriers or money mules.
- In recent years, smugglers have started to widely use social media and encrypted digital communication services in their operations for recruitment and coordination.
- Migrant smuggling groups also appear to increasingly outsource their ML activities to professional laundering networks.
- Overall, there is limited information available on the connections between terrorist financing and migrant smuggling. However, there is evidence of terrorists receiving money from smugglers along various African migration routes in the form of 'tolls' for safe passage through the territory they control, and links with facilitation of foreign terrorist fighters.
- Understanding of the ML/TF risks varies among countries. While some countries have access to qualitative information and case studies, a large percentage of countries were unable to provide complete statistics, on aspects of the performance of their AML/CFT systems in relation to migrant smuggling.
- Migrant smuggling is a transnational crime, yet national and international collaboration between relevant authorities has been challenging for many countries. To prevent migrant smuggling, countries need to proactively follow the money linked to migrant smuggling. The report identifies a number of good practices and recommendations. These include strengthening inter-institutional, international and regional cooperation, with a particular focus on supporting countries that are directly affected by migrant smuggling.

The report is available on the FATF website at:
https://www.fatf-gafi.org/media/fatf/documents/ML-TF-Risks-Arising-from-Migrant-Smuggling.pdf

Terrorism Financing Risk Indicators

In June 2021, the FATF published a report on Financing of Ethnically or Racially Motivated Terrorism (EoRMTF). This report focuses on the funding behind ethnically or racially motivated terrorism, also referred to as extreme right-wing terrorism. Following publication of the report, the FATF has developed risk indicators for operational authorities.

The report can be found at the following link:

https://www.fatf-gafi.org/media/fatf/documents/reports/Ethnically-or-racially-motivated-terrorism-financing.pdf

ISIL and Al-Qaeda and Affiliates financing

The FATF has been regularly collecting and analysing information on the financing of the Islamic State in Iraq and the Levant (ISIL), Al-Qaeda, and their affiliates since 2015. Experts from the public sector should get in contact with their FATF representatives should they want a copy of the FATF's latest analysis.

Joint Experts' Meeting 2021 (JEM 2021)

The FATF organized the Joint Experts' Meeting (JEM) 2021 as four separate virtual sessions from 29 November to 20 December 2021 to allow global operational experts to discuss emerging ML/TF risks. These sessions covered four separate issues:

- TF risk indicators, including indicators on ethnically or racially motivated TF;
- ML/TF risks arising from migrant smuggling;
- The use of art, antiques and other cultural objects (AACO) as a tool for ML/TF;
- The proceeds of the trafficking of fentanyl and other synthetic opioids.

In total, 384 participants from the FATF Global Network attended this virtual event, while 28 speakers from relevant jurisdictions, the academic community and private sector presented during these sessions and shared their experiences and studies. The discussions at the JEM 2021 provided useful practical inputs and additional information to FATF's recent works on risk, trends and methods.

4.2 Middle East and North Africa Financial Action Task Force

Money Laundering resulting from the Human Trafficking and Migrant Smuggling Crimes (August 2021)

The report covers regional and international efforts to combat human trafficking and migrant smuggling crimes. It sets out the MENAFATF member countries' status with respect to conventions and treaties against human trafficking and migrant smuggling and explains their efforts to implement these conventions and to establish legal frameworks that address these crimes. The report examines challenges and difficulties faced by member countries in implementing international conventions. The report also presents an overview of the impact of the pandemic on human trafficking and migrant smuggling victims, due to the closure of shelters and the suspension of health care, and the changes which occurred to the forms of exploitation and methods used by traffickers and smugglers. The report further examines the methods used by criminals and criminal organizations to launder the illicit proceeds relating to the human trafficking and migrant smuggling crimes. The report aims to increase the capacities of member countries in the Middle East and North Africa region to prevent, detect and reduce the risk of these crimes.

Recommendations contained within the report for MENAFATF members include:

- To include human trafficking or migrant smuggling in NRA reports prepared by members.
- Urge countries to establish national departments specialised in combating human trafficking and migrant smuggling crimes.

- The importance of updating and developing red flag indicators of human trafficking and migrant smuggling crimes for LEAs and all the stakeholders, to facilitate the detection of human trafficking and migrant smuggling gangs.
- Increase spontaneous exchange of intelligence information concerning the proceeds of human trafficking which contribute to ML/TF.
- There is a strong need for bilateral cooperation among national LEAs which should be broadened to include other government bodies such as (FIUs).
- The importance of exchanging expertise between LEAs and their counterparts in other countries in order to examine the latest developments and the best techniques to fight and reduce these crimes.
- Ensure training for those who work at financial institutions in the field of combating human trafficking and migrant smuggling and raise awareness among authorities and financial institutions.
- Ensure the training of individuals working in the NPO sector including awareness raising about the seriousness of human trafficking and migrant smuggling.

The report is available on the MENAFATF website at:
https://www.menafatf.org/sites/default/files/Newsletter/ML%20Resulting%20from%20the%20HT%20and%20MS_0.pdf

Coronavirus Pandemic (COVID-19) and its impact on AML/CFT systems in the Middle East and North Africa Region - Update (November 2021)

In late October 2020, the MENAFATF issued a study on the "Coronavirus Pandemic (Covid-19) and its impact on AML/CFT systems in the Middle East and North Africa region," which focussed on the pandemic risks associated with ML/TF crimes. The first section of this updated report includes an overview of the Coronavirus pandemic (Covid-19), and its impact on the AML/CFT systems as well as a summary of the previous study that MENAFATF issued in October last year.

The second section of the report presents an update of the study on the Coronavirus pandemic (Covid-19) and its impact on the AML/CFT systems in the MENA region, which looks at the recent developments in ML/TF crimes in the MENA region. A sample of the MENAFATF member countries that responded to the request for information and a case studies questionnaire reported the spread of fraud, such as obtaining financial aids from foreign countries. The countries also reported a trend of the establishment of shell companies as well as the use of public funds for the purchase of medical equipment.
The third section of the report includes case studies related to ML/TF crimes related to the Coronavirus pandemic.

Recommendations contained within the report for MENAFATF members include:
- Emphasis should be placed on strengthening AML/CFT systems on a continuous and sustainable basis so that they are not vulnerable in times of the crises like the pandemic.
- Ensure that financial services can be provided remotely through modern financial technologies, including mobile phone applications and Internet Banking. Ensure coordination between Internet Service Providers and modern financial technology service providers to support the use of digital identity and combat electronic fraud.

- A risk-based approach should be adopted (classifying clients according to their level of risk) to determine the CDD measures based on those risks, and to encourage financial institutions to carry out EDD measures towards financial transactions executed electronically.
- Provide appropriate remote training programs in AML/CFT for employees of financial institutions.

The report is available on the MENAFATF website at:
https://www.menafatf.org/sites/default/files/Newsletter/MF.21.TATWG32.02.E.%28V1.0%29_0.pdf

4.3 Eurasian Group on combating money laundering and financing of terrorism

Methodology of the Eurasian Region ML/TF Risk Assessment (2021)

The EAG methodology document sets out the framework for carrying out the assessment of risks in EAG states and for developing joint measures to mitigate such risks and increase the effectiveness of AML/CFT efforts. The document firstly sets out the objectives of a regional risk assessment. The document then lists the organisations who are likely to use a regional risk assessment including international and regional organisations, EAG member states' government agencies, law enforcement and investigative authorities, supervisors, financial institutions and DNFBPs and non-profit organisations. The document then sets out that the Eurasian region will be split into four subregions for risk assessment purposes, namely Belarus and Russia (East European subregion), Eurasian Economic Union subregion, Central Asia and Russia subregion and India and China subregion. The document sets out the data sources to be used in regional risk assessments before establishing a regional risk assessment procedure.

The report is available on the EAG website at:
https://eurasiangroup.org/files/uploads/files/other_docs/Eurasian%20region%20MLTF%20Risk%20Assessment/Methodology_RRA_en.pdf

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

AML/CFT supervision in times of crisis and challenging external factors (2022)

This best practice paper provides an overview of business continuity measures that supervisors may wish to consider in the context of the COVID-19 pandemic and challenging external factors. The report takes account of examples and considerations provided by supervisors in response to a questionnaire sent by the Project Team to the MONEYVAL member states and beyond and on qualitative data obtained through subsequent interviews and additional written contributions. The main sources of information of this paper were experiences and actions of authorities taken to overcome the difficulties caused by the COVID-19 pandemic.

Key findings of the report include:
- Business Continuity Plans (BCP) proved to be a useful tool to helping countries swiftly overcome crisis situations.

- Due to the physical movement limitations, and the need to make use of the virtual meetings and other forms of communication, involving IT and internal security departments in the development of business continuity strategies and plans and in their implementation appeared to be a good practice.
- BCPs may include protocols with the reporting entities to ensure their collaboration and active participation in the crisis management arrangements and allow access to data/information and documents under special circumstances.
- When the AML/CFT supervision is dissipated amongst several supervisors, setting a coordination committee showed positive results.
- The COVID-19 pandemic proved that in crisis situations where employees are unable to return to the office, technology is key, both software and hardware.
- Shifting to remote or hybrid inspections to replace traditional on-site visits was the main solution found to continue the AML/CFT supervision during the crisis.
- Cross-border cooperation between supervisors in times of crisis could be enhanced by simplifying existing regulations and procedures relating to cross-border cooperation and data exchange.

The report is available on the MONEYVAL website at:
https://rm.coe.int/typologies-report/1680a54995

4.5 Egmont Group

Best Egmont Cases – Financial Analysis Cases 2014-2020 (2021)

The Best Egmont Case Award (BECA) annual competition was developed in 2011 by the Training Working Group — now called the Technical Assistance and Training Working Group (TATWG). FIU members submit cases to the competition which are then scored by a panel of four to six judges who determine the two best cases. The finalist FIUs would then be invited to present their case to the plenary. The Heads of FIU would be asked to vote for the case that they considered as the "best case" and the winner would be awarded the BECA trophy.

The report includes 26 case studies submitted to the competition. Case submissions were received from a range of countries including FIUs from Australia, Bolivia, Brunei Darussalam, India, Indonesia, Italy, Korea, Nepal, New Zealand, Philippines, Poland and South Africa. The cases are organised by category of predicate offence with the categories being bribery and corruption, cybercrime and cryptocurrency, drug trafficking, fraud and embezzlement, smuggling and gambling, trade-based ML and third-party ML and terrorism, organised crime and human trafficking. Each section on a predicate offence includes an explanation of the crime type and a list of indicators for that crime type.

The report is available on the Egmont Group website at:
https://egmontgroup.org/wp-content/uploads/2022/01/2021-Financial.Analysis.Cases_.2014-2020-3.pdf

Egmont Group Public Bulletin: FIU's capabilities and involvement in the fight against the financing of extreme right-wing terrorism: State of Play and Perspectives (July 2021)

The purpose of this Egmont Group public bulletin is to present key lessons, best practices and representative case examples to help enhance the fight against extreme right-wing terrorism financing (ERWTF) both at the national and international levels. The information in the bulletin is intended to assist the establishment of national strategies and facilitate effective cooperation between FIUs and law enforcement and with judicial authorities. It is also aimed at helping reporting entities better detect extreme right-wing terrorism behaviours. The bulletin includes a range of case examples of ERWTF.

Recommendations contained within the report for Egmont Group members include:

- Widen the scope of the national risk assessment (NRA) and, if needed, explicitly analyse the threat of ERWTF.
- Consider the creation of a task force that will deal with TF or specifically with ERWTF, including FIUs.
- Consider the role of the domestic FIU in the risk analysis of the threat at the domestic level, especially regarding the operational and strategic information sharing to leverage financial intelligence.
- Organise public-private information sharing including sharing information between the task force or the national coordination mechanism and relevant actors of the private sector. This may occur via a public-private partnership (PPP) or by scheduling periodic meetings between the parties to discuss relevant matters.
  The creation of risk indicators appears essential for the detection and investigation of ERW cases. Risk indicators can be designed by the FIUs, attested by competent authorities, or jointly created. Once completed, these indicator sets should be widely shared with competent authorities and reporting entities.

The report is available on the Egmont Group website at:
https://egmontgroup.org/wp-content/uploads/2022/01/IEWG-ERWTF-public-bulletin2.pdf

FIUs' role in the fight against ML of corruption proceeds (within the context of COVID-19 pandemic)

The Egmont Group recently published a public report (in May 2022) which presents a corruption-related risk environment snapshot during the COVID-19 pandemic's first year and considers how FIU efforts contributed to overcoming its challenges.

The report includes a variety of information to present a concise and pragmatic analysis of information submitted by member FIUs: the organisational and operational responses put in place in jurisdictions across the globe, corruption-related risks detected and associated mitigating measures, relevant case experiences, lessons learned, emerging best practices and future challenges. We anticipate this will allow jurisdictions, specifically FIUs and public entities tasked with AML/CFT compliance, to ensure readiness and preparation for similar future emergencies/crises. The report captures the period since the start of the COVID-19 pandemic from the FIU perspective and sheds light on the emerging risks and FIU measures to make their actions more effective.

Corruption-related risks were identified where specific risk assessments were carried out (and in general, where real impacts have been observed on domestic and/or transnational corruption risks):

- Misuse/diversion of COVID-19 aid funds;
- COVID-19 related fraud (medical supplies);
- Exploitation of the loosening of controls surrounding the pandemic, evading due diligence and submitting suspicious transactions;
- International links of COVID-19 related fraud and suspicious transactions;
- Corruption related to public tenders and direct purchases;
- Favoritism in the awarding of government contracts;
- Bribery for special treatments;
- Insider trading (particularly on an international level);
- Counterfeiting of medical equipment;
- Frequent use of supplementary and larger budgets or additional funds not always properly accounted for.

The report can be found at the following link:
https://egmontgroup.org/wp-content/uploads/2022/05/FIU-Role-in-Fight-Against-ML-of-Corruption-Proceeds_COVIDContext_Public_Final.pdf

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

Money laundering risks of Casinos and the Gambling sector in West Africa (2021)

The report attempts to identify the risks of the casino sector in West Africa, including the risks of ML and other forms of illicit finance in the sector. In particular, the report focuses on the casino and gaming sectors in six GIABA Member states (Ghana, Nigeria, Senegal, Cape Verde, Côte d'Ivoire, and Benin). This GIABA report is a stand-alone report that complements and expands upon earlier international work and guidance, notably the FATF reports, *Vulnerabilities of Casinos and Gaming Sector* (March 2009) and *Risk-Based Approach Guidance for Casinos* (October 2008). These high-level reports at the international level offer a solid framework through which AML practitioners and experts can approach the casino and gaming sectors. This regional report hopes to build on the red flags, good practices, and suggested actions identified in these reports at the international level, offering a roadmap for future actions by regulators, supervisors, and operational authorities in West Africa to reinforce their AML systems.

Key findings of the report include:

- Key deficiencies were identified in regards to legislative gaps (in particular, regarding the licensing and regulation of online casinos operating across the region).
- A lack of domestic cooperation to license, monitor and supervise casino activity for AML purposes was identified.
- A lack of STR reporting and information sharing between casino and gaming establishments in the region and the Financial Intelligence Units of the countries surveyed was identified.
- New trends were identified including in regards to increasing foreign acquisition of casinos, as well as foreign ownership and management of casinos across the region (often

manifested as increasing participation in the ownership structure, as most countries in the region require local majority ownership).

- A shifting customer profile was identified with an increased frequency of foreign customers.
- The presence of online casinos and sports betting companies increased, including as a result of the coronavirus pandemic that has put pressure on land-based casinos across the region.
- New risk indicators were identified in regards to: ML risks associated with the use of mobile payments in casinos, ML risks associated with online casinos and games, and ML risk indicators associated with the growing use of ticket or card-based slot machines.

Recommendations contained within the report include:

- FIUs or supervisors should circulate this report in its entirety to licensed casino operators in their jurisdiction. The timely circulation of this report will ensure that casino operators are made aware of their risk exposure and potential vulnerabilities associated with their business model.
- Authorities should review national legislation to cover technical compliance gaps identified in this report, and in particular to ensure that online casinos are fully covered for AML purposes.
- As a priority, online casinos should be licensed, implement internal AML controls, and file STRs and other applicable threshold reports.
- Supervisors should be given adequate resources and sector-specific training to conduct on-site and off-site AML supervision of physical casinos.
- Non-compliant casinos should be sanctioned with warnings, pecuniary fines, other administrative and criminal fines, and/or temporary or permanent operating license revocation. The existence of non-compliant, licensed casinos and illegal casinos disincentivizes good behaviour in the industry and harms the working relationship between authorities and the sector.
- At the regional level, GIABA should consider how to address deficiencies in cooperation between countries for AML purposes. Some formal mechanisms exist today to facilitate information sharing, notably the West African Network of Central Authorities and Prosecutors (WACAP), in addition to cooperation through bilateral Memoranda of Understanding (MoUs) and Egmont Group channels. Generally, authorities consider that these channels are not sufficient to request and ascertain information in a timely manner for investigative purposes. Regional cooperation on casino matters today is quasi non-existent.
- Investigations into suspicious behaviour in casino establishments are not occurring across the region. In part this is due to a lack of reporting to authorities from the sector, itself, and in part this is due to the lack of police capacity to conduct casino-related investigations. Specialized training for casino-related financial investigations is needed, and a specialized police unit or investigator (depending on the country and size of the sector) should be trained.

The report is available on the GIABA website at:
https://www.giaba.org/media/f/1195_CASINO_Study_GIABA_ENG_finale%203%20--.pdf

5. MONEY LAUNDERING AND TERRORISM FINANCING METHODS

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

Indonesia

Mr. ES, the Director of Company A (a State Owned Airline Company) and a politically exposed person (PEP), procured a shipment of RR Trent 700 engines and three Airbus aircraft and CRJ 1000 NG aircraft. ES is also the founder and beneficial owner of Company B, a company incorporated under the laws of Jurisdiction A (an offshore financial center).

ES received a fee, which constituted a bribe, when procuring aircraft and engine maintenance from Company F, Company G and Company H which was received through Company I and Company J (owned by Mr. STK). Ultimately, this fee was received from Company K through Company L in Jurisdiction B.

ES used Company B's account at Bank U in Jurisdiction C to receive the fee received from the procurement and used MB's (ES' wife) bank account as a holding account for SGD 480,000 (approx. USD 350,787), before transferring it to another party by breaking up the transaction to SAB (daughter of ES) of SGD 162,124 (approx. USD 118,479) and SGD 45,300 (approx. USD 33,104), transferring SGD 291,785 (approx. USD 213,229) to the account in the name of MS (Parent of ES) and transferring SGD 2,476 (approx. USD 1,809) to the account in the name of ER (Son of ES) .

While ES had attempted to obscure the ownership of Company B using the establishing of a trust, cooperation between PPATK (Indonesia FIU) and law enforcement agencies abroad identified that Company B belongs to ES and SAB (daughter of ES).

A number of foreign bribes were received into Company B's account, then ES deposited the money amounting to USD 1,458,364 to STK through STK's personal account, then he provided a means to return the deposit of funds belonging to ES by setting up a company in Jurisdiction A along with their accounts, namely Company M in Jurisdiction C and Company N's account in Bank A. An underhand agreement accompanied by AR (lawyer) was then made as if buying and selling apartments in Jurisdiction C and avoiding a stamp duty of 13% of the selling price. This underlying transaction appears to be legitimate economic activity in the form of buying and selling apartments between ES and STK.

5.2 Use of virtual assets (cryptocurrencies or other virtual assets).

Australia

<u>New South Wales Police Force Cybercrime Squad Investigation</u>

In 2020, the New South Wales Police Force (NSWPF) Cybercrime Squad commenced an investigation into organised money laundering. The investigation confirmed the existence of a well-established, organised and ongoing criminal group that knowingly dealt with the proceeds of crime, further facilitating other illegal activities. Police allege that the criminal group

received vast quantities of Australian currency from various persons and methodically converted these quantities of cash into Bitcoin cryptocurrency before returning the cryptocurrency to those persons who had provided the cash.

The group laundered the currency via two main methods. The first method was to take cash to a digital currency exchange where the cash was used to purchase an equivalent quantity of Bitcoin over the counter, handing large quantities of cash to staff. After completion of the appropriate documentation, staff electronically transmitted cryptocurrency into a digital "wallet" provided by members of the group. The second method involved large amounts of cash being handed to persons who would later deposit the cash into bank accounts on the group's behalf before being converted to cryptocurrency.

In early 2021, a number of individuals were arrested and charged. NSWPF identified in excess of AUD 5,700,000 (approx. USD 3,892,763) being laundered by the group. Of all the cash seized during the investigation, 11 notes matched the serial numbers of cash used in drug supply investigations to purchase prohibited drugs.

Source agency: New South Wales Police Force

Operation AVARUS-BELLUM

In July 2021, the Australian Federal Police-led (AFP) High Volume Crime Taskforce Vanguard was established, partnering with the Australian Transaction Reports and Analysis Centre (AUSTRAC) to combat money laundering activities in NSW. Taskforce Vanguard commenced Operation Avarus-Bellum in November 2021 after receiving intelligence from AUSTRAC relating to a network of individuals who were laundering cash offshore through cryptocurrency.

AUSTRAC identified that between September and November 2021, the network deposited over AUD 2 million (approx. USD 1,365,638) in cash at ATMs in Sydney, and quickly transferred the funds to a cryptocurrency exchange.

On 19 November 2021, the AFP arrested two nationals of jurisdiction A in Western Sydney. One man was arrested after the AFP observed him attempt to deposit cash at an ATM and seized AUD 30,000 (approx. USD 20,484). An associate located in a vehicle close to the bank was questioned by police, resulting in the seizure of a further AUD 477,000 (approx. USD 325,704) in cash. Both men were charged with dealing in the proceeds of crime of more than AUD 100,000 (approx. USD 68,274), contrary to section 400.9 (1) of the Criminal Code (Commonwealth).

Sources:
https://www.afp.gov.au/news-media/media-releases/two-sydney-men-charged-over-money-laundering-activities
https://www.afp.gov.au/news-media/media-releases/afp-targets-criminals-laundering-dirty-money
https://www.afp.gov.au/news-media/media-releases/new-afp-led-taskforce-vanguard-makes-significant-impact-high-volume-crime
Source agency: AFP

Chinese Taipei

Case 1

The suspect, Mr. C, has been the owner of Company T since 2017. Mr. C established four investing platforms and promoted his cryptocurrency investment programs in online chat groups, promising investors that his programs can generate 80% to 720% returns per year. However, many of the investment programs did not exist. To invest, investors could either deposit cash into Company T's bank account or transfer cryptocurrencies to the crypto wallets provided by Company T or Mr. C's personal wallet. In order to convince investors that these programs could genuinely make profits, Mr. C sent cryptocurrencies to investors as returns from his own crypto wallets or Company T's bank accounts. However, Mr. C was fraudulently operating a pyramid scheme. Finally, in order to conceal and disguise the illegal gains, Mr. C sold his cryptocurrencies through over-the-counter trading (OTC) markets, then transferred the money into Company T's bank account and withdrew the cash. In August 2021, a District Prosecutors Office prosecuted Mr. C for fraud and offenses against Article 29 of the Banking Act.[38]

Case 2

The members of criminal syndicate A opened a few accounts on a crypto exchange X, and purchased a small number of cryptocurrencies, then those members took advantage of the design loopholes in X's trading system. Members of the syndicate logged onto the system with different mobile phones or web interfaces, clicked on the withdrawal transaction of the same amount of cryptocurrencies, and pressed "Confirm" and "Cancel" within a similar time interval, making the system falsely withdraw the cryptocurrencies while at the same time deposit the same amount of cryptocurrencies into those accounts, resulting in a total loss of approximately TWD 12,673,339 (approx. USD 435,290).

In order to disguise and conceal the criminal proceeds, members of criminal group A created a new virtual currency wallet to deposit those illegal cryptocurrencies, then sold those cryptocurrencies through over-the-counter trading (OTC) markets in an attempt to conceal the source of funds.

Fiji

Case Study: Cryptocurrency Trading

Company Q was brought to the attention of the Fiji FIU for unregulated trading of cryptocurrencies in Fiji. Mr D was reported for creating and promoting a cryptocurrency investment group on a social media platform. Mr D asked potential investors in the investment group to deposit their investment funds into the bank account of Company Q. Mr D appeared to be an agent of Company Q.

Fiji FIU's analysis revealed that Company Q was a new company that intended to engage in cryptocurrency activities. Company Q's bank account received approximately FJD 8,000 (approx. USD 3,677) in less than one month from various investors for the purchase of

[38] Article 29, Banking Act: Unless otherwise provided by law, any person other than a Bank shall not accept deposits, manage Trust Funds or public property under mandate or handle domestic or foreign remittances.

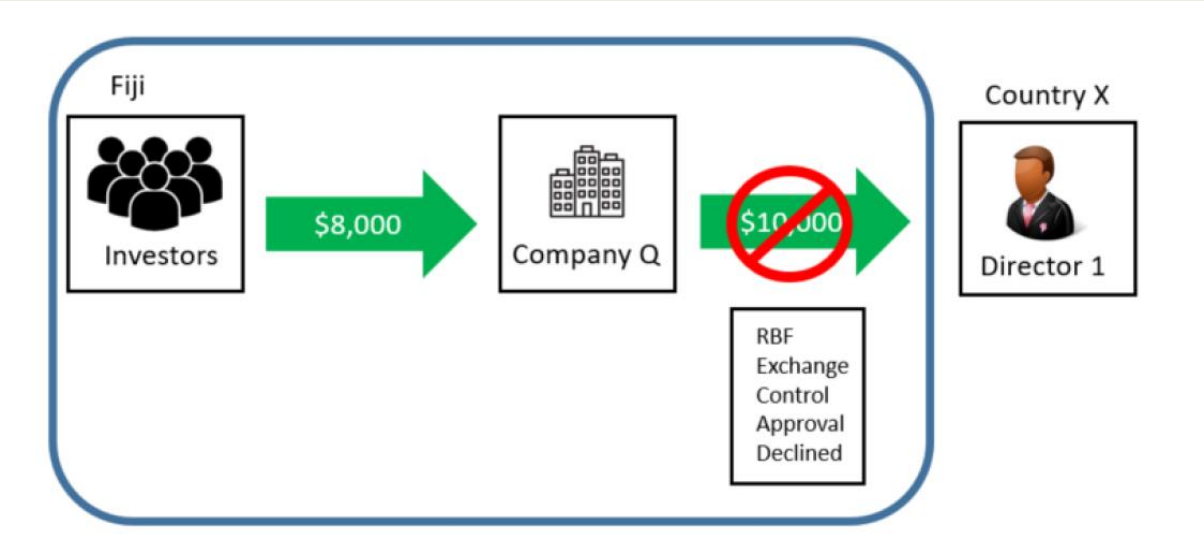
cryptocurrency. Company Q intended to remit approximately FJD 10,000 (approx. USD 4,596) to a director in Country X to purchase the cryptocurrency. The application to remit these funds to purchase cryptocurrency was declined by the Reserve Bank of Fiji (RBF) because of the restrictions under the Exchange Control Guideline.

Fiji FIU's analysis also established that a director of Company Q was also engaged in a multi-level marketing scheme aimed at promoting and selling online courses on various topics. Members of this scheme received a commission for each new individual they could sign up for a monthly subscription of these online courses. Fiji FIU analysis also established that the entity attempted to remit funds overseas to purchase virtual currency.

A case dissemination report was sent to RBF for possible Exchange Control violations.

Indicators:
• Small, frequent deposits and transfers from third parties
• Income is subject to the recruitment of more individuals

Possible Offence:
• Exchange Control violations
• Operating and/or promoting an illegal pyramid scheme



Hong Kong, China

Case 1

In mid-2021, the Hong Kong Police and Jurisdiction X jointly targeted a cross-jurisdictional deception syndicate with eight core members arrested in the operation centre in Jurisdiction X and 15 money mules arrested in Hong Kong, China during a synchronised raid. The syndicate set up at least 89 bank accounts in Hong Kong, China under the names of their money mules for receiving and laundering the criminal proceeds of scam cases amounting to HKD 739M (approx. USD 94,152,200). An in-depth financial investigation revealed that part of the proceeds of crime received were used to purchase Bitcoin and Tether (USDT), a cryptocurrency stablecoin pegged to the U.S. dollar, via exchange platforms and the funds were

subsequently dissipated to other virtual asset wallets. HKD 1.92M (approx. USD 244,618) was withheld in the identified bank accounts and an investigation is ongoing.

Case 2

Analysis of Mr. A's personal bank account unveiled the abnormal turnover of HKD 620M (approx. USD 78,991,648). It was revealed that the bank account in question was used as the second or third layer for receiving the proceeds of crime from four reported deception cases. Part of the deposits was swiftly transferred to bank accounts in three other jurisdictions, including a bank account in Jurisdiction X belonging to a Bitcoin trading platform. A joint investigation with Jurisdiction X was conducted and the funds in the account in Jurisdiction X were frozen. Mr. A was arrested with over HKD 33M (approx. USD 4,204,508) frozen in his personal bank account. A court proceeding is ongoing.

Case 3

Company A was a financial company in Jurisdiction X and Company B was a cryptocurrency trading company in Hong Kong, China. The two companies had a sale agreement under which Company B would sell cryptocurrencies upon Company A's payment. Company B requested Company A to remit funds totalling HKD 93.6M (approx. USD 11,931,409) to the account of a trust company in Hong Kong, China (Trust C). Immediately after the receipt of the funds, Trust C was instructed by Company B to transfer the said funds to a cryptocurrency platform and then transfer the funds to an external wallet. The case was reported by Company A which did not receive any cryptocurrency as agreed. An investigation is ongoing.

Indonesia

The Indonesian FIU (PPATK) has suspended 121 accounts related to illegal investments owned by 46 parties in 56 financial service providers with a total nominal value of IDR 353.98 billion (approx. USD 24 million).

Based on cooperation with law enforcement officials and related authorities, it was identified that proceeds from illegal investments involving two trading affiliates were sent abroad, including to Latin America and the Caribbean, Europe and Central Asia. Currently, PPATK has collaborated with five FIUs abroad. Furthermore, there are several hidden assets including cryptocurrency assets in two exchanges in Indonesia and abroad amounting to IDR 60 billion (approx. USD 4 million). In an effort to hide and disguise the proceeds of their crime, criminals also used the Payment Gateway, an electronic service that allows merchants to process payment transactions using payment instruments such as cards, electronic money, and/or Proprietary Channels. The illegal investment fund is also affiliated with an entity that manages a number of online gambling sites.

Japan

Virtual Asset "Monero"

In 2021, the Drug Enforcement Agency in Japan arrested a trader who received the virtual asset "Monero". The funds were sourced from the proceeds of illegal drug sales by two Cannabis

traffickers. The trader was investigated by the public prosecutor's office on the charge of violation of the Anti-Drug Special Provision Law (Receipt of drug-related criminal proceeds, etc.).

It was the first time that the Japanese Drug Enforcement Agency pursued a case of drug criminal proceeds using virtual assets. The traffickers used the internet for communicating with potential buyers of Cannabis, and used the highly confidential and difficult to trace virtual asset "Monero" as a means of payment. It was suspected that the suspect played a role of exchanging "Monero" to yen in reward for 10 percent commission.

Virtual Asset "Bitcoin"

Person A, an employee of S company in charge of the settlement business, was seconded to the subsidiary branch of S company. He accessed the bank account of P company in Q jurisdiction from his house when he was working from home. He fraudulently executed a transfer stating that he had the approval of his superior and sent 17 billion yen (approx. USD 133,871,988) to a bank account in the name of a virtual asset service provider in Q jurisdiction. After the transfer, he immediately exchanged the money for a virtual asset, "Bitcoin", and managed it by himself. It was revealed that approximately 17 billion yen (approx. USD 133,871,988) was illegally remitted from the bank account of P company to a bank account in Q jurisdiction as a result of a LEA in Q jurisdiction providing this information.

S company immediately reported the transfer to the police. After the police received the report, person A was arrested and prosecuted on the charge of fraud and illegally transferring approximately 17 billion yen (approx. USD 133,871,988). After that, person A's violation of the Act on Punishment of Organized Crime and Control of Crime Proceeds (Concealment of Criminal Proceed, etc.) was sent as an additional offense to the prosecutor's office for the fact of exchanging illegally obtained money for Bitcoin and managing it by himself.
Concerning the criminal proceeds, the police in Japan identified the "Virtual Asset Wallet" where person A had kept the Bitcoins, and requested the law enforcement agency in Q jurisdiction to provide assistance. The LEA in Q jurisdiction then confiscated all of the criminal proceeds.

Virtual Asset "Bitcoin"

Members of a criminal group specialised in fraud were arrested and prosecuted for engaging in false foreign exchange dealing and defrauding victims. There were around 700 victims in total and around 200 million yen (approx. USD 1,574,032) of total financial damage. The money which was obtained by fraud was remitted to the branch company in the name of B Co. Ltd. The suspects made B Co. Ltd. buy Bitcoins with the funds which the victims remitted to the bank account of B Co. Ltd., and sent the Bitcoins to the suspect's Bitcoin address which the suspect managed. Subsequently, the suspects sent almost the same amount of Bitcoins to B Co. Ltd.'s address, and made B Co. Ltd. sell the Bitcoins. Finally, the suspects received the cash obtained by selling the Bitcoin from B Co. Ltd.

Macao, China

Case: Money laundering related to a virtual asset scam

As part of a crackdown on cryptocurrency fraud in mid-October 2020, the Judiciary Police arrested and transferred four local men to the Public Prosecutions Office for follow-up action. During the investigation, the Judiciary Police identified that four local individuals (Suspects A, B, C and D) had been transferring and concealing criminal proceeds.

During the investigation of the whereabouts of the involved proceeds, the Judiciary Police found that another local individual, Suspect E, was involved in the aforementioned case. The involved individuals, Suspect A and E, acted in collusion to commit fraud. The involved man, Suspect E, had sent to himself around HKD 8.3 million (approx. USD 1,057,494) of the transaction proceeds, while the Macao bank account of Suspect D was credited with HKD 419,000 (approx. USD 53,385) of cash in total after the incident.

When the Judiciary Police summoned the aforementioned suspects and conducted searches at the residences of several involved individuals in November 2021, luxury watches worth over MOP 1,000,000 (approx. USD 123,698) in total were found. In view of the compelling indications that Suspect E had committed fraud of a considerably large amount and money laundering by collusion, and that Suspects A, B, C and D had processed, transferred and concealed criminal proceeds, there were strong indications of the commission of money laundering. The Judiciary Police, having detained Suspects A and B earlier, also transferred the other three suspects C, D and E, to the Public Prosecutions Office under the same case.

New Zealand

NZ Customs received information about a package being sent containing NZD 10,000 (approx. USD 6,526) of concealed cash. The cash was given back to the sender, however Customs put alerts on the consignee of the packages and later intercepted a money remitters debit card concealed between two “circuit boards” (likely to evade x-ray) that was linked to the consignee address in February 2021. The card was believed to be loaded with funds from card skimming activities and was being sent to the United Kingdom. The card was subsequently seized. In June 2021 a further linked package was intercepted and seized because it contained a skimming device.

Enquires conducted on the sender of the cash found that the funds were also likely linked to the card skimming activity. The funds were deposited into a newly opened bank account before using a New Zealand cryptocurrency exchange to transfer the cash into Bitcoin. The Bitcoin was then transferred to several wallet addresses before going to a crypto exchange likely to be exchanged back to cash. It is suspected that Bitcoin was being used to layer the funds. The case was referred to NZ Police.

Philippines

Several online news articles and stories circulated in social media regarding several accounts hacked by unknown perpetrators. Based on the report submitted by a bank (which was shared by a Supervising Agency), certain accounts were identified as recipients of the funds from

another bank (alleged hacked accounts). Most of the identified recipients had financial transactions, particularly inter-account transfers (outflows), during the period when the alleged hacking incident transpired.

The aforementioned funds which may possibly represent the funds that were unlawfully transferred from multiple accounts were then transferred by the subjects to another bank's accounts (layering), which may indicate that the accountholders may likely be money mules and that their accounts may have been used as a pass-through account. Furthermore, the second beneficiaries, who are either individuals or businesses, appear to be engaged in cryptocurrency trading based on their financial activities.

STRs related to the subjects indicated that their accounts were involved in phishing activities or had received unauthorised fund transfers. The initial beneficiaries had outgoing transactions (inter-account transfers) involving significant amounts which were transacted after the period of the alleged hacking incident. The total amount of debit transactions of some of the subjects almost totalled the amount of their credit transactions, indicating that their accounts were merely just pass-through accounts. According to an online news article, the hacked funds were used to buy cryptocurrencies. During the layering stage, the initial beneficiaries (possible money mules) transferred funds to businesses and individuals (second beneficiaries), some of which were allegedly engaged in cryptocurrency trading. Some of the second beneficiaries have had outgoing transactions to companies who are associated with cryptocurrency exchanges. The second beneficiaries received significant amounts of incoming fund transfers from numerous individuals, which appeared not to be commensurate with their declared businesses and financial capacities.

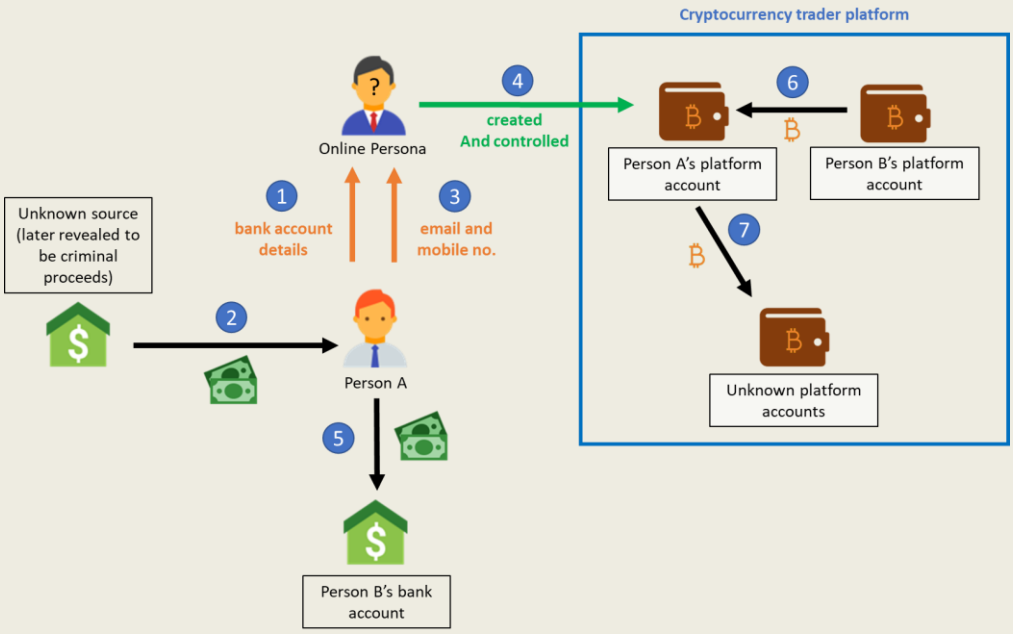
Singapore

This case features a mix of money laundering techniques, including the misuse of bank accounts and virtual assets as means to launder criminal proceeds.

Under the guise of friendship, Person A was coaxed into providing his bank account details online. Consequently, he received funds in his bank account, which turned out to be criminal proceeds from a business email compromise scam conducted outside Singapore. Person A further provided his personal information to facilitate the creation of an account with a cryptocurrency trading platform based outside Singapore, control of which was ceded to the unknown person.

Under the instructions of the unknown person, Recipient A then transferred most of the criminal proceeds to the bank account of Recipient B. Consequently, investigations revealed that Recipient B sent Bitcoin to Recipient A's trading account, and the proceeds were further laundered via cryptocurrency.

Investigations are currently ongoing as of February 2022.



Thailand

Mr. S, a self-acclaimed "cryptocurrency wizard", deceived numerous victims into investing in a Bitcoin portfolio while using Facebook and streaming games to persuade people. He claimed that investors would receive high returns of around 30 percent of their investment and posted pictures of money transfers. Victims received returns initially, but later on they did not receive further returns. Mr. S claimed that the bank had a problem with money transfers so the returns might be delayed and then Mr. S closed his Facebook and his portfolio. Victims claimed to have lost around 22 billion baht (approx. USD 643,881,741) to the scheme and filed complaints with the Royal Thai Police. Finally, Mr. S was arrested in January 2021.

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

Chinese Taipei

Mr. Y is the responsible person of Corporate Group A. Ms. W is his spouse. Mr. Y and several other individuals used fraudulent techniques to loan a total of about TWD 38.6 billion (approx. USD 1,332,291,416) from the bank. In order to conceal the illicit gains obtained by fraudulent loans through fraudulent transactions, Ms. W purchased 16 properties with the illicit proceeds and registered them with nominees. In addition, since April 2019, law practitioner Mr. J has discussed with Ms. W and several other individuals in regards to the fraudulent loans on several occasions and accepted TWD 12.5 million (approx. USD 431,455) of fraudulent loan proceeds from Ms. W and others using his own account and the account of his law firm P.

After Mr. Y and Ms. W fled the country in early June 2019, members of Group A continuously withdrew funds at the bank from Group A's account, and transferred a total of more than TWD 20 million (approx. USD 690,431) of criminal proceeds to various accounts owned by law firm P and Mr. Y's other accounts. Members of Group A also transferred TWD 6 million (approx. USD 206,769) in cash to Bank F in an attempt to hide the proceeds of crime and avoid investigation.

5.4 Trade-based money laundering and transfer pricing.

Chinese Taipei

Mr. T and Mr. L are the owners of company A and company B respectively. Since 2017, Mr. T and Mr. L set up and operated a gambling website named EZ overseas. Company A was responsible for the software development, modification and maintenance of the gambling website and Company B was responsible for the online customer service of the gaming website. In order to disguise or conceal the illicit gains from operating the EZ gambling website, Mr. T and Mr. L decided to launder money through an underground remittance syndicate. Mr. T first used the communication software WhatsApp to inquire about the exchange rate from the underground remittance operator Mr. S, and then deposited the RMB funds to bank accounts designated by Mr. S. After Mr. S received the confirmation, Mr. S asked staff in Chinese Taipei to deliver a total of TWD 1,280,774,900 (approx. USD 44,064,735) in cash to Mr. T. In addition, Mr. T and others forged the contracts signed by Company A and Company B with foreign companies and used those documents as proof to justify transactions totalling USD 2,999,231 remitted by the overseas companies.

Fiji

Case Study: Trade Based Money Laundering

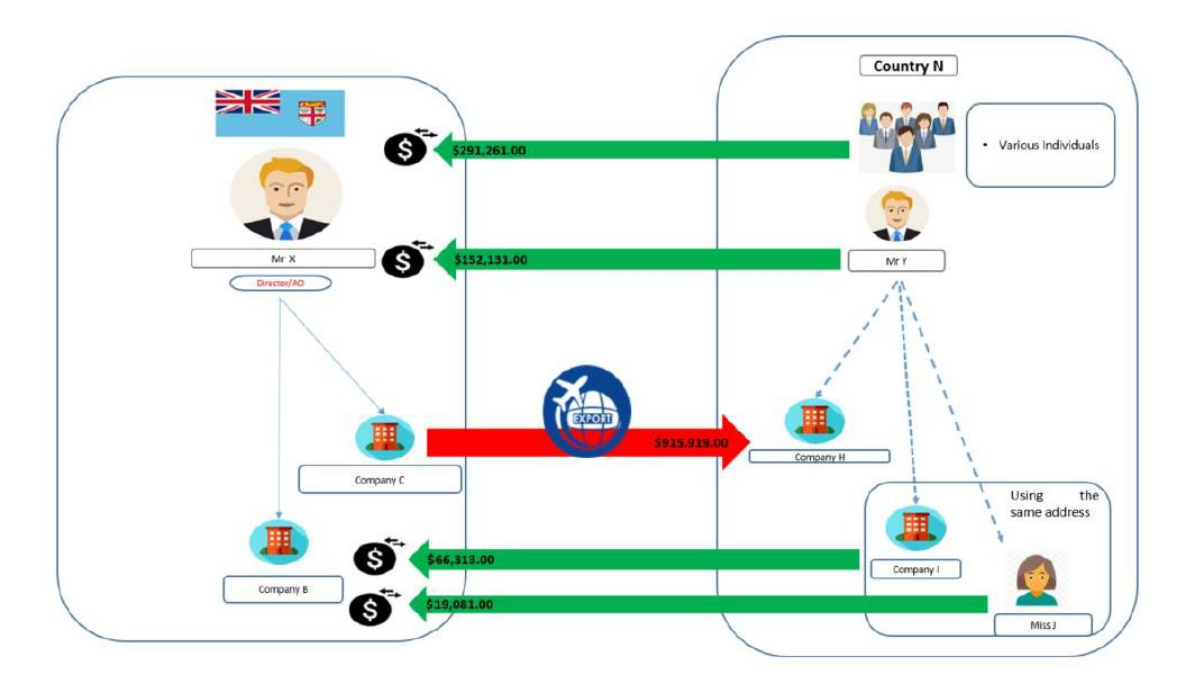
Mr. X, who is a lecturer at a local university, was reported to the Fiji FIU for receiving an international remittance of over FJD 152,000 (approx. USD 70,421) from Mr. Y in Country N. The remittance was allegedly payment from Mr. Y for the import of vegetables and purchase of farming equipment from Mr. X.

Fiji FIU analysis established that Mr. X is also a director of companies B and C whereby Company C conducts export activities while Company B and Mr. X receive the remittance payments for these export activities. Fiji FIU analysis also established that there was a discrepancy of FJD 350,000 (approx. USD 162,155) between the remittances received by Company B and Mr. X and the export activities of Company C.

Fiji FIU analysis established that Company C conducted exports to Company H in Country N totalling FJD 915,919 (approx. USD 424,347). Fiji FIU analysis also established that Ms. J and Company I in Country N remitted FJD 66,313 (approx. USD 30,722) and FJD 19,081 (approx. USD 8,840) respectively to Company B in Fiji. Fiji FIU analysis established that six other individuals in Country N remitted FJD 291,261 (approx. USD 134,941) to Mr. X in Fiji. A case dissemination report was provided to the Fiji Revenue & Customs Service.

Indicators:
• Large remittances from offshore

Possible Offence:
• Money laundering
• Unexplained wealth



Case Study: Profit Shifting

Company ABC, which operates in Fiji, was brought to the attention of the Fiji FIU for sending a remittance of USD 58,331 to its parent company, Company XYZ, in Country C. The invoice supporting the remittance transaction showed that approximately 25% of the transaction amount was for freight charges while the balance was for payment of stock. A review of previous invoices revealed that freight charges comprised of a large component of the total invoice amount.

Fiji FIU analysis established that from 2019 to 2021, Company ABC sent remittances totalling FJD 12.8 million (approx. USD 5,930,269) to Company XYZ for the purchase of stock. Fiji FIU analysis also established that within the same time period, Company ABC imported goods totalling FJD 9.7 million (approx. USD 4,494,031) from companies other than Company XYZ. It appeared that Company ABC overvalued its stock purchases to evade taxes locally and shifted funds to Company XYZ, its parent company, in Country C.

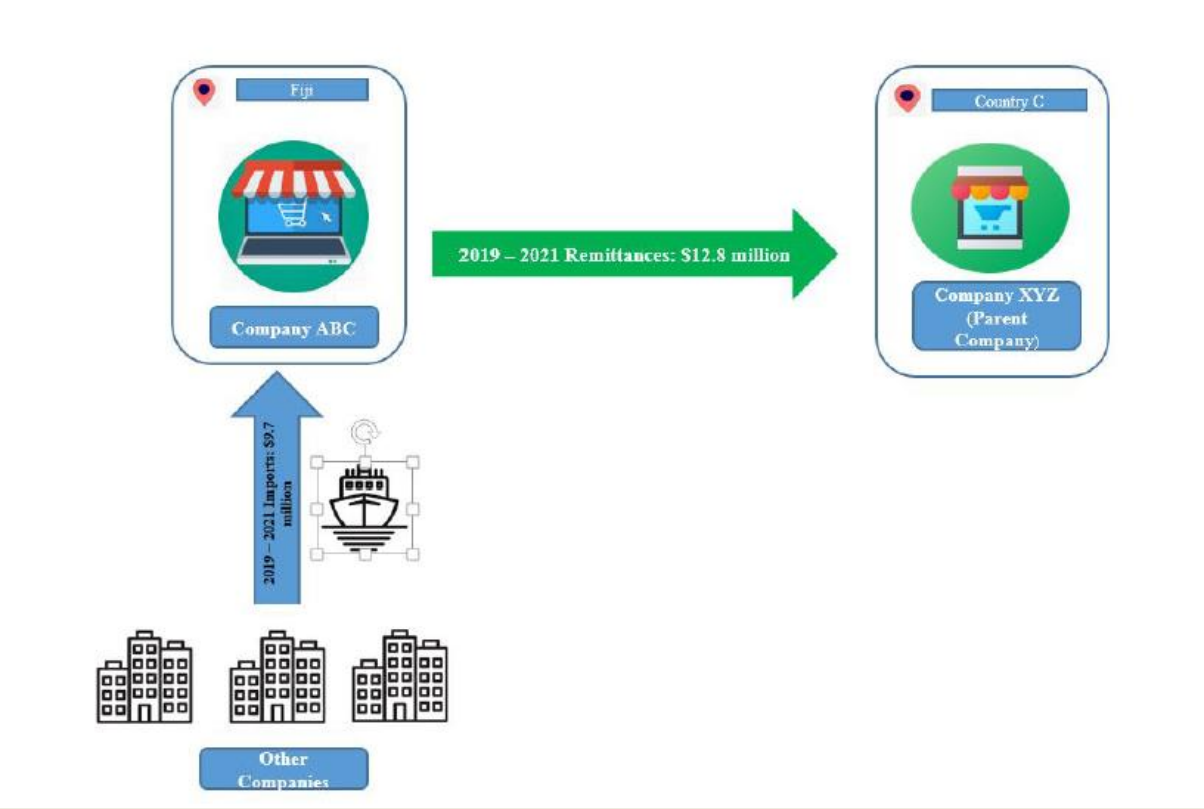
A case dissemination reported was provided to the Fiji Revenue and Customs Service.

Indicators:

- Unusually large freight charges
- Frequent remittances to parent company
- Discrepancies between invoices and remittance transaction details

Possible Offences:

- Trade based money laundering
- Profit shifting
- Tax related offence/tax evasion



Pakistan

Investigation of Trade-Based ML (Precious Stones): suspected origin of proceeds of crime/ML

An LEA commenced a ML investigation based on a financial intelligence report disseminated by Pakistan FIU (FMU) relating to suspected tax evasion (including under invoicing and misdeclaration which are predicates under Pakistan's AML law) and ML. The suspects were involved in trade-based ML in relation to the exportation of precious stones by Company A and the sole owner Mr. X, both in Pakistan, to Companies B and C in Country A and Country B.

Highlights of ML investigation

Information gathered and analysis undertaken by investigators included financial evidence such as tax declarations, wealth statements, bank account statements, as well as a family tree, criminal records, travel history, analysis of Company A's export declarations, in-depth forensic analysis of Mr. X's and Company A's bank accounts and evaluation of wealth/assets accumulated by Mr. X. The accused's bank accounts and assets were identified.

Mutual Legal Assistance (MLA) requests have been forwarded to ascertain if Mr. X or Company A have any moveable or immovable properties in other jurisdictions. Moreover, the import values of goods exported by Company A have been queried to investigate under-invoicing or further over-invoicing at the import clearance stage in other jurisdictions. Corporate records and the tax profiles of Companies B, C, and D, have also been requested from two other jurisdictions to ascertain their business and tax profiles, which might lead to

additional MLA requests including in relation to the ultimate beneficial owners' information and possible relation with Mr. X.

Findings so far

An investigation revealed that company A, a registered exporter of precious stones, was initially falsely undervaluing exported stones to avoid paying excise/customs and income taxes in Pakistan. The export records of company A between 2006 and 2014 reveal that Mr. X has been exporting precious stones at very low export values to himself as an importer abroad and also from Pakistan to two jurisdictions Country A and Country B. Records indicate Mr. X has been keeping the income abroad.

From 2014 onwards, Mr. X has been exporting precious stones to Companies B and C in Country A and to Company D in Country B with false values. The precious stones export records therefore showed that the export duties were undervalued. The stones were sold by him in foreign markets at much higher values which accumulated as Proceeds of Crime (POC).

Afterwards, since 2019, Mr. X has been exporting precious stones to companies in Country A and Country B at highly inflated export values while over-invoicing and reporting correspondent income and paying associated duties and income taxes. However, payments by the importers to Mr. X's accounts are higher than the value of his already inflated / over-invoiced exports and he has not reported these larger amounts. Funds over the years were deposited by Mr. X in bank accounts in foreign jurisdictions and then appeared to have been transferred back to Pakistan through over-invoicing, over payments and through informal channels to avoid detection or suspicion.

The case is currently under investigation and so far collusion between Company B with Mr. X and his Company A, has been identified. Scrutiny of income tax returns and wealth statements of the accused revealed a sudden and disproportionate increase in the assets of Mr. X.

The proceeds of crime generated from the export/import activities was laundered through company A's accounts and other bank accounts controlled by Mr. X. The proceeds of crime was largely withdrawn in cash from company accounts along with bank transfers, shown as payments to suppliers. It has been determined that the assets and business values of exported items did not correspond to the value that was reported as export revenues by Company A. This has been confirmed by the export information given in export declaration forms and the amount received in Mr. X's bank accounts and the accounts of Company A.

Highlights of the case

So far, the case involves at least three legal persons and one export business located in three countries and the movement of proceeds of crime across jurisdictions. Two foreign jurisdictions are relevant to the investigation. This is a complex financial investigation given the ML aspects combined with tax evasion predicates related to customs/excise duties and income tax, which is also related to both personal and business income combined.

The case involves suspected trade-based money laundering, with both under-invoicing and over-invoicing of the same goods in the same state. It also involves the repatriation of the proceeds of crime in Pakistan from abroad through disguised export revenues and other

informal means. The accused used multiple bank accounts, foreign exchange companies, and cash withdrawals.

Status of the case

The investigation is ongoing, including in relation to the repatriation of funds by Mr. X back to Pakistan and responses to international requests.

Singapore

Subsequent to the publication of a best practices document about trade-ML/trade financing by Singapore's public-private partnership – the AML/CFT Industry Partnership (ACIP), the Commercial Affairs Department of the Singapore Police Force (CAD) commenced investigations in collaboration with ACIP with the suspicion of trade-based ML.

Investigations were directed at Company A, where it was uncovered that its former Chief Financial Officer (CFO), Person A, deceived 16 financial institutions into providing Company A with credit facilities through the provision of false financial statements. Through this manner of deception, Person A induced the affected financial institutions into delivering up to approximately USD 1.08 billion in drawdowns from credit and loan facilities to Company A.

Since 2021, Person A was charged with a series of offences including cheating and abetting the falsification of accounts. Court proceedings are still ongoing.

5.5 Underground banking / alternative remittance services / hawala.

China

Money laundering via underground banking

Individual A purchased fraud software online and used a corporate account of an industrial company in Shanghai for an online fraud scheme while conspiring with individual B to launder the illegal proceeds. Individual B asked individual C, who worked overseas, to assist in the laundering process. Individual C received criminal proceeds of RMB 548,700 (approx. USD 82,123) in total from the account of the industrial company, and exchanged the funds for a total of USD 76,000 through underground banking in country A. Then, USD 65,200 was exchanged for RMB several transactions through underground banking. Finally, a total of RMB 266,900 (approx. USD 39,943) was transferred to the bank account of individual A, and a total of RMB 195,900 (approx. USD 29,316) and RMB 71,200 (approx. USD 10,654) respectively to the bank account and third-party payment account of individual B. Individuals B and C were convicted of disguising or concealing criminal proceeds.

Hong Kong, China

Intelligence suggested that a proclaimed clothing trading company (Company A) was in fact an unlicensed money service provider as same day mirror transactions and repository of funds were found in two corporate bank accounts of Company A. Company A's sole director (Mr.

B) was interviewed and he made admissions that he was engaged in an unlicensed money remittance business between Hong Kong, China and Jurisdiction X. An investigation revealed that deposits made into the two accounts were proceeds from deception cases. Funds amounting to HKD 1.4B (approx. USD 178,442,563) and USD 57.2M were laundered via the two accounts respectively. Mr. B was charged with two counts of money laundering. A court proceeding is ongoing.

Pakistan

1. Hawala & Smuggling

The transactional activity in the accounts of Mr. DWK and his family members was reportedly suspicious as a high value of funds was transacted from their accounts which apparently did not align with their profiles. The individuals were also transacting with unrelated counterparties located in remote areas of the country. The suspicion was raised that the individuals were probably involved in Hawala/Hundi.

Mr. DWK was involved in the business of selling raw materials for building constructions. Mr. DWK maintained multiple personal and business accounts at different banks and his transactional activity was unusual comprising of home remittances, online transfers, clearing of cheques, cash deposits and withdrawals. The transactions were conducted with various unrelated counterparties including clearing/forwarding agents, jewellers, car dealers, real estate dealers, overseas Pakistanis etc. A few counterparties were identified to be involved in illegal foreign exchange businesses which strengthened the suspicion of the involvement of Mr. DWK in Hawala/Hundi. During analysis, STRs were also found on the family members of Mr. DWK including 1) Mr. RWK (brother), 2) Mr. TWK (brother), 3) Mr. AUK (brother), 4) Mr. YK (son), 5) Mr. AK (son), whereby similar transactional activity was identified and suspicions were reported. Some of the family members were residing in Country A and involved in businesses related to transport, while a few of them were living in Pakistan and involved in trading businesses.

Flow of Funds: During the analysis, a large number of individuals and their family members were found who were working in country A and they received home remittances from Country A in their accounts maintained in Pakistan. The remittances were subsequently transferred to the accounts of Mr. DWK and family members or withdrawn in cash by the family members of Mr. DWK. The family members also sent/ received funds from unrelated counterparties in Pakistan such as clearing forwarding agents, car dealers/drivers, a gold dealer, property dealers and an import-export business located in remote areas.

Hawala/Hundi: The pattern of transactions, nature of counterparties and rapid movement of funds indicated that the individuals were probably involved in Hawala/Hundi. Furthermore, one of the family members, Mr. TWK, was already under investigation by a law enforcement agency (LEA) for his involvement in Hawala/Hundi. Therefore, it was suspected that the family members were operating a group of Hawala/Hundi in the Buner district, Pakistan.

Gold Smuggling: During analysis, Mr. DWK was found to be under investigation by a law enforcement agency (LEA) in Pakistan for his involvement in the smuggling of gold. The individual was apprehended for smuggling of gold from the airport. The LEA informed that the individual managed to import artificial jewellery against the export of pure gold, which is

in violation of the Procedure for Export of Gold Jewellery and Precious / Semi-Precious Stones and Import Facility.

Car Smuggling: The reporting entity informed that the family members living in Pakistan collect passports from different persons for the clearing of imported cars from customs. Moreover, frequent transactions with car dealers/drivers and clearing forwarding agents were observed. It appeared that these agents apparently provided funds to non-resident individuals, retrieved the funds by remittance via a remitter's own account and obtained a Proceed Realization Certificate (PRC) to use it for vehicle import and to obtain a tax benefit on behalf of the remitter. A Proceed Realization Certificate is also known as an encashment certificate which is issued by the bank to the beneficiary customer at the time of handing over the remittance funds in Pakistani Rupees. Therefore, it was suspected that the individuals were also involved in the unauthorized import of cars.

Based on analysis, it was determined that the group of individuals were suspected of operating a Hawala/ Hundi network in Pakistan and were facilitating the smuggling of different kinds of goods like gold smuggling and the unauthorised import of cars. The financial intelligence was shared with LEAs for the investigation of Hawala and for probing matters related to smuggling.

2. Group of individuals operating an illegal money or value transfer services (MVTS) business (Hundi/Hawala)

Five individuals were suspected of being involved in the business of hundi/hawala due to high turnovers, structured transactions and transactions with unrelated counter parties. Some of these individuals were already under investigation by law enforcement agencies.

Multiple STRs were reported against an individual, Mr. W, by banks due to the high volume/frequency of transactions conducted in his account and transactions conducted with unrelated parties. Upon further analysis and a search in the database, a few more individuals/businesses were found to be linked via multiple factors like similar addresses /geographical locations, contact numbers, transactions to/from accounts maintained by these individuals and a similar nature of businesses. The individuals included Mr. P, Mr. C, Mr. A and Mr. B against whom multiple STRs were reported by different banks too.

The details of the accounts maintained by the individuals were sought from various banks. The individuals were mainly maintaining proprietorship accounts in the names of multiple businesses. The status of the majority of their accounts was active. A high volume of funds was routed through the accounts and turnovers of billions of rupees were noticed in those accounts. The transactions in the accounts were conducted with various individuals/entities engaged in varied and unrelated businesses located in different regions. The individuals declared themselves as the proprietors of various businesses dealing in dried fruits and rice. The individuals were found running their businesses and accounts mainly in AK City which is close to the border area.

From the dissemination database, it was identified that three financial intelligence reports related to the concerned individuals and their associates were already disseminated to a domestic investigation agency on the suspicion of their involvement in the offence of Hundi/Hawala.

The tax database was accessed for further information on the five individuals which showed that all of the individuals were registered with the tax authority and the individuals mentioned different businesses in their tax profiles. The individuals paid a nominal amount of income taxes to the tax authority as compared to the billions of rupees of turnovers in their accounts.

From the activity noticed in the accounts and the businesses being located in a high risk area, the financial intelligence was shared with a domestic investigation agency to further probe into the matter.

Singapore

During an anti-unlicensed moneylending (UML) operation, the Singapore Police Force arrested a local syndicate member (Person A) for collecting and handing over UML proceeds to other persons in Singapore. During an investigation, it was revealed that Person A had on several occasions handed over UML proceeds to a local licensed foreign exchange business (Person B).

Person B was investigated for possible money laundering offences. An investigation revealed that since COVID-19 struck Singapore in 2020, Person B entered into an arrangement with his business partner, an individual operating a foreign exchange business = (Person C) based in Country X, to operate a hawala-like system. They would each maintain a pool of cash in their respective currencies of Singapore's and Country X's. Whenever Person B needed to disburse cash to his clients in Country X, he would arrange for Person C to handover the cash (in Country X's currency) to his clients in Country X, and vice versa. In order to ensure that there was always sufficient cash in their respective pool of currencies, they would arrange for their associates to handover cash to either party, i.e. Person C would get his associates to handover SGD to Person B in Singapore, and vice versa.

Person B confirmed that Person A was instructed by Person C to handover SGD to him, each time ranging between SGD 6,000 (approx. USD 4,362) to SGD 8,000 (approx. USD 5,817), since 2021. The funds would be kept by Person B as the pool of SGD to be handed over to Person C's clients in Singapore. At times, Person C would also request Person B to deposit funds into designated Singapore bank accounts.

A total of SGD 213,215 (approx. USD 155,032) was seized from Person B's foreign exchange business. Investigations are ongoing in relation to the ML charges. As of the time of writing, efforts are underway to reach out to the Country X to seek information on Person C.

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

Japan

Person A created an account under a false name to sell a copied Blu-ray disc for internet auction without notifying the copyright holder. Person A used the account and put up the copied Blu-ray disc for sale on the internet auction. The payment from the individual who made the successful bid was conducted using an online payment system. Person A made the buyer send the funds to a wallet holding bank details which was linked to the aforementioned false account. After that, the money was transferred to person A's bank account.

Nauru

The FIU received a report of an Advance Fee fraud scam operated out of country A. This involved the use of identity fraud whereby the profile of a Nauru member of Parliament (MP) was used by the offender purporting to be the MP.

Victims were sent a friend request by the suspect and persuaded to apply for a grant which the suspect claimed was a United Nations funded scheme. The suspect advised victims that the scheme could be used for starting a new business, education for children, disabled persons, widows etc. The suspect communicated via an online messaging application and victims were sent a link which led to another person, person A, purportedly an agent of the suspect.

Victims were then persuaded to make a payment to the account located in Country A of another suspect person. It was highly suspicious that a single person was impersonating three different people while changing profile pictures on an online messenger application. One of the victims from Nauru paid AUD 2,500 (approx. USD 1,707), but later after checking with the MP realised it was a scam.

The matter was already reported to the police, but the FIU escalated the matter to Country A's FIU, whereby Country A's FIU confirmed that the suspect was under investigation by an LEA in Country A. Unfortunately, funds for the victim could not be recovered. The FIU issued an alert notice advising the citizens of Nauru to exercise caution.

Philippines

The case pertains to an alleged sextortion incident involving individual FC and an unknown individual with the username MZ, whom the former met through a social networking site "Instagram". After meeting through Instagram, FC and MZ continued their conversation and engaged in a nude video call through a messaging application called Line. Thereafter, MZ sent screenshots of their nude video to the victim's contacts on Instagram and demanded USD 400 to be sent to a local bank account, otherwise her nude video would be published online. A database search on MZ pointed to a certain individual ZM whose pattern of transactions suggests that MZ and ZM are probably the same person. Confidential information exposed that ZM received remittances from senders in country A and country B. These senders disclosed in an interview that the funds were sent as a "blackmail payment" to keep their private videos from being released to the public.

5.7 Use of new payment methods / systems.

Hong Kong, China

In mid-2021, Hong Kong Police identified an organized crime group engaging in illegal gambling and drug trafficking activities. An operation mounted against the organisation resulted in the arrest of 317 persons and the seizure of HKD 735,000 (approx. USD 93,672) in cash in late 2021. A parallel financial investigation revealed that at least HKD 1.35M (approx. USD 172,055) of drugs proceeds were laundered through bank accounts, stored value facilities and the Faster Payment System (a payment financial infrastructure enabling payments across different banks and stored-value facilities on a 24/7 basis introduced in 2018) by the drug

traffickers. HKD 1.35M (approx. USD 172,055) was withheld in the identified accounts and an investigation is ongoing.

Indonesia

In 2021, the Indonesian Police collaborated with the Indonesian FIU (PPATK) and related authorities to target crimes in illegal information technology-based lending and borrowing services (peer to peer lending).

There are at least 89 cases that have been identified involving 65 suspects, of which four involve foreign nationals. As for several cases of illegal peer to peer lending, including company A with business names including Vloan and fintech applications available in the marketplace, including Supercash, Rupiah Cash, Super Funds, Plus Loans, Super Wallets and Super Loans.

Company A is not based in Indonesia and the location of the Vloan application server is located in country A with hosting servers in country B. Company A used payment gateway services to send loan funds to customers. If in the process of 7 to 14 working days the service user returns the loan, Company A, through the payment gateway, provides a Virtual Account number from each bank account in the name of Company A.

In addition, there were also cases of illegal peer to peer lending involving Company B. The Indonesian Police have identified 13 suspects with details of seven suspects acting as debt collectors, four suspects consisting of two foreigners and two Indonesian citizens who are directors of Company B. One foreigner is the owner of the Joint-Owned Innovation Savings and Loan Cooperative which has an illegal peer to peer lending service application and another person registered a sim card illegally. The Indonesian Police have blocked and confiscated an account belonging to Company B which was used as a repository for funds with a nominal amount of IDR 239 billion (approx. USD 16 million).

Japan

CEO A of V company and individual B of an affiliated company scammed an individual by informing them that the individual's membership fee for an e-commerce site was unpaid and instructing the individual to pay 50 thousand yen (approx. USD 384) by purchasing pre-paid cards and informing them of the card numbers. After obtaining the card numbers from the individual, they resold the numbers. They concealed the proceeds obtained by the illicit resales, approximately 37 thousand yen (approx. USD 284), in B's bank account. Finally, they were arrested on the charge of the violation of the Act on Punishment of Organized Crime and Control of Crime Proceeds (Concealment of Criminal Proceeds etc.).

Singapore

This case involves the misuse of payment service providers, more specifically via virtual accounts. Virtual accounts are typically offered by banks to their selected corporate clients, such as payment service providers, to allow for the easier identification of their various payers and the purpose of payments for reconciliation purposes.

A Singapore victim of a business email compromise fraud scheme was persuaded into transferring funds to a virtual account maintained by a Singapore bank. Investigations revealed that the Singapore bank had offered virtual account services to a payment service provider operating in Country Y. In turn, the payment service provider operating in Country Y assigned virtual accounts to its clients. The virtual account was later traced to an individual based in Country X.

The proceeds were successfully intercepted. Efforts are underway to ensure the return of these funds to the victim.

5.8 Laundering of proceeds from tax offences.

Fiji

Case Study: Tax Evasion

Mr. X was reported to the Fiji FIU for possible tax evasion and ML following a cash deposit of FJD 34,250 (approx. USD 15,840) that he conducted into the bank account of Night Club A. Mr. X is the owner of Night Club A and the cash deposit was allegedly sourced from the club's overnight sales.

Fiji FIU analysis established that Mr. X is a business taxpayer, who has not lodged his income tax returns since 2006. In addition, Fiji FIU analysis established that Mr. X also operates and trades as Bottle Shop B, Tyre Shop C and Liquor Land D. However, he had not registered his Liquor Land D business activity with the Fiji Revenue & Customs Service for tax purposes.

Fiji FIU analysis further established that during the 2020 – 2021 pandemic period when all night clubs were closed, Night Club A's bank account continued to receive deposits whereby large cash deposits, FJD 10,000 and above (approx. USD 4,624) totalling approximately FJD 3.9 million (approx. USD 1,803,700) were conducted from 2019 to 2021. Within the same time period, Liquor Land D conducted large cash deposits of FJD 10,000 and above (approx. USD 4,624) totalling approximately FJD 883,000 (approx. USD 408,376).

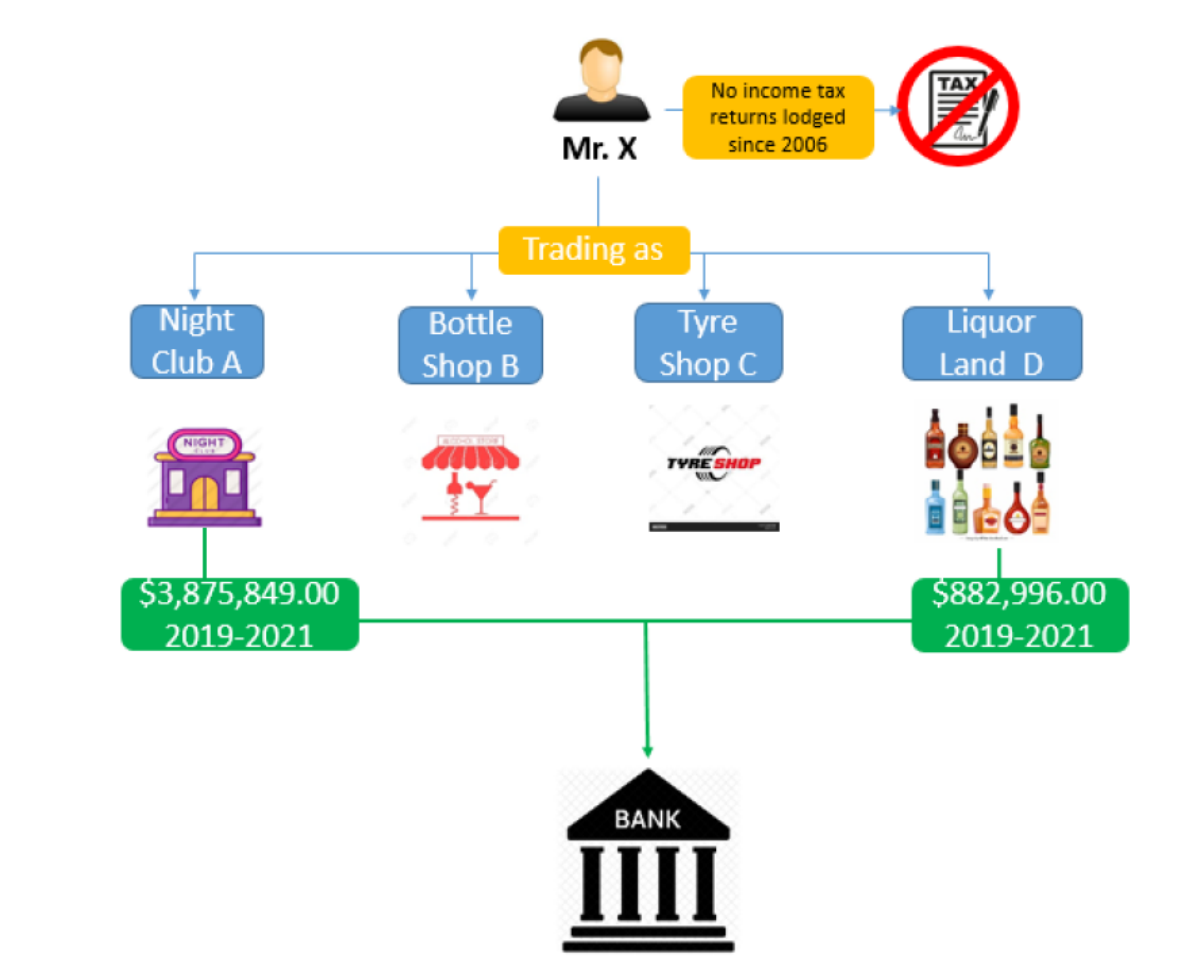
A case dissemination report was provided to the Fiji Revenue & Customs Service (FRCS).

Indicators:

- Frequent large cash deposits from a business that was closed.
- Business not registered with FRCS for tax purposes.
- Tax returns not lodged for a number of years.

Possible offence:

- Tax related offence/tax evasion
- Money laundering



Indonesia

Mr. RW is Director of Finance and Operations of Company A. Individual DC credits invalid tax invoices obtained from taxpayers from tax invoice issuers that are not based on actual transactions where the credited value-added tax (VAT) was purchased at a price of approximately 25% of the value of VAT.

RW credits the tax invoices which are not based on actual transactions and have never been issued and reported the output tax on behalf of Company A. DC. Then Mr. RW, in order to make it look as if there was an actual purchase transaction, used an invalid tax invoice as a proof of payment voucher (as if to pay for the purchase of goods) accompanied by a cheque and giro transfer to Company A. The cheque and giro transfer amounted to taxes totalling IDR 12,021,810,949 (approx. USD 825,051).

The cheques and giro transfer were never received and disbursed for the companies issuing the tax invoices, but were disbursed into the accounts of Company A. Individual DKJ disbursed cash and transferred funds out of the defendant's personal account to the account of Company A. In 2011, from the total amount of IDR 42,997,126,116 (approx. USD 2,951,642), DKJ disbursed IDR 1,103,305,500 (approx. USD 75,712) including an amount of IDR 347,526,637 (approx. USD 23,853) that was disbursed to RW's personal account. The money was then used by RW to buy a number of apartments with a total price of IDR 5,225,128,328 (approx. USD 358,498).

The money obtained by RW from the proceeds of tax crimes by using tax invoices that are not based on actual transactions in 2010 – 2011 was IDR 10,254,308,910 (approx. USD 703,741). The funds were used by RW to buy properties by means of payments in cash and also by means of transfers. RW then sold the apartments that he purchased with the intention of concealing the source of funds which were the proceeds of tax crimes, namely the proceeds from the sale of fictitious tax invoices (FPTBTS) or tax invoices that are not based on actual transactions.

Mongolia

Case 1

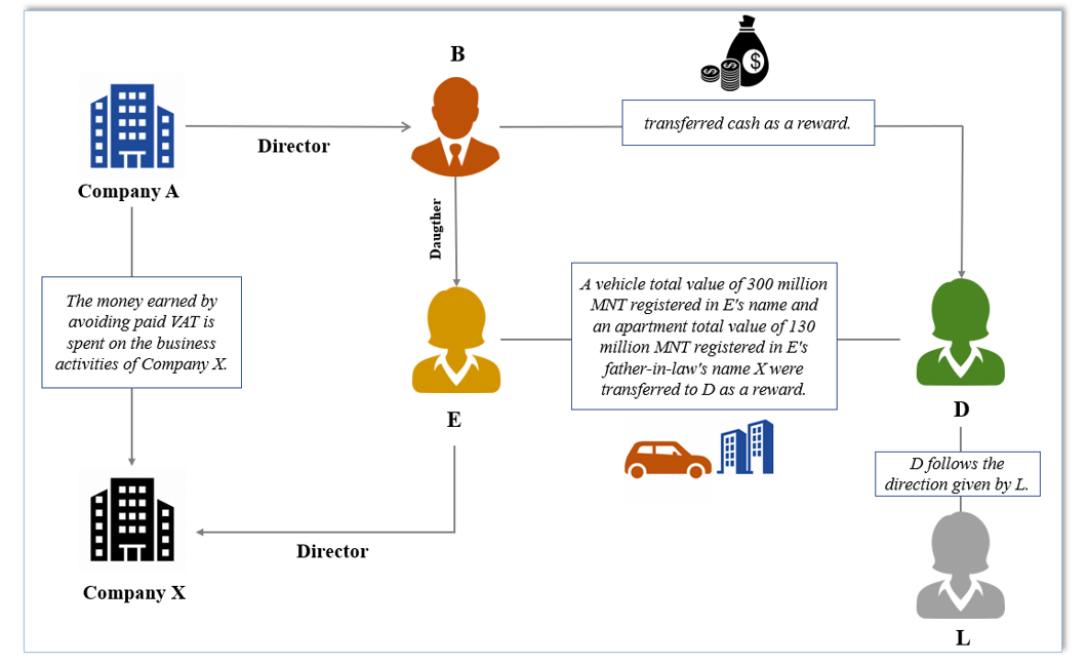
An LEA opened a criminal case under Articles 18.3 and 18.6 of the Criminal Code of Mongolia for allegedly evading large amounts of taxes paid to the state by a group of persons.

Director B of Company A signed an illegal contract to provide a "Financial advisory service" to person D who is unemployed in order to conceal the company's operating income between 2017 and 2020 and to deliberately avoid paying VAT of MNT 3.5 billion (approx. USD 1,118,113) which is 10 percent of MNT 35 billion (approx. USD 11,179,714). With this intention, they aimed to make a false record of MNT 3.5 billion VAT (approx. USD 1,118,113).

Person D and L made a false entry in the database of the General Department of Taxation of Mongolia as it appears that purchases were made from three legal entities to cover MNT 3.5 billion (approx. USD 1,118,113)VAT debt of Company A.

It was found that the above-mentioned group of persons were rewarded MNT 300 million (approx. USD 95,825) worth of vehicles, MNT 130 million (approx. USD 41,509) worth of apartments, MNT 140 million (approx. USD 44,702) in cash and MNT 50 million (approx. USD 15,967) through wire transfers to their bank accounts for facilitating illegal tax evasion for Company A.

Authorities seized a total amount of MNT 275,120,000 (approx. USD 87,857) in cash, 190 pieces of jewellery, one apartment, and four vehicles.



Case 2

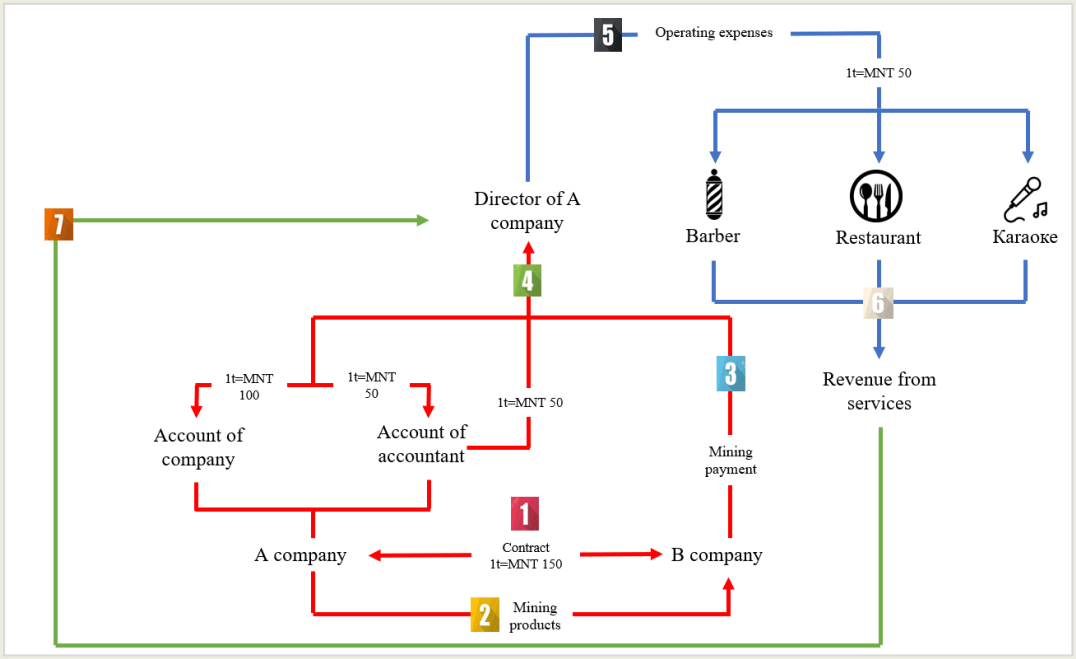
Company A is a mining company and Company B is a manufacturer of spare parts for heavy equipment.

The two companies have entered two types of contracts for the transportation of mining products (with an intention to commit tax evasion). One agreement was to sell one tonne of mining products for MNT 150,000 (approx. USD 47). The second agreement was a fraudulent contract for the lower price of MNT 100,000 (approx. USD 31) and the purpose of the second agreement was to pay less tax than is meant to be paid to the tax authority. Accordingly, the tax was paid by deducting MNT 50,000 (approx. USD 15) from each tonne of mining products supplied by Company A to Company B.

When Company B made the contract payment, it transferred the amount of MNT 100,000 (approx. USD 31) per one tonne of mining products to Company A's account and wired the amount of MNT 50,000 (approx. USD 15) per one tonne of mining products to an account of Company A's accountant. Afterwards, an accountant of Company A withdrew the money in cash and sent funds via multiple wire transfers and gave the funds to the director of Company A.

The director of Company A then spent the illicit funds generated from tax evasion on the operations of Company A as well as his own personal expenses, effectively mixing the illegitimate proceeds with legitimate funds.

The case is currently under investigation.

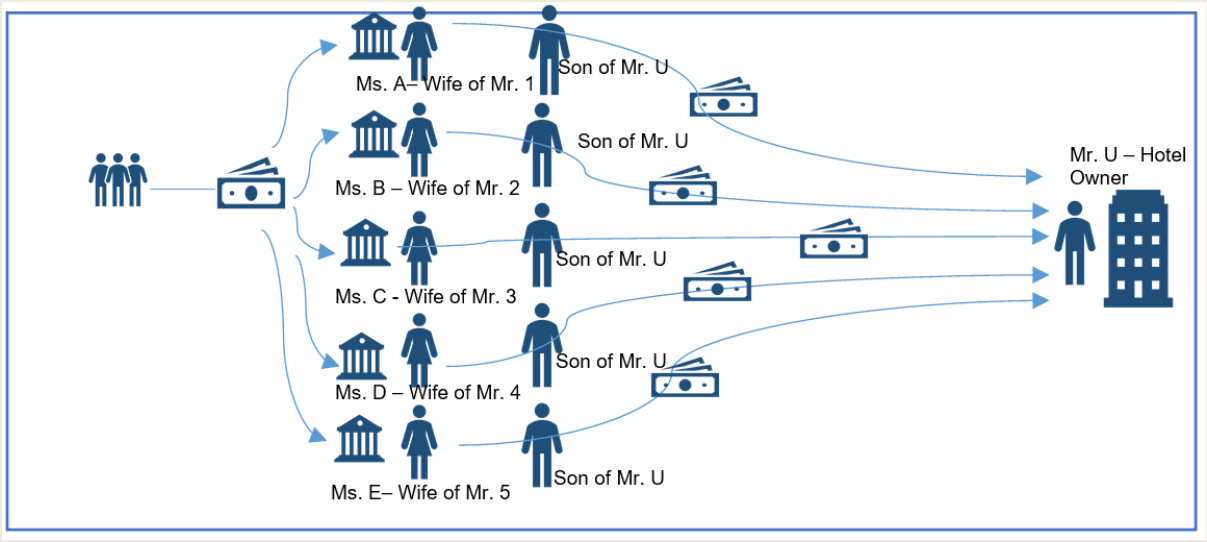


Pakistan

Routing of funds to family member accounts for tax evasion

STRs related to housewives associated with each other by different family relationships were reported to the Financial Monitoring Unit (FMU) as they were receiving large cash deposits into their accounts without any valid justification. The transactional activities of these housewives did not match with their profiles.

During the analysis at FMU, the linkages through the goAML software solution were identified which revealed that the reported housewives were linked to the same family. Their father-in-law was the owner of famous hotel in Pakistan. The following is a diagram showing the family and the movement of funds.



The family members opened multiple accounts in the same bank and every housewife was maintaining a separate bank account for herself. During the review of the statements of accounts of the daughters and daughters-in-law of Mr. U, it was identified that all of these accounts were opened in May 2016 and a large amount of cash was deposited into all the accounts in same manner. Mostly the funds were deposited into the accounts through structured transactions in order to avoid currency transactions reports (CTRs). Subsequently the funds were transferred to Mr. U's account.

The pattern of transactions followed by the housewives indicated that Mr. U might have been routing business proceeds through cash deposits to his family members' (daughters and daughters in law) accounts and later on funnelled the funds to his own accounts to avoid paying income tax. Mr. U might be the beneficial owner of the funds deposited and withdrawn from his daughters' and daughters' in law accounts.

A record of the tax history of the housewives revealed that they had paid a reasonable amount of tax initially, but gradual decline in the amount of tax paid was noted during later periods and no tax was paid at all in the most recent year. Based on the findings, the financial intelligence was shared with an LEA for further investigation.

Philippines

Tax Evasion

This case relates to the request of an FIU for information on Mr. X and his family members and a possible associate. The FIU believed that Mr. X may have understated his income earned in the Philippines on his personal income tax returns from 2015 to 2018. Apparently, this pertains to the principal violation of tax evasion in that foreign country.

The subject and his wife were born in the Philippines. Mr X became a naturalised citizen of the requesting FIU's country in 2010. However, he frequently travelled back and forth to that specific country and the Philippines. According to the information obtained by the FIU, Mr. X was employed as the Chief Risk Officer and Vice President of Business Processes of a transnational company located in the Philippines since 2014.

Mr. X was reported in 410 covered transaction reports (CTRs) with the total reported funds amounting to PHP 1.191 billion (approx. USD 22,681,469) from 4 April 2006 to 21 December 2020. For the period 2015 to 2018, the said subject might have understated his income and tax returns while employed in the Philippines. It was further observed that in February 2015, the subject sent international transfers to accounts of his wife and a presumed relative maintained in the Philippines amounting to PHP 22.134 million (approx. USD 421,548).

Submitted income tax return (ITR) does not support declared monthly income during account opening

A client made several suspicious transactions valued at PHP 1.92 billion (approx. USD 36,570,375). The client owned a business engaged in wholesale/retail of electronic devices and hardware supply, with a declared monthly income of PHP 9 million (approx. USD 171,423). The bank reportedly identified the client as blacklisted due to alerts generated, resulting from the subject's high volume of cash deposits that were subsequently withdrawn. A review of the

subject's account movement also showed similar attributes of being a pass-through account due to the high volume of deposits which were subsequently debited mostly through cashing cheques and cheque issuances. It was further noted that while the client submitted business documents, such as an ITR and receipts/sales invoices (mostly issued to individuals), the substantial transactions were deemed not commensurate with the client's declared income. Moreover, the amounts of sales and net income reflected in the submitted ITR were only PHP 140,000 (approx. USD 2,666) and PHP 20,000 (approx. USD 380) respectively.

Singapore

In December 2021, seven Singaporeans were recruited to travel to Country Z to commit value added tax (VAT) fraud. Each of them received two pieces of fake jewellery, a false invoice and a completed VAT refund claim form. Investigations showed that the jewellery was quoted at grossly inflated prices in order to qualify for VAT refund claims at Country Z. The accused persons intended to make the refund applications at Country Z's airport before taking a return flight back to Singapore. Three of the seven suspects' applications went through, and the acquired funds were handed to their recruiter in Singapore.

Investigations revealed that the jewellery store's purported operating premises had in fact never been tenanted before. This suggests that the transactions were invalid.

As the VAT refunds were fraudulent, they were considered to be the proceeds of crime. In bringing the VAT refunds back to Singapore and delivering it to the recruiter, the parties involved had possibly committed ML offences.

Investigations are ongoing for this case.

5.9 Real estate, including roles of real estate agents.

Philippines

Transactional activity (substantial cash deposits) deviates from nature of business (a real estate business)

Two likely related entities were involved in several suspicious transactions with an estimated value of PHP 6.12 billion (approx. USD 116,050,274). Both entities were engaged in real estate activities and simultaneously opened joint automatic transfer accounts in August 2019. The majority of the questionable transactions include cash deposits, ranging from PHP 10 million (approx. USD 189,638) to PHP 300 million (approx. USD 5,689,153) per transaction, with an estimated total value of PHP 4.89 billion (approx. USD 92,736,497), which were transacted between September 2019 and March 2020. The registration records presented by both entities showed approvals of similar dates (i.e., April 2019, May 2019). Based on the covered persons' customer due diligence (CDD) checks, both entities are assessed as start-up companies and the nature of business is not considered to be cash intensive. The substantial flow of cash deposits into both entities' accounts is viewed as not commensurate with and a deviation from their financial capacity and profile.

The extensive use of substantial cash is viewed as a red flag, considering the entities' nature of business. Aside from doubts as to the actual source of funds, it is also possible that the actual proceeds derived from the businesses are unreported for tax purposes.

Singapore

Between 2017 and 2020, a Director of a security company gave bribes amounting to SGD 121,000 (approx. USD 87,911) to an employee who was in charge of the security contract of a department store. The bribe was given in return for the department store's employee not issuing liquidated damages to the security company for under-supplying manpower. The liquidated damages of SGD 419,934 (approx. USD 305,093) were deemed to be the benefits derived from the corrupt act.

Between October 2017 and May 2021, the company used part of the benefits, i.e. SGD 247,551 (approx. USD 179,869, to fund the down-payment and monthly property loan instalments of a shop unit purchased for SGD 1,150,000 (approx. USD 835,584).

The Director of the security company was convicted of corruption and sentenced to ten months' imprisonment. The bribe receiver was also convicted of corruption and sentenced to ten months' imprisonment together with a penalty of SGD 42,500 (approx. USD 30,883). Investigations against the legal person, i.e. the security company, for ML offences are ongoing.

5.10 Trade in gems and precious metals.

Hong Kong, China

Mr. A was the owner of a local seafood trading company which had a business partner in Jurisdiction X. In mid-2021, Mr. A met Mr. B who offered a remittance service to Jurisdiction X with a better exchange rate. Upon the instruction of Mr. B, Mr. A transferred HKD 3M (approx. USD 382,354) to a bank account held by a gold trading company (Company C) for remittance to his business partner in Jurisdiction X. Mr. B informed Company C that the funds were transferred as payment for purchasing HKD 3M (approx. USD 382,354) worth of gold bars and he later collected the gold bars from Company C. Mr. A's business partner confirmed the funds were not received which revealed that it had been a scam. Mr. B was arrested after an investigation, but the gold bars could not be retrieved. HKD 3M (approx. USD 382,354) was withheld in Company C's bank account. An investigation is ongoing.

5.11 Association with human trafficking and people smuggling.

Hong Kong, China

Hong Kong Police and Jurisdiction X jointly dismantled a human smuggling syndicate, which provided forged identity documents and arranged passage for illegal immigrants from Jurisdiction X to travel to Jurisdiction Y via Hong Kong, China. A total of 11 syndicate members were arrested in the synchronised raid in Hong Kong, China and Jurisdiction X. A subsequent financial investigation revealed that transactions amounting to HKD 3.5M (approx.

USD 446,146) were incommensurate with their financial background and showed signs of ML. An investigation is ongoing.

Indonesia

Case 1

The Indonesian FIU, PPATK, traced transactions through the International Funds Transfer Instruction (IFTI) database and Open Source Intelligence (OSINT) media. It was found that parties suspected of being linked to a people smuggling network (led by AS) were arrested in Majalengka. The parties suspected of being the recipients of migrant workers/trafficked persons are SSA, a citizen of Jurisdiction A, SSR, a citizen of Jurisdiction B, and BAS, a citizen of Jurisdiction C.

The Indonesian citizens who sent funds from Jurisdiction A, AS and NF, are suspected of acting as distributors/facilitators, while those in Indonesia who are suspected of being suppliers are AHY, AF, WK, and SRM. HJT is suspected of being the recipient of funds in Indonesia during the period 2018-2020. It is suspected that AS' people smuggling network engaged in ML by using money remittances to conceal the source of funds. In addition, distributors/facilitators were used to disguise the source of the sender and the destination of the recipient of funds. The funds that enter and are managed by this network are also allegedly used for its business operations.

Case 2

Mrs. LH (Indonesian citizen) together with a citizen of Jurisdiction D named IKH were arrested in a Jakarta apartment on the suspicion of people smuggling. The Indonesian Financial Transaction Reports and Analysis Center (PPATK) analysed records of international funds transfers and identified a flow of funds to Indonesia from high-risk people smuggling countries such as Jurisdiction E, Jurisdiction F, Jurisdiction D, Jurisdiction G, Jurisdiction H, Jurisdiction I and Jurisdiction J.

LH was recorded to have travelled to Jurisdiction E twice in February 2020. Most of the cross-border funds she received came from Jurisdiction E. LH admitted that she acted as a collector of funds from overseas distribution agents. One of the parties suspected of being the recipient of migrant workers/people trafficked abroad is AFA. AFA is suspected of actively traveling to several countries at high risk of human trafficking. Based on the identified transactions, AFA transferred funds from Jurisdiction G, Jurisdiction D and Jurisdiction J.

It is suspected that this network committed ML offenses using transaction methods involving money remittance and pawnshops, which are aimed at obscuring the source of funds and avoiding reporting. The funds that come in and are managed by this network are also allegedly used for business operations such as renting apartments and tickets for overseas trips.

Philippines

A mother and daughter with an address abroad were allegedly involved in human trafficking. Apparently the two identified suspects harboured undocumented immigrants in a foreign

country by assisting and providing them with shelter in exchange for money. The two suspects were believed to have purchased a house through a mortgage loan and collected money from undocumented immigrants as their tenants. It was identified that the suspects had investments in several countries abroad and that the daughter had utilised a bank account in their area of residence to conduct wire transfers. The suspects received an estimated USD 90,000 annually in illegal profits from harbouring undocumented immigrants.

Notable transactions identified were three international remittances totalling PHP 4.4 million (approx. USD 83,163) from 2018 to 2020 sent by the daughter to the bank account of her mother. Two inward remittances were also identified in June 2010 totalling PHP 1,378,500 (approx. USD 26,053) made in favour of a certain individual.

In addition to the aforementioned facts, the following are possible suspicious indicators of the financial transactions: a) transfer of funds is sent by the daughter, who is known to be involved in human trafficking; b) suspect's transactions pertain to international remittances in large amounts wherein most of them are credited to the accounts maintained in domestic banks; and c) the large transfer of funds from one account to another. Same day withdrawals were also observed from another account with the same bank or with other banks which correspond to large deposits from one account to another. It is possible that the high value transactions are proceeds from the illegal activity of sheltering and concealing undocumented immigrants.

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

Fiji

Case Study: Internal Theft

Mr. K was brought to the attention of the Fiji FIU in a request for financial information from a law enforcement agency. Mr. K was under investigation for fraudulently appropriating over FJD 3 million (approx. USD 1,404,946) from his employer between December 2018 and March 2021.

Mr. K is a senior officer who fraudulently transferred funds from his employer's bank account to his personal bank accounts and other business bank accounts, and concealed his fraudulent activity by manipulating his employer's accounting records and system. Mr. K allegedly received a commission from businesses whose bank accounts received the fraudulent funds.

Mr. K was also brought to the attention of the Fiji FIU in a suspicious transaction report on his spouse, Mrs. K, for unusual financial activity involving the use of their daughter's (Ms. K) savings account to conduct large transactions. One of the large transactions was a FJD 150,000 (approx. USD 70,247) inward international remittance from Company A in a foreign country.

Mr. K was brought to the attention of the Fiji FIU in another suspicious transaction report involving a FJD 1.5 million (approx. USD 702,473) loan provided by Mr. K's entity, Company K, to Company B in Fiji as financial support for a land subdivision development project. Mr. K and Company K were reported when Company B did not receive any response regarding the delay in loan repayments, which raised suspicions, particularly on the source of the loan funds.

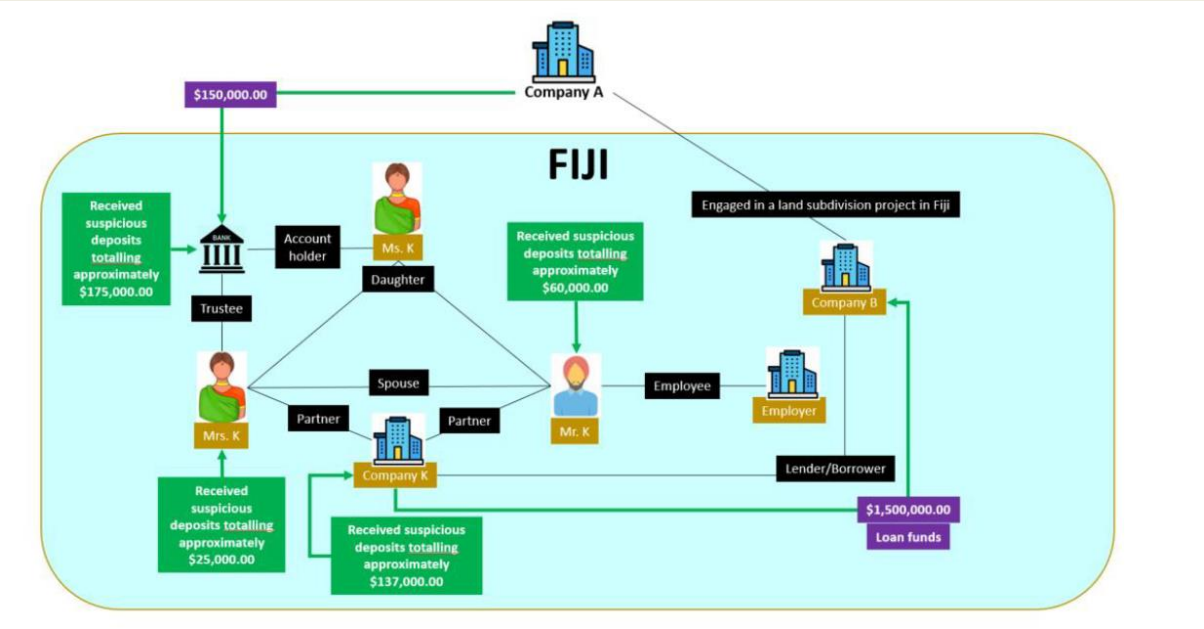
Fiji FIU analysis established that Company B and Company A were related parties as both entities were engaged in the same land subdivision development project.

A case dissemination report was provided to the Fiji Police Force.
Indicators:

- Regular receipt of unusual deposits that are inconsistent with the bank account holder's financial background.
- Use of a minor's savings account to conduct unusual transactions.
- Loan products offered by unlicensed and/or unregistered financial institutions or service providers.

Possible offence:

- Fraud
- Bribery



Indonesia

Observations:

Based on PPATK's (Indonesia FIU) research on ML typologies in 2021, the following related parties were used to commit ML in the following percentage of cases:

RELATED PARTIES	2019	2020
Colleagues	59,1%	51,8%
Stranger	0,0%	14,0%
Spouse	13,6%	13,2%
Family Members	4,5%	6,1%

Singapore

Case Study 1

Two Singaporean nationals created and operated a multi-tiered professional ML network that involved recruiting friends and family members as money mules. They had been introduced to a business opportunity by friends based in Country A to contacts in Country A and subsequently agreed to assist these contacts in Country A to launder criminal proceeds.

In addition to receiving criminal proceeds via their own bank accounts, the duo recruited seven individuals to similarly use their bank accounts to launder scam proceeds.

From December 2013 to June 2017, a total of 25 corporate and individual bank accounts were used to receive approximately SGD 1.35 million (approx. USD 984,890) of criminal proceeds. Some of the funds were then withdrawn in cash and transported to criminals in Country A without making the requisite border declaration on 32 occasions.

One of the two masterminds was convicted of ML and sentenced to imprisonment of 84 months and 4 weeks while court proceedings against the other is still ongoing. Two of the seven individual mules have also been convicted and sentenced to periods of imprisonment between 3 to 10 months. Prosecution is still in progress against the remainder of the seven individual mules.

Case Study 2

Police investigations led to the arrest of seven foreigners in Singapore who were allegedly recruited by a syndicate based in Country A to transfer criminal proceeds from technical support scams perpetrated in Country B.

These scams involved the perpetrators deceiving victims into granting them remote access to their computers on the pretext of receiving a refund for software subscriptions, but instead stealing their victims' internet banking credentials and transferring money out from the victims' bank account.

Students were directed by the syndicate to receive the funds derived from various tech support scams through unknown overseas sources into their personal bank accounts. From August 2020 to September 2020, they collected more than SGD 300,000 (approx. USD 218,853) in that manner, later withdrawing the money to hand over to unknown individuals in Singapore. In return, they were given about SGD 30,000 (approx. USD 21,885) in commission.

The accused persons have been convicted and sentenced to a range of 6 to 40 months' imprisonment for ML offences and offences under the Payment Services Act, namely carrying on a business of an unlicensed payment service.

Solomon Islands

The FIU received an STR on Person A who deposited SBD 30,100 (approx. USD 3,696) into her personal bank account and claimed that it was for the purchase of land (no proof provided).

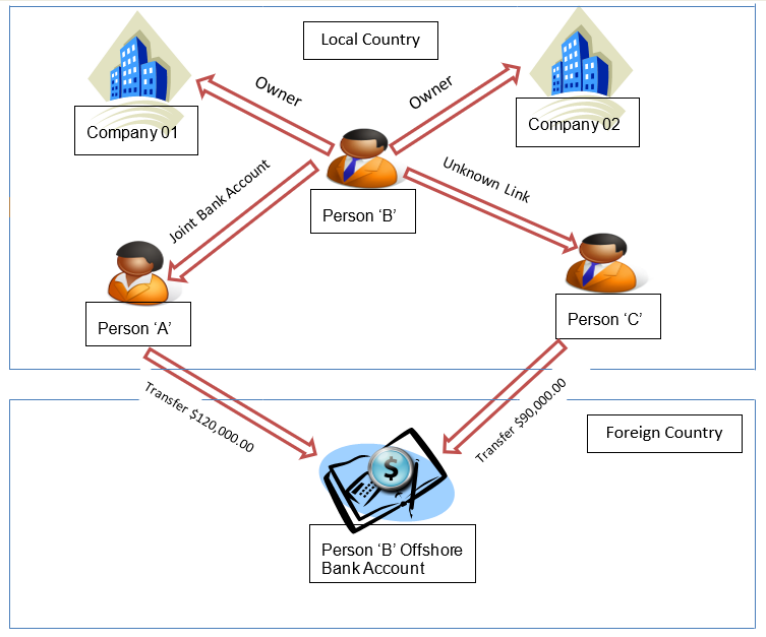
A week later, around SBD 30,000.00 (approx. USD 3,684) (minimum threshold limit)) was transferred to Person B's personal bank account who resides offshore in a foreign country. When conducting profiling on Person A, it was revealed that she is a public servant (government employee) earning less than SBD 1,000 (approx. USD 122) fortnightly. Person B on the other hand is a foreigner and business partner of Person A. The FIU conducted an analysis of the bank accounts owned by Person A and it was revealed that she has a joint bank account with Person B.

In addition, analysis of Person A's bank account revealed that there were other similar transactions conducted into the bank account within a period of four months (Aug-Nov 2021). Moreover, there were five transfers made totalling SBD 157,000 (approx. USD 19,281) where four of the transfers went into Person B's offshore account and one was for the import of miscellaneous goods.

In addition, the FIU also found that there was an STR raised that has links to Person B. Based on the STR, it was revealed that Person C conducted similar transactions to Person A during the same period (October to November 2021). Around SBD 30,100 (approx. USD 3,696) was deposited into Person C's personal bank account (claimed to be for the purchase of a vehicle) and then SBD 30,000 (approx. USD 3,684) was immediately transferred into Person B's offshore bank account on the same day.

Based on the profiling conducted on Person B, it was revealed that Person B owned two companies. However, there were no bank accounts created or maintained for the two companies.

After conducting its analysis, the FIU disseminated two Case Dissemination Reports to relevant Law Enforcement Agencies (LEAs) on the assumption that this was a case of Tax Evasion and ML by Person B.



5.13 Use of shell companies/corporations.

Hong Kong, China

A financial investigation into Mr. A, an organised crime group member, revealed that he had established a trading company and an associated corporate bank account in mid-2021. There were immediately 69 deposits totalling HKD 8.3M (approx. USD 1,058,005) and USD 12.5M into the account and the funds were swiftly withdrawn. As the transactions were incommensurate with the financial profile of Mr. A and his company, it was believed that the funds in question were the proceeds of crime and the trading company was a shell company laundering the aforementioned proceeds. Mr. A was arrested in early 2022 and authorities froze around HKD 734,000 (approx. USD 93,563) in the account. An investigation is ongoing.

Indonesia

Case 1

Mr. HB together with Mr. MDS, Mr. BA, and Mr. IM were asked by Mrs. NA to establish a fictitious company and a company account that would receive funds to be sent from abroad. The three companies were named Company A, Company B and Company C. The compensation received by the four perpetrators was 15% of the total funds received and was to be divided equally among each of them. The company documents such as the deed of establishment, business license, company registration were all forged documents.

After Company A's account was successfully created, on 16 May 2019, there was an incoming transfer received of 4.9 million Euros or around IDR 79,035,806,380 (approx. USD 5,477,158). The funds belonged to a company from Country A, Company D, which was successfully hacked by a foreigner named Mr. JEA through the takeover of the emails of the Financial Treasurer of Company E and Company D in order to execute the company's account transaction at XX Bank to XY Bank.

The funds that had entered Company A's investment account were then transferred to the defendant's account and cash withdrawals were then made. The cash was then deposited at a foreign exchange business and then handed over to Mrs. NA who handed the funds over to Mr. JEA. In return, Mr. HB received approximately IDR 2 Billion (approx. USD 138,607), Mr. BA received IDR 2 Billion (approx. USD 138,607) and Mr. MDS received IDR 45 Million (approx. USD 3,118).

Case 2

EN (Indonesian Citizen) acted as the recipient of funds from a narcotics business network (RK and ED) in country A. The network bought and sold narcotics from prisoners in three High Risk Narcotics Correctional Institutions in Indonesia. EN established companies offering services such as maintenance, IT, e-commerce, travel etc. Proceeds for the narcotics trade were received through personal accounts or 12 companies founded by EN who acted as the companies' management. EN then transferred funds abroad to companies he controlled in several countries, attaching invoices for the purchase of heavy equipment, website design, website creation and the purchase of computer equipment.

Macao, China

Case: Use of shell companies and use of family members

The Macao, China Government launched the "P Fund" subsidy program in 2007 to support non-profit educational institutions in promoting their developmental educational programs. Suspect J was the computer equipment and after-sale services supplier of V Secondary School in Macao, China, and Suspects K and L were the principal and vice principal of V Secondary School. Since 2013, Suspects J and K plotted and arranged that Suspect J would help formulate proposals and budget plans for V Secondary School with the intention to mislead the "P Fund" in granting a subsidy. Suspect L later joined this scheme.

Suspect J set up six companies with Suspect M (J's mother) and Suspect N (J's sister) respectively. Together with his own existing company, J used these companies to bid for the activities and projects of V Secondary School subsidised by the "P Fund", including construction projects. During the course of the crime, Suspect J created false proposals and with the help of Suspects K and L, undertook the subsidised projects without other competitors. However, many of the construction and projects were not completed. Meanwhile, Suspects K and L gave an inaccurate account of the execution status of the concerned projects and construction during an inspection by government officers, thereby misleading the "P Fund" into granting MOP 29,000,000 (approx. USD 3,588,979) worth of funds. The majority of the funds, with only a small amount of funds used for construction and activity costs, were received by Suspect J, who then made multiple transactions between various bank accounts of the companies established by him with his family members M and N. Suspect J finally transferred the funds back to his personal bank account before sharing it with the other four suspects.

In this case, the five suspects defrauded the government by falsifying information to mislead the authority into granting the "P Fund" subsidy. The suspects also disguised the illicit source and destination of the proceeds by making multiple transfers between accounts in different banks. Suspects J, M and N were charged with fraud, the falsification of documents and ML by the Macao, China Public Prosecutions Office in 2021, with Suspects K and L charged with fraud and the falsification of documents.

Singapore

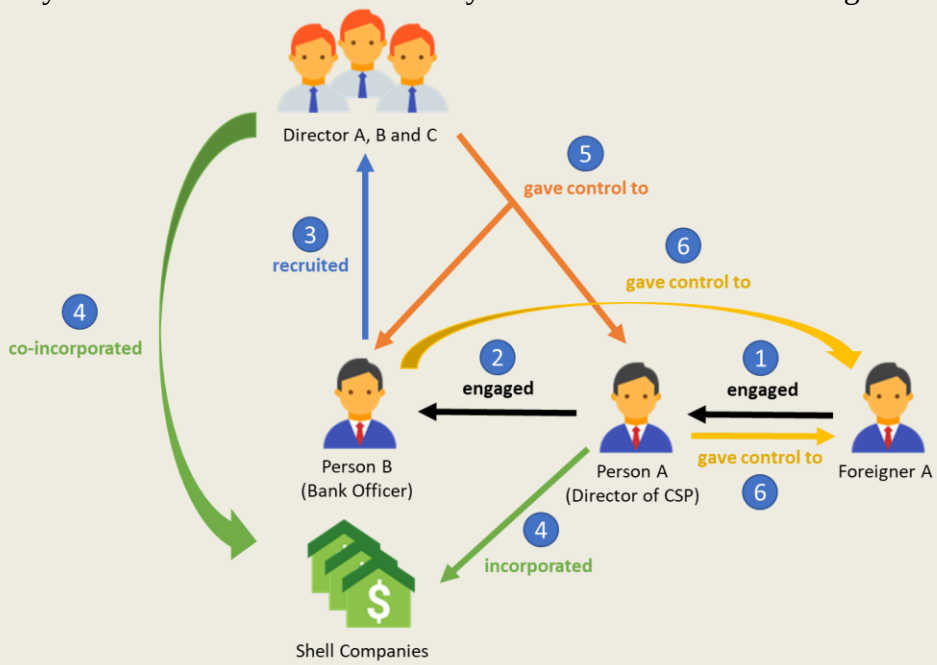
Two professional intermediaries and three directors of Singapore-incorporated shell companies were prosecuted for their alleged involvement in laundering criminal proceeds.

Between 2016 and 2019, the Commercial Affairs Department of the Singapore Police Force (CAD) received police reports from scam victims who were allegedly deceived into wiring a total of USD 1,676,737 into the corporate bank accounts of Singapore-registered companies. Follow-up investigations revealed a professional ML syndicate, which comprised five individuals and seven shell companies, that was involved in the laundering of proceeds from the scam incidents.

CAD found that Person A, a director of a corporate secretarial services provider, was engaged by an unidentified Foreigner A, believed to be engaged in criminal conduct, to incorporate shell companies in Singapore and set up their respective corporate bank accounts. As part of the incorporation process, Person A allegedly engaged Person B, who was a bank officer at that

time, to recruit individuals, i.e. Director A, Director B and Director C, to act as directors of the shell companies. Thereafter, control of those corporate bank accounts was transferred to Foreigner A via Person A and Person B.

From March 2021 to April 2021, Person A and Person B were charged for ML offences. Director A and C were also charged with failing to carry out their director duties honestly and exercise reasonable diligence. Director B was charged with ML offences and with failing to carry out their director duties honestly and exercise reasonable diligence.



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

Hong Kong, China

Case 1

Intelligence suggested that 23 virtual bank accounts, which shared the same prefix in the corresponding email addresses, were linked to an illegal online gambling platform. The accounts were utilised by a crime syndicate for receiving bets from gamblers and laundering gambling proceeds with a turnover of over HKD 30.8M (approx. USD 3,926,099) between mid-2020 and early 2021. It was discovered that two common sets of IP addresses were frequently used to access the virtual bank accounts in questions and their registered locations were the residence of Mr. A, who was later found to be the mastermind of the syndicate. In mid-2021, Mr. A and eight syndicate members were arrested for bookmaking and ML with cash of HKD 2.6M (approx. USD 331,419) seized. An investigation is ongoing.

Case 2

A bookmaking syndicate, with a view to receiving and laundering the proceeds of illegal gambling, set up 23 virtual bank accounts in Hong Kong, China under the names of their brokers and money mules. Gamblers transferred bets to the virtual bank accounts and the funds

were then transferred to several bank accounts of core syndicate members. A financial investigation on the targeted accounts revealed signs of ML such as a high frequency of transactions and a pattern of depositing funds into intermediary accounts, then withdrawing the same amounts after a short period of time. The suspicious transactions occurred between mid-2020 and early 2021 and involved a total of HKD 181M (approx. USD 23,072,246). Hong Kong Police mounted an operation in mid-2021 with eight core syndicate members and 14 money mules arrested. A total of HKD 7M (approx. USD 892,285) in the identified bank accounts was withheld. An investigation is ongoing.

Philippines

Unsubstantiated significant transactions linked to online gaming operations

Certain individuals and a business process outsourcing company (BPO) made significant transactions, estimated to total PHP 1.76 billion (approx. USD 33,365,380), which were deemed suspicious by the reporting covered person. The subject entity is purportedly an IT BPO of a licensed gaming company and is also an operator of a casino junket. The entity reportedly made several significant cash deposits, totalling PHP 1.3 billion (approx. USD 24,644,704) in the span of seven months. The individuals, who are mostly foreign nationals, also made substantial transactions regarded as not commensurate with their declared source of funds. The individuals are purportedly employed with the subject entity. The transactions involving the subjects are largely cash deposits, which tend to obscure the source of proceeds.

Source of funds (e.g., employment) not commensurate with significant transactions

Eight individuals with similar transactional behaviours, profiles, and business details were involved in several suspicious transactions with an estimated value of PHP 155 million (approx. USD 2,952,203). These individuals were identified as online booking agents under Company A, a registered gaming corporation.

The financial institutions/covered persons (CPs), however, discovered that Company A's permit/license, which was allegedly issued by a casino regulator, had expired. The individuals were then asked to present updated identification details (IDs) and a license/permit to operate of Company A. Instead, they presented new IDs under Company B, an entity engaged in software solutions. The CP noted that upon checking the government website for business name registration (BR), no registration records were found on Company B. Moreover, the eight individuals, who were also alleged gamblers, declared themselves either as liaison officers or sales representatives of Company B, and most of them declared salaries as source of funds/income. The transactions of the eight individuals with various pawnshops and money service businesses (MSBs) showed similar patterns of domestic and international remittances from/to various sources/beneficiaries that were deemed not commensurate with their profiles. The nature of both outgoing and incoming remittances was further declared as either one or a combination of the following: (1) payments for online software, (2) purchase of goods, supplies, and services, (3) funds from business partners or friends, (4) payments or winnings of bettors for online cockfighting, and (5) payments for other online businesses.

Singapore

Case Study

On 27 November 2016, Persons A and B, among others, were arrested as part of an operation conducted by the Singapore Police Force against an organised crime group which operated multiple online betting portals. An array of computers and mobile devices were seized as case exhibits. Upon enforcement, close to SGD 57,000 (approx. USD 41,579) of illegal proceeds was seized from Person A and a caveat was subsequently lodged against Person A's property.

Person A and Person B jointly managed illegal lottery operations of a remote gambling business. In late-2008, Person A was recruited by Person B to digitalise their illegal lottery operations. They purchased an illegal online betting website through the help of two foreigners with Person A assuming the key administrator's role. The website was officially launched in December 2009. Thereafter, Person A ran the illegal remote gambling business through the creation of betting accounts, collection of bets and the disbursing of prize monies.

A financial investigation was conducted to investigate the illegally obtained profits by Person A and ML offences he committed. It was established that Person A had benefitted significantly throughout the years and had deposited illegally obtained profits into his Central Provident Fund account through a third party.

Person A was convicted of six charges and 13 charges were taken into consideration for ML offences under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act, and offences under the Common Gaming House Act, Remote Gambling Act and Organised Crime Act. Person A was sentenced to five years imprisonment and a fine of SGD 500,000 (approx. USD 364,738) while Person B was also charged in Court for his involvement in remote gambling activities and sentenced to three years and six months imprisonment and a fine of SGD 300,000 (approx. USD 218,842).

Vietnam

Online gambling rings generally operate card games where players deposit money through a system of dealers to obtain points, then bet and exchange points through the game for real money.

Gambling websites (betting, dice, lotto etc.) have servers located abroad, but website interfaces in Vietnamese. The foreign operators of these gambling websites collude with domestic partners to establish many organised gambling rings for Vietnamese citizens to play online. This is a form of secured/indemnified gambling as gamblers who want to play must set up an account on the website, then transfer money to the operators' bank accounts (VND accounts at Vietnamese commercial banks which are rented by the operating subjects from the Vietnamese). Upon receiving the gamblers' money, the gambling website will transfer a number of points equivalent to the value of the gamblers' money to their accounts on websites. Gamblers then use these points to play on the gambling website.

The hiring of people to open bank accounts and using bank accounts is completed through two steps: Step 1: organisers hire a number of Vietnamese to open accounts using their national identification numbers at multiple banks; they provide these people with phone numbers to

register for services with the bank (One Time Password, SMS banking, internet banking). Step 2: Once bank accounts are opened, the overseas operators of gambling websites directly manage the fund transfer between accounts using internet banking or SMS banking and they direct the account holder(s) to withdraw cash then bring it to people of their choosing.

Some notable cases which have been discovered and dismantled by the Vietnam Ministry Public Security (MPS) in 2021 were:
(i) Quang Ninh Provincial Police, in coordination with the Department of Cybersecurity and High-tech Crime Prevention of MPS dismantled an organised gambling ring with over 10,000 billion dong (approx. USD 429,306,508) in proceeds identified, which was led by individuals A and B;
(ii) Hanoi City Police dismantled an online organised gambling ring with 14,000 billion VND (approx. USD 600,944,893) in proceeds identified which was led by individual C;
(iii) Criminal Police Department - MPS dismantled the online organised gambling ring which operated online casino games with proceeds of 30,000 billion VND (approx. USD 1,287,982,341) identified which was led by individual D;
(iv) Criminal Police Department - MPS dismantled an international gambling ring which created games on a website which were played by millions of individuals with proceeds amounting to over hundreds of trillions of VND.

5.15 Casinos (including use of casino value instruments, casino accounts or currency exchange facilities, and casino junkets).

Hong Kong, China

Intelligence suggested that the large amounts of deposits into the personal bank accounts of Mr. A and his two associates were incommensurate with their financial statuses and tax records. An investigation revealed that Mr. A was in control of seven VIP junket rooms in casinos in Jurisdiction X while Mr. A's associates worked as junket promoters at Mr. A's junket rooms. As an entrenched practice for junkets, Mr. A and his associates deposited their clients' debt repayments into their personal bank accounts in Hong Kong, China. However, the account activities did not match the business profile of the junket rooms as deposits amounting to a total of HKD 1B (approx. USD 127,481,700) were made into the bank accounts in a period of eight years and these deposits could not be found in casino transaction records. Indicators of ML were identified in the accounts. Mr. A and his two associates were charged with ML while HKD 400M (approx. USD 50,992,198) worth of assets were restrained. A court proceeding is ongoing.

Indonesia

HH was President Commissioner of Company A. He is the party who arranged and controlled the Company B's stock and mutual fund from 2010 to 2018. From 2008 to 2018 Company B had collected funds from Company B's products in the form of non-saving plan products, saving plan products, and corporate premiums which in total were worth approximately USD 5,996,926,990. From the fundraising, Company B made an investment by buying shares and Medium-Term Notes (MTN) which formed part of Company B's portfolio in the form of a fund management contract and limited participation mutual funds that were under the control

of HH (President Director of Company MI) and BT (President Director of Company HI) through JHT (Director of Company IMR and Advisor of Company MI) as professional.

The arrangement and control of Company B's stock investment and mutual funds was conducted by HH and BT due to an agreement with HP (Director of Finance of Company B), S (Head of Investment Division of Company B) and HR (President Director of Company B) reached in several meetings that agreed to hand over the management of Company B's stock and mutual funds to HH and BT through JHT;

In arranging and controlling Company B's stock and mutual funds, JHT used two instruction schemes.

1. To support the arrangement scheme, JHT set 10 brokers (securities companies) controlled by HH and BT through JHT.
2. Using nominee accounts that have been prepared by HH and BT, JHT controlled as many as 75 entities.

The management of Company B's stock and mutual funds during the investment period of 2008 – 2018 that was arranged and controlled by the defendant HH and BT through JHT had caused losses to the state totalling USD 1,106,324,603 from four stock investments and 21 mutual fund investments.

Funds totalling USD 1,106,324,603,41, which constituted losses to the state, were received by HH and BT through an account in the name of HH and BT on behalf of a number of nominees.

During the period 2010 to 2018, funds were received by HH as a result of corruption in managing and controlling Company B's stock and mutual fund investment. HH also concealed the source of funds of the proceeds of crime by:

A. Placing funds into a bank account in the name of defendant HH and other parties with the aim of disguising the origin of wealth through nominees (corporation and individuals);

B. Spending money from corruption crimes by buying three units of land and buildings;

C. Spending money from corruption crimes with the aim of disguising the source of funds through JHT by purchasing land and property in the name of UPS (nominee);

D. Spending money from corruption crimes by buying four vehicles on behalf of HH and other parties;

E. HH concealed the source of funds from corruption crimes by exchanging the funds for foreign currencies

F. Making purchases with the purpose of concealing the source of funds from corruption crimes by acquiring (taking ownership) of three companies and capital investments totalling USD 1.9 billion.

G. Making purchases to conceal the source of funds from corruption crimes by giving some money to JH who is the son of HH, which was then used to buy several apartment units.

H. Transferring the funds with the aim of concealing the source of funds from corruption crimes to FG's (nominee person) account which was then used by FG in the following way:

   Transfer of the funds to FG's account where the funds were used to:

   - On 09/06/2017 to pay the casino an amount of USD 320,563
   - On 13/02/2018 for the renovation of the 4th floor of a building which cost USD 164,560
   - On 09/04/2018 to build a sailing ship in which cost USD 263,296

I. Placing the funds into their bank account for the purpose of gambling payments at the casino:
   - On 24/03/2015 to pay a casino in Country S an amount of USD 60,032
   - On 18/06/2015 to pay a casino in Country S an amount of USD 45,418
   - On 14/12/2015 to pay a casino in Country S an amount of USD 59,241
   - On 23/12/2015 to pay a casino in Country S an amount of USD 32,912
   - On 22/01/2016 to pay a casino in Country S an amount of USD 65,824
   - On 17/03/2016 to pay a casino in Country S an amount of USD 32,912
   - On 29/04/2016 to pay a casino in Country S an amount of USD 32,912
   - On 16/05/2016 to pay a casino in Country S an amount of USD 32,912
   - On 07/06/2016 to pay a casino in Country N an amount of USD 230,384
   - On 08/06/2016 to pay a casino in Country N an amount of USD 98,736
   - On 09/08/2016 to pay a casino in Country S an amount of USD 96,761
   - On 06/09/2016 to pay a casino in Country M an amount of USD 144,813
   - On 23/11/2016 to pay a casino in Country M an amount of USD 329,120 in two transfers of USD 164,560
   - On 19/07/2013, HH transferred to a bank account the amount of USD 728,672 to pay off casino debts in Country M.
   - On 22/07/2013, HH transferred to a bank account the amount of USD 661,173 to pay off casino debts in Country M.

J. HH purchased stock and mutual funds, with the aim to conceal the source of funds of corruption crimes, totalling USD 125,065.

The court sentenced HH to life in prison and imposed an additional penalty of paying compensation to the state totalling IDR 10.7 trillion (approx. USD 741,084,145).

Macao, China

Case: Use of gambling activities and casino instruments to deceive a casino

Suspect A and others falsified bank statements as a source of CDD information. After that, with the help of his acquaintance Y (who worked in casino Z), Suspect A was able to circumvent relevant control procedures in place and applied for gaming credit in casino Z in the name of a third person Q, who was then granted a line of credit. Q then withdrew promotional chips from the credit, using the full amount, which were then received and transferred by Suspects B, C and others, and finally given to Suspects A and D. By placing only small bets in a casino, Suspects A and D exchanged the promotional chips into cash chips and brought them out of the casino. Suspect A then instructed Suspect D to store the cash chips worth HKD 2,710,000 (approx. USD 345,451), exchanged through structuring and frequent minimal gambling, and promotional chips worth at least HKD 30,000 (approx. USD 3,823) in two different locations, respectively.

In this case, Suspect A and others committed fraud by using false information to deceive casino Z into providing credit so that they could withdraw chips of the equivalent amount. Suspects B and C assisted in receiving and transferring the said promotional chips knowing that they were gained illegally through fraud. To obscure the illegal source of the scammed chips, Suspects A and D intentionally transformed the proceeds of crime by betting small amounts. In 2021, the Macao, China Public Prosecutions Office laid fraud and ML charges against Suspect A, reception charges against Suspects B and C, and reception and ML charges against Suspect D.

5.16 Structuring (smurfing) / refining.

Hong Kong, China

Intelligence suggested that a loansharking syndicate collected repayments from their debtors via multiple money mules' bank accounts in small amounts and the funds were withdrawn in one transaction afterwards. All deposits were slightly less than HKD 100K (approx. USD 12,747) and over 60 money mules' accounts received funds totalling HKD 25M (approx. USD 3,186,803) over a period of two years. Five account holders were identified and arrested in 2021 with HKD 4.6M (approx. USD 586,371) frozen in their bank accounts. An investigation is ongoing.

Pakistan

Laundering of proceeds from drug trafficking through a real estate business

The partners of two partnerships, Partnership A (5 partners) and Partnership B (4 partners), opened their personal accounts and partnership business accounts with different banks. The individuals deposited a high volume of cash in their multiple personal accounts and then

transferred the funds to the business accounts of the aforementioned partnerships. The source of funds was unclear to the reporting entities.

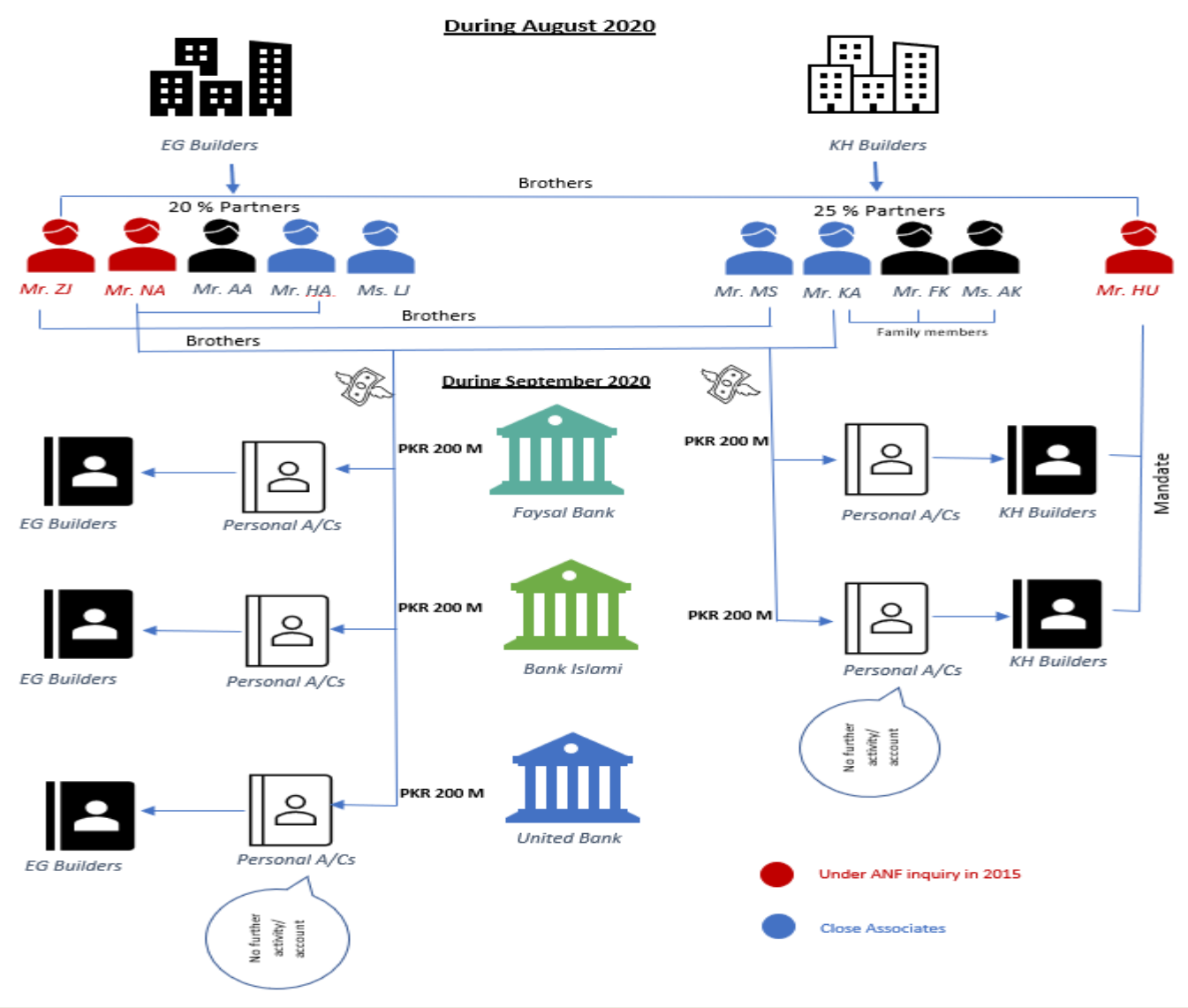
Partnership A and Partnership B were involved in the construction of buildings, were registered under the Partnership Act, 1932 with the Registrar of Firms in August 2020. The partners of both of the entities were apparently relatives from different cities. The individuals registered their companies in a large city and opened their personal and entity accounts with different banks during September 2020.

The transactional activity in the accounts revealed that the individuals (partners of the firms) deposited a high volume of cash in their personal accounts in a structured manner in order to avoid the reporting of Currency Transaction Reports (CTRs). Later on, the funds were transferred to the accounts of Partnership A and Partnership B which were opened in different banks. Part of the transferred funds was then debited to the accounts of Partnership A and Partnership B through the clearing of cheques, issuance of pay orders and cash. No further transactional activity other than those as mentioned earlier was observed in the personal accounts of the partners thereafter.

Upon inquiry by the bank, the individuals stated that the accounts were opened to pool funds in order to use the amnesty scheme announced by the Government for builders and developers. Furthermore, the individuals failed to provide documents to the bank relating to projects undertaken by Partnership A and Partnership B that raised suspicion as to the legitimacy of the business.

Upon further analysis and database searches, some of the individuals (partners of the entities) and their family members were found to be allegedly involved in drug trafficking and using the subsequent criminal proceeds to purchase assets. The Anti-Narcotics Force (ANF) recovered 1000 kilograms of hashish from a truck driven by the accused Mr. RU in 2015. During an investigation, the ANF found that the hashish was supplied by the partners of the aforementioned entities and their names were included in the charge sheet. On the basis of the inclusion of their names on the charge sheet, the assets of some partners which were acquired with the proceeds of crime were frozen by the ANF. Furthermore, some of the partners had also undertaken frequent trips to foreign countries.

Based on the analysis, it was concluded that a high volume of funds was deposited through cash into the accounts in a structured manner to avoid the attention of authorities. Various personal accounts opened in different banks were used to hide the source of funds. It was suspected that the funds might be derived from drug trafficking, therefore the financial intelligence was shared with law enforcement agencies (LEAs) to investigate the matter. An LEA registered a new case against the individuals and investigated the source of funds.



Solomon Islands

A suspicious transaction report was filed on 7 August 2020 by Bank A that showed large cash deposits of around SBD 1,365,000 (approx. USD 167,622) were deposited into Person X's bank account. Analysis conducted on the account revealed overseas ATM withdrawals totalling around SBD 1,304,163 (approx. USD 160,151) were subsequently conducted from the account in a Foreign Country, country A, during the period from 16 July 2018 – 10 June 2020.

During the period 16 July 2018 – 10 June 2020, 36 cash deposits were made into Person X's bank account, ranging from SBD 25,000 (approx. USD 3,070) to SBD 50,000 (approx. USD 6,140), with transaction references as 'for salary/allowance payments'. In addition, based on transactions carried out in Foreign Country A, there were around 368 ATM withdrawals conducted across multiple locations in Foreign Country A, ranging from SBD 1,000 (approx. USD 122) to SBD 3,700 (approx. USD 454), while no withdrawals were conducted locally.

Based on the analysis, the FIU has disseminated a report on this case to the relevant law enforcement agency for further investigation on possible tax evasion.

5.17 Purchase of valuable/cultural assets (art works, antiquities, race horses, vehicles, etc).

Indonesia

Case 1

The Attorney General's Office of the Republic of Indonesia's (AGO) Asset Recovery Center has auctioned 16 luxury vehicles (consisting of 15 luxury cars and one luxury motorcycle) that were confiscated after criminal acts of corruption in insurance management and ML. In the process of purchasing the luxury vehicles, the perpetrator used the name of another party in the ownership of the assets.

Case 2

A case of narcotics crime was uncovered by the National Narcotics Agency (BNN). The case involved an Indonesian citizen, namely SA and a foreign citizen, namely HWJ aka Mr Tan, Mr Lee, Mr FU. Mr SA conducted a narcotics business by using the account of another party to receive funds from prisoners with a total value of IDR 27 billion (approx. USD 1,870,007). The ML scheme was carried out using cash, credit transactions, fund transfers, motor vehicle purchases, apartment purchases, overseas travel, cash purchases of eight types of paintings and transfers worth IDR 115 million (approx. USD 7,964).

Case 3

Three defendants were accused of corruption in the management of social insurance funds and proven to have laundered money by purchasing luxury vehicles, property and gold paintings, and exchanging foreign currencies. The three defendants charged with ML were Mr. BT as President Director of Company A, Mr. JS as Director of Company B, and HH as President Commissioner of Company C.

In 2013, Mr. JS met with Mr. BT through Mrs. CCW and told Mr. JS to help and manage the transactions of shares controlled by Mr. BT in the investment management of the company. Company D created and used a stock account owned by JS, an account in JS' name or parties affiliated with BT and JS.

Mr. BT's request was approved by Mr. JS. Until 2019, JS after receiving shares from BT through the "Received Free of Payment" (RFOP) mechanism, then transferred the shares to raise the price of the shares through the Negotiation market mechanism involving 373 transactions. As a result of the defendant's actions, it has resulted in losses to the state of IDR 22.7 trillion (approx. USD 1,572,186,039).

From the state financial losses amounting to IDR 22.788 trillion (approx. USD 1,578,280,857), JS obtained illegitimate profits from the management and investment control of the company. Company D obtained the amount of IDR 781,153,675,000 (approx. USD 54,102,167). Furthermore, during the period 2013 - 2019, the money received by JS as a result of corruption was hidden or disguised by:

1. Placement into a bank account in the name of Mr. JS and the accounts of other parties (6 accounts)

2. Mr. JS spent the proceeds of corruption by purchasing eight apartment units and one housing unit in Indonesia.
3. Purchased three units of luxury cars.
4. Purchased 14 luxury watches and gold jewellery.
5. Exchanged money into foreign currencies, namely AED, SGD, THB, HKD, JPY, EUR, TWD, NZD and MYR.
6. Purchased 36 luxury gold paintings with the aim of selling them in an exhibition to disguise the origin of these assets worth IDR 109 billion (approx. USD 7,549,964).

Furthermore, the defendant Mr. HH as the party that regulated and controlled the instruments for managing investment in shares and mutual funds of Company D, from 2016-2019 together with Mr. JHT and Mr. PR, used companies that are included in the Company E Group. From the state financial loss amounting to IDR 22,788,566,482,083 (approx. USD 1,578,545,676) the defendant HH obtained an illegal profit of IDR 12,421,886,211,772 (approx. USD 860,476,144). Then from 2016-2019 the money that HH received from Company D was concealed by ML which involved:

1. Spending the proceeds from the property whose sale and purchase deed are in the name of another person. The properties included one apartment unit and three plots of land with an area of 16,888 m2.
2. Purchasing one luxury car.
3. Purchasing PCAR shares totalling 58,360,000 shares in a securities account in the name of Company F.
4. Acquiring ownership of a company, namely Company C
5. Requisition of Company G along with the company's assets in the form of a ship with the name LNG AQUARIUS Ship.

The third defendant, Mr. BT, received a profit of IDR 5,968,626,189,161 (approx. USD 413,457,954) from Company D’s investment funds from Company D stock and mutual fund transactions during the period 2012 - 2018. The proceeds of the crime were disguised and hidden using ML which involved:

1. Payment of bank loans (principal instalments to four banks) so that the funds seem legitimate.
2. Purchased 23 plots of land in the name of other parties, both individuals and corporations.
3. Diverted the proceeds of corruption from investing in shares and mutual funds of Company D by conducting a mining business using Company H.
4. Invested in another company by buying 967,500 shares of Company I through Company J.

Macao, China

Case: Falsification of artwork transactions to cover up the illicit proceeds of a fraud syndicate

Upon the request of the Public Prosecutions Office, the Judiciary Police investigated two local companies in connection with a number of suspicious transactions. The two companies received the proceeds of a fraud scheme equivalent to approximately HKD 8,850,000 (approx. USD 1,128,155) through bank accounts in the second half of 2017. The funds were subsequently withdrawn and transferred within a short period of time.

An investigation also revealed that the two involved companies were solicited by members of a fraud syndicate from Jurisdiction A to provide corporate bank accounts for receiving the proceeds of fraud, which were subsequently withdrawn through the cashing of cheques by two local individuals (Suspect A and Suspect B). The funds were later returned to the members of the fraud syndicate.

On 14 April 2021, the Judiciary Police summoned Suspect A and another overseas shareholder of one of the companies for investigation, and arrested Suspect B at a casino in Cotai district. Suspect A admitted the commission of the previously mentioned crime through forging contracts for the sale of art works to cover up the crime.

The Judiciary Police transferred the three individuals to the Public Prosecutions Office for the offences of ML and forgery of documents respectively, and continued to pursue the other involved individuals. (for the analysis of relevant suspicious transactions, please refer to Section 8.2).

Singapore

The Suspicious Transaction Reporting Office (STRO), Singapore's Financial Intelligence Unit, received STR information which flagged several individuals' bank accounts for suspicious transactions with Company O and Company R. STRO's analysis of the supporting documents obtained that related to some of the transactions caused them to question the legitimacy of the transactions. STR information also revealed that those individuals were part of a larger syndicate that remitted a total of SGD 300 million (approx. USD 217,992,355) to Company O's bank accounts in a year. A significant proportion of the funds was subsequently remitted to Person Q, the director and majority shareholder of both companies. Person Q layered the monies across multiple local and foreign bank accounts.

While analysing information from various sources, STRO identified numerous red flag indicators suggesting that Company O, Company R and Person Q could be operating a massive Ponzi scheme, and referred the case to a domestic LEA for further investigation.

Through the overt investigations, it was uncovered that Company O and subsequently Company R entered into investment agreements with investors with promised returns deriving from trading activities that did not exist. A substantial portion of funds received from investors were diverted to Person Q's personal bank accounts for the purported purpose of funding trading positions. Person Q also used those funds for personal expenses, including the purchase of 49 artworks with a total sale price amounting to around SGD 5.9 million (approx. USD 4,287,171). The most expensive artwork is a painting purchased from a private art gallery for around SGD 2.85 million (approx. USD 2,070,922).

The credible actionable leads stemming from STRO's dissemination allowed the LEA to commence an investigation for fraud related and ML offences among others. This led to the arrest of Person Q and other persons, successfully disrupting the Ponzi scheme in Singapore.

5.18 Investment in capital markets, use of brokers.

Hong Kong, China

The Securities and Futures Commission initiated a market manipulation investigation in which a ML syndicate was identified to have colluded with major shareholders of three local listed companies to orchestrate a pump-and-dump scam generating HKD 176M (approx. USD 22,435,665) from the stock markets in Hong Kong, China and Jurisdiction X for the syndicate. The case was referred to the Hong Kong Police, the Police Force of Jurisdiction A and the Monetary Authority of Jurisdiction A for parallel financial investigations, and it was revealed that the illegally obtained earnings were transferred to Jurisdiction X via a bank account of a shell company. An unprecedented cross-border operation amongst the four agencies was mounted in late 2021, resulting in the arrest of ten syndicate members in Hong Kong, China and Jurisdiction X. A total of HKD 46.8M (approx. USD 5,965,848) was withheld in the bank accounts of syndicate members. An investigation is ongoing.

Indonesia

Mr. GW, who is a private employee, raised funds from the public through an investment scheme in Company A domiciled in Jurisdiction A without a business license from Bank Indonesia or Commodity Futures Trading Regulatory Agency (CoFTRA). To persuade the victims, he made a promotion with a presentation explaining that this investment will never lose value including because it has a hedging system (protection). In this case, the funds collected amounted to IDR 3,868,538,854 (approx. USD 267,975) which was then used for the personal interests of the defendant. As a result, the defendant was charged with criminal acts in banking and ML.

Through Company A, Mr. GW raised public funds by promising a profit of 13% - 22% per week. Mr. GW assured that the money from investors will be guaranteed safe because investment funds have been guaranteed by Bank A and the system is equipped with hedging or ceiling protection. To further convince potential investors, Mr. GW even pretended to invite and provide facilities for these potential investors to visit Company A's head office in Jurisdiction A.

The funds that were collected by Mr. GW were then used to purchase a car worth a total of IDR 2 Billion (approx. USD 138,544), to buy a house worth IDR 2.5 Billion (approx. USD 173,180) and to purchase luxury watches, luxury bags and belts and diamond jewellery.

Solomon Islands

Between December 2019 and March 2021, Person X and Person Y operated an unlicensed financial scheme known as OLP. The modus operandi of the scheme was that, members of the public were lured to invest in various investment plans offered by OLP ranging from SBD 250 (approx. USD 30) to SBD 5,500 (approx. USD 675) and after 30 days, members were entitled to receive interests ranging from 173% to 300% according to the investment plans selected.

According to the investigation undertaken, between December 2019 and March 2021, Person X and Person Y deceitfully obtained around SBD 56,440,475 (approx. USD 6,930,925) from many vulnerable and struggling Solomon Islanders.
Right from the beginning of the scheme, only a few members managed to obtain their interests based on the investment they had with OLP; whilst the rest or majority of members never received any interests along with their initial investments in the scheme.

The case was reported to the Police who carried out investigations on Person Y and Person X. On 13 August and 8 December 2021, the Magistrate Court respectively tried the two individuals (Person Y and Person X) and found both of them guilty of one count each, of operating an Unlicensed Financial Institution contrary to section 3(2) (a) of the Financial Institution Act 1998 ("FIA 1998") and five counts of simple theft.

Both Person X and Person Y were convicted and sentenced to imprisonment for two and three year terms respectively. The successful convictions of Person Y and Person X resulted from the cooperation between the FIU, regulatory agencies, private sector and law enforcement agencies in the Solomon Islands.

Thailand

In January 2022, an investigation team responsible for the case arrested Mr. A, a wanted suspect under the Criminal Court's arrest warrant for using a purported foreign exchange trading website to scam the general public. Mr. A and his associates were suspected of running a Ponzi scene to defraud 8,437 people through his Company A.

They persuaded victims to invest in foreign exchange (forex) by offering returns at a rate of 60-80% of profits. The victims were persuaded to invest in Company A's fund through a platform and make the transaction to Company B. Victims had received returns initially and were then unable to receive the whole investment.

The total damage from this Ponzi scene was estimated at more than USD 66 million and relevant authorities managed to recover around USD 36.5 million in assets. Mr. A was charged with the offence of jointly lending loans amounting to public cheating under the Emergency Decree on Loan of Money Amounting to Public Cheating and Fraud, B.E. 2527 (1984). Additionally, the Transaction Committee issued seizure orders on assets over USD 10 million to return to the victims. At present, the case is being considered by the public prosecutor.

5.19 Mingling (business investment).

Philippines

Unlicensed investment-taking or solicitation activities from the public

Roughly 900 individuals were reported in substantial suspicious transactions estimated to total PHP 226 million (approx. USD 4,274,603) in which were linked to unauthorized and fraudulent investment schemes. The scheme involves investing in livestock products with a promise of a 100% return in as quick as two months.

The majority of the 900 subjects received funds via payroll credits from a travel and tours agency, which was allegedly used as the beneficiary account of the investment taking activities of three entities. A Securities and Exchange Commission (SEC) advisory was released in 2019 against the three entities, warning the public to stop investing in the said companies. The SEC further warned that those involved will be reported to tax authorities so that penalties and/or appropriate taxes be correspondingly assessed.

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

Fiji

Case Study: Illegal Fishing

Person N, a foreign national and frequent traveller to Fiji was found in possession of 660 kilograms of preserved, prohibited fish products at his residence. The prohibited fish products were estimated to have been purchased for FJD 33,050.

It was established that Person N travelled to Fiji on a visitors permit and did not have any financial transactions or bank accounts in Fiji. He was listed as a director of Company X and acquired and disposed of three vehicles in 18 months. There were no financial transactions associated with these purchases and consequent disposals. Two of the vehicles were transferred to two individuals from the same country as Person N.

Person N paid a FJD 20,000 fine for being in possession of prohibited fish products. Given Person N's frequent visits to Fiji, he may be a mule used by a local network to carry the prohibited fish products out of the country. He may also be carrying undeclared currency when he travels across the border.

Indonesia

In 2018, Indonesian authorities identified a large-scale syndicate that was responsible for trafficking pangolin scales worth approximately USD 9 million between 2012 and 2017. The syndicate leaders in this case were Mr. S, Mr. A, Mr. B, and Mr. C (the latter three being siblings that owned Company A).

Company B, a frozen fish company, used a network of intermediary bank accounts under false names to disguise the relevant payments. The vast majority of the intermediary accounts were set up under the pretence of being legitimate animal or farm suppliers. Further examination of the financial transactions of Mr. S and Mr. A showed a financial flow of around USD 6 million from convicted drug dealers. The Indonesian authorities identified that Mr. A, B and C used the company accounts to co-mingle revenue from their legal fishing company, and illegal proceeds from pangolin and drug trafficking.

Pakistan

The Financial Monitoring Unit (FMU) received four STRs from ABC Bank on individuals Mr. SK, Mr. MH, Mr. HS (son of MH) and Mr. KZ during the period 2019-2021. They are linked as counterparties and associated with the fishing and oil businesses. Moreover, Mr. SK and Mr. MH also own fishing boats. They were running their businesses in the same locality.

The STRs reported were based on high turnover in the accounts and transactions with unrelated counterparties such as teachers, oil lubricant distributors, scrap dealers, medicine dealer and wholesalers/retailers of general items such as dry fruit, sugar, wheat, etc.

Very high turnovers were observed in the sole proprietorship accounts which did not match the profiles of the individuals. Funds were largely deposited through clearing cheques and were withdrawn on a daily basis in the form of cash. It has also been observed that the account holders were frequently conducting transactions with unrelated counterparties.

Mr. HS declared himself as an exporter of seafood, but while reviewing the account statements, it was observed that huge trade transactions were routed through one of his sole proprietorship accounts. Moreover, while reviewing the trade documents, it was revealed that Mr. HS received export payments from multiple unrelated counterparties dealing in clothing, shoes, hats, ceramic, resin, bags, wooden products, arts & crafts products, plastic products, wholesale of products, wool, chemicals and fibre. As per travel records, Mr. MH, Mr. HS and Mr. KZ have conducted multiple visits to different countries.

Based on the findings of the analysis, high turnover in sole proprietorship accounts, transactions with unrelated counterparties, cross border trade transactions, associated with fishing and oil businesses, FMU shared the financial intelligence with LEAs with the suspicion of involvement in Smuggling, IUU Fishing, Hawala or any other illegal activity.

Channel used: Cash deposits, clearing and inter-bank funds transfers (IBFTs) and foreign remittances.

Thailand

Mr. B allegedly smuggled 14 rhinoceros horns worth USD 1 million from Africa into Thailand in December 2017 and was arrested in January 2018 in Nakhon Phanom. The Anti-Money Laundering Office (AMLO) conducted a further investigation and as a result in March 2021 the Transaction Committee issued a seizure order on assets worth 30 million baht (approx. USD 872,916) which were believed to belong to Mr. B and his associates. Officials searched several locations in Nakhon Phanom and Chaiyaphum provinces connected to Mr. B. They seized 22 items valued at more than 3.2 million baht (approx. USD 93,138) which included cash, jewellery, firearms and wild animals. As a result of the operation, AMLO confiscated further assets worth more than 3 million baht (approx. USD 87,333) from the network of Mr. B. and his associates.

5.21 Currency exchanges / cash conversion.

Fiji

Case Study: Possible Breach of Currency Reporting at the Border

Mr. X, a dual citizen of Fiji and Country E, was brought to the attention of the Fiji FIU for the possible breach of border currency reporting (BCR) requirements. It was reported that Mr. X converted FJD 54,400 (approx. USD 25,459) worth of foreign currency into Fijian dollars and deposited the funds into the bank account of Company A to purchase a motor vehicle. Mr. X claimed that he was well connected to officials in Country E and was allowed to carry large amounts of funds without declaring it at the border.

Fiji FIU analysis established that Mr. X is a frequent traveller and he did not declare the FJD 54,400 (approx. USD 25,459) worth of foreign currency when he entered Fiji.

In addition, Fiji FIU analysis established that Mr. X is a manager of companies A and B in Fiji, and a manager of Company C in Country E.

Fiji FIU analysis of Mr. X's financial transaction details suggested that he may have carried large amounts of foreign currency when travelling to Fiji. Fiji FIU analysis established that Mr. X received remittances from a politically exposed person in Country E, and that he had not lodged his income tax returns since 2018.

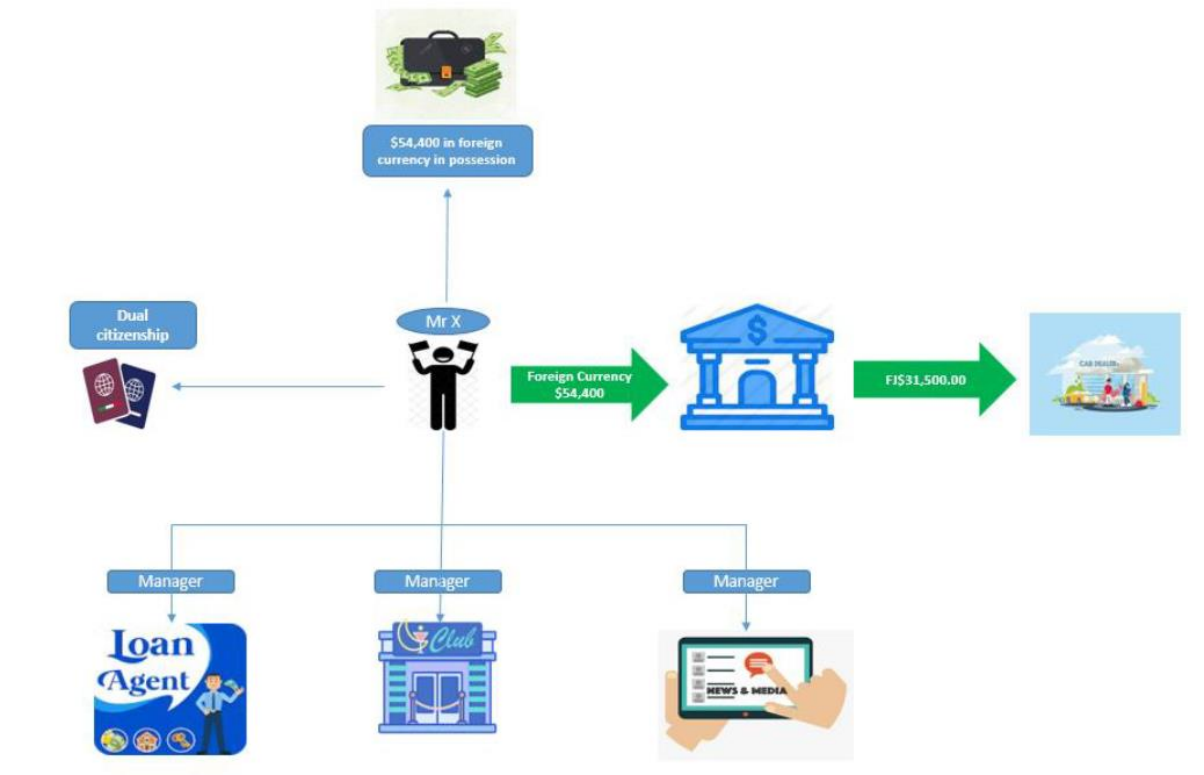
A case dissemination report was provided to the border enforcement unit and taxation division of the Fiji Revenue and Customs Service. A case dissemination report was also provided to the FIU in Country E.

Indicators:

- Excess foreign currency used without supporting BCR
- Unusual bank account activity

Possible Offence:

- Breach of currency reporting at the border under section 32(1) of the FTR Act
- Tax related offence/tax evasion
- Corruption (in a foreign jurisdiction)



Hong Kong, China

Ms. A possessed personal bank accounts in both Hong Kong, China and Jurisdiction X. She was requested by her acquaintance Mr. B to transfer HKD 17,200 (approx. USD 2,192) to a Hong Kong bank account for purchasing a collectible figure. Ms. A complied upon the receipt of a deposit equivalent to HKD 17,200 (approx. USD 2,192) in the currency of Jurisdiction X. She was later notified by an LEA of Jurisdiction X that the funds transferred to her bank account in Jurisdiction X were in fact illegally obtained profits from fraud cases. An investigation is ongoing.

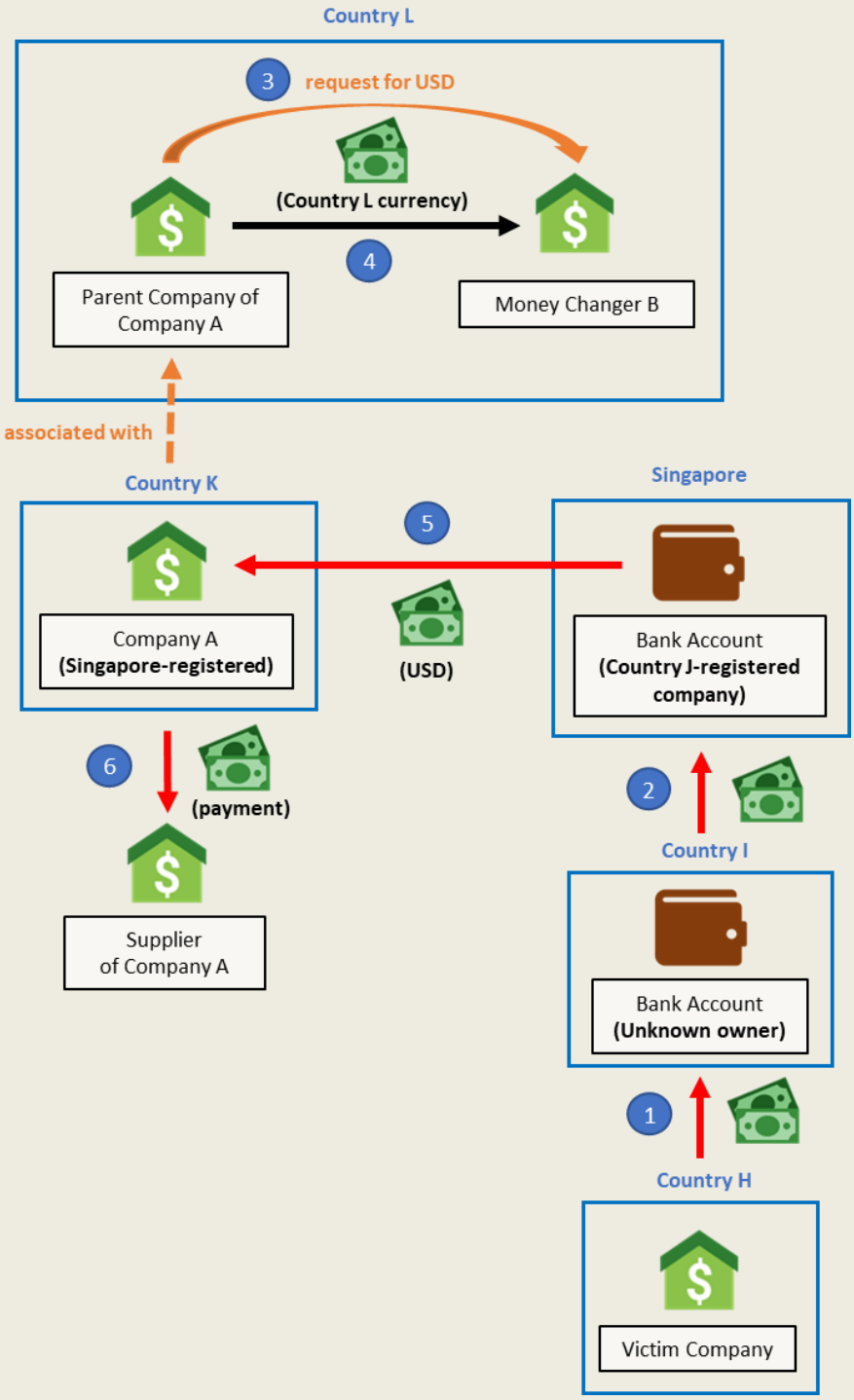
Singapore

This is a complex ML case, where the criminal proceeds were layered through a mix of techniques, including via corporate bank accounts spanning several countries, cash integration involving companies with legitimate business operations and foreign currency exchange businesses.

A company incorporated in Country H fell victim to a business email compromise scam which led to an initial transfer of EUR 2 million (approx. USD 2,143,857) to a bank account in Country I. Thereafter, the funds were transferred to a Singapore bank account maintained under a purported shell company incorporated in Country J, and were co-mingled with other sources of funds. Subsequently, the co-mingled funds were disbursed to multiple entities, including a bank account in Country K held by Company A, a Singapore-incorporated company in the business of trading. Following which, the funds were purportedly used by Company A for normal operating expenses for supplier payments.

Investigations revealed that the funds received by Company A were allegedly sourced from a purported business arrangement facilitated between Company A's parent company in Country L and a foreign exchange business domiciled in Country L, foreign exchange business B. Company A sought assistance from foreign exchange business B to obtain US dollars in exchange for the local currency of Country L, as Company A required US dollars for normal/operating expense payments. In turn, foreign exchange business B made further arrangements with one of its intermediaries to 'obtain' the US dollars. The consequence of these arrangements was a transfer of funds in Country L's local currency from Company A to foreign exchange business B, and a transfer of US dollars to Company A via the scam described previously.

Investigations are ongoing for this case.



5.22 Currency smuggling (including issues of concealment & security).

Indonesia

Mrs. NL worked at Company A and Company B which were in the foreign exchange business. The companies belonged to the accused's brother named Mr. AH and the companies were used as a means of receiving and making transfers using funds sourced from narcotics crime. The accused received a transfer from an account both in the name of NL and in the name of another

person controlled by NL. The accused received funds from the bank account in the name of NL which was controlled by himself and had received money from the following parties:

1. Mr. FS (account controlled by CSN-foreign citizen) who had been convicted of ML involving the proceeds from a narcotics network and with the involvement of Mr. CH. The proceeds of crime totalled IDR 645,961,975 (approx. USD 44,747).

2. Mr. PC who had been convicted of ML involving the proceeds from a narcotics network and with the involvement of Mr.CH, with the proceeds of crime amounting to IDR 2,174,680,000 (approx. USD 150,646).

3. Mr. LB who had been convicted of ML involving proceeds from narcotics, amounting to IDR 4,296,722,000 (approx. USD 297,646).

4. Mrs. MRN, who had been convicted of ML involving the proceeds from a narcotics network and with the involvement of Mr.CH, with the proceeds of crime totalling IDR 7,843,250,000 (approx. USD 543,324).

5. Company C (account is controlled by Mr.CH) with the proceeds of crime totalling IDR 629,600,000 (approx. USD 43,612).

6. Mr. HB (account controlled by Mr. HC) who had been convicted of trafficking narcotics with the proceeds of crime totalling IDR 197,500,000 (approx. USD 13,680).

7. Mr. FS (account controlled by Mr. CSN-foreign citizen) who had been convicted of ML involving the proceeds from the sale of narcotics with the proceeds of crime totalling IDR 3,251,291,458 (approx. USD 225,218).

Money Laundering scheme:

1. NL was arrested on 27 July 2018 at the Customs Office of SH Airport, where NL had just returned from jurisdiction A with the aim of getting medical treatment. NL carried foreign currency into Indonesia with as many as 2,166 notes of cash hidden in their suitcase. NL did not declare to authorities that they were carrying cash into Indonesia.

2. Mr. AH and NL are known to own foreign exchange businesses under the names Company A and Company B which are used as a means to receive and make transfers related to narcotics business activities and use various bank accounts, held in their own names and those of others as well as held in the name of companies.

3. The accounts controlled by NL are not only used to receive money transfers from people involved in the narcotics trafficking network, but were also used to transfer money from one account to another with the funds then sent abroad. In addition, NL often transferred their money from one account to another account under their control as well as to other people's accounts with the excuse (camouflage) of exchanging money.

4. NL benefited from these actions with money still held in their bank account.

5. NL and Mr. AH concealed the origin of their assets and used and controlled accounts in the names of other people.

6. In addition, NL also established several companies that did not have any activities, but were only used as a cover and the company's accounts were used as a means for transferring money.

7. The proceeds of narcotics crime were stored in accounts in the name of the foreign exchange business, in the suspect's personal name and in the name of another person and then used for buying and selling foreign currency.

8. The actions of NL and Mr. AH involved using the foreign exchange company as a means to receive and make transfers related to the sale and purchase of narcotics and using company accounts or other people's names to accommodate assets sourced from narcotics crime. Funds were also used to buy a vehicle or asset in someone else's name. The foreign exchange business was used to mix the proceeds of crime from narcotics trafficking with legitimate business profits.

Prosecution resulted in a fine from the Directorate General of Customs and Excise for ML and carrying cash totalling SGD 2,195,000 (approx. USD 1,594,973) and the case was reported to the Indonesian FFIU (PPATK) as a suspicious report on carrying cash across the border for violating Article 34 paragraph 1 of Law No. 8 of 2010 on ML.

Thailand

An investigation revealed that small amounts of cash was carried out of the country and used for the travel and operational costs of the perpetrator. The perpetrator group met together in a neighbouring country where they planned to make, assemble and bring explosive devices to place at many important public places and government offices in Bangkok and nearby provinces.

The Anti-Money Laundering Office with the consent of the Transaction Committee gathered information as evidence and referred this matter to the public prosecutor. Finally, the Civil Court ordered these persons as designated persons and AMLO issued a notification of the list of these persons designated by the Court in November 2021. Additionally, AMLO also filed complaints with the Royal Thai Police against these persons for a criminal TF offence.

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

Fiji

Case Study: Credit Card Fraud - Shell companies, EFTPOS machines & stolen foreign credit cards

Between October and November 2017, three foreign nationals were charged by the Fiji Magistrate’s Court under the Proceeds of Crime Act 1997 for ML involving credit card skimming activities. Individuals A, B and C used false documentation to establish two entities in Fiji, Company A and Company B. The setup of the two entities and opening of bank accounts were facilitated by a consultant based in Fiji. Following this, EFTPOS machines were installed at the offices of Company A and Company B, which were used by Individuals A, B and C to swipe stolen credit cards. The syndicate was in possession of approximately 500 stolen foreign credit cards.

From 9 – 25 June 2015, over 250 fraudulent credit card transactions totalling FJD 719,852 (approx. USD 336,893) were credited to the bank accounts of Company A and Company B. Additionally, from 18 – 22 June 2015, four cash cheque transactions totalling FJD 40,300 (approx. USD 18,860) were withdrawn from the two entities' bank accounts by Individuals A, B and C for the alleged purchase of shoes and bags.

The three individuals pleaded 'not guilty' in respect of the charges they faced. On 22 February 2019, the Fiji Magistrates Court delivered its judgement finding them 'not guilty' and dismissing the ML charges against the three individuals. The DPP appealed the decision of the Magistrates Court.

In February 2021, the Fiji High Court ordered that:
1) The appeal be allowed;
2) The acquittal of Individual A in respect of the first count of ML charges, be quashed and replaced with a conviction on the basis of being found guilty;
3) Individual A be convicted for the first count of ML contrary to section 69(2)(a) and 3(a) of the Proceeds of Crime Act; and
4) Individual A be remanded in custody and produced before the Fiji Magistrates Court for sentencing.

Individual A was sentenced in April 2021 to a custodial term of 5 years and 10 months imprisonment with four years as non-parole. Individual A appealed his conviction in September 2021 and the appeal was dismissed by the Court of Appeal.

Hong Kong, China

A credit card fraud syndicate headed by Mr. A set up a number of shell companies and provided false employment records for his money mules for credit card applications. Fictitious transactions were made with the credit cards at a purported business owned by Mr. A. Funds received were transferred to the personal account of Mr. A and further channelled to the bank accounts of money mules for settling credit card repayments so that more credit cards could be successfully applied on top of the increase in credit limits.

As a result over 250 credit cards were issued by six local banks with transactions amounting to HKD 85.8M (approx. USD 10,936,836) made at Mr. A's purported business. The money mules eventually failed to repay HKD 46M (approx. USD 5,863,571) to the card issuing banks. Mr. A and 22 credit card holders were arrested in mid-2021 with over HKD 1.2M (approx. USD 152,962) withheld in their personal accounts. An investigation is ongoing.

Indonesia

Mrs. PSM was found guilty of corruption and ML with of the proceeds of crime totalling USD 375,229 or around IDR 5.25 billion. She was sentenced to a period of imprisonment of four years and received a fine of IDR 600 million (approx. USD 41,555).

She received a bribe of USD 500,000 from Mr. DT through Mr. AIJ, part of which amounted to USD 50,000 for a lawyer. Of this amount, USD 337,600 were exchanged for rupiah at a currency exchange worth IDR 4,753,829,000 (approx. USD 329,247). Mrs. PSM also used

nominees in the names of other people, including drivers, her husband's staff and other parties who engaged in structuring and smurfing to avoid reporting thresholds.

The results of the exchange of money were partially made in cash or transferred to accounts belonging to Mrs. PSM and her younger siblings. The proceeds of these crimes were used for personal purposes through money laundering, including:

1. Purchase of one luxury car worth IDR 1.7 billion (approx. USD 117,741) in the name of Mrs. PSM with cash used as the payment method in several stages of payment as well as a transfer from a bank account as a result of a credit card overpayment.

2. Payment of apartment rental in Jurisdiction A of IDR 412 million (approx. USD 28,534) via bank account transfer.

3. Payment of beauty doctors in the Jurisdiction A costing IDR 418 million (approx. USD 28,950).

4. Payment for home care doctors costing IDR 176 million (approx. USD 12,189).

5. Bank A's credit card payments with a total of IDR 467 million (approx. USD 32,344) in intentionally overpaid credit card payments from the credit limit that should be IDR 33 million (approx. USD 2,285) with the aim of obtaining overpayments from financial service institutions to disguise credit card transactions as if they were legal transactions.

6. Payment of Bank B credit card with a total of IDR 185 million (approx. USD 12,813).

7. Payments on two Bank C credit cards with a total of IDR 483 million (approx. USD 33,452).

8. Bank D credit card payments with a total amount of IDR 950 million (approx. USD 65,796), where the payment amount exceeds the credit card limit that should be IDR 67 million (approx. USD 4,640) via internet banking or cash.

9. Payment of an apartment rental costing USD 68,900 through cash payments in stages through a property agent with the funds then transferred to the account of the owner of the apartment unit.

10. Payment of an apartment rental costing USD 38,400 in cash.

Japan

The following are examples of misusing cheques and credit cards for money laundering:

- A case where an illegal money-laundering business operator made many borrowers draw and send cheques etc. by post for principal and interest payments. The cheques were then collected by deposit-taking institutions and transferred to accounts opened in the name of another party.
- A case where shop owner operating a loansharking business executed a fictitious sale and purchase contract with a borrower in lieu of receiving repayment of a loan from the borrower, and transmitted a false sale and purchase information to a credit card issuing company and received the payment of the price.

Philippines

Subject VA was being investigated for potential violation of R.A. No. 3019 or the Anti-Graft and Corrupt Practices Act. Between 29 October 2004 and 12 January 2021, VA figured in 314

covered transactions and four suspicious transactions ranging from PHP 39,227 (approx. USD 741) to PHP 15 million (approx. USD 283,504) and totalling PHP 410.439 million (approx. USD 7,757,420).

One suspicious transaction pertained to a purchase of a life insurance policy in cash by VA's son in August 2020. The named beneficiaries in the insurance policy were the wife, daughter, and another son of VA. The three remaining suspicious transactions pertain to unauthorised credit card purchases totalling PHP 168,326 (approx. USD 3,181) made in VA's account in May 2019.

In addition to these, VA was also found to have various large investments in different high-yielding products with three domestic banks, which are likely methods to launder the proceeds of unlawful activities, particularly for graft and corruption.

It is noteworthy to mention that VA made three large credit card purchases ranging from PHP 500 thousand (approx. USD 9,450) to PHP 1 million (approx. USD 18,900) in 2019. There were also large transfers of funds, through cheques between VA and his presumed relatives.

Based on the reports on salaries and allowances of a domestic government agency, VA's average monthly salary in prior years was less than PHP 100 thousand (approx. USD 1,890). After being promoted in 2016 to his current position, VA's average monthly salary ranged between PHP 187 thousand (approx. USD 3,534) and PHP 240 thousand (approx. USD 4,536). The compensations of VA are significantly lower compared with his reported transactions from 2004 to 2021; hence, VA's transactions are perceived not commensurate with his known source of income (his salary) and financial capacity.

5.24 Wire transfers / Use of foreign bank accounts.

Fiji

Case Study: Tax Evasion

Company M, registered in Country O, was reported to the Fiji FIU for sending remittances totalling FJD 477,447 (approx. USD 223,447) to Ms. Z, a Fiji citizen, and Mr. M, a citizen of Country O with a bank account in Fiji. The remittances were sent over a period of eight months.

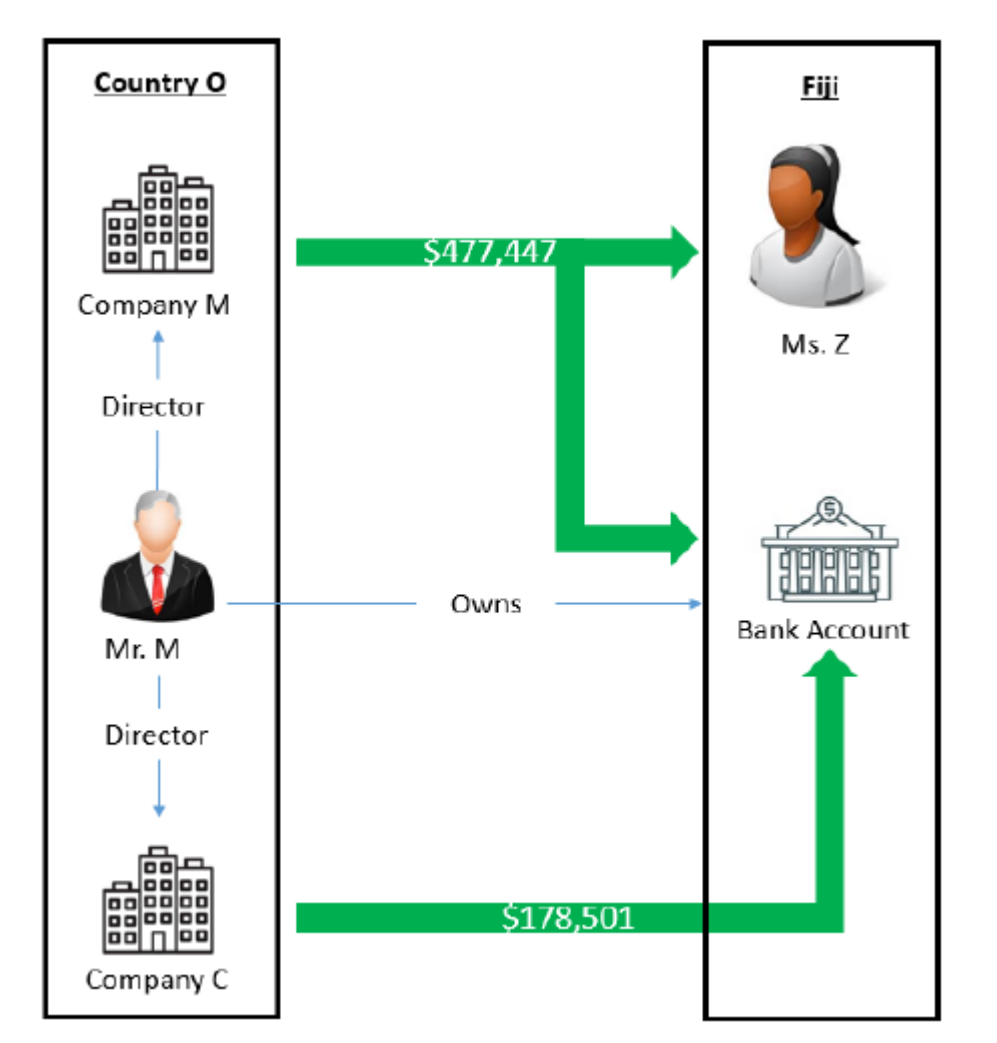
Fiji FIU analysis revealed that Mr. M also received remittances totalling FJD 178,501 (approx. USD 83,539) from Company C in Country O. Mr. M was a director of Company M and Company C. The remittances were allegedly to purchase property in Fiji.

Furthermore, Fiji FIU analysis of Company M established that it was proposed to be de-registered by the Registrar of Companies in Country O during the same period that the remittances were sent to Fiji.

A case dissemination report was sent to the FIU in Country O.

Indicators:
• Unusually large remittances to unrelated parties
• Multiple entities sending remittances to the same individual

Possible Offence:
• Obtaining financial advantage by deception
• Possession of proceeds of crime



Hong Kong, China

Ms. A was an accounting employee of a local company and she was in control of the company's e-banking account. In late 2021, Ms. A stole HKD 45M (approx. USD 5,736,312) by conducting 13 unauthorised remittances to 12 local bank accounts, of which HKD 13M (approx. USD 1,657,156) were further wired to a number of foreign bank accounts. Ms. A and eight account holders were charged with theft and money laundering, with around HKD 29M (approx. USD 3,696,734) frozen in the bank accounts in question.

Japan

International Romance Fraud Cases

Case 1

A foreign criminal organisation deceived a victim living in Jurisdiction A and made the victim transfer around 11 million yen (approx. USD 84,043) to the bank account of a legal person which was opened in Japan and managed by office worker B.

Japan Financial Intelligence Centre (JAFIC) received the information from a foreign agency and analysed it. Then they provided the information to a LEA. The LEA conducted the required investigation and determined that the office worker received the payout and claimed it to be a legitimate payment. As a result, he was arrested on the charge of the violation of the Act on punishment of Organized Crime and Control of Crime Proceeds (Concealment of Criminal Proceeds etc.).

Case 2

Three men and women were arrested who had conspired with people in G jurisdiction and defrauded men in their 40s to 60s. The victims were targeted on a dating website and social media and defrauded of a total of 5.4 million yen (approx. USD 40,057). The victims were approached online by individuals pretending to be a doctor working in E jurisdiction, a journalist from H jurisdiction, and a diplomat.

There were at least 55 victims and the total financial damage was 120 million yen (approx. USD 916,825). Suspect A persuaded the victim to transfer funds to a bank account opened by suspect A. Then, the money in A's bank account was transferred to a bank account in the name of Company A, which was managed by the suspect B, or to another bank account of suspect A. Finally, the money was transferred to an overseas bank account in G jurisdiction. The proceeds of crime were thereby concealed.

Philippines

Case 1:

The client is the subject of a request for investigation from a law enforcement agency. Based on the complaint, an amount of PHP 87,500 (approx. USD 1,654) was allegedly sent to the client's account in July 2020. The client's major source of funds came from deposits totalling PHP 4.497 million (approx. USD 85,057) while fund outflows were made through over-the-counter withdrawals totalling PHP 0.61 million (approx. USD 11,537).

Suspicious transaction reports were filed on the client for alleged involvement in fraud and a face shield scam. The subject had various cash deposit transactions ranging from PHP 3,000 (approx. USD 56) to PHP 0.246 million (approx. USD 4,651) which were deemed to be not commensurate with the client's source of funds as a housekeeper. In addition, the client received remittances from individuals located in other countries with no business or apparent purpose, and their relationship with the senders and the subject remains unclear.

Case 2:

In November 2021, a case involving a Filipino national, CGY, was referred by an FIU for her alleged involvement in money laundering activity and violation of the foreign country's Banking Law. Prior to this, in October 2021, the law enforcement agency of the foreign country received information that CGY was running an underground financing activity in its jurisdiction. Upon investigation, it was found out that CGY had received numerous deposits from unidentified persons and that these funds were subsequently remitted to four other individuals.

Information collected by the Anti-Money Laundering Council (AMLC) on CGY suggested that CGY received six transactions amounting to PHP 14.989 million (approx. USD 283,489) between 18 May 2021 and 31 May 2021. The amounts of the aforementioned transfers ranged from PHP 1.143 million (approx. USD 21,618) to PHP 4.6 million (approx. USD 87,003). While CGY's KYC documents indicated business as her source of income, CGY failed to submit documents to support the existence of those supposed businesses, hence, it was also highly unlikely that the funds in question were generated from CGY's businesses.

KYC returns from a foreign exchange service business revealed that for the period 10 May 2017 – 20 December 2019, CGY sent three remittances totalling PHP 22,875 (approx. USD 432) to her sister CBG. KYC returns further disclosed that CBG received five other remittances from different individuals in other countries. Four out of five remittances indicated that they were for family support, which seems questionable due to a lack of association/relationship.

Singapore

Case Study 1

In July 2021, Singapore prosecuted Person N, a Singapore national for providing money to be used for the purpose of facilitating terrorist acts. The accused was detained since January 2019 for investigation into his terrorism-related activities. The accused was an associate of Person M, a Country X national and an ISIS militant. Person M was believed to be the most senior ISIS fighter in Country Y prior to his reported death in March 2019.

A parallel TF investigation conducted by the Commercial Affairs Department of the Singapore Police Force found that the accused, who had allegedly provided funds totalling approximately SGD 1,026 (approx. USD 746) to Person M, purportedly intended for these funds to be used for the purpose of facilitating terrorist acts in Country Y.

The funds were transferred between 2013 and 2014 over three occasions, the first by handing over cash directly to Person M in Country X, and the other two occasions using licenced remittance businesses in Singapore and Country X respectively, to Person M's intermediaries in Country Z.

Case Study 2

The Suspicious Transaction Reporting Office (STRO), Singapore's Financial Intelligence Unit uncovered a network of Singapore bank accounts which were used to receive suspected scam

proceeds. Initially, there was little to suggest that these bank accounts were linked to the same syndicate.

Through STRO's analysis, it was uncovered that a criminal syndicate had amassed these bank accounts fraudulently from a mix of Singapore residents who understood they were involved in criminal activity and others who did not. Some of the individuals (i) sold their bank accounts to the syndicate, or (ii) relinquished their personal Singpass credentials for monetary benefits to the syndicate, for the creation of new bank accounts. SingPass is Singapore's digital identity service provided to all Singapore citizens and permanent residents that allows access to various e-services requiring proof of personal identification.

As a result, the criminal syndicate used the SingPass credentials to open bank accounts online to receive funds from victims of various scams. As the criminal syndicates had full access to a several bank accounts, they were able to launder funds within this network of accounts to hinder funds tracing and recovery efforts by the authorities.

Investigations are ongoing. Six individuals have been arrested for their suspected involvement in the case.

5.25 Use of false identification.

Chinese Taipei

Case 1

Mr. A, Mr. B and Mr. C were all members of the scam group T. These members first deceived buyers into sending their money by means of falsely advertising health products on a website. After the victims were led to mistakenly bid and then remit their money to the head account designated by the scam group. Mr. C then used an ATM card to withdraw the illegal funds from the above head account by using a convenience store's ATM. Mr. A then used those funds to purchase online game point cards and distributed the point cards to the members of scam group T.

Case 2

In April 2020, the police in country A requested our cooperation to run a joint investigation for a fraud case targeting residents of country A. The investigation revealed a national of country B residing in country A had fallen victim to fraudsters impersonating prosecutors and police officers and lost TWD 2.38 million (approx. USD 81,348). Subsequently, more and more nationals of country B working in Country A fell victims to the same fraud scheme and suffered significant losses. According to the investigation conducted by the police of country A, the fraudsters' IP address was located in Chinese Taipei. The police forces of Chinese Taipei and country A exchanged intelligence and decided to conduct a joint investigation.

The task force conducted secret surveillance for days on the main suspect, person A, who operated a fraud syndicate while cooperating with a ML syndicate. The ML syndicate was responsible for recruiting individuals in their early twenties to be money mules. After months of surveillance and evidence gathering, on June 30 2021, the task force obtained search warrants to conduct raids. The first targeted a ML syndicate. Following the evidence gathered,

the task force subsequently raided another property and targeted a fraud operation (line one). The task force further targeted another fraud operation (line two). Meanwhile, the task force found four more members of the ML syndicate, including person B. On 13 September 2021, 23 September 2021 and 6 October 2021, summons were issued to the suspects.

The investigation revealed that the fraud syndicate mainly targeted nationals of country B especially those working in country A. The first fraudster impersonated a member of customer service of the Communications Authority and called the victim, claiming that the victim's phone number had been sending out scam messages and was used by a criminal syndicate to commit crimes that violated the telecommunication act and the AML law. Subsequently, the second fraudster impersonated a police officer of country B and the third fraudster impersonated a prosecutor, requesting to monitor the victim's bank account and asking the victim to transfer funds to a designated bank account. As a result, the victims suffered heavy losses. From mid-June 2021 to the dates of the raids, within a period of two weeks, a total of 15 nationals of country B had fallen victims to the fraud and suffered losses of over RMB 100,000 (approx. USD 14,956). Further investigation revealed that the fraud syndicate also committed catfishing and investment scams on many domestic victims, as well as running a ML syndicate. In June 2021, a total of 16 domestic victims were scammed and the losses suffered amounted to over TWD 34 million (approx. USD 1,162,701).

Fiji

Case Study: Mistaken Identities

Mr. A, Mr. B and Mr. C were brought to the attention of the Fiji FIU for possible money laundering of approximately FJD 7.5 million (approx. USD 3,510,032) following the receipt of over FJD 300,000 (approx. USD 140,402) each by Mr. A and Mr. B from an individual in Country 1. Mr. A, Mr. B and Mr. C are nationals of Country 2 who also hold Country 3 passports, and are sole shareholders and directors of Company A, Company B and Company C respectively. Mr. A, Mr. B and Mr. C use the same Suva residential address, however, their personal bank accounts were opened at a Nausori bank branch and their business bank accounts were opened at a Namaka bank branch. Fiji FIU analysis established no travel records to Fiji for Mr. A, Mr. B and Mr. C, however, their bank account information noted that they were physically present to open the bank accounts. Company A, Company B and Company C have the same registered business address and phone number.

It is important to highlight that Mr. A, Mr. B and Mr. C are allegedly tenants of Ms. D, who is an associate of an individual sentenced by the Fiji Magistrates Court for one count of money laundering involving credit card skimming activities. Ms. D allegedly assisted with the creation of companies and bank accounts using identification documents of individuals not present in Fiji and believed to be fraudulent.

Fiji FIU analysis also established that Company A, Company B and Company C each pay Ms. D salary expenses of FJD 3,000 (approx. USD 1,404) per month.

A case dissemination report was provided to the Fiji Police Force.

Indicators:

- Newly established companies receiving offshore remittances (particularly start-up capital) from a jurisdiction not related to the foreign shareholders/directors.
- Personal and business bank accounts are opened at different bank branches.
- Unrelated, foreign shareholders/directors using the same residential and business addresses, and contact information.
- Newly established companies paying unusually large salary expenses to a single employee.
- Use of passports from countries where citizenship can be easily obtained.

Possible offence:

- Money laundering.
- Provision of false or misleading information.
- Economic fugitives.

Indonesia

Mr. KHA as the Chairman of an Employee Cooperative committed a crime of corruption and money laundering which resulted in losses to the state of IDR 24.8 billion (approx. USD 1,717,632). It is known that Mr. KHA together with Mr. NRH as Account Officers of Company A and Mr. WZD as Branch Heads of Company A have conspired to intentionally make credit loans through the state-owned enterprises of an employee cooperative on behalf of approximately 500 members of the cooperative using falsified documents. Based on the results of the credit disbursement, Mr. KHA has used the proceeds of crime amounting to IDR 12.3 billion (approx. USD 851,890) by disguising the source of funds as follows:

1. Issuing loans in the form of back to back loans by a Bank.
2. Purchase of land or property using the name of his wife and children.
3. Purchase of four vehicles.
4. Transfer of ownership to other parties through asset sales.

Pakistan

Suspected origin of proceeds of crime

KHS, the principal accused, a Pakistani national located in Country A, scammed people on a large scale through a false identity. KHS would call different high-profile Government officials and threatened them with immediate arrest and dire consequences by pretending to be a senior official of an LEA. KHS collected the proceeds of crimes in cash through accomplices. Four accomplices namely AH, SC, SA and SH were engaged by KHS in Pakistan. KHS and his accomplices collected information from the newspapers and other open sources about their targets.

Highlights of the ML investigation

At the beginning, in relation to the predicate offence, multiple complaints were received by an LEA from government officials and political persons that they had received telephone calls (on

social media apps) from an impersonator (KHS). Based on such complaints, an inquiry was authorised in June 2021 to initiate an investigation to determine the owners of the numbers making threatening calls. Information obtained from telephone companies revealed that these numbers were registered in the names of different individuals. Subsequently, in order to trace the actual culprits and the money, forensic analysis (Geo Fencing) of all the places where proceeds of crime were collected by the accused persons, was conducted with the help of an Intelligence agency.

From forensic analysis, two numbers were found which were common to all places where the proceeds of crime were collected. From these numbers, the ownership details of commonly associated mobile numbers were obtained and subsequently two accused persons (AH and SC), who were collecting the extortion money (proceeds of crime) on behalf of the main accused, were tracked though electronic surveillance and were arrested.

Both accused persons were taken into custody after completing due judicial procedure. During remand they revealed their complete network. On the basis of this information, two other persons were arrested; SH, another accomplice who collected the extortion money and MS who was involved in the business of Hawala/Hundi (illegal MVTS) and used this illegal channel to send the proceeds of crime to KHS in Country A.

Further development

Another accomplice of the accused KHS identified as SA was arrested using investigative techniques, a sting operation and controlled delivery, when SA was approaching a victim to collect the proceed of crimes (The victim had approached the LEA, informed them about threatening calls he had received from KHS, and cooperated with the authorities). SA was arrested in a raid with the assistance of police.

Cooperation from police, an Intelligence agency, FIU, and other authorities was obtained during investigation proceedings. A request has also been initiated to obtain financial intelligence of the accused persons from the FIU of Country A through Pakistan FIU.

Findings

After collecting the extortion money and taking a cut, the accomplices transferred the remaining value of the proceeds of crime of the extortion to KHS in Country A in a variety of ways.

AH, an accused and son of KHS, admitted that he had collected money from different pick-up points along with SC and SH. AH further admitted that he had invested some money from this illegally obtained money in an online business of Company B, which is suspected of being a Ponzi scheme (another investigation has been initiated against Company B for cheating the public at large).

The accused MS has been convicted and part of the proceeds of crime received by him from accused AH has been forfeited.

Highlights of the complexity of ML case

This case involved two legal persons (Company A and Company B) related to the proceeds of crime being transferred to Country A. Company A has a global presence and operates a social media application. It has regional offices in Pakistan and Country A. The proceeds of crime were used to buy virtual assets through the social media application operated by Company A.

The investigation also revealed the use of non-banking channels (Hawala/ Hundi) to transfer the proceeds of crime out of Pakistan making it more difficult to trace the proceeds of crime.

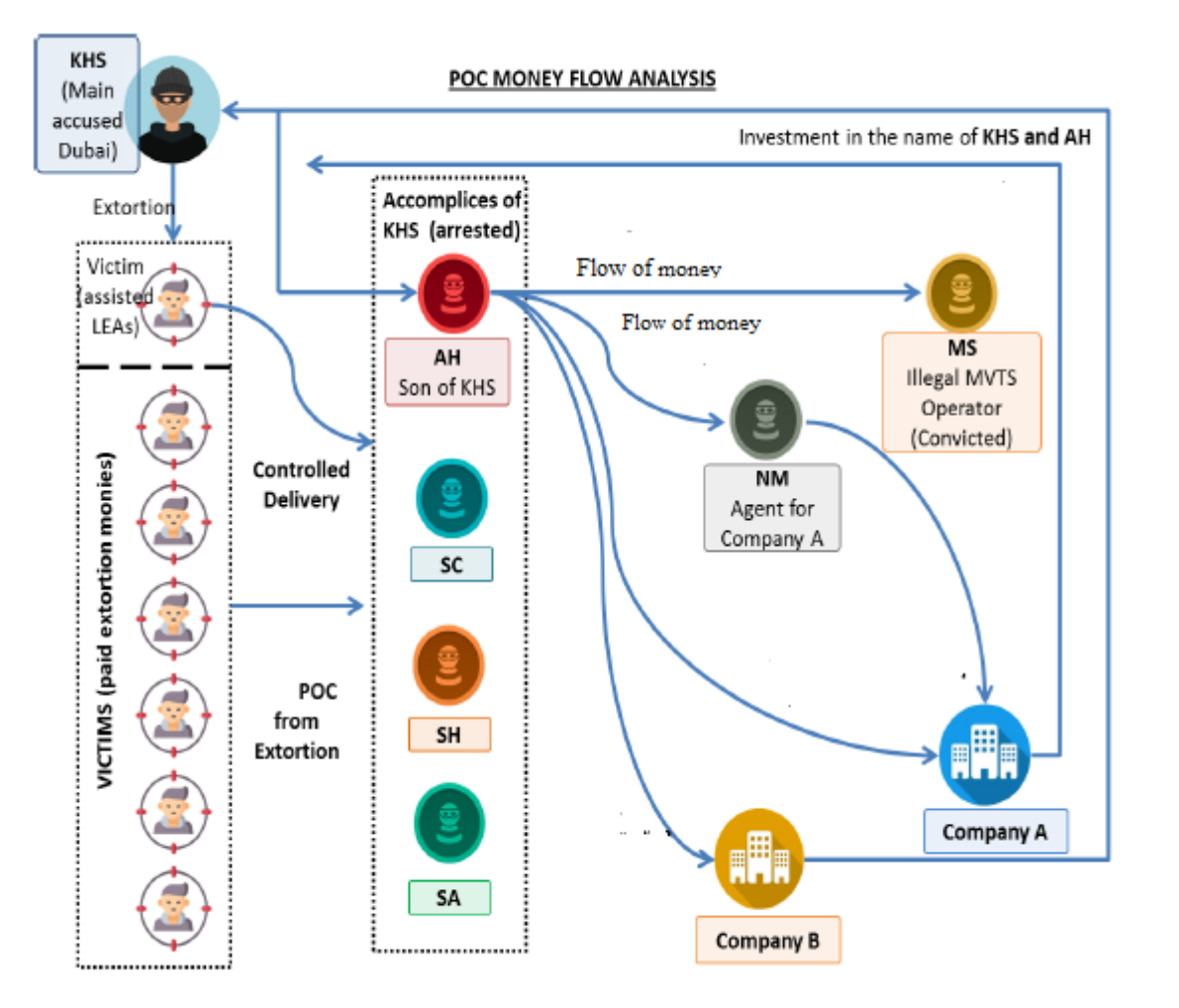
The principal natural person accused (KHS) was operating from a foreign jurisdiction. The accomplices of KHS usually collected proceeds of crime at crowded public places and changed locations often. The proceeds of crime was subsequently transferred around Pakistan and to Country A.

The investigations involved inter-agency cooperation with several departments and international cooperation with one jurisdiction.

Status of the case

There were eight suspects (natural persons) which also included two representatives of legal persons. To date, six of the suspects have been charged. One person (MS) has been convicted (MS). Four suspects (AH, SC, SH and SA) are facing trial for the offences and one (KHS) is considered to have absconded as he is outside the jurisdiction.

The predicate crime and money laundering activity of the principal accused KHS is under investigation. Formal and informal cooperation with counterparts in Country A has been initiated to trace, freeze and confiscate the proceeds of KHS's criminal activity. NM and a representative of Company B also remain under investigation for ML.



Philippines

The case arises from an alleged violation by a subject covered person of Article 315 (Swindling/Estafa) of the Revised Penal Code in relation to Section 6 of Republic Act No. 10175, otherwise known as the "Cybercrime Prevention Act of 2012." Based on a law enforcement agency's initial investigation, the victim was allegedly defrauded online for an amount of PHP 27,990 (approx. USD 528), which was transferred to the subject's domestic bank account on 20 August 2021.

Information gathered revealed that the subject used fictitious names and company institutions, and celebrity names, among others. The account number indicated in the complaint belonged to a different owner, RO. The limited available information provided on the case did not clearly establish RO's actual participation, but it is possible that he is not the ultimate beneficiary of the funds, but was only hired as a mule. However, available information suggests that the account was likely used as a pass-through account as the funds were immediately withdrawn.

Solomon Islands

On 26 July 2021, Person A (foreigner) entered into a financial institution and attempted to remit funds to her home country offshore using the passport of a third party. A frontline officer

of the financial institution detected the passport mismatch and immediately instigated an investigation on the concerned passport. Based on the outcome of the investigation, it was revealed that, the facial image of Person A does not match the facial image contained in the third-party passport. Also, there was no immigration stamp on the passport. Thus, the financial institution decided to cancel the transaction of Person A and an STR was immediately filed to the FIU.

Upon receipt of the STR, the FIU conducted its analysis and forwarded its report to the Immigration Department for further investigation under its powers. Also, the FIU sent out alert notices to all financial institutions, alerting them of the possible use of fake or duplicate passports for financial transactions especially in relation to international transfers.

5.26 Association with corruption/bribery

Indonesia

Mr. ADI was the Director of Company A. Company B together with Mr. MAL as the Head of the Treasury Division of Bank SUT was involved in a corruption case involving the issuance of Medium Term Notes (MTN) from Company C for additional operational costs.

These securities were then offered to Bank SUT as the investor represented by Mr. MAL while the underwriting transaction with Company B was represented by Mr. ADI through three consecutive bidding schemes. Mr. MAL did not analyse the request for a line of credit from Company C in setting the Maximum Limit for Credit Applications to the company.

Meanwhile, Mr. ADI served to expedite the underwriting process carried out by Company B so that the nominal offer was approved. Even though the offer was not reasonable and not commensurate with the funds spent considering that Company C is a finance company that is engaged in the retail business and has a very large default risk. As a result, this action was detrimental to the state by the amount of funds issued by Bank SUT. From the funds that have been collected, in addition to being received by Company C as debtors, the two defendants also received a sum of money which was then used to purchase assets and transferred to partners at Bank SUT. In this case, the two perpetrators are suspected of committing criminal acts of corruption and money laundering.

Malaysia

Several enforcement officers and frozen food companies including their directors and employees were charged with various offences for alleged involvement in a meat cartel syndicate. The cartel operation included giving bribes to officers from several government agencies to bypass local checks for importation and to enable the cargoes and containers of non halal certified frozen meats to be released at the ports. The meats would then be sent to the cartel's warehouses for re-packaging and re-labelling with counterfeited halal certificate[39] for

[39] Halal Certification is an official document that refers to the Halal standardization of products and/or services in accordance with the Malaysian Halal Certification Scheme only issued by the Department of Islamic Development Malaysia. The term "Halal" is referred to food or goods that are described as halal or are described in any other expression to indicate that the food or goods can be consumed or used by Muslims.

local distribution. The cartel was able to profit from this activity by sourcing cheaper meats from non-certified processing plants, avoiding the costs involved in the halal certification process and applicable tax and duties.

The cartel was also able to gain dominance of the local market for halal meat imports by predatory pricing against smaller competitors. Several financial intelligence disclosures were made to the Ministry of Domestic Trade and Consumer Affairs and the Malaysia Anti-Corruption Commission relating to the syndicate involving 50,398 subjects prior to the arrest of relevant individuals. Currently, there are ongoing investigations led by the Ministry of Domestic Trade and Consumer Affairs and assisted by other agencies including the Royal Malaysia Customs Department, the Malaysia Anti-Corruption Commission, the Royal Malaysia Police, and the Inland Revenue Board for possessing and distributing unauthorised frozen products, using false and unauthorised Halal logos, possession of prohibited items, corruption, submitting false information, tax offence and money laundering. Several of the actions taken against the suspects include the seizure of frozen meat, trucks, fake labels and stamps and sales and purchase invoices.

Mongolia

An STR was initiated from an information request made by a foreign FIU to FIU-Mongolia. FIU-Mongolia conducted analysis on that STR and disseminated it to a law enforcement agency in accordance with the legislation. Accordingly, a law enforcement agency conducted an investigation and opened a criminal case under Article 22.1 "Abuse of power and position", Article 22.4 "Bribery", and Article 18.6 "Money laundering" of the Special Part of the Criminal Code of Mongolia.

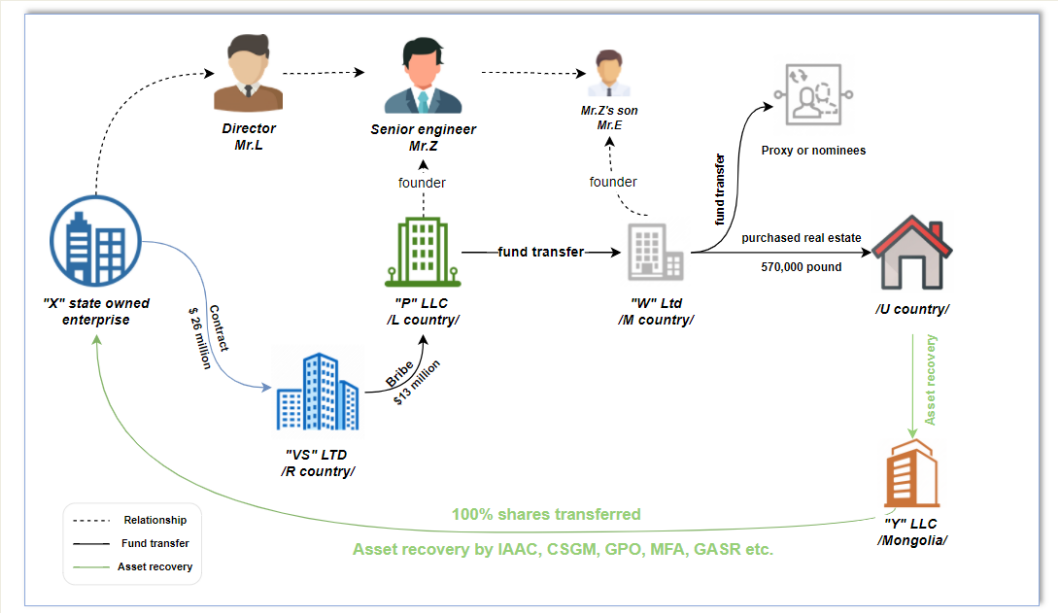
In addition, former officials of the State-Owned Enterprise "X" of Mongolia, Mr. L and Mr. Z, colluded to grant "P" LLC, a legal entity founded by themselves in an offshore jurisdiction, a contract to supply goods to the Stated-Owned Enterprise "X" by abusing their positions. In addition, Mr. Z and Mr. L abused their positions and took bribes from "VS" LTD of "R" country that concluded multiple procurement contracts worth about USD 26 million. Further, the investigation revealed that they took the bribe money through "P" LLC's account at the "A" Bank of country L.

Further, Mr. Z used an account of "W" Ltd. and his family member established in "M" country, to receive bribe money in Mongolia and committed money laundering by receiving a total amount of USD 3,375,000 in multiple transactions into accounts of proxies and nominees. During the investigation, it was also revealed that a family member of Mr. Z purchased real estate in country U with a portion of the bribe.

During the investigation of this case, FIU-Mongolia and a law enforcement agency extensively cooperated and collaborated with domestic competent authorities, reporting entities as well as foreign counterparts and FIUs. In particular, five requests for information were sent to four countries' FIUs through FIU-Mongolia via the Egmont network for the purpose of collecting additional information, as well as three requests for mutual legal assistance were submitted to three countries' competent authorities for the purpose of gathering evidence.

On 28 February 2022, Mr. Z and Mr. L were convicted and found guilty on all charges of abuse of office, bribery and money laundering.

In addition, a law enforcement agency, in cooperation with domestic and foreign authorities, successfully recovered and returned stolen assets and real estate bought by Mr. Z in country U to Mongolia.



Pakistan

Tax Evasion & Corruption

The transactional activity in the account of Ms. KZ was reportedly suspicious as high value funds were transacted from the accounts which apparently did not align with her profile. Further, the source of funds and true beneficiary of funds were also unclear.

Reportedly, Ms. KZ was a salaried individual, a marketing manager for ABC (Pvt) Company. She was maintaining multiple local and foreign currency accounts at different banks wherein a high level of transactional activity was observed. A rapid surge in her transactional activity was noted when a significant amount of funds were deposited in her PKR account in the form of cash deposits during the month of June 2020.

Upon inquiry by the bank about the funds, Ms. KZ stated that the funds were the settlement amount received from her ex-in-laws after her divorce and she also benefited from the Tax Amnesty Scheme announced by the Government in 2020. However, the justification provided by her was not satisfactory to the bank. The funds were immediately withdrawn through cash withdrawals (to purchase foreign currency), issuance of pay orders (to purchase properties) and clearing of cheques (to her own account in another bank). The cash withdrawn from her account was used to purchase foreign currency which was afterwards deposited into her foreign currency account. The foreign currency that was deposited was finally remitted out of country. Further, the analysis revealed that Ms. KZ purchased properties and remitted a significant sum of foreign currency out of country from her own accounts.

During the analysis, it was found that Ms. KZ was the daughter of Mr. ZM, who was a senior level retired government official and now the CEO of ABC (Pvt) Limited and Ms. KZ was an employee of the company. It was ascertained from the asset declaration forms and tax returns of Ms. KZ that she declared assets of PKR 260 million (approx. USD 1,314,834) in the year

2019-20. The declared assets decreased to PKR 150 million (approx. USD 758,558) in the year 2020-21 due to personal expenses of PKR 10,000,000 (approx. USD 50,570) and the gifting of PKR 100,000,000 (approx. USD 505,705), thus raising suspicion about the legitimacy of the funds and their beneficial ownership as declared in the Amnesty Scheme by Ms. KZ.

As the Amnesty Schemes did not provide immunity from the application of the Anti-money laundering Act (AMLA), 2010 in Pakistan, the financial intelligence was shared with an LEA to investigate the source and beneficiary of the funds declared by Ms. KZ in the Amnesty Scheme.

Philippines

A client, who is an officer in a government agency, was reported by a bank since his transactions were not commensurate with his declared profile. The client had numerous covered and suspicious transactions during the period of October 2006 to July 2018 with amounts ranging from PHP 500 (approx. USD 9) to PHP 105 million (approx. USD 1,983,758), totalling PHP 557.901 million (approx. USD 10,540,387).

The bank also reported that a certain person, with the same name as the client, was one of the identified collectors of bribes in a government agency. However, the bank could not confirm whether its client was the same person as the person in the news. The account with one branch was opened in 1990 and was already dormant while the account in another branch was opened in 2011 and the last transaction was made in 2017. The client declared a government agency as his employer with a monthly income of only PHP 10,000 (approx. USD 188). A review of the accounts of the client revealed that the transactions and account balances from 2007 to 2017 had significant amounts which were not commensurate with his declared profile.

The client is possibly engaged in bribery and/or corruption and money laundering based on the following observations: (a) there were multiple cash and cheque deposits credited to the client's accounts and he also made cash and ATM withdrawals which were not commensurate with his declared profile; (b) the withdrawals were made by the client on the same day or within a short period of time after the deposits were credited to his accounts giving the appearance that the funds were just transferred in and out of his bank accounts; and (c) the client is one of the identified collectors of bribes at a government agency as alleged by a senator in 2017 and it is possible that the aforementioned deposits credited to his accounts are bribes from individuals at the government agency. However, it cannot be ascertained whether the client has violated and/or is engaged in graft and corruption. The transactions made by the client and his wife which include large loan payments, life insurance policies, time deposit placements and other cheque deposits and cash withdrawals need to be further verified to determine whether these are the proceeds of bribery and/or corruption and any other unlawful activity.

<u>Unsubstantiated significant transactions of politically exposed persons (PEPs)</u>

Certain PEPs made suspicious transactions valued at PHP 2.1 billion (approx. USD 39,997,364) between 2019 and 2020. The PEPs declared business ownership as source of funds, which was discovered to be inexistent as per the covered persons' (CPs') customer due diligence (CDD) and enhanced due diligence (EDD) checks. They also declared income as founders of a delivery business. The said PEPs reportedly amassed roughly PHP 280 million (approx. USD 5,333,393) in their checking, savings, and time deposit accounts which was

deemed not commensurate with their business or financial capacity. It was also noted that the majority of their cheque issuances were also payable to themselves.

Thailand

Ms. J, who was an ex-Governor of the Tourism Authority of Thailand, and her associates committed the corruption and bribery offence by accepting 60 million baht (approx. USD 1,747,901) from an American film producer in exchange for a contract to organise the annual Bangkok International Film Festival in 2003. Bribes in cashier's cheques and international money transfers were sent to the accounts of Ms. J's daughter and other nominees in Jurisdiction A, Jurisdiction B, Jurisdiction C, Jurisdiction D and Jurisdiction E.

The National Anti-Corruption Commission (NACC) charged Ms. J and her associates under The corruption and unusual wealth offence. The Supreme Court sentenced Ms. J and her daughter to prison in 2020. Additionally, the NACC and the Office of the Attorney General (OAG) as a central authority for mutual legal assistance are working to recover the seized assets of Ms. J in the five countries mentioned above. In 2021, the Anti-Money Laundering Office in collaboration with the NACC and the OAG, seized an account of Ms. J's daughter with 500,000 USD in Jurisdiction A. Finally, the Civil Court ordered these assets to be returned to the State. At present, Thailand is coordinating with Jurisdiction A to implement asset recovery and collect evidence to prosecute Ms. J and her associates under the ML offence.

5.27 Abuse of non-profit organisations (NPOs).

Indonesia

Densus 88, an Indonesian National Police counter-terrorism squad, seized 1,540 charity boxes during a raid on the office of the Syam Organizer Foundation in Bandung district, West Java province in August 2021. The foundation, managed by Jemaah Islamiyah (JI), a militant extremist Islamist terrorist group, claimed it was collecting funds for humanitarian programs, but the funds were instead destined to finance terrorist activities. The seized charity boxes were empty and ready to be distributed to different regions.

Police also identified payroll deductions from the foundation's staff to raise money, with the funds used to send JI members to fight in Syria between 2013 and 2017. Alongside the raids which seized the charity boxes, Densus 88 also arrested at least 48 suspected terrorists, 45 JI members and three members of another terrorist group, Jamaah Ansharut Daulah (JAD), during raids in 11 regions including West Java and Central Java provinces.

Further information can be found at the following link:
https://www.ucanews.com/news/indonesian-police-seize-terror-financing-charity-boxes/93773#

Source: UN CTED

Thailand

A few NPOs in the Southern border provinces of Thailand such as religious schools and humanitarian foundations are abused by perpetrators to access funds, materials, recruitment, training and other supports for TF.

6. PROLIFERATION FINANCING METHODS & TRENDS

6.1 Recent research or studies on PF methods and trends

Indonesia

Although the potential threat of PF is still relatively low in Indonesia, efforts need to be made to be aware of the potential for PF, especially with regard to trade transactions carried out with parties from high-risk countries in line with UN Security Council Resolutions 1718 and 1737. In addition, other potential threats can arise from the accounts of foreign nationals who come from high-risk countries based on the UN Security Council Resolution, who no longer live or work in Indonesia, and are subsequently abused by other parties.
(Source: NRA TF/PF 2021)

PF risk assessment:

Indonesia finalised its National Risk Assessment on PF in 2021. Overall, Indonesia identified a medium level of PF risk, considering existing diplomatic and economic relationships with Iran and the Democratic People's Republic of Korea (DPRK), and the country'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 where their accounts have subsequently been misused by other parties. Nevertheless, some PF risk mitigation has been conducted, such as enacting a Joint Regulation that designates persons or entities based on the UN list, both for Iran and DPRK, concerning financing for the proliferation of weapons of mass destruction (WMD) purposes. The Joint Regulation also allows for the freezing of funds without delay to be conducted where the funds are owned by persons and entities listed on the list related to financing for the proliferation of WMD, which was enacted on 31 May 2017.

Implementation of the Joint Regulation was expanded to require financial institutions to identify and freeze the assets of individuals or entities, including those affiliated with UN designated persons and entities. Moreover, in order to mitigate the PF risk, some of Indonesia's financial institutions limit international fund transactions related with Iran and DPRK, including wire transfers, and a few financial institutions will not open any business relationship with Iran and DPRK.

Indonesia also established a WMD Task Force in 2017 that consists of PPATK (FIU), State Intelligence Agency, Indonesian National Police, Ministry of Foreign Affairs, and NERA (Nuclear Supervision Authority). The taskforce has the main task to identify and monitor activities and the financial activity of individuals or entities, including those affiliated with UN designated persons and entities, through ensuring the spontaneous exchange of information.

The document of Indonesia's NRA on TF and PF can be accessed at the following link: http://www.ppatk.go.id/backend/assets/uploads/20220412140054.pdf

Malaysia

Bank Negara Malaysia (BNM) had in August 2021 published the sanitised version of the Proliferation Financing Risk Assessment Report 2021 (PFRA) directed at reporting institutions and the public at large, which is made available on BNM's AML/CFT website (https://amlcft.bnm.gov.my), upon the endorsement of the National Coordination Committee to Counter Money Laundering (NCC).

Based on the assessment, Malaysia's net risk for PF is rated as at the medium low level, considering the medium low level of overall inherent risks (threats, vulnerabilities and likelihood of occurrences) and acceptable level of control measures. The findings are summarised as follow:

1. Inherent risks
   • High overall risk for weapons of mass destruction (WMD) proliferation mainly due to risks and threats emanating from the potential support network, compounded by several structural factors that are assessed as medium to high risks.

   • Low overall vulnerabilities risk mainly due to no financial services provided to any UNSC designated person, low exposure to high-risk customers, services and sectors.
   • Likelihood of PF risk is assessed as medium low in comparison with crimes assessed under the National Risk Assessment 2017.

2. Control measures
   • Country's overall control measures against threats, vulnerabilities and likelihood of P/PF is assessed to be acceptable mainly due to having a comprehensive legal framework to combat P and PF supported by an acceptable level of domestic and international cooperation as well as adequate financial sector oversight. In addition to the above findings, the report also featured the scope and methodology used in the assessment and an illustration of a common modus operandi of proliferation of WMD and PF. Future works on the recommendations will be driven and carried out by the existing domestic coordination platforms such as the NCC (led by BNM) and the Strategic Trade Action Committee (STAC) (led by the Ministry of International Trade and Industry).

Philippines

Possible Proliferation of Weapons of Mass Destruction

This case pertains to a resulting Financial Intelligence Report brought about by the request for assistance by an international agency regarding a Filipino national who may be involved in a case of the possible proliferation of weapons of mass destruction. Organization Y was registered in a foreign country as confirmed by the authorities on 24 April 2019. Ms. Y was provided as the director/shareholder/beneficial owner of Vessel Y. Based on information on specialised maritime databases, Vessel Z was sold and changed its name to Vessel Y with the ownership changed to Organisation Y in June 2019.

The area of concern is the apparent travel of Vessel Z from one communist country to another in August 2019. The resulting investigation revealed that Ms. Y had a conflicting declaration as to the sources of funds. The covered person's review of the account of the subject showed 10 cash deposits ranging from PHP 400,000 (approx. USD 7,557) to PHP 2,991,000 (approx. USD 56,509) from December 2015 to December 2016. Notably, the bank account was already closed on 26 January 2017.

The subject had a high volume of cash deposits and cheque clearing transactions from 2015 to 2020 which was around the time of the registration of Organisation Y in the foreign country and the purchase of Vessel Z by Organisation Y where Ms. Y is provided as the organisation's director/shareholder/beneficial owner. Aside from a conflicting declaration of sources of funds, an initial verification disclosed that the aforementioned entities were not registered with a government agency in the country. In addition, Ms. Y and her husband were the subjects of STRs filed by a covered person in 2017 since the subjects' transactions seem to have no underlying economic purpose.

Proliferation financing risk assessment

The Anti-Money Laundering Council (AMLC), in coordination with the National AML/CTF Coordinating Committee's (NACC) Terrorism Financing and Proliferation Financing Subcommittee (TFPFSC), is in the process of gathering qualitative and quantitative data and information from law enforcement and government agencies, and other relevant stakeholders, to support the drafting of the Philippines' proliferation financing (PF) risk assessment. The assessment of PF risks will be incorporated in the terrorism and terrorism financing risk assessment update, which is set to be finalised by December 2022.

Thailand

Progress on Thailand's PF risk assessment

Thailand is drafting a national risk assessment (NRA) which also captures PF. The PF risk assessment is conducted to comply with revised Recommendation 1 by focusing on the breach, non-implementation, or evasion of PF-TFS identified in the United Nations Security Council (UNSC) Resolutions on the Democratic People's Republic of Korea (DPRK) and Iran. The assessment also considers other issues affecting PF risks. Threats, vulnerabilities and consequences of PF are assessed. In terms of threats, Thailand assesses the potential breach, non-implementation, or evasion of the targeted financial sanctions obligations referred to in Recommendation 7 including direct and indirect activities which might generate income to support WMD. Regarding vulnerabilities, Thailand considers related laws including competent authorities and concerned private sector implementation. The updated NRA will be finalised in June 2022.

The initial result shows that Thailand's PF risk is quite low due to no PF cases related to the evasion of targeted financial sanctions by designated persons or entities and no illegal activities or businesses performed to generate income to support WMD. The main laws are the Counter-Terrorism and Proliferation of Weapons of Mass Destruction Financing Act B.E. 2559 (2016) and the Control of Item in Relation to the Proliferation of Weapons of Mass Destruction Act B.E. 2562 (2019). However, Thailand needs to strengthen public and private collaboration to

increase the awareness of relevant private businesses, develop an internal work system to control WMD items, and share information on controlled items related to WMD and suspicious items including dual-use items.

Singapore

Building on its existing understanding of proliferation financing (PF) risks from cases, intelligence and supervisory engagements, Singapore is now updating its PF risk understanding via a national PF risk assessment (PF NRA). To ensure that the PF NRA is comprehensive and takes into account the elements recommended by the FATF, Singapore has placed this under an interagency framework involving relevant law enforcement agencies, the financial intelligence unit and supervisory agencies, which would also factor in industry feedback and exchanges of information between the public and private sectors.

In addition, we have set up a Work Group under the auspice of Singapore's AML/CFT Industry Partnership to seek industry feedback from financial institutions (e.g. banks and insurers) and DNFBPs (e.g. lawyers and company service providers). We expect to complete the PF NRA by end-2022. Concurrently, Singapore agencies continue to raise industry PF risk awareness through sharing about PF cases and the revised FATF requirements such as at the July 2021 Association of Banks of Singapore Financial Crime Seminar.

Vietnam

In 2021, Vietnam had not discovered any violations related to proliferation financing of weapons of mass destruction.

Regarding the promulgation of legislative documents, Vietnam has issued documents such as: Decision No. 262/QyĐ-BQP dated 27/01/2022 of the Minister of the Ministry of Defense (MOD) on Regulations on Inclusion and removal from the list of organisations, individuals involved in proliferation and financing of proliferation of weapons of mass destruction; Decision No. 263/QyĐ-BQP dated 27/01/2022 of the Minister of MOD on Regulations on receiving information and requests related to proliferation and financing of proliferation of weapons of mass destruction from other countries.

On international cooperation, Vietnam has coordinated with the US Program on Export Control and Border Security (EXBS) to organize three international seminars on dual-use goods control; participating in the Workshop of the ASEAN network of military experts on chemistry, biology and radioactivity (CBR); participated in the Workshop on Capacity Building for the Implementation of UN Sanctions Resolutions organised by The Federal Office for Economic Affairs and Export Control (BAFA) of the Federal Republic of Germany; participated in the Training on Identification of Dual-Use Goods (CIT) organised by the US Embassy in cooperation with the General Department of Customs; participated in meetings on anti-money laundering, counter-terrorism financing, counter the financing of proliferation with the APG.

Regarding the training exercises for counter proliferation, Vietnam has been developing scenarios to combat against the proliferation of weapons of mass destruction; successfully arranged the first meeting of the Vietnam National Focal Agency on February 23, 2022;

approved the Report on implementation results of Decree No. 81/2019/NĐ-CP on preventing and countering proliferation of weapons of mass destruction.

6.2 Guidance materials provided to FIs and DNFBPs on identifying, assessing and mitigating PF risks.

Chinese Taipei

On 7 November 2018, Chinese Taipei passed the Amendments to the Counter-Terrorism Financing Action (CTF Act). The title, Amendments to CTF, specified that the amendments made to the CTF Act were to ensure that the scope of Targeted Financial Sanctions (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 the international regulations.

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 a foundation with high risk by the competent authorities through the procedures of risk assessment, to avoid those foundations being abused for the means of money laundering and terrorist financing.

In addition, the MoJ promulgated “Guidance” in September 2021, indicating that lawyers shall take appropriate acts to identify, match and filter the TF and PF list as well as enhance CDD measures and continuously monitor TF and PF activities for the purpose of preventing money laundering and combating terrorist financing.

POJK 23 2019 and PBI 19 2017 are AML CFT Regulations that require financial institutions to identify, assess and mitigate ML/TF/PF Risk. These regulations require financial institutions to conduct CDD and other preventive measures.

PPATK (Indonesia FIU) as a regulator on DNFBPs enacted guidance (Circular Letter 02 2017) on how to implement freezing orders without delay on PF, including how DNFBPs must identify all transactions and activities that indicate having affiliates with designated persons.

Japan

The Japanese Ministry of Finance (MOF) published the "Foreign Exchange Inspection Guideline" on measures that financial institutions should take to comply with obligations related to economic sanctions under the Foreign Exchange and Foreign Trade Act and to mitigate proliferation finance risks.

For details, please refer to the following link.
https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/e_g_zenbun.pdf

Thailand

1. In 2021, the Anti-Money Laundering Office (AMLO) published guidance on Counter-Terrorism and Proliferation of Weapon of Mass Destruction Financing Act B.E. 2559 (2016) to all reporting entities including a detailed approach of internal auditing on TF/PF risks covering assessing, managing and mitigating risks in various factors such as products, services, channels of customer service and geography of the reporting entities.

2. In 2022, AMLO published the guidance on CDD for reporting entities including a detailed approach in assessing the TF/PF risks which apply to internal risk management, customer risk assessment and risk mitigation. Procedures, methods, and examples of risk assessment are described in the guidance.

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

Chinese Taipei

Illegal transaction between company J and Iran: In November 2018, company J intended to export and sell electronic control equipment to company S in Iran, but failed to apply for an export license in accordance with the "Regulations Governing Export and Import of Strategic High-tech Commodities." In the export process, the Chinese Taipei Customs Administration twice recognised that some of the commodities were strategic high-tech commodities with no export license application, and rejected providing customs clearance. However, to seek a successful export for commercial benefits and evade relevant export control regulations, company J arranged the private shipment of the goods to Iran through Jurisdiction D's logistics company Z. After verification of the case, individual B, the business manager of company J, was transferred to the Prosecutor's Office in May 2020 for violating the Foreign Trade Act by illegally exporting strategic high-tech commodities. In March 2021, the prosecutor filed a lawsuit, which is now pending the judgment of the court of first instance.

Illegal transaction between company B and Iran: Individual C, the actual person in charge of company B, knew that some of the water purifiers (filters) and their parts and components sold by the company qualified as "strategic high-tech commodities" and the company should in advance apply for and obtain an export license before exporting them to Iran.

However, with the intention of exporting and selling water purifiers (filters) and their parts and components for profit, individual C colluded with the Iranian company F in providing false information about a number of receiving companies in Jurisdiction E, and circumvented relevant export control regulations and privately transferred the commodities to Iran. After verification of the case, individual C was transferred to the Attorney's Office in September 2021 for violating the Foreign Trade Act by illegally exporting strategic high-tech commodities. In December 2021, the prosecutor filed a lawsuit, and the judge sentenced individual C to six months in prison in January 2022.

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

Hong Kong, China

- The 2nd Hong Kong Money Laundering and Terrorist Financing Risk Assessment (HRA) is being carried out, and the report will be published in due course.

- The Financial Intelligence and Investigation Bureau of the Hong Kong Police published the Strategic Analysis Report on ML trends relating to the Dealers of Metals and Precious Stones. The Joint Financial Intelligence Unit of Hong Kong also 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.

The Strategic Analysis Report on ML trends relating to the Dealers of Metals and Precious Stones can be found at the following link:

https://www.jfiu.gov.hk/info/doc/SAR_ON_DPMS.pdf

Indonesia

ML:

- Corporations and individuals are perpetrators of ML offences which are included in the high risk category.
- Legislative and Government Officials, and employees of State-Owned Enterprises and Regional-Owned Enterprises are types of individual job profiles that are categorised as high risk.
- Limited Liability Companies (PT) have a high risk as perpetrators and facilitators for ML offences.
- Motor Vehicle Traders, Property Companies or Property Agents, Commercial Banks and foreign exchange businesses are industrial sectors that are categorised as high risk entities for involvement in ML offences.
- Use of false identities, use of nominees (loan names), trusts, family members or third parties, property/real estate including the role of property agents, smurfing, structuring, use of Professional Services, use of new payment methods/systems and corporate use (legal persons) are typologies that are categorized as high risk for ML offences.

TF:

Sequentially, the profiles of terrorist financing actors at risk are: entrepreneurs/entrepreneurs, private employees, and traders.

(Source: NRA ML and TF/PF 2021
https://www.ppatk.go.id//backend/assets/images/publikasi/1637374266_.pdf)

Japan

The National Risk Assessment-Baseline Analysis was published in December 2014 by the working group, which consisted of the National Police Agency and other relevant ministries and agencies, including the Financial Services Agency.

Since then, pursuant to the provisions (Article 3, paragraph 3) of the Act on Prevention of Transfer of Criminal Proceeds, which were newly established when the act was revised in 2014, the National Public Safety Commission has prepared and published a National Risk Assessment-Follow-up Report, that describes risks, etc. in each category of the transactions carried out by business operators, in keeping with the contents of the NRA-Baseline Analysis.

Macao, China

Common ML methods detected from STRs received are as follows:

- Irregular large cash withdrawals;
- Significant cash deposits with non-verifiable sources of funds;
- Chips conversion without / with minimal gambling activities;
- Use of ATM, phone banking, cash deposit machines;
- Chips conversion/marker redemption/gambling on behalf of a third party;
- Possible match with screening system watch-list or other black list;
- Use of cheques/account transfer etc. to transfer funds;
- Currency exchange/ cash conversion;
- Suspicious wire transfers;
- Suspected to be engaged in illegal financial activities.

Malaysia

In July 2021, the National Coordination Committee to Counter Money Laundering (NCC) endorsed the report on Malaysia's Money Laundering / Terrorism Financing (ML/TF) Risk Assessment on Legal Arrangements. The report is the country's first in-depth risk assessment conducted specifically on legal arrangements and was aimed at:
• Mapping out the landscape of legal arrangements in Malaysia;
• Assessing the overall ML/TF vulnerabilities of legal arrangements by sector and types of legal arrangement; and
• Recommending measures to mitigate the identified ML/TF risks and address gaps in relation to the transparency of legal arrangements in the country.

The report was disseminated to all relevant stakeholders including the NCC members and reporting institutions in both the financial and DNFBP sectors in August 2021.

Philippines

Based on the Anti-Money Laundering Council (AMLC) Study "An Assessment of the Philippines' Exposure to External and Internal Threats based on Suspicious Transaction Reports (STRs) for 2018-2020":

Drug Trafficking

Based on STRs submitted by various covered persons (CPs) from 2018 to 2020, it was observed that the majority of the illicit funds from drug trafficking remained within the Philippines and circulated around the financial system generally through banks. There were also international inward remittances that are associated with transactions of perpetrators arrested in buy-bust operations (an undercover operation by narcotics detectives to catch unsuspecting drug dealers), persons possibly involved in selling and possession of illegal drugs, persons allegedly involved in bringing drugs into jail facilities, or an alleged member of a drug syndicate, among others. For outward international transfers, these are connected to persons allegedly involved in drug trafficking, selling and possession of narcotics, or who have been identified as possible members and financiers of a drug group.

Plunder and Corruption-related crimes

It was observed that the majority of illicit funds sourced from corruption-related offences were generated and circulated within the Philippines' financial system mainly through banks. For inward international transfers, these were attributable to various subjects found guilty of graft and direct bribery, and to a person administratively charged with a serious irregularity in the performance of their duties including dishonesty and grave misconduct by a certain executive department in 2019.

While for outward international transfers, some of the remittances were transactions of persons with an alleged connection to a case involving a fund scam, or a confirmed match with a politician who was charged with graft and corrupt behaviour over alleged irregular agriculture development programs.

Investment Scams and Fraud

Violations of the Securities Regulation Code (SRC)

The proceeds of fraud mostly circulated and remained within the Philippines' financial system.

Although violators commonly used pawnshops to transfer the criminal proceeds, a substantial amount of the illicit funds was still channelled through banks. For international inward remittances, some of these represented the proceeds from victims of investment scams, such as those involving cryptocurrencies, Ponzi schemes or pyramid schemes, and boiler room operations. One of the outward international remittances included a transaction worth PHP 39.29 million (approx. USD 742,285) which was associated with one of the biggest Ponzi scheme operations in the country. The aforementioned amount was intended to be a down payment for a franchise that the perpetrators were interested in acquiring.

Swindling

Based on the STRs submitted by various covered persons for the period January 2018 to December 2020, it was observed that the Philippines has been the predominant source of proceeds of fraud that mostly circulated and remained within the Philippines' financial system.

Although violators also used money service businesses to move the criminal proceeds, banks remained as the primary financial channel used, both in volume and peso value of fraud related STRs. It should be noted, however, that PHP 29.0 billion (approx. USD 547,882,212) of the peso value of inflows is attributable to one STR that was filed in September 2020 on a certain individual, representing a Foreign-based company, who attempted to victimise a domestic corporation by issuing a falsified document.

The high value of reported funds resulted from the reporting by the covered person of the value of the falsified document as the transaction amount of the STR. For transaction inflows, some of these represent proceeds of different cases of fraud, such as advance fee fraud, boiler room operations, phishing/hacking, issuances of falsified financial documents, pyramid schemes, and different kinds of scams (package, romance, inheritance, etc.). While for outward international remittances, these include funds representing the proceeds of different types of fraud, such as investment scams, romance scams, and counterfeiting of financial documents, e-mail hacking, consumer fraud, employment scams, among others.

Smuggling

Based on the STRs submitted by various covered persons from 2018 to 2020, it was observed that all transactions related to smuggling occurred within the Philippines. These were generally transacted through banks. Most of the domestic transactions were generally linked to the smuggling of carrots, cigarettes, rice, used clothing (colloquially known as "ukay-ukay"), sugar, jewellery, luxury vehicles, and medical supplies. Also included are transactions reportedly involving tithes and donations from members of a church, whose founder was featured in the news for alleged USD smuggling and gunrunning.

Trafficking in Persons, Child Exploitation, and other Related Crimes

Violations of the Anti-Trafficking in Persons Act of 2003

Based on the STRs submitted by various covered persons from 2018 to 2020, it was observed that the bulk of the reported transactions associated with trafficking in persons occurred within the Philippines. Most the transactions were channelled through banks (39.91%) and pawnshops (34.53%). The majority of these transactions were linked to cyber and child pornography (including online child exploitation activities), facilitation of prostitution, and illegal smuggling of people from the Philippines or trafficking in persons.

Violations of the Anti-Photo and Video Voyeurism Act of 2009

The majority or 55.28% in terms of volume and 62.31% in terms of peso value of suspicious transactions linked to photo and video voyeurism occurred within the Philippines. Most of these transactions were linked to selling pornographic videos. Also, there are transactions that were reported by the covered person due to the adverse news that the client allegedly threatened to leak sex videos of his former girlfriend.

Violations of the Anti-Child Pornography Act of 2009

It was observed that majority of the illicit funds from child pornography came from sender-countries abroad. In terms of peso value, most of the funds reported in STRs were channelled through banks and money service businesses (MSBs), while volume-wise, the bulk of the suspicious proceeds were transacted through MSBs and pawnshops.

For inflows, the majority of the transactions were reported as a result of an in-depth review conducted on consumers, who were identified based on a transaction pattern related to possible child exploitation. The activities were identified as suspicious due to possible child exploitation concerns, a possible intention to mask activity and avoid the detection of multiple transactions for similar dollar amounts and multiple geographical locations to one or many receivers in the Philippines within the same day or consecutive days. There were also inward remittances of a client who was identified by the covered person as an exact match with one of the employees of a company, who was arrested for allegedly engaging in online dating and cyber pornography-related activities.

Thailand

1. The Anti-Money Laundering Office (AMLO) is updating the National Risk Assessment (NRA) which will be finished in 2022.
2. AMLO conducted and distributed reports and typologies on ML/TF methods and trends to public and private sectors as follows;

(1) Exploiting cryptocurrency in crime and money laundering
(2) Situation on committing public fraud
(3) Typologies on crime and money laundering related to gambling
(4) Typologies on crime and money laundering related to corruption, fraud and misappropriation of government subsidies

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

Brunei Darussalam

In 2021, theft and fraud (including forgery for the purposes of cheating) were seen to be among the most common predicate offences in Brunei.

Case Study: Sale of stolen property

On 8 March 2021, a Bruneian man (Mr MSH) was convicted of selling stolen items under the Criminal Asset Recovery Order, 2012 (CARO, 2012). The Magistrate's Court based its conviction on the prosecution's evidence of having proven that the defendant had knowledge or reasons to suspect, or failed to ensure that the property he dealt with was not derived from criminal activity.

The defendant failed to prove his innocence against the charges which stated that he had sold a BenQ projector along with its bag, a Sony PlayStation Vita, 13 branded sunglasses and five other sunglasses along with their cases between 1 June and 29 July 29 2019. He then sold 15 top-up cards each valued at BND 10 (approx. USD 7) between 19 June and 29 July 2019.

Between 24 June and 29 July 2019, the defendant sold six luxury watches, five branded watches and foreign currency notes including two 10,000 notes of Cambodian riel (approx. USD 4), five 1,000 notes of Cambodian riel (approx. USD 1), 17 notes of 500 Cambodian riel (approx. USD 2), eight notes of 100 Cambodian riel (approx. USD 0.1), one note of 10,000 Colombian peso (approx. USD 2), five notes of 1,000 Colombian peso (approx. USD 1), one note of 10 Cuban peso, one note of one Cuban peso (approx. USD 0.4), one note of 5,000 Lao kip (approx. USD 0.35) and one United States dollar (USD).

The defendant owned a shop in the Jaya Setia Square commercial area and started dealing with an individual from Jurisdiction A named Mr FP since June 2019 after which he accumulated all of his illegally obtained property. The defendant in his defence said that he had no reason to suspect Mr FP of supplying him with stolen items.

However, in the course of the trial, the prosecution's case showed the court otherwise, in particular an instance where the defendant bargained with Mr FP to agree on very low payments for the luxury watches.

Chinese Taipei

The Criminal Investigation Bureau (CIB) recently received intelligence that a criminal group was planning to smuggle illegal narcotics into Chinese Taipei using international express packages. An investigation was promptly launched and a task force was set up under the command of Prosecutor Chiang from the Taipei District Prosecutors' Office. A suspect, individual A, was eventually identified by the task force after a month of investigations as the recipient of marijuana packages.

Once the time was right, individual A was arrested as the recipient. Individual B, Individual C and a suspect from Jurisdiction A involved in drug smuggling were also arrested. Collaboration between agencies (Customs Administration and Finance) helped to impound an express mail package imported by the group from Jurisdiction B. 4kg of marijuana was hidden inside a latex mattress. The task force determined that Individual B was the real owner with Individual C being responsible for sales. Individual A was responsible for receiving the drug packages and communicating the quantity of drugs required to the suspect from Jurisdiction A.

The suspect from Jurisdiction A then contacted the seller in Jurisdiction B to send the shipment. The suspects used multiple mobile phone numbers to communicate and had no fixed address, so the task force took over a month to determine the route used for drug smuggling and their current address. Three waves of raids were subsequently launched to track down the owner, seller and suspect organising foreign drug shipments. The suspects were interrogated before the whole case was transferred to the Taipei District Prosecutors Office for prosecution in accordance with the Narcotics Hazard Prevention Act.

Analysis found that most of the marijuana packages intercepted really came from Jurisdiction C and Jurisdiction B, where marijuana has been legalised. Marijuana is however classified as

a grade 2 drug in Chinese Taipei. Those found guilty of its manufacture, transport and sale could be sentenced to life imprisonment or more than 10 years in prison.

Hong Kong, China

- Hong Kong, China continues to be exposed to both external and internal ML threats, in particular transnational /cross-border ML syndicates given its status as an international finance, trade and transportation centre.

- Fraud-related crime continued to be the most prevalent predicate offences in terms of the quantity of investigation/conviction cases and proceeds involved, and is thus considered the most significant threat factor, followed by drug-related offences.

Case

Under an anti-narcotics operation, Hong Kong Customs arrested two men for drug trafficking, where 11.3 kilograms of gamma-butyrolactone (GBL), 1.5 kilograms of methamphetamine, other quantities of assorted dangerous drugs and HKD 0.38 million (approx. USD 48,437) of cash were seized from an inbound parcel and in their residential premises. A subsequent financial investigation revealed that the drug proceeds were deposited into the joint bank account held by the two men for the purpose of money laundering. In August 2020, one of those arrested was convicted of drug trafficking and money laundering offences and sentenced to 16 years and four months' imprisonment, and in October 2021, the other was convicted of money laundering and sentenced to two years and four months' imprisonment. HKD 5.58 million (approx. USD 711,271) worth of properties were also restrained by court order pending confiscation.

- Other predicate offences including foreign tax and foreign corruption continued to be major global and regional concerns and were therefore assigned a higher threat rating, though enforcement statistics indicated a stable trend.

Indonesia

ML:
Domestic Risk:

Corruption and narcotics are types of crimes from ML offences which are categorised as having a high risk of ML offences.

Inward Risk-Foreign Predicate Crimes:
Fraud, Corruption, Funds Transfer, Narcotics, Electronic Transaction Information (ITE) or cybercrimes are types of predicate crimes of ML which are categorised as having a high threat of ML.

Outward Risk-Laundering Offshore:
Corruption and Narcotics are types of predicate crimes which are categorised as having a high threat of ML offences.

TF:
At the fundraising stage, in the form of: personal sponsors (terrorist financier/fundraiser), irregularities in collecting donations through mass organisations, and legitimate business ventures.

At the fund transfer stage, in the form of: through Financial Service Providers, cross-border cash carrying, and using new payment methods.

At the stage of using the funds, in the form of: purchasing weapons and explosives, training in the manufacture of weapons and explosives, training in the use of weapons and explosives, and travel expenses to and from the location of acts of terrorism.
(Source: NRA ML and TF/PF 2021)

Malaysia

Case study 1: Organised crime

In March 2021, the Royal Malaysia Police (RMP) launched a massive operation to arrest the mastermind of an organised crime group (Mastermind A) and all of his accomplices. A total of 70 raids were conducted, with 118 individuals questioned and 68 arrested with 41 bank accounts worth more than RM 4 million (approx. USD 911,242) frozen.

RMP also seized cash worth RM 770,000 (approx. USD 175,414), foreign currencies worth more than RM 7 million (approx. USD 1,594,674), 16 luxury vehicles worth RM 6.67 million (approx. USD 1,519,497), 35 vehicles worth RM 8.86 million (approx. USD 2,018,402) as well as a Glock pistol and 40 bullets.

16 of the suspects were subsequently charged under the Security Offences (Special Measures) Act 2012 for involvement in organised crime activity and RM 7 million (approx. USD 1,594,674) worth of cash and vehicles were seized.

The case was opened following RMP's investigation into counterfeit phone sales, where the proceeds were sent to a mule account under the name of companies owned by Mastermind A. Mastermind A was found to be a close associate of several other companies and individuals linked with fraudulent activities (i.e., investment scam) and illegal coin mining operations. Intelligence sources also linked Mastermind A to a former convict and leader of a foreign organised crime group (Individual B) as well as individual C, who used to operate a get-rich-quick scheme. Individual C is currently serving a jail term in Country A. Mastermind A, who was on the run, surrendered to the police in April 2022 and is currently facing 26 ML charges involving proceeds totalling RM 36 million (approx. USD 8,201,183).

Case study 2: Sexual Exploitation – A joint investigation between Jurisdiction A and Malaysia

A 40-year-old child sex offender from Lundu, Sarawak was found to have shared more than 1,000 child abuse files on multiple online platforms in the dark web since April 2007, while operating discretely through the usage of an online alias as his unique identity to remain anonymous and avoid detection by law enforcement agencies. An internal police report from global LEAs in 2019 had listed the offender's online alias as one of the top ten offenders in the world for online child exploitation on the internet.

Following years of futile attempts to uncover the offender's identity, an identification unit from Jurisdiction A made a breakthrough when they finally identified the suspect in August 2020. The Jurisdiction A Police-led operation, which included members of a Jurisdiction A state police taskforce for child victim identification, came across a possible image of the suspect on social media, which was then submitted to the RMP and officers from Jurisdiction A based in Malaysia as well as investigators from Jurisdiction B.

Subsequently, Jurisdiction A's FIU was able to identify the sex offender after coming across the same photo with the identifying information of the sex offender. With the assistance of the Jurisdiction A authorities, Malaysian authorities managed to track the child sex offender to a COVID-19 quarantine centre in Sarawak where he was in compulsory quarantine. The globally wanted offender was then taken into custody and sentenced to 48 years and six months imprisonment in Malaysia with 15 strokes of whipping. This successful operation demonstrates that collaboration among the FIUs and law enforcement authorities around the world is critical to combat sexual exploitation. The success also emphasised the need for cutting-edge technology to expedite investigations involving digital technology and cyberspace.

Nauru

The Nauru Police Force registered 16 drug related cases in 2021. Out of those 16 cases, one was in court (hard drug). Most of the reports related to cannabis.

Nauru Police conducted a raid on a foreign national who had a pending arrest warrant for another drug related matter. During the raid, Police found more than AUD 10,000 (approx. USD 7,206) as well as white powder like substance. A presumptive test was conducted and tested positive for cocaine. The money is currently in Police custody and Nauru Police will pursue forfeiture upon conviction since Nauru has a conviction-based regime for Proceeds of Crime.

Pakistan

<u>Defrauding the General Public through a Ponzi Scheme</u>

The accounts of a sole proprietorship business, Company A, were reported by a bank, upon the suspicion of high turnovers in the accounts through numerous small value inter-bank fund transfers received from multiple locations.

As per the account details, the aforementioned business was owned by Mr. S, who was engaged in digital marketing and advertising services through social media. Mr. S along with Mr. O registered the business with the Securities & Exchange Commission of Pakistan (SECP) as a private limited company with the name as "Company A" and another business with the name "Company B", with similar principal activities. The individuals were attracting the public to invest in online paid-to-click programs with the promise to investors of a share of the program's profits in exchange for paying an upfront fee or buying products.

During the analysis, it was determined that Mr. S and Mr O were using sole proprietorship accounts instead of company accounts for conducting business related transactions. The

individuals received significant funds in more than 25,000 inter-bank funds transfer transactions ranging between PKR 3,000 (approx. USD 15) to PKR 50,000 (approx. USD 252). As per records provided by the reporting entity, the individual received funds in one account from a number of branches of the same reporting entity while the funds were mostly transferred from unrelated counterparties like housewives, students, and salaried persons' accounts. Company A was also reported in the news media and social media campaigns as the members of the public protested and reclaimed their investments.

Based on the findings, financial intelligence was shared with an LEA which initiated an inquiry against the reported individuals. After the completion of the LEA's investigation, both of the individuals were arrested.

Abuse of Trade/Workers Union welfare funds

The funds for welfare activities from a union's account were embezzled by persons holding influential designations who withdrew all of the funds in cash without conducting any welfare activity.

A workers union account was reported by XYZ bank due to some unusual activity. Upon scrutiny of its documents, it was revealed that the union is a registered labour union with the Registrar of Trade Unions. As per available information, Mr. Red, Mr. Yellow and Mr. Green held the positions of President, Finance Secretary and General Secretary respectively in the union. Interestingly, all the three individuals lived in remote areas.

Very high turnover was noticed in the account and the activity in the account seemed to be inconsistent with the profile of the union. The deposits were made via clearing cheques issued by different businesses while withdrawals were made in cash immediately after being credited in the account.

The source of credits were mainly the cheques issued by different business firms/enterprises which could be the donations for the welfare of the workers or labour class. However, nearly all of the funds from the account were withdrawn in cash which created doubts as to how the funds withdrawn were used. The only public domain presence of the workers union was just a Facebook page, but nothing was available on this page which explained any welfare activity conducted by the workers.

Financial intelligence was disseminated to an LEA for investigation and to investigate the utilisation of significant amounts of cash withdrawals from the union's account.

Thailand

Acquiring assets for the commission of terrorism by gang robbery

A parcel delivery pick-up truck of K company was robbed by perpetrators to make a car bomb. Explosive devices were placed inside the stolen truck which was then parked behind a police station which was next to the district office. The car bomb was defused by authorities before it could explode. This case is under investigation by the Anti-Money Laundering Office.

7.3 Emerging trends; declining trends; continuing trends.

Australia

Australian Charities and Not-for-profits Commission (ACNC)

- COVID has resulted in less oversight by Australian NPOs on their work overseas because of the difficulty in visiting other countries and impacts on the reporting of overseas partners.
- Banks de-risking is an ongoing theme in this space with charities that operate in high-risk countries experiencing difficulties with banks closing their accounts.

Source agency: Australian Charities and Not-for-profits Commission

Brunei Darussalam

Continuing Trends

In October 2021, the FIU issued a FIU Bulletin to financial institutions and designated non-financial businesses and professions. The FIU shared statistics of terrorism financing Suspicious Transaction Reports (STR) that were received by the FIU including the number of STRs received with the identified potential crime to be terrorism financing as well as the number of STRs received in which the red-flag indicators related to high risk jurisdictions.

In general, the number of TF-related STRs has increased over the past years since 2014. It is considered that there is an improved awareness of TF matters in the banking sector. Based on the STRs received, the FIU has observed that reports were filed based on one or more of the following triggers:

- Reaction to adverse or negative published information
  The customer or the beneficiary of the transaction has been found to be a match to an adverse piece of news reporting

- Match to a sanctions list or watchlist
  The customer or the beneficiary of the transaction has been found to be a match to a sanctions list or a watch list

- Detection through transaction monitoring
  Cross-border transactions were made to or received by customers from parties in high risk or sanctioned countries.

Fiji

Emerging Trend

Pyramid Scams

The FIU noted an increase in the number of individuals engaging in pyramid scams earlier in 2021. Some of these schemes were marketed using other structures and names such as gifting circles. People who joined pyramid scams at the beginning of the scheme benefitted the most from this scam, but those who joined the scheme at a later stage made large losses as they joined multiple schemes.

Case Study– Cash Gifting

Ms. M, Ms. V and Ms. G were brought to the attention of the Fiji FIU for operating and/or promoting a cash gifting scheme on social media.

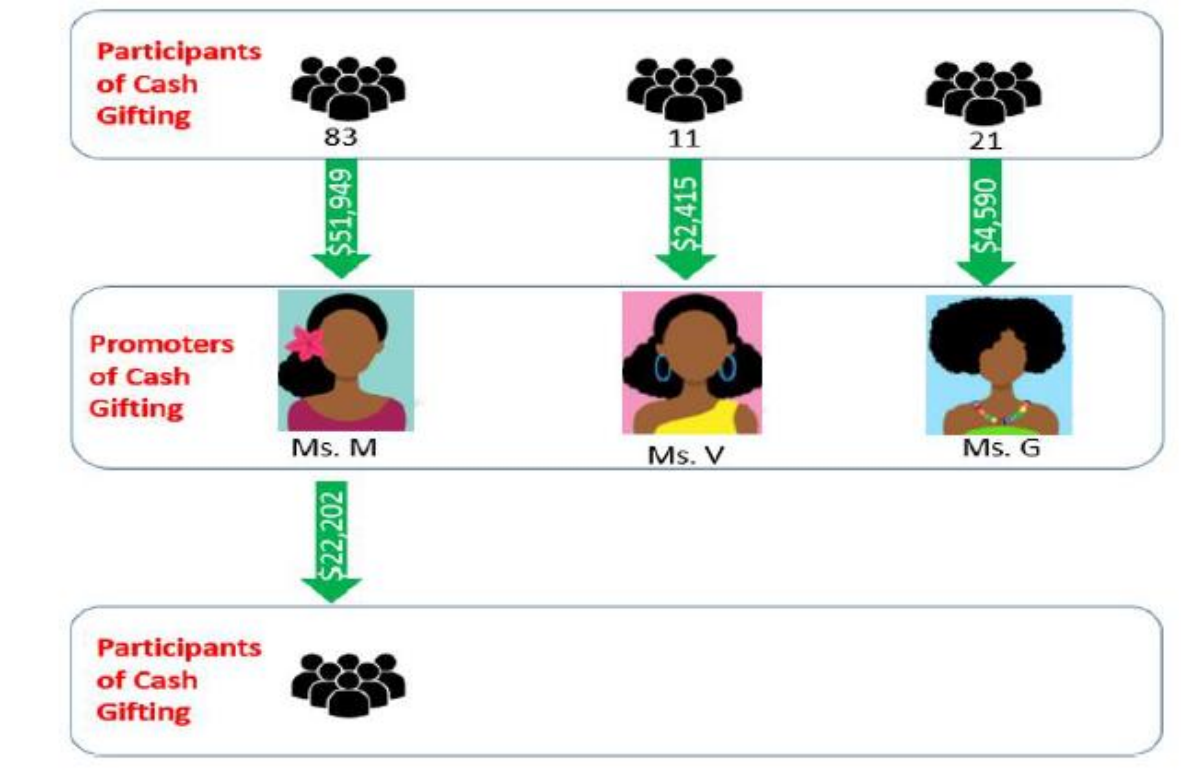
Fiji FIU analysis established that from 2019 to 2021, Ms. M received remittances totalling FJD 3,100 (approx. USD 1,450) and sent remittances totalling FJD 2,079 (approx. USD 972). Fiji FIU analysis also established that Ms. M owned two mobile money wallet accounts and that from January 2020 to March 2021, Ms. M received 83 transfers totalling approximately FJD 51,949 (approx. USD 24,312). Within the same time period, Ms. M conducted 80 transfer payments totalling approximately FJD 22,202 (approx. USD 10,390).

Ms. V was reportedly residing in Country 1, but held a savings bank account in Fiji, which was operated by her alleged nephew in Fiji. It was further reported that from 8 – 19 March 2021, Ms. V received 11 third party cash deposits totalling approximately FJD 2,415 (approx. USD 1,130). The cash was deposited into her savings bank account, which was later withdrawn by Ms. V's alleged nephew and remitted to her in Country 1.

Similarly, Ms. G was reportedly residing in Country 2, but held a savings bank account in Fiji, which was operated by her alleged boyfriend in Fiji. It was further reported that from 24 February to 15 March 2021, Ms. G received 21 third party cash deposits totalling FJD 4,590 (approx. USD 2,148). The cash was deposited into her savings bank account, which was later withdrawn by Ms. G's alleged boyfriend and remitted to her in Country 2.

Indicators:
• Frequent deposits and inward transfers from unrelated third parties immediately followed by withdrawals and outward transfers of similar amounts.
• Deposits and transfers described as "gift".
• Frequent ATM withdrawals from a bank account held by an individual who largely resides abroad.

Possible Offence:
• Operating and/or promoting an illegal pyramid selling scheme.



Case Study: Cash Gifting

Ms. Q, Ms. S and Mr. R were reported to the Fiji FIU for operating and/or promoting a cash gifting scheme. It was further reported that Ms. Q and Ms. S resided in Country 3 and were promoting a cash gifting scheme on social media whereby they received funds from various individuals in Fiji. One of those individuals was Mr. R.

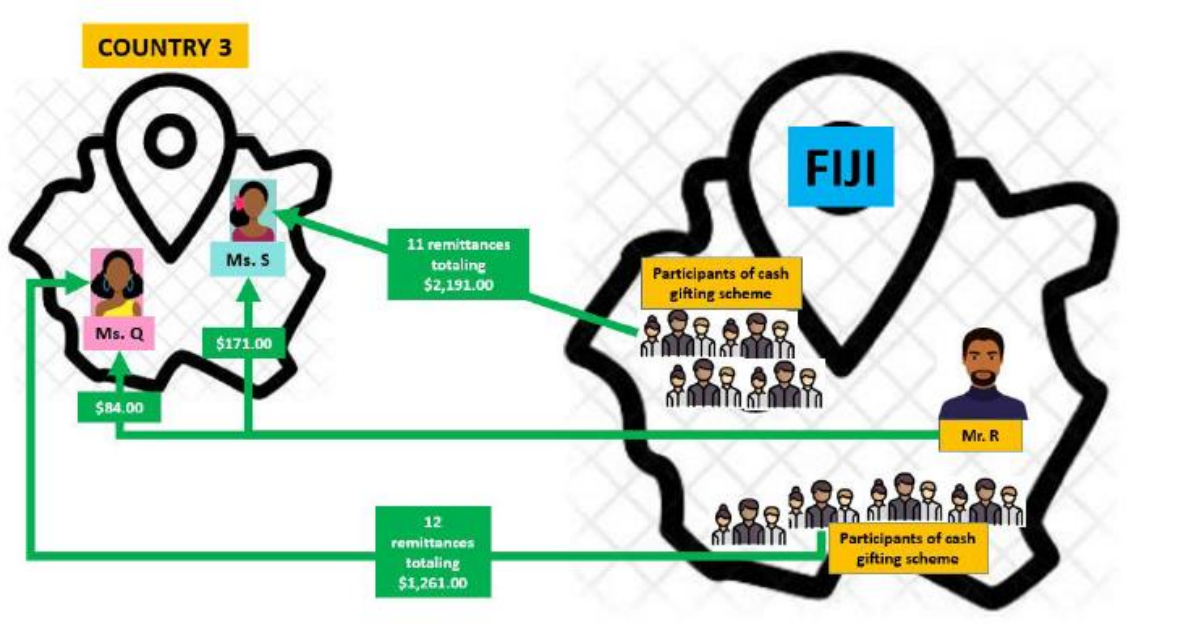
Fiji FIU analysis established that in 2021, Mr. R sent two remittances totalling FJD 255 (approx. USD 119) to Ms. Q and Ms. S in Jurisdiction A.

Fiji FIU analysis also established that from 18 – 25 February 2021, Ms. Q received 12 remittances totalling FJD 1,261 (approx. USD 590) from various individuals in Fiji. The remittances ranged between FJD 84 (approx. USD 39) and FJD 240 (approx. USD 112).

Furthermore, Fiji FIU analysis established that from 26 February to 1 March 2021, Ms. S received 11 remittances totalling FJD 2,191 (approx. USD 1,025) from various individuals in Fiji. The remittances ranged between FJD 78 (approx. USD 36) and FJD 261 (approx. USD 122).

Indicators:
• Frequent remittances of similar amounts sent by unrelated third parties to the same beneficiary.
• Remittances described as “gift”.

Possible Offence:
• Operating and/or promoting an illegal pyramid selling scheme



Use of Mobile Money Wallets and Visa Debit Cards

The FIU noted an increase in the usage of mobile money wallets to facilitate various scams including pyramid scams.

The FIU also observed the use of Visa Debit cards to perpetuate scams. Visa Debit card credentials of mule accounts were used by scammers to make online purchases and withdrawals for various scams.

Continuing Trend

Scams

Other types of scams, including romance, investment, loan and lottery scams continued to be observed in 2021. While most of the perpetrators of these scams were based abroad, the FIU noted a few cases where the perpetrators were local.

Case Study: Parcel Scam

Ms. A was brought to the attention of the Fiji FIU for receiving a third party cash deposit of FJD 2,500 (approx. USD 1,170) into her bank account. The third party mentioned that the funds were allegedly for a parcel sent by her brother from overseas. A few days later, another third party deposited FJD 1,000 (approx. USD 468) into Ms. A's bank account. The third party mentioned that she was instructed by Individual B to deposit money into Ms. A's bank account to receive her parcel from Jurisdiction B.

Fiji FIU analysis established that a police search warrant was produced at the bank on the same day for information on Ms. A. Fiji FIU analysis further established that earlier in the year, Ms. A presented an employment letter to the bank that stated her position as an Office Assistant with an overseas entity. Fiji FIU analysis of her bank account established that she received multiple third party deposits totalling FJD 43,200 (approx. USD 20,217) within five months.

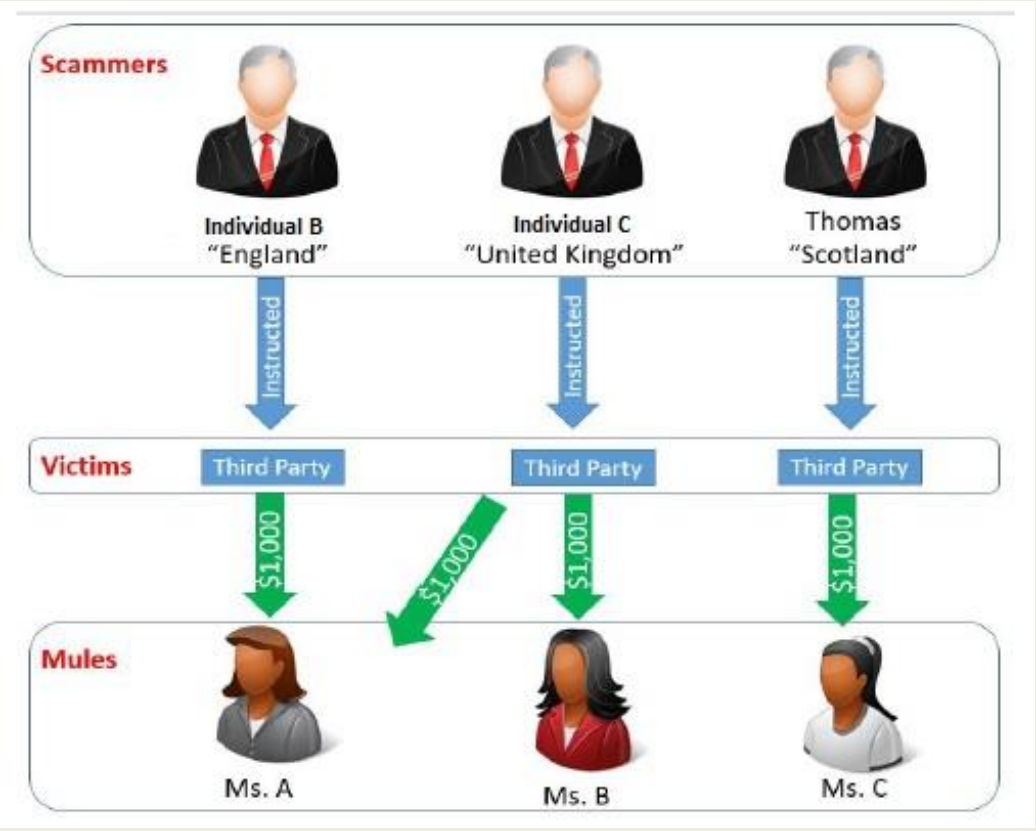
The funds were withdrawn from her bank account through various ATMs in Fiji and a cross border platform that was linked to her Visa debit card.

Case Study: Parcel Scam

Ms. B, who maintains a social welfare bank account, was brought to the attention of the Fiji FIU for an attempted cash deposit of FJD 1,000 (approx. USD 468) by a third party. The third party was allegedly approached by Individual C on Facebook who instructed her to deposit cash into Ms. B's bank account in order to receive a package from Jurisdiction B. Ms. A's bank account was also provided as an alternate bank account for the payment of the package. Fiji FIU analysis of Ms. B's bank account established that she received deposits totalling FJD 7,752 (approx. USD 3,627) within five months. The funds were withdrawn from her bank account through various ATMs in Fiji.

Case Study: Parcel Scam

Ms. C, who maintains a social welfare bank account, was also brought to the attention of the Fiji FIU for a cash deposit of FJD 1,000 (approx. USD 468) by a third party. The third party mentioned that a "Thomas" in Scotland advised to make payments to Ms. C's bank account for customs clearance of a package he had sent. The package allegedly contained an iPhone and other gadgets.



Case Study: Romance Scam

Mr. S, a known conman who was previously brought to the attention of the Fiji FIU in 2012, 2014, 2018, 2019 and 2020, was again reported to the Fiji FIU in 2021. Mr. S formed a fake online relationship with Ms. N to gain her trust and sympathy. Mr. S used the newly formed

relationship to manipulate Ms. N to transfer money to him using funds sourced from her savings account and term deposits, which she prematurely closed. Over a period of three months, Mr. S was able to fraudulently obtain FJD 200,000 (approx. USD 93,600) from Ms. N, and used an accomplice, Ms D., to receive the bank transfers.

Fiji FIU analysis established that Mr. S also purchased a motor vehicle without a loan during the three months period. It is highly likely that the motor vehicle was purchased using the proceeds of crime. Mr. S also conducted a large number of transactions through his mobile money wallet.

Fiji FIU analysis of the financial transactions of Mr. S also established that he is also being investigated by law enforcement for other similar crimes.

A case dissemination was provided to the Fiji Police Force.

Indicators:
• Premature closing of multiple term deposits
• Unusual transfers to third party accounts

Possible Offence:
• Obtaining financial advantage by deception
• Possession of proceeds of crime

Hong Kong, China

- Continuing trend: Banking sector continued to be the most popular sector for money launderers.

- Emerging trend:

  (i) Misuse of stored value facilities (SVF): In some cases, suspect even used misappropriated identity cards to transfer proceeds. In some illegal gambling cases, bookmaking syndicates received payments via SVF.

  (ii) Misuse of virtual bank (VB): Money mules were recruited to open VB accounts. In some cases, ML syndicates / money mules even used fake identity documents to open VB accounts.

  (iii) Misuse of virtual assets in the layering process is also observed in some cases.

Indonesia

Emerging ML threats:
1) The practice of buying and selling and using accounts on behalf of other parties by syndicates.
2) Misuse of E-Commerce as an illegal transaction; and
3) Unlicensed peer to peer lending

Declining ML trends: N/A
Continuing ML trends:
1) Use of false identities
2) Use of nominees for assets
3) Use of new payment methods

Emerging TF threats:
1) Virtual Assets; and
2) Online Loans.

Declining TF trends:
1) Criminal acts to raise funds

Continuing TF trends:
1) Raising funds through social media
2) Moving funds through financial service providers
(Source: NRA ML and TF/PF 2021)

Japan

- Predicate offences of the cases of the concealment of criminal proceeds in 2021 included fraud and theft. Such cases involving the concealment of criminal proceeds consisted largely of cases in which offenders attempted to transfer frauds to bank accounts in the names of other persons. Bank accounts constitute a major infrastructure used in money-laundering crimes.
- In addition, criminals used various methods to keep investigative authorities off their track, including hiding stolen properties in lockers and selling stolen goods by using other people's identification cards.
- Predicate offences of the cases involving the receipt of criminal proceeds processed in 2021 included theft, fraud, gambling and violation of the Amusement Business Act. Such cases involving the receipt of criminal proceeds included cases where offenders received criminal proceeds they gained directly via bank accounts and cases where offenders received stolen property, including by purchasing them. These cases show that criminal proceeds are transferred from one criminal to another by various means.
- There were a total of 60 cases processed as money laundering related to Boryokudan (criminal gangs) in 2021, consisting of 32 cases of the concealment of criminal proceeds and 28 of the receipt of criminal proceeds. This number accounts for 9.6% of all cases processed as money laundering under the Act on Punishment of Organized Crime in 2021.

In terms of ML crimes related to Boryokudan (criminal gangs) members by predicate offence, there were 19 fraud cases, 10 theft cases, eight violation cases of Act on Control and Improvement of Amusement Business and six loan shark cases. The Modus Operandi of these money laundering cases included using accounts in the name of other people for receiving the criminal proceeds and receiving the criminal proceeds of gambling cases, including under the pretext of protection rackets. This shows that Boryokudan (criminal gangs) commit a variety of offences and launder the criminal proceeds.

Money Laundering conducted by Foreign Visitors to Japan

- In processed cases of money laundering under the Act on Punishment of Organized Crimes in 2021, there were 91 cases related to foreign visitors to Japan, representing 14.6% of all cases. They consisted of 60 cases of concealment of criminal proceeds and 31 cases of receipt of criminal proceeds.

With regard to the predicate offences of the cases of money laundering related to foreign visitors to Japan, there were 37 fraud cases, 28 theft cases and 13 violations of the Immigration Control and Refugee Recognition Act. The Modus Operandi of money laundering cases included using bank accounts in the name of other people which were opened in Japan for receiving criminal proceeds and buying stolen items.

Lao People's Democratic Republic

Continuing trends:

In 2021, the continuing trends (indicators) of STRs received from reporting entities were as follows:

- Conduct high value transactions without sufficient reason;
- Use personal account to conduct business;
- Failing to provide or avoiding providing sufficient information.

Macao, China

Throughout the period from January to December 2021, a total of 2,435 STRs had been received by the Financial Intelligence Office (GIF), with 1,330 STRs from the gaming sector, 793 STRs from the financial sector (including banking, insurance and financial intermediaries) and 312 STRs from other sectors. During the same period, 101 STRs were disseminated to the Public Prosecutions Office for further investigation by Law Enforcement Agencies. These cases were mainly related to fraud.

Malaysia

The National Risk Assessment (NRA) 2020 was endorsed by the National Coordination Committee to Counter Money Laundering (NCC) in July 2021, which represents the 4th iteration of the risk assessment in Malaysia since 2013. The NRA examines ML/TF related threats affecting the country and identifies ML/TF vulnerabilities across various financial and non-financial sectors. The assessment draws on a wide range of quantitative and qualitative data sources including statistics from various agencies and reporting institutions, as well as internal and external reports. It also draws on input from surveys and focus group discussions conducted with law enforcement agencies, reporting institutions and other domestic and international stakeholders. Similar to the NRA 2017, the identified top high-risk crimes are fraud, corruption, illicit drug trafficking, organised crime and smuggling which remain as prevalent crimes in the country, where a higher number of cases and value of proceeds were observed particularly for fraud, corruption and illicit drug trafficking.

Continuing Trends:

Similar ML/TF trends were identified, where telecommunication scams remained prevalent in Malaysia. The continuous increase of STRs on fraud were seen as criminals continue to take advantage of the pandemic to exploit victims with scams related to medical products, investment opportunities and government assistance programmes. In addition, fraud has become more sophisticated with criminals utilising networks across multiple jurisdictions and taking advantage of advanced technologies such as spoofing technology i.e. Voice over Internet Protocol (VoIP)).

Fraudsters are found using individual mules through non-conventional methods such as non-bank remittance service providers and e-money issuers, as well as corporate mules to launder fraudulent funds. In addition, there were also signs of the exploitation of companies incorporated onshore and offshore by international fraud syndicates in moving or layering illegal proceeds via business email compromise (BEC) scams.

Emerging Trends:

Based on the NRA 2020's finding, the emergence of the digital economy, including the use of virtual assets (VA), poses a growing threat to the ML/TF landscape in Malaysia. Technologies such as online marketplaces and cryptocurrencies are likely to be abused and exploited by criminals in perpetrating their illicit activities for criminal purposes. Malaysia is largely susceptible to the ML/TF/PF risk of VAs from activities conducted in its unregulated space. While it is noted that there has been an increase in ransomware attacks associated with VAs globally in 2021, Malaysia's ML/TF/PF risk from these assets is primarily derived from illegal activities related to scams, electricity theft, identity theft and TF. It is anticipated that the scope of ML/TF/PF risk from VAs for Malaysia may increase and evolve to include tax evasion and other cybercrime activities.

Nauru

Emerging trends; Drugs related to Cannabis

Declining trends; Corruption. The National Risk Assessment for Nauru in 2018 rated corruption as a high-risk issue. However, this was based on a desk-based review and presumptive analysis. According to the Nauru Police Force there have been no reported cases since 2018.

Continuing trends: Inconclusive since Nauru is a low risk jurisdiction and no fixed patterns to confirm any continuing trends.

Solomon Islands

Emerging Trends

The FIU has noted an increase in the purchasing of digital tokens for investment in 2021. This includes the use of banks to facilitate telegraphic transfers for purchase of digital tokens offered abroad.

Continuing Trends

The FIU continues to see reported cases of illegal pyramid schemes and online scams in 2021. With the financial difficulties brought about by the COVID 19 situation, home grown illegal pyramid schemes and online scams continue to offer fake loans, monetary/material benefits and relationships to vulnerable members of the community which resulted in thousands and millions of dollars being lost to these schemes.

Thailand

ML
1. Continuing trends
(1) Using social media to conduct a Ponzi Scheme
(2) Using nominees or third parties
- To purchase real estate and luxury products to launder proceeds of crime
- To open bank accounts to receive proceeds of crime and to conceal beneficial owners
(3) Concealing proceeds of crime by investment in the stock markets or mutual funds
(4) Using unregulated exchanges including peer-to-peer exchanges to transfer illegal cash to virtual assets and to purchase virtual assets
(5) Using illegal cross-border cash couriers, underground banking and trade-based money laundering
(6) Conducting transactions via e-money and e-payment due to accessibility and non-face-to-face meetings
(7) Using shell companies and cooperatives

TF
1. Emerging trends: Using social media for fundraising

2. Continuing trends:
(1) Gang robbery for procuring assets
(2) Abuse of NPOs
(3) Use of third parties or third parties' accounts
(4) Small amounts of cash moved across borders by individual cash couriers

Vietnam

Recently, there is a rising trend of predicate offences of money laundering in cyberspace. The Ministry of Public Security has discovered and dismantled many criminal rings in cyberspace with a high risk of money laundering involved in organised gambling and fraud.

Predicate offences with a high risk of ML are increasing both in the number of cases as well as the consequences of crimes in cyberspace and the cases are becoming more serious and transnational.

Cybercrimes, money laundering and terrorist financing are becoming more sophisticated with many advanced methods. Strict supervision and control are required to minimise the risks of money laundering and terrorist financing.

7.4 Criminal knowledge of and response to law enforcement / regulations.

Hong Kong, China

While transnational criminals continued to be more sophisticated in the ML methods they employ, it is observed that for both domestic and external crimes, it is increasingly commonplace for the use of the Internet, email and social media to be involved in the commission of predicate offences. This is both due to the advancement of technology and prevalence of electronic financial services, and the social distancing norms introduced by the COVID-19 pandemic.

Thailand

Perpetrators often combine various methods in an attempt to avoid the detection of TF.

Frequently combined methods include the following:
1. Use of encrypted internet communication services for anonymous communication related to the planning of terrorist acts
2. Preferring the use of cash couriers rather than banking and Money or Value Transfer Services (MVTS).
3. Using third parties who are not connected with perpetrators and designated persons to conduct transactions

The Anti-Money Laundering Office (AMLO) has raised awareness among government agencies, reporting entities and telecommunication service providers and promoted the exchange of information through the public-private partnership on CTF measures.

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

Highest offence outcomes under the Criminal Code (section 400) and Anti-Money Laundering and Counter Terrorism Financing Act 2006 between 1 February 2021 and 28 February 2022

Row Labels	Count of Highest Outcome
Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Commonwealth)	**12**
Discontinued/Withdrawn	3
Proven	6
Schedule s16BA Crimes Act	2
Transferred to State/Territory Prosecuting Authority	1
Criminal Code (Commonwealth)	**117**
Discontinued/Withdrawn	30
Form 1 s.32 Crimes (Sentencing Procedure) Act 1999	1
Proven	79
Schedule s16BA Crimes Act	4
Transferred to State/Territory Prosecuting Authority	1
Warrant issued	2
Grand Total	**129**

*There were no offence outcomes under the Financial Transactions Reports Act 1988 or the Proceeds of Crime Act 2002

*If a matter has more than one of the same charge with either the same or different offence outcomes, the charge is listed once with the highest offence outcome selected (see example 2020PR02578).

Highest penalty outcomes under the Criminal Code (section 400) and Anti-Money Laundering and Counter Terrorism Financing Act 2006 between 1 February 2021 and 28 February 2022

Row Labels	Count of Highest Penalty
Anti-Money Laundering and Counter Terrorism Financing Act 2006 (Commonwealth)	**6**
Fine	1
Gaol	3
Gaol (Fully Suspended)	1
Recognizance Release Order	1
Criminal Code (Commonwealth)	**79**
Community Correction Order	13
Fine	13
Gaol	33
Gaol (Fully Suspended)	10
Intensive Correction Order	2
Recognizance Release Order	8
Grand Total	**85**

*There were no penalty outcomes under the Financial Transactions Reports Act 1988 or the Proceeds of Crime Act 2002

*If a matter has more than one of the same charge with either the same or different offence outcomes, the highest penalty for those charges is included.

*The reason that there is a discrepancy between the number of offence outcomes and the number of penalties is because some of the offence outcomes do not have a penalty (e.g. if outcome is withdrawn, if it is a s16BA schedule outcome, etc.).

Source agency: CDPP

China

In 2021, China reported that it criminalised self-laundering by amending the Criminal Law.

Self-laundering

From March to April 2021, Individual A gained RMB 12,350 (approx. USD 1,854) from drug trafficking and then transferred a total of RMB 8,850 (approx. USD 1,328) of the proceeds in three transfers through an online third-party payment service to his sister. The law enforcement agency identified that (1) Individual A had no legal income during that period; (2) the three online payment transfers were initiated just after completing the three drug trafficking transactions; and (3) the amounts of the two transfers were identical to those received from the transactions. Finally, the court concluded that the funds transferred were the proceeds of drug trafficking, and found Individual A guilty of the crime of money laundering in accordance with

Article 191 of the Criminal Law. In October 2021, Individual A was convicted of drug trafficking and money laundering.

Chinese Taipei

In response to recommendations related to legislation in the 3rd round mutual evaluation report of Chinese Taipei, MoJ prepared an amendment to the Anti-Money laundering Control Act in 2021. MoJ held 11 law revision consultation meetings during 2021. The draft amendment was announced on 27 December 2021 and distributed for public comment.

The 3rd round mutual evaluation report also recommended amendments to the regulations concerning DNFBPs. Chinese Taipei amended a number of sector-specific regulations in 2021 and added a number of new obligations on some of the sectors that addressed gaps identified in the MER. The amendments to the regulations particularly relate to CDD obligations, including enhanced CDD and third-party requirements, as set out below:

a. Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Notaries (January 2021), that entered into force on 25 January 2021;
b. Regulations Governing Anti-Money Laundering and Counter-Terrorist Financing for Certified Public Bookkeepers and Bookkeeping and Tax Return Filing Agents (January 2021), effective on 11 January 2021; and
c. Regulations Governing Implementation and Reporting of Anti-Money Laundering and Countering the Financing of Terrorism for Jewellery Businesses (April 2021), which came into force on 26 April 2021;
d. Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing for Land Administration Agents and Real Estate Brokerages (June 2021) which entered into force on 1 September 2021.
e. Regulations Governing Anti-Money Laundering and Counter-Terrorism Financing for Attorneys which entered into force on 15 October 2021

In compliance with Recommendation 15, the Financial Supervisory Commission (FSC) promulgated the "Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for Enterprises Handling Virtual Currency Platform or Transaction" (that is virtual asset service providers, VASPs, defined by the Financial Action Task Force, FATF) in 2021, pursuant to the 2018 amended Money Laundering Control Act that places VASPs into the AML/CFT regime, and requires VASPs to establish internal control and audit systems, and conduct customer due diligence (CDD), record keeping, cash transaction reporting and suspicious transaction reporting.

With the aim of enhancing cooperation between the law enforcement and private sectors, the FSC asked relevant financial industry associations to hold compliance forums periodically. For example, the Bankers Association invited law enforcement to share money laundering methods and cases of sanctions evasion, the Financial Examination Bureau of FSC to share financial examination deficiencies typologies and improvement advice for trade finance, and financial institutions to share due diligence and related AML measures toward third-party payment enterprises in 2021. These measures could help financial institutions better understand risks and threats and effectively assist law enforcement authorities to investigate proceeds of crime.

In 2021, the FSC revised the AML/CFT questionnaire, and updated the risk rating and risk profile of financial institutions in early 2022.

The FSC will continue to implement its AML/CFT Strategy Map, review the related regulations to conform to international standards, and supervise financial institutions to comply with AML related regulations.

Indonesia

Previously the interpretation of Law No. 8 Year 2010 (ML Law) Article 74 was that "predicate criminal investigators" are the only officials from agencies authorised by law to carry out investigations, namely the Indonesian National Police, the Prosecutor's Office, the Corruption Eradication Commission (KPK), the National Narcotics Agency (BNN), and the Directorate General of Taxes and the Directorate General of Customs and Excise, Ministry of Finance of the Republic of Indonesia. However, after a request of judicial review of the Article by civil servant investigators (PPNS) of the Ministry of Environment and Forestry (PPNS KLHK) and the Ministry of Marine Affairs and Fisheries (PPNS KKP), it was decided that "predicate criminal investigators" also include civil servant investigators from related ministries/agencies in addition to the predicate criminal investigators mentioned in the Law. The effect of the judicial review is the expansion of the number of money laundering investigators.

Japan

"National Risk Assessment-Follow up Report" was publicised by National Police Agency on 16 December 2021.

Number of STRs received:

The number of reports received in 2021 was 530,150, exceeding 500,000 for the first time.

Possible underlying factors which explain this increasing trend include the following:

○The spread of compliance culture among the general public has encouraged financial institutions' efforts to conduct stringent monitoring of potential criminal activity and illegal money transfers.
○The effects of education provided on the need to report suspicious transactions, such as seminars, held for financial institutions and others.

Number of STRs disseminated:
The number of STRs disseminated to LEAs in 2021 was 524,462, which was the highest number ever.
The number of analysis reports which used STRs and were disseminated to LEAs has continued to rise every year and in 2021 it reached a record high of 12,769.

Use of STRs by the Law Enforcement Authorities:

The number of STRs used by prefectural police departments for investigations in 2021 was 353,832.

The number of cases cleared that were initiated based on STRs and closed with arrests (STR-initiated cases) was 1,045 in 2021, and the number of arrests made by using STRs in the course of already ongoing investigations (STR-use cases) was 1,501.

Macao, China

Legislative or regulatory developments

AML/CFT Legislative or Regulatory Developments in 2021:

- Both the Convention for the Suppression of Unlawful Acts against the Safety of Maritime Navigation and the Protocol for the Suppression of Unlawful Acts against the Safety of Fixed Platforms Located on the Continental Shelf have been extended to Macao, China through the Notice of the Chief Executive no. 5/2021. With this progress, all the nine conventions covered by the International Convention for the Suppression of Financing of Terrorism were fulfilled.

- An AML/CFT supplementary guidance on remote on-boarding of customers was issued in March 2021 by the Monetary Authority (AMCM), requiring financial institutions to equip themselves with appropriate risk mitigation measures to control the ML/TF risks and other risks when leveraging technology to on-board customers remotely. The newly issued guideline has no impact on detecting and/or preventing particular methods.

- As part of the AMCM's efforts to strengthen the AML/CFT regulatory regime of the insurance sector, in July 2021, AMCM issued "Conduct Rules for Insurance Intermediary Activities", "Guidelines on Conduct Requirements for Insurance Agents' Activities" and "Guidelines on Conduct Requirements for Insurance Brokers' Activities" with an effective date from 1 Jan 2022, which includes mandatory observance of the AML/CFT law and regulations by individual insurance agents, and an AML/CFT compliance requirement regarding premium handling. The guidelines also require insurers to have control policies in place regarding funds being handled by insurance intermediaries, so as to mitigate the risk of breaching AML/CFT requirements.

Overall statistics and cases developed directly from suspicious or cash/threshold transaction reports

i. In the year 2021, a total of 2,435 STRs have been received and 101 STRs were reported to the Public Prosecutions Office.

ii. In the year 2021, the number of AML investigations, prosecutions and convictions were as follows:

	AML/CFT
Investigations by the Judiciary Police	35
Investigations by the Commission Against Corruption	2
Investigations by the Public Prosecutions Office	23
Prosecutions	7

Convictions	6*

* Two cases are still under appeal.

There were no STRs, investigations, prosecutions or convictions related to TF and PF in 2021.

The Judiciary Police has continued to exchange terrorist financing related intelligence with the Financial Intelligence Office (GIF) and provide feedback to GIF in relation to counter terrorist financing measures. GIF has spontaneously disseminated overseas TF intelligence to the Judiciary Police for early prevention. The Judiciary Police has also actively conducted intelligence gathering and analysis and initiated follow-up investigations in order to identify any assets in Macao, China that are involved in any terrorist financing related activity. No indication suggested that any terrorism financing activities occurred in Macao, China.

Malaysia

On 21 December 2021, as part of its on-going initiatives to combat fraud, Bank Negara Malaysia (the Central Bank of Malaysia) published a Guidance on Financial Institutions Response to Fraud (the Guidance), focussed particularly on scams involving the use of mule accounts as a primary tool. While the Guidance is of a non-binding nature, it aims to improve financial institutions' responses in preventing the dissipation of fraudulent funds, improve coordination mechanisms between financial institutions and authorities as well as ensure the fair treatment of customers that fall victim to fraudulent activities.

The Guidance was also developed in collaboration with the banking associations and the Royal Malaysia Police (RMP) with the intention to help financial institutions to effectively implement the on-going customer due diligence and risk profiling requirements that are prescribed under the Anti-Money Laundering, Countering Financing of Terrorism and Targeted Financial Sanctions for Financial Institutions Policy Document.

In response to the amendments to Recommendation 15 of the FATF Recommendations relating to new technologies in 2019, Malaysia recently expanded the regulatory net of virtual asset service providers to include safekeeping, custodial, intermediation and advisory services. The changes came into force on 30 December 2021.

Further legislative changes were also made to include new serious offences relating to false or misleading statements for services, contests and games, false representations of approval for the supply of goods or services and the selling of controlled goods without license, amongst others. The amendments which came into effect on 30 December 2021 would enable the relevant law enforcement agency to more effectively follow the money trail and conduct investigations pursuant to the Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001.

Nauru

A Technical Assistance Project by APG is underway to enact a new Anti- Money Laundering Act and an Amended Proceeds of Crime Act aligned to the FATF Recommendations in order to strengthen technical compliance and effectiveness. Upon successfully enacting the

legislation, supporting regulations and guidance will be issued to stakeholders to ensure Nauru meets the standards to combat Money Laundering, Terrorism Financing and Proliferation Financing.

Under the Technical Assistance program, law enforcement agencies such as Nauru Police, Customs, and the Justice Department received virtual financial investigation trainings. Another Australian Border Force (ABF) virtual Aviation Border Fundamentals training was provided to Nauru Police, Immigration and customs relating to human trafficking, intelligence and document detection. These specialised trainings have boosted the capacity of Nauru in combatting/preventing money laundering and terrorism financing.

AUSTRAC is currently developing a software analysis database program for the Nauru Financial Intelligence Unit to enhance analysis capacity for detection and prevention. AUSTRAC has also provided Intelligence Fundamental Training to the FIU and Nauru Police Force.

The establishment of the Pacific Islands Intelligence Community led by AUSTRAC (Secretariat) further enhances detection and prevention capacity collaboratively at a regional level. This will strengthen intelligence and information sharing capabilities for the Pacific FIU's and Law Enforcement Agencies.

The Australian Federal Police (AFP) continues to provide support to the Nauru Police Force and the establishment of the Transnational Crime Unit is an additional boost for detection and prevention methods.

Singapore

The Estate Agents Act was amended to include the duties of estate agents and salespersons in the prevention of money laundering and financing of terrorism. The amendments, which came into effect on 30 July 2021, comprise the following:

1. Sec 44A – The licensed estate agent or a registered salesperson must take the relevant measures, consistent with the measures set by the FATF, in the prevention of money laundering and financing of terrorism.
2. Sec 44B – Customer due diligence measures
3. Sec 44C – Keeping of records
4. Sec 44D – Disclosure of suspicious transactions
5. Sec 44E – A licensed estate agent or a registered salesperson who contravenes the Estate Agents (Prevention of Money Laundering and Financing Terrorism) Regulations would be liable to disciplinary action.

The details of the duties of estate agents and salespersons on the prevention of money laundering and terrorism financing have been prescribed in the Estate Agents (Prevention of Money Laundering and Financing of Terrorism) Regulations 2021, which also came into effect on 30 July 2021.

The Estate Agents Act was also amended to allow the Council of Estate Agents (CEA) to take stronger disciplinary actions against licensed estate agents and registered salespersons that contravene the law.

The key changes to CEA's disciplinary regime include the introduction of a new Letter of Censure (LOC) disciplinary regime for minor disciplinary breaches. Under this new LOC disciplinary regime, CEA can issue an LOC and impose a financial penalty of up to SGD 5,000 (approx. USD 3,631) per case on estate agents / salespersons for minor disciplinary breaches. CEA will also publish the penalties in the estate agent's or salesperson's disciplinary records in the CEA Public Register, in order to allow the public to verify the licence status of estate agents.

The maximum financial penalty that can be imposed by the CEA Disciplinary Committee for serious disciplinary breaches was increased from SGD 75,000 (approx. USD 54,477) to SGD 200,000 (approx. USD 145,274) per case for estate agents and to SGD 100,000 (approx. USD 72,642) per case for salespersons.

Thailand

To prevent criminals or their associates from being beneficial owners or controlling or holding management functions in financial institutions, the Cooperative Promotion Department issued a Ministerial Regulation on the Operation and Supervision of Savings and Credit Cooperatives, B.E. 2564 (2021), which came into force on 10 February 2021.

In 2020, the Anti-Money Laundering Board (AMLB) issued the AMLB Ordinance on the Provision of Training to the Reporting Entities under Section 13 and Section 16, B.E. 2563 (2020) by a Legal Person. The Ordinance requires the Anti-Money Laundering Office (AMLO) to provide training to reporting entities or grant approval to other legal persons to provide training to such reporting entities. Since the Ordinance came into effect, it is evident that the knowledge and understanding of reporting entities in detecting and preventing ML/TF/PF has improved. At present, 282,864 compliance officers of such reporting entities have been trained.

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

China

Online gambling

The China Anti-Money Laundering Monitoring and Analysis Center (CAMLMAC) identified suspicious transactions conducted by H and other individuals who were laundering gambling funds. The STRs showed H and other suspects had received gambling funds and used intermediary accounts to launder the funds. Ultimately, the funds were sent to the accounts of gamblers who received money in return for the use of their accounts.

Then, CAMLMAC disseminated the financial intelligence to the police. In August 2021, the police investigated H and other suspects and found that the gang applied new ML methods by means of a large number of third-party payment tools to transfer proceeds and provided ML services for illegal activities such as online gambling. The gang connected with overseas gambling websites and operated an online gambling and ML scheme. The source and flow of illicit funds involved more than 10 provinces in China.

Japan

Illegal remittance case involving international hacking

The Japan Financial Intelligence Center (JAFIC) received information from an FIU in Jurisdiction A concerning a large account of illegal remittances received by a number of bank accounts in Japan. After analysing the information, it was revealed that the funds received in the incoming remittances had already been withdrawn from the bank accounts.

JAFIC then provided the information to an LEA. After the LEA conducted the required investigation, it identified suspect B. B was arrested on the charges of fraud and the violation of the Act on Punishment of Organized Crime and Control of Crime Proceeds. Illegal remittances from Jurisdiction A were sent not only to Japan, but also to several other jurisdictions.

Macao, China

Case: Falsification of artwork transactions to cover up the illicit proceeds of a fraud syndicate (related to Macao, China's case under section 5.17)

Several STRs received by the Financial Intelligence Office revealed that two local companies (Company B and Company S) were linked to fraud transactions. Company B was a locally registered company (incorporated in May 2016) with one of its registered businesses related to the artwork trade. In September 2017, Company B received two remittances from Country A, with a total amount of approximately EUR 113,000 (approx. USD 121,177). Soon after that, one of its shareholders and its "employee" (Suspect C), withdrew almost the whole amount in cash (local currency), claiming the transaction purposes were to buy artwork. About one week later, the bank of Company B received a notification from its corresponding bank that the two remittances were the proceeds of fraud. This triggered an STR on Company B that was filed with the Financial Intelligence Office.

Company S was a locally incorporated fashion trade company, incorporated in April 2017. A few months after its incorporation, in July 2017, Company S received a remittance from Country J, the total amount involved was approximately equivalent to USD 266,000. Due to the significant transaction amount and the inconsistency with its business profile, the bank of Company S returned the funds to the remitting bank in August.

Around two months later in October 2017, Company S received another remittance of USD 1 million from another company in Country A. Just two days later, Company S performed a series of transactions over the week, including the issuance of five cheques, ATM cash withdrawals and online payments via a card network. The five cheques were made payable to five individuals (one of which is Suspect C, who was the same person claimed as the "employee" of Company B above), of which four cheques were deposited into another bank. Similarly, the bank of Company S subsequently received a notification of fraud proceeds from its corresponding bank, thus triggering a STR filed on Company S.

Moreover, based on information sharing among the banking industry regarding Company S' fraudulent transaction, a third STR was filed by the bank where the four cheques were deposited.

By analysing the account transaction patterns, the Financial Intelligence Office discovered a number of red flags, including the short-term establishment of two companies without apparent and legitimate business transactions, the registered addresses of two companies in residential units, common remitting location and common suspect, fraud proceeds notifications from various corresponding banks, etc. Therefore, the Financial Intelligence Office disseminated the STR cases to the Public Prosecutions Office.

Singapore

Case of an unlicensed cross-border money transfer service developed directly from STR

The Suspicious Transaction Reporting Office (STRO) received information that Person C received fraudulent proceeds in his personal bank account. The Commercial Affairs Department's (CAD) investigations revealed that Person C later transferred the fraudulent proceeds to Person D's personal bank account. It was further established that Person D's personal bank account was one of several bank accounts that Person D used to receive funds from overseas for and on behalf of another person.

Person D was believed to have provided an unlicensed payment service in the form of facilitating the receipt of cross-border money transfers amounting to around SGD 251,000 (approx. USD 182,549) as well as facilitating cash withdrawals amounting to around SGD 189,700 (approx. USD 137,966) via third-party bank accounts between February and May 2020.

Between 14 and 21 May 2020, Person D also withdrew about SGD 94,500 (approx. USD 68,732) in cash, after which he delivered the funds to persons unknown to him.
Person D was charged for his suspected involvement in providing unlicensed money transfer services involving more than SGD 250,000 (approx. USD 181,831), money laundering and the obstruction of justice.

Person prosecuted in a forgery case developed directly from STR

STRO received an STR on two business loan applications submitted by Company A. In the first application, the income tax bill provided by Company A had irregularities. In the second application, the company's financial figures for the same financial year differed from the figures provided in its first application.

Pursuant to the STR, the Commercial Affairs Department (CAD) of the Singapore Police Force commenced an investigation and established that Person B, who was the loan broker of Company A, had forged the supporting documents submitted for the loan applications, involving SGD 200,000 (approx. USD 145,466), to increase the chances of Company A obtaining a bank loan. Person B would receive a commission based on the loan amount disbursed.

Person B was convicted of forgery for the purpose of cheating and sentenced to three months' imprisonment.

Thailand

Case developed directly from a suspicious transaction report

In January 2021, the Anti-Money Laundering Office (AMLO) received an STR from a Gold shop that it had received money from Ms. W who was unknown. After AMLO's investigation, Ms. W was prosecuted by the Royal Thai Police since she had persuaded the public via social media to purchase low-price gold which she claimed could be sold for a higher price. Ms. W delivered the gold as scheduled every time until she had numerous victims. However, Ms. W subsequently stopped delivering the gold and the victims were unable to contact her.

The AMLO Transaction Committee issued orders to freeze and seize assets of Ms. W over 710,000 baht (approx. USD 20,659).

Vietnam

In 2021, after analysis of suspicious transaction reports (STRs) received from credit institutions, the Anti-Money Laundering Department of the State Bank of Vietnam (Vietnam FIU) disseminated information to the Ministry of Public Security (MPS) about individuals who made highly frequent transactions through internet banking. The individuals would receive funds and then immediately transfer the funds out of the account.

The large amounts of money involved in the transactions did not align with the individuals' income and business activities according to the bank's CDD. After investigation, the MPS determined that subjects had opened multiple accounts in order to provide accounts to other individuals to transfer the proceeds of crime.

Pursuant to Resolution No. 03/2019/NQ-HĐTP dated 24 May 2019 of the Judicial Council of the Supreme People's Court, it was determined that the offence of money laundering specified in Article 324 of the Penal Code had been committed. The MPS handled the investigation of the case of "Using computer networks, telecommunications networks, electronic means to commit acts of property appropriation and money laundering" which occurred in Long Xuyen city, An Giang province, Vietnam.

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

In 2021, Brunei Darussalam continued to observe a border closure that was initially implemented in March 2020 by the Government of Brunei Darussalam. Since then it has been observed that there continues to be an increase in the discoveries of drug-related offences involving large amounts of illegal narcotics and physical cash believed to be the proceeds of crime.

Case Study: drug-related offences

In May 2021, the Brunei Narcotics Control Bureau (NCB) conducted a series of raids on a suspected drug distribution syndicate nicknamed Operation Bullseye. A total of 38 individuals were arrested including both local Bruneians and foreigners. The syndicate was believed to be led by a local Bruneian man named Mr MSS who is currently under arrest.

The NCB found and seized methamphetamines weighing 497.79 grams with an estimated street value of BND 97,000 (approx. USD 70,535) and cash of over BND 22,506 (approx. USD 16,365) during the operation. Other items seized included a Erimin (the brand name for a drug called Nimetazepam, a type of Benzodiazepine) pill, and a number of drug paraphernalia were also confiscated along with property believed to be proceeds from the drug trade, including jewellery, branded watches, electronic devices, musical instruments and eight cars.

The arrested individuals are facing charges under Section 3A, Chapter 27 of the Misuse of Drugs Act (MDA) for the possession of over 100 grams of controlled drugs for the purpose of distribution.

The cases are being investigated under Section 3 of the Criminal Asset Recovery Order (CARO), 2012 for ML; Section 6(a) of the Misuse of Drugs Act (MDA) for the possession of controlled drugs; Section 6(b) of the MDA for consuming controlled drugs; Section 7 of the MDA for possession of drug paraphernalia to consume controlled drugs and Section 10; Chapter 27 of the MDA for abetting.

Case Study: drug-related offences

In September 2021, the NCB conducted another raid on a family suspected to be involved in drug trafficking activities, in an operation called Operation Black Widow.
A total of five individuals including four women and man who are local Bruneians were arrested. The masterminds of the drug syndicate are believed to be two sisters who are aged 33 and 41 years old and were based in the Belait district.

During the operation, the NCB seized packets containing syabu (a solidified form of powdered methylamphetamine) weighing 57.4 grams with an estimated street value of BND 11,000 (approx. USD 8,003). According to a calculation, the amount of drugs seized was enough to

supply 2,000 individuals. Other items seized included BND 19,942 (approx. USD 14,507) in cash, five cars, furniture, jewellery, mobile phones and driving licences. All are believed to have been sourced from drug trafficking activities.

The case carries offences under Section 3 of the CARO, 2012 for money laundering, Section 3A of the MDA for drugs trafficking, Section 6(a) of the MDA for possession of controlled drugs, Section 6(b) of the MDA for consuming controlled drugs and Section 10 of the MDA for abetment of the offences.

In addition, the pandemic also saw a continuing increase in the number of foiled smuggling attempts of contraband goods such as alcohol and cigarettes as well as various other items such as raw and frozen meat. These cases are investigated by the Royal Customs and Excise Department (RCED) for offences under the Customs Order, 2006 and the Excise Order 2006 as well as ML offences under the CARO, 2012.

Chinese Taipei

Drug trafficking case A:

The Criminal Investigation Bureau (CIB) has been cooperating with EU law enforcement agencies over a long period of time. In October 2020, the liaison officer in the Netherlands was informed by the Belgian Customs that a drug cartel was smuggling large amounts of ketamine into the jurisdiction for sale. After matching the identities of the suspects, the Bureau's International Criminal section immediately reported the case to a District Prosecutors Office, and formed a task force to investigate the case. After months of surveillance to collect evidence, the task force found that the suspect was constantly changing vehicles, and other methods, to avoid being traced, and was allegedly transporting a large number of prohibited items to hide elsewhere. The task force also continuously changed the tracing method and finally found the suspect's location and the criminal evidence.

Drug trafficking case B:

On 29 May 2021, a large amount of narcotics hidden in coffee bags was seized from the suspect's vehicle at two parking lots in Taipei City, including 1503 bags of category 3 narcotics coffee bags at one parking lot and 6403 bags of category 3 narcotics coffee bags, unidentified blue pills, orange pills, white crystals and powder at another parking lot. The four suspects including Individual A were arrested. The suspects were detained by a District Prosecutors Office, and the court order was granted. A four-person drug cartel, including Individual A, attempted to take advantage of the severe pandemic situation in the country and the police force's staff shortages to make money by selling illegal drugs to the public.

Most drug addicts gather in groups to use narcotics in coffee bags and this is therefore a problem for pandemic prevention.

Company manufactures face masks without a licence

Due to the poor sales of Company D’s original products, person H in charge of company D began to set up machines for the production of masks in the factory of company D since August 2020, and produced masks for sale. At that time, company D did not obtain the “medical

equipment license" and was not allowed to manufacture medical equipment or sell medical equipment manufactured without permission.

However, person H designed the outer box of the mask with the text "Meltblown cloth – key raw material for epidemic mask to capture virus" and "Purpose: to prevent droplet transmission and filter microorganisms, bodily fluids and particulate dust," and then ordered an unaware printing factory to produce these mask outer boxes. After the production preparation was completed, company D, without government permission, began to use the mask production machine to produce masks from September 2020 onwards, and put some of the masks in the aforementioned outer boxes and sold them under the name of "Reassuring Masks."

As of 5 January 2021, a total of 2,398,400 masks were sold, and an illegal profit of TWD 8,105,521 (approx. USD 275,471) was made. On 15 June 2021, a District Prosecutor's Office charged the company with the crime of manufacturing medical equipment without prior permission, which is in violation of paragraph 1 of Article 84 of the Pharmaceutical Affairs Act.

Cook Islands

A general observation on the trend of predicate activities linked to COVID-19 is shown in the table below. In the Cook Islands, cybercrime has increased significantly in numbers and value from 2019 to 2020 as the COVID-19 situation escalated globally. In 2021, the trend showed a decrease in numbers and value, as a result of the outreach awareness and education campaign. Another contributing factor to the increase in cybercrime, is the connection of the Manatua underwater fibre optic cable to the Cook Islands in 2020. The cable has increased the speed capacity of the internet in the Cook Islands, resulting in more usage time.

Table 1: Total Cybercrimes Reported in the Cook Islands

Year	Number of Cybercrime	Value from the Effect of Cybercrime
2021	30	123,942
2020	42	379,501
2019	24	83,726

Hong Kong, China

Different forms of surgical masks/medical equipment scams were observed, through cold-emailing or bogus advertisements on various social media platforms. Fraudsters created bogus websites under various pretexts (such as the selling of surgical masks, lotteries for surgical masks or appeals for donations for vaccine development) to cheat victims and collect their personal information.

Case - Proof of vaccination

The Hong Kong government announced the implementation of a vaccine pass system requiring visitors to show proof of vaccination on the government's anti-pandemic mobile application 'LeaveHomeSafe' when entering various premises. After intelligence analysis, Hong Kong Police successfully identified two scammers, who not only offered forged vaccination records for sale for uploading onto the mobile application, but were also involved in a series of online shopping scams.

Scammers instructed the victims to transfer payments via stored value facilities and the Faster Payment System (a payment financial infrastructure enabling payments across different banks and stored-value facilities on a 24/7 basis introduced in 2018). The total loss of the series of online fraud cases involving the duo was HKD 250,000 (approx. USD 31,862). The duo was arrested in early 2022, and an investigation is ongoing.

Indonesia

Case 1: Covid-19 related Business Email Compromise (BEC) ML Case

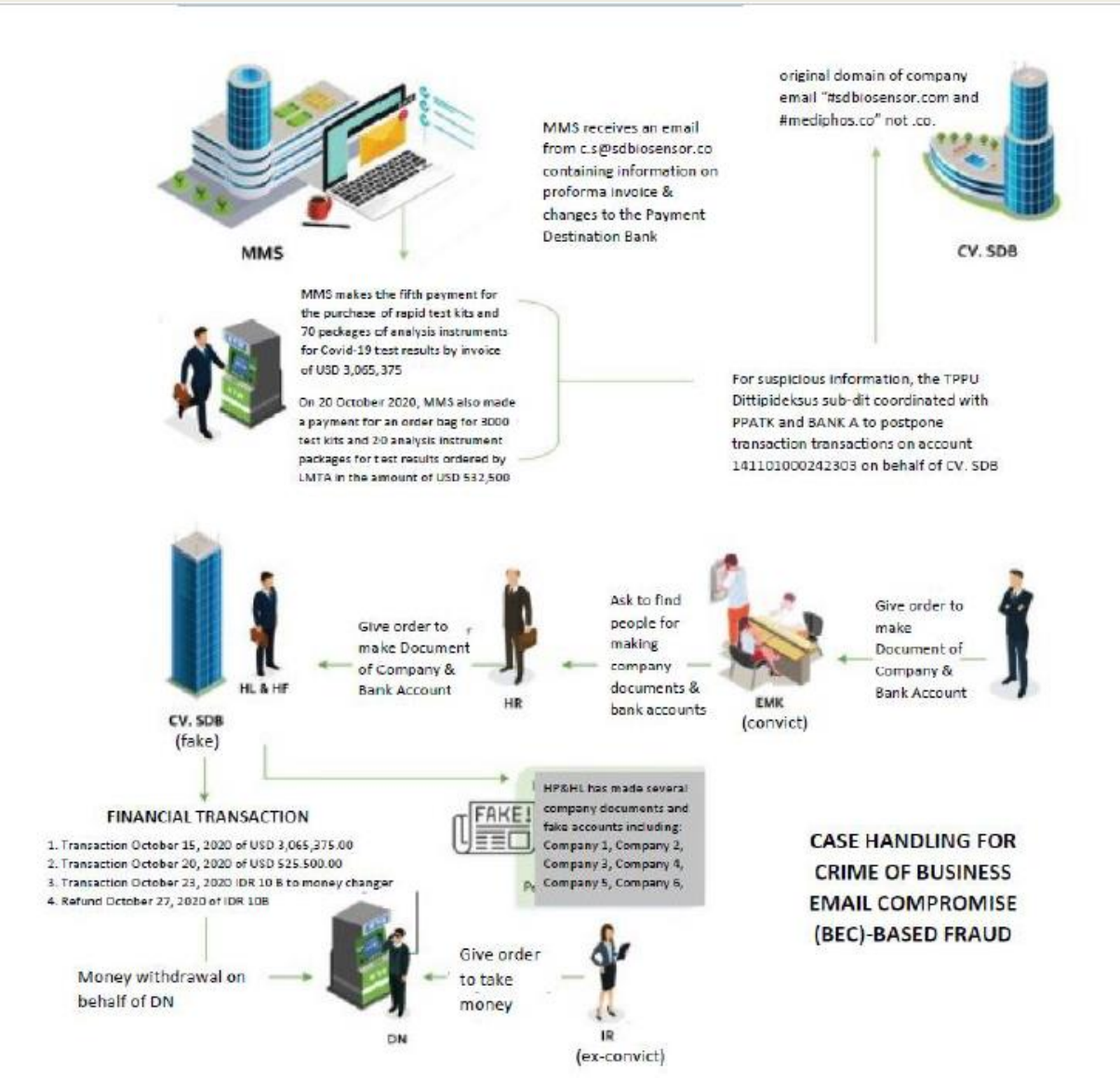
On 14 October 2020, Company A received an email from c.s@sdbiosensor.co containing information on proforma invoices (temporary invoices) and changes to the destination bank for payment to Bank A's account in Indonesia in the name of Company B for the fifth stage of payment for the purchase of 50,860 packages of rapid test kits and 70 instrument packages for the analysis of COVID 19 test results with a total bill of USD 3,065,375. The original domain of the company email was "@sdbiosensor.com and @mediphos.com".

On 15 October 2020, Company C in Jurisdiction A transferred funds from Bank I overseas in the name of Company A to Bank A in the name of Company B with funds transferred amounting to USD 3,065,375 or equivalent to IDR 44.738 billion in accordance with Proforma Invoice SHJ201009-6 FIN.

On 20 October 2020, Company A also made payments for the order of 3000 packages of test kits and 20 packages of test results analysis instruments ordered for a total of USD 532,500.

Based on STRs, PPATK (Indonesian FIU) requested Bank R in Indonesia to suspend the account transactions in the name of Company B (according to Law Number 8 of 2010 on Prevention and eradication of ML article 65: "INTRAC may request financial service provider to temporarily suspend all or part of the transactions as referred to in Article 44).

Furthermore, Bank X has succeeded in delaying the transaction amounting to IDR 27,832,829,812 (approx. USD 1,925,082) while the funds that have been released amounted to IDR 24,505,000,000 (approx. USD 1,695,060).



Case 2: Business Email Compromise (BEC) by a syndicate related to the purchase of ventilators and Covid-19 monitors

This is a case of alleged fraud committed by Company B from 6 May 2020 to 22 May 2020 and involved a business email compromise scam concerning the sale and purchase of ventilators and COVID-19 monitors. The suspects claimed to be the seller of medical devices and instructed the victim to send the amount of money according to the agreement to the SM Bank account in Indonesia. The following is a description of the case:

On 31 March 2020, a company in Jurisdiction A engaged in the field of medical equipment, Company A, entered into a sale and purchase contract with a company from Jurisdiction B , Company B for the procurement of medical equipment in the form of ventilators and COVID-19 monitors, with several payments made to Bank C accounts abroad in the name of Company B.

On 6 May 2020, an unknown party emailed Company A by introducing himself as General Manager (GM) of Company C in Europe and provided information concerning the change in

the payee's account for the purchase of the ordered COVID-19 ventilators and monitors. The new account was in the name of Company B in Indonesia.

NCB Interpol Indonesia received information on alleged criminal acts of fraud from NCB Interpol in Jurisdiction A which was then forwarded to the Sub-Directorate of ML Dittipideksus Bareskrim of the Indonesian National Police. The information concerned Company A who had made three transfers of funds to the SM Bank Account with a total value of EUR 3,672,146 (approx. USD 3,937,214) equivalent to IDR 56,928,903,066.

Indonesian National Police, NCB Interpol Indonesia, and NCB Interpol in Jurisdiction A succeeded in uncovering an international fraud syndicate involving a network from Jurisdiction C and two perpetrators from Indonesia related to ML with the modus operandi of email hacking and fraud. The perpetrators consisting of "SB" (Indonesian) were arrested by a joint team of the Criminal Investigation Police, North Sumatra Police and Simalungun Police in Padang Sidempuan, North Sumatra.

The Sub-Directorate of ML Directorate of Specific Economic Crimes of Criminal Investigation Agency of the Indonesian National Police arrested three Indonesian citizens whose task it was to prepare company documents and accounts of the shell company SMC in Indonesia. The perpetrator "SB" (Indonesian) was arrested by a joint team of the ML Sub-Directorate of the Criminal Investigation Unit of the Police, North Sumatra Police and Simalungun Police in Padang Sidempuan, North Sumatra. From the results of the arrest of "SB" it was revealed that there were other Indonesian citizens involved, namely "R" who was involved in planning and making documents to conduct fraud and was arrested in Bogor, West Java and "TP" who was also involved in planning and making documents to commit fraud who was arrested in Serang, Banten.

Proceeds of crime totalling IDR 58,831,437,451 (approx. USD 4,066,976) were successfully withdrawn and used by the suspect "SB" for personal purposes.

The joint Criminal Investigation Agency (Bareskrim) team and Interpol Indonesia's NCB are currently still working to uncover other actors involved, especially those suspected of being foreigners.

Macao, China

Residents from other jurisdiction visit Macao, China during pandemic to purchase life insurance products

Most of the insurers in Macao, China are branches from Jurisdiction A and their product features are similar to the features that are attractive to customers in Jurisdiction B. Due to strict border-control during the COVID-19 pandemic, more customers from Jurisdiction B visited and purchased life insurance products in Macao, China instead of Jurisdiction A.

The Monetary Authority of Macao (AMCM) remained vigilant to emerging trends on cross-border fund flows and third party payments. Existing AML/CFT related guidelines/notices have required insurers and intermediaries to have control measures to ensure the required CDD/EDD procedures are well-implemented according to the risk identified and assessed.

Moreover, considering a mechanism of close communication with and on-going monitoring of insurers has been established by AMCM, the potential risks are controllable.

Online presence of terrorist groups increased during the pandemic

Since the mobility of the population has been limited by the government's preventive measures during the pandemic, the online presence of terrorist groups/organisations has significantly increased. In order to prevent any online terrorist online propaganda or terrorist financing from infiltrating into Macao, China, the Judiciary Police has paid close attention to the situation through intelligence exchange and investigation, so that relevant preventive measures can be implemented promptly. Currently no relevant activity is noted in Macao, China, therefore no information or case study can be provided in this section.

Philippines

For the year 2021, the Anti-Money Laundering Council (AMLC) received a total of 11,979 suspicious transaction reports (STRs) containing pandemic-related keywords such as "COVID", "COVID-19", "COVID 19", "COVID19", "CORONA VIRUS", "ECQ", "QUARANTINE"," QUARANTIN", "NCOV", "LOCKDOWN", "PANDEMIC". The months of February and March recorded the highest submissions with a share of 15.2% and 15.0% respectively. The lowest number of STRs received can be seen in the months of January, November and December. Collectively, the aforementioned months contributed to only 7.3% of the total pandemic related STRs received in 2021.

The majority or 32% of the STRs submitted are filed due to the reason "There is no underlying legal or trade obligation, purpose or economic justification". This was followed by "Violations of the Child Pornography Act of 2009" and "Graft and Corrupt Practices".

Solomon Islands

Fraudulent Activity linked to COVID 19 Economic Stimulus Package Program

Person A, a farmer who resides in one of the remote islands of the Solomon Islands, applied for financial support from the central government under the COVID 19 Economic Stimulus Package program. Person A's application was approved and he was advised and notified that he would receive a sum of SBD 120,000 (approx. USD 14,736) for his application.

Individual B, who was on the COVID 19 Economic Stimulus Package committee, happened to meet Person A and told him that if he wants to get his payment processed quickly, Person A needs to give him a commission of SBD 20,000 (approx. USD 2,456) for the payment process to be fast tracked. Considering the long waiting time and costs involved in travelling from the Island to Honiara to get his payment, Person A agreed and gave SBD 20,000 (approx. USD 2,456) to the insider within the Stimulus Package program and thereafter, he received his payment as promised by the insider.

Thailand

Fraud

Individuals collected money from people who came to receive their COVID-19 vaccination at the Central Vaccination Centre despite the government providing free vaccines. The director of the Vaccination Centre noticed a suspiciously large number of people registered for vaccination since June - July 2021and notified the Railway Police Surveillance. In a collaboration between the Ministry of Public Health, the Central Investigation Division and the Railway Police Department, the individuals who were collecting fraudulent payments for COVID-19 vaccines were arrested. The suspects confessed and the authorities are continuing their investigation.

Drugs

The COVID-19 outbreak provided an alternative channel to trade drugs online which reduced the risk of being arrested by the authorities. Drug dealers and retail customers can contact each other directly, distribute drugs through private transport systems or avoid being arrested by the police by wearing a food delivery jacket as a rider. Drugs can be ordered via social media for 3,000 baht (approx. USD 87) per sachet of coffee, where drugs are contained in the coffee sachets. The coffee sachets contain crushed ecstasy mixed with Erimin 5 (a street name for a drug called Nimetazepam, a type of Benzodiazepine) and other drugs. Drug traders claim that it will give more effect than ecstasy.

Corruption

In August 2021, an accounting officer in a provincial public health office embezzled the COVID-19 budget. Financial irregularities were found with more than 12.7 million baht (approx. USD 369,575) transferred into the officer's account. The accounting officer was dismissed from government service. The National Anti-Corruption Commission (NACC) sent this case to the Anti-Money Laundering Office (AMLO) to conduct a financial investigation.

Vietnam

In the context of the recent COVID-19 pandemic, there is a rising trend of some predicate offences of money laundering related to violations in the bidding process for the procurement of medical supplies and equipment for the prevention of COVID-19.

A notable case in 2021 which was discovered and prosecuted by the Police Investigation Agency of the Ministry of Public Security was Company A which was charged with “Offenses against regulations of law on bidding that lead to serious consequences; Abuse of power or position in performance of official duties; Giving bribes; Receiving bribes".

In this case, the Police Investigation Agency verified the violation of the provisions of the Bidding Law during the bidding process to purchase COVID-19 test kits manufactured by Company A, which in total were worth more than 148,310 billion VND (approx. USD 6,361,995).

At the same time, there were out-of-contract agreements for kickbacks which amounted to over 44 billion VND (approx. USD 1,888,931) made/transferred by Company A. Currently, the case is being expanded in order to clarify the nature of the case, target perpetrators under the provisions of law, and thoroughly review and recover state assets.

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.).

Hong Kong, China

For both domestic and external crimes, it is increasingly commonplace for the use of the Internet, email and social media to be involved in the commission of predicate offences. This is both due to the advancement of technology and prevalence of electronic financial services, and the social distancing norms introduced by the COVID-19 pandemic.

Japan

Cases have been identified where financial support offered to companies in the context of COVID-19 was fraudulently obtained.

In the context of COVID-19, the number of visitors to Japan has decreased and authorities have noted a corresponding decrease in the use of foreign exchange businesses.

Sri Lanka

A trend has been observed arising out of COVID-19 pandemic related import restrictions that banned imports of turmeric and other spices from Country A have increased. Several incidents were identified where IUU fishing vessels were involved in smuggling restricted items such as turmeric.

Source: https://www.indiannavy.nic.in/ifc-ior/Final_MMSU_Jul_20.pdf

- **Domestic Product Smuggling/ Off Mannar, Sri Lanka/ 28 Jul 20**. *(Dried Turmeric)*

On 28 Jul 20, Sri Lanka Navy apprehended a person smuggling a stock of dried turmeric in the beach area of Oluthuduwai, Mannar. Upon investigation it was discovered that there were 20 sacks containing dried turmeric weighing approx 1000 kg. The suspect along with the consignment was taken under custody.

IUU fishing incidents have increased with the onset of the COVID-19 pandemic.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 01 Jul 20**. *(Local)*

On 01 Jul 20, Sri Lanka Navy sighted a person who was running landwards from a dinghy. Subsequently, upon searching the dinghy three explosive charges prepared for illegal fishing were recovered. The dinghy, explosives and fishing gear were taken into naval custody.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 04 Jul 20**. *(Local)*

On 04 Jul 20, Sri Lanka Navy apprehended 15 personnel for engaging in illegal fishing, from the sea areas off the Trincomalee harbour. The suspicious dinghies and nine personnel were apprehended for engaging in fishing without valid passes and another six personnel were arrested for using 225 mtrs long unauthorised nets to catch fish. Reportedly, two dinghies, two outboard motors, 126 kg of illegally caught fish and fishing gear were taken into naval custody.

Comments. *Recently, a special protection force assigned by the administration of Union Territory of Lakshadweep seized 1,716 sea cucumbers from an uninhabited island named Suhali. Weighing 882 kg and priced at USD 535,000 in the international market, the shipment was kept ready for smuggling to Sri Lanka. According to marine biologists, the seizure was the largest ever of its kind in the entire world*. Reportedly, a*verage prices rose almost 18% worldwide between 2011 and 2020. The rarer these endangered species get, the deeper divers are swimming to find them. That's when the fishing gets dangerous.*

- **IUU Fishing/ Off Mullaitivu, Sri Lanka/ 08 Jul 20**. *(Local)*

On 08 Jul 20, Sri Lanka Navy apprehended five personnel for engaging in illegal fishing using banned nets during a search operation carried out in Kokilai area, Mullaitivu. Officials seized the banned net and other fishing gear used by the fishermen.

- **IUU Fishing/ Off Thalaimannar, Sri Lanka/ 09 Jul 20**. *(Local)*

On 09 Jul 20, Sri Lanka Navy apprehended six personnel for engaging in illegal fishing without valid permits, and seized diving and fishing gear in the seas off Thalaimannar. The apprehended personnel were taken into the naval custody.

- **IUU Fishing/ Off Kalmunai, Sri Lanka/ 09 Jul 20**. *(Local)*

On 09 Jul 20, the officials apprehended nine personnel onboard a craft for engaging in illegal fishing using divng gears without valid permits in the seas off Kalmunai area. Reportedly, these personnel along with the craft, diving gear and other fishing gear were taken into naval custody.

- **IUU Fishing/ Off Talaimannar, Sri Lanka/ 21 Jul 20**. *(Foreign)*

On 21 Jul 20, Sri Lanka Navy apprehended 19 foreign fishermen for poaching in the country's waters in the north of Talaimannar. The officials seized four trawlers along with the fishermen and handed over to the authorities for further legal action.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 11 Jul 20**. *(Local)*

On 11 Jul 20, Sri Lanka Navy apprehended 15 personnel for engaging in illegal fishing using unauthorised nets in the seas off the Elisabeth Island in Trincomalee. The officials apprehended three dinghies, two banned nets and other fishing gears used by the fishermen.

- **IUU Fishing/ Off Pulmoddai, Sri Lanka/ 05 Jul 20**. *(Local)*

On 05 Jul 20, Sri Lanka Navy apprehended nine personnel onboard two dinghies for engaging in illegal fishing using unauthorised nets in the sea area off Pulmoddai. Alongwith the suspects, about 200 kg of illegally caught fish, two unauthorised fishing nets and two dinghies were taken into naval custody.

- **IUU Fishing/ Off Kakathivu, Sri Lanka/ 05 Jul 20**. *(Local)*

On 05 Jul 20, Sri Lanka Navy apprehended five personnel for engaging in illegal fishing in the seas South of Kakathivu island. The suspects were using banned nets and did not have any permit. Reportedly, the suspects along with 24 banned nets, a traditional fishing craft (Wallam) with OBM, fishing gears and 70 kg of fish were taken into custody.

- **IUU Fishing/ Off Mannar, Sri Lanka/ 07 Jul 20**. *(Local)*

On 07 Jul 20, Sri Lanka Navy apprehended nine personnel for engaging in illegal harvesting of sea cucumber in the seas of Muddalampiddy, Mannar. As per reports, 22 sea cucumber caught by them, one dinghy, diving and fishing gear were taken into naval custody.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 13 Jul 20**. *(Local)*

On 13 Jul 20, Sri Lanka Navy apprehended 19 personnel for engaging in illegal fishing in the sea areas of Kumburupiddi and Nayaru in Trincomalee. Reportedly, along with the suspects, seven dinghies, two unauthorised fishing nets and other fishing gears were taken into the naval custody.

- **IUU Fishing/ Off Valalthottam, Sri Lanka/ 15 Jul 20**. *(Local)*

On 15 Jul 20, Sri Lanka Navy apprehended 15 personnel and two dinghies in the seas off Valalthottam area in Trincomalee for engaging in illegal fishing using banned nets and illegal fishing gears. Reportedly, the suspects along with dinghies, banned nets and other fishing gear were handed over to the authorities for onward action.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 17 Jul 20**. *(Local)*

On 17 Jul 20, Sri Lanka Navy apprehended a person for engaging in illegal fishing in the seas off Elephant Point in Trincomalee and seized four banned fishing nets casted in the Batticoloa lagoon. Reportedly, one dinghy, three safety fuses, nine non electric detonators, 100 gm of water gel sticks and other fishing gear were also taken into custody.

- **IUU Fishing/ Off Trincomalee, Sri Lanka/ 17 Jul 20**. *(Local)*

On 17 Jul 20, Sri Lanka Navy apprehended 47 personnel for engaging in illegal fishing using unauthorised nets in the sea area of Foul Point in Trincomalee. Along with the suspects, eight dinghies, eight unauthorised nets, 557 kg of illegally caught fish and several other fishing gear were taken into naval custody.

9.3 Cases related to COVID-19 developed directly from suspicious or cash/threshold transaction reports.

Hong Kong, China

To alleviate the financial burden of unemployed individuals during the COVID-19 pandemic, the Hong Kong Government has launched a "100% Personal Loan Guarantee Scheme ("PLGS")" for citizens to borrow a maximum of HKD 80,000 (approx. USD 10,196) with an interest free loan.

Upon analysis and investigation by Hong Kong Police, it was discovered that a syndicate had recruited money mules to apply for the PLGS with false employment and account evidence. A total of HKD 2.8M (approx. USD 356,883), in relation to 35 false PLGS applications, was deposited into the money mules' bank accounts and immediately dissipated to the other bank accounts controlled by the syndicate before the funds were remitted out of Hong Kong, China through a licensed Money Service Operator (MSO). In October 2021, seven syndicate members were arrested for fraud and money laundering. An investigation is ongoing.

Japan

Fraud Case

The Japan Financial Intelligence Centre (JAFIC) received an STR indicating a bank account which was reported for the following reasons:

- Even though the age of the nominee was young, a large amount of financial assets were declared
- Transactions did not align with the customer's stated occupation
- A suspicion was formed that illegal transactions in virtual assets were being conducted which involved fraud
- Login to the account was noted from various physical locations
- Suspicious use of a fictitious name and name of another person

The police, which received the information, started the investigation and it was revealed that the financial support for COVID-19 was transferred to the suspect's account from a public institution. As a result of further investigation by the police, it was revealed that the suspect received the financial support by using a false declaration. The suspect was arrested on the charge of fraud.

Macao, China

In terms of STRs, there was a very limited number of STRs related to suspected medical scams, but they were reported at the early stage of the pandemic (2020) when there was a shortage of medical supplies. There is no sustained trend related to COVD-19 observed from STRs.

Malaysia

Illegal selling of COVID Vaccine

The FIU received several STRs on a group of companies with a similar nature of business, i.e., beauty, hair and skin-related products or services, due to suspected unauthorised possession or illegal selling of COVID-19 vaccines. In the STRs, the Bank observed that the company accounts received transactions ranging from RM 420 to RM 426 (approx. USD 95 to USD 97) from multiple individuals with transfer references such as "covid", "vaccine" and "sinovac".

The observation was in line with recent action taken and a modus operandi shared by the Royal Malaysian Police whereby three marketing officers were arrested for having offered and illegally sold COVID-19 vaccines to the public. The investigation conducted revealed that the suspects had sold two doses of the vaccine for RM 420 (approx. USD 95) and the payment would only be made once the vaccines were administered. In addition, the national body in charge of COVID-19 vaccine supply and the immunisation program did not give any approval to openly sell COVID-19 vaccines at that point in time. The case was investigated under Section 420 and 511 of the Penal Code for cheating and dishonestly inducing delivery of property.

Philippines

Unlicensed investment-taking

The client is allegedly associated with an investment entity. A Securities and Exchange Commission (SEC) advisory was released in 2020 and cautioned the public on the activities of the person behind the said investment entity. The investment entity which primarily engaged in online captcha typing jobs is registered with the Department of Trade and Industry.

The said entity offers two accounts for its incoming members, the starter account worth PHP 499 (approx. USD 9) and the builder account worth PHP 1,000 (approx. USD 18). Additionally, the entity also offers multiple accounts wherein a member will receive 120% return on investment for three accounts; 134% return on investment for seven accounts; 148% return on investment for 15 accounts; and 155% return on investment for 31 accounts. Based on the covered person's investigation, the client had been posting and promoting the investment company in his Facebook account which encourages the public to join and invest with the entity especially during this time of pandemic. His members also endorse the said ventures in their respective social media accounts.

Based on the covered person's review of the client's records, the client received remittances from various individuals who were presumed as investing members of the said entity. Such transactions were conducted in amounts ranging from PHP 499 (approx. USD 9) to PHP 16,000 (approx. USD 302).

Based on the information gathered by the covered person, the client's transactions are suspicious since he is affiliated with the networking firm which is not duly registered with the SEC to solicit investment from the public.

Alleged smuggling of COVID-19 vaccines

Corporation X was reported to have been involved in the alleged smuggling of COVID-19 vaccines, which were misrepresented as vegetables. Based on a news article that triggered the transaction report, Corporation X is an importer of fresh fruits and vegetables based in Pasig City and registered with the Department of Agriculture's Bureau of Plant Industry. The reporting covered person, on the other hand, stated that Corporation X was involved in the importation of agricultural and non-agricultural products such as construction materials.

Corporation X has one account, a peso commercial savings account, with the reporting covered person. The account was opened in August 2019 and closed in February 2021. In between these

dates, the reporting covered person noted cash deposits as the usual mode of credit transactions in the account of Corporation X; while its debit transactions typically consisted of over-the-counter bills payment. Beginning March 2020, Corporation X's bank account with the reporting covered person had minimal movements. Notably, its transactions consisted of credits via cheque deposits from other banks and debits through cash withdrawals. It was also noted that the cheque deposits received by Corporation X were from shipping companies. It also had fund transfers to and from legitimate importers. Over the period 2019-2020, Corporation X's total debit and credit transactions amounted to PHP 10.37 million (approx. USD 196,057) and PHP 10.35 million (approx. USD 195,679), respectively. The last activity recorded by the reporting covered person for corporation X's bank account was in August 2020.

Case involving no underlying legal or trade obligation, purpose or economic justification

This is a case referred by an employee of a business establishment in Province X regarding a female subject who is suspected of an unlawful activity. Notably, the said subject has sent remittances to various individuals within Province X and neighbouring Province Y.

According to the branch employee, when the country was placed under community quarantine due to COVID-19, the subject was authorised by Person Y, a resident of Province Y, to collect payment for vegetables from customers and remit the funds to him through a certain covered person. Person Y is a vegetable dealer with business documents such as a Mayor's permit and Barangay permit (Barangay Business Clearance is one of the permits or documents required when registering a new business in the Philippines) to support the claim.

There was a notable increase in the amounts of the subject's remittances starting in 2020 which totalled PHP 20,578,064 (approx. USD 389,120) from only PHP 18,050 (approx. USD 341) in 2019. The covered person found the transactions of the subject to be suspicious due to the unusual volume of transactions which was not commensurate with their earning capacity.

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

Cook Islands

The Cook Islands Financial Intelligence Unit (CIFIU) have taken a proactive step to reduce the impact of cybercrimes on victims. Work has been done around raising public awareness of online scams. This campaign was called "Be Kukiwise – STOP the Scam".

The campaign was launched in early-2021. Initial groundwork for the campaign commenced in mid-2020 due to the increase of reported COVID-19 pandemic related online scams. The FIU capitalised on the frequently utilised media platforms to get the message to the public. Posters in English, Cook Islands Maori, Fijian, and Philippines' versions were posted around the districts of Rarotonga including major public and private business premises. The scam campaign was also extended to Aitutaki only. Local newspapers, radio talkbacks, and social media were the common platforms used. In December 2020, the FIU engaged a local business to create an animated video production called "Be KukiWise – STOP the Scam" which was launched in early-2021. This campaign ran over a four-month period with the awareness video being run on Cook Islands television (CITV) three times per week at peak viewing times. The video has both an English and Cook Island Maori version and was uploaded on YouTube and

shared via Facebook. Around June 2021, “Get Safe Online” another awareness product on scams and cybercrimes was launched on the Cook Islands online platform hosted by the Office of the Prime Minister’s ICT division.

CIFIU also intends to support any government related national policy/directive around cybercrime and addressing this threat to the Cook Islands. We have also identified our office as a point of first contact for members of the public to report a cybercrime after which we will assess the report before referring it to the relevant agency for further investigation.

Indonesia

ML

Based on the results of the analysis, it is known that the proceeds of fraudulent crimes have the greatest potential risk of ML. This is due to the government's policy of strict lockdowns and ordering the closures of businesses which has caused the unemployment rate in Indonesia to increase compared to the previous period.

Furthermore, the implementation of physical restrictions makes business actors turn to online systems (e-commerce), due to the large increase in the need for medical supplies which has also seen criminals take advantage of the situation. This is evidenced by cases of fraud, especially online fraud being the most prevalent crime reported to the Police during the COVID-19 Pandemic. Under these conditions, the Ministry of Communication and Information Technology has coordinated with e-commerce platforms to be able to carry out strict supervision of the sale of all products that violate policies and to take firm action against such violations.

Another type of predicate crime that has a high potential for ML during the COVID-19 pandemic is corruption. In the context of controlling the handling of COVID-19 in Indonesia, the Corruption Eradication Commission (KPK) issued Circular Letter (SE) Number 8 of 2020 concerning the Use of the Budget for the Implementation of the Procurement of Goods/Services in the Context of Accelerating the Handling of Covid-19 related to the Prevention of Corruption. Corruption-prone points during the pandemic include the procurement of goods and services, the allocation of state and regional budgets, donations from third parties as well as defrauding economic and social welfare programs.

Narcotics is the third highest risk for proceeds of crime, with narcotics cases having increased during the pandemic. The COVID-19 pandemic has led to perpetrators of narcotics crimes using technology in new ways, but the police can thwart perpetrators' actions, both in smuggling, distribution, storage, and when transacting. The National Narcotics Agency (BNN) continues to coordinate with the Directorate General of Customs and Excise in carrying out efforts to eradicate narcotics crimes.

Furthermore, policies during the COVID-19 pandemic such as social distancing or physical distancing caused access to banking and other financial services to become a challenge and the use of digital-based transaction services subsequently increased. Criminals took advantage of digital-based transaction services including by transferring funds sourced from Business Email Compromise scams. This means funds transfer crimes are at a high risk of ML.

TF

During the pandemic, many terrorists have consolidated their strength and supporters through online networks such as social media, including through recruitment and funding, which is most often done with fundraising schemes. Throughout 2020 (until June 2020) there were 24 intelligence reports related to alleged criminal acts of terrorism and/or terrorism financing (PPATK, 2020). This shows that the COVID-19 pandemic does not necessarily stop terrorists from taking actions to collect, transfer, and use funds to carry out their actions.
(Source: NRA ML and TF/PF 2021)

Malaysia

Bank Negara Malaysia (BNM) continued to produce a Fraud advisory in 2021 for selected financial sectors on scams and COVID-19 related crimes, ML/TF trends and red flags to assist them in transaction monitoring and the detection of suspicious transactions during the pandemic. The advisory serves as a response to the continuous prevalence of fraud activities in both the domestic and international landscape amid the COVID-19 pandemic.

Pacific Transnational Crime Coordination Centre (PTCCC)

The Pacific Transnational Crime Coordination Centre (PTCCC), as the information coordination hub of the Pacific Transnational Crime Network (PTCN), are gradually seeing an increase in reporting of ML through the Pacific Transnational Crime Units (TCU's), but are still receiving limited detail. We are continuing to build awareness through the TCU's, including assisting the APGML whenever possible. The following information has been obtained from the annual PTCN Transnational Crime Assessment 2020-2021:

- Report received regarding significant amounts of money being remitted offshore, the suspicious transactions were investigated in a multi-agency response, but limited details provided as the case is currently before the court.
- Exploitation of various citizenship schemes across the Pacific by foreign investors and a number of Pacific islands are likely being used as tax havens. Pacific Islands are more vulnerable because of the loss of tourism from the impact of COVID-19.
- Minimal reporting of the use of proceeds of crime and forfeitures.
- Cryptocurrency being used for the purchase of illicit drugs in several Pacific islands.
- Large volume of pyramid style schemes across the Pacific over 2020-21.
- Increased reporting on business email compromise scams and the use of money mules to create accounts in country.
- The use of observers on vessels has been suspended due to COVID-19 restrictions, their absence has likely increased incidents of illegal, unreported and unregulated (IUU) fishing.
- Increased reporting of illegal fishing and harvesting across the Pacific and the bribery of locals and officials to assist/and or be complicit in the illegal activities.

UN Counter-Terrorism Committee Executive Directorate (CTED)

During the pandemic, terrorism finance vulnerabilities have revolved around changing financial behaviours, in particular a rise in remote transactions, with impacts on financial institutions' ability to detect anomalies (more difficult to conduct effective customer due diligence or ongoing monitoring; lower effectiveness of reporting entities' due to remote working arrangements).

Many experts, including the Financial Action Task Force, have noted that pandemic-related changes in financial behaviours (especially the increase in the volume of contactless transactions and increased digital onboarding) have exacerbated terrorism-financing vulnerabilities. These have impacted financial institutions' ability to conduct customer due diligence (CDD) and detect anomalies.

Member States have expressed concern at the use of proceeds from pandemic-related relief efforts for terrorism-financing purposes and new opportunities for terrorist groups to abuse fundraising platforms and the non-profit sector for terrorism financing, under the guise of charitable giving.

As terrorist groups increasingly rely on donations to generate income, it has made potential abuse of relief payments, humanitarian aid, donation campaigns more likely.

- Enhanced attention is required on the effective use of new technologies for AML/CFT purposes to prevent, detect and suppress the use of new payment modes for TF purposes.

- There may be additional vulnerabilities linked to the misuse of virtual assets (VAs) in pandemic-related schemes, such as fraud schemes linked to the pandemic. While increased use of VAs for terrorism finance purposes has been observed globally, it is unclear whether this is due to the pandemic (and shift towards online activities) or due to changes as terrorist groups continue to adapt their terror finance activities to the cyber age.

- Member States are also concerned with the continuous and potentially growing links of terrorism finance with criminal proceeds, especially COVID-19 related frauds.
    - These scams have often used sophisticated cyber tools, including solicitations of cryptocurrency donations.
    - There are reports of an Islamic State in Iraq and the Levant (ISIL) facilitator conspiring to sell fake COVID-19 personal protective equipment online.
    - Due to the loss or significant reduction in income of terrorist groups, including ISIL, during the pandemic, there are reports of alternate ways to raise funds.

<u>Extracts from the CTED 2021 Global Implementation Survey (GIS):</u>
The economic consequences of the COVID-19 pandemic appear to have led terrorists to increase their reliance on criminal activities. Increased reliance on drug smuggling, trafficking in minerals and precious stones, fraud through electronic means, the sale of counterfeit medicines, and cybercrime has been reported. Some experts warn that restrictions on

international travel may lead to the emergence of new human trafficking and cash smuggling routes and increase the popularity of informal money transfer services.

As States continue to strengthen their CFT legislation and operational measures, there is considerable debate as to the extent to which those measures might impact purely humanitarian activities, including in conflict zones with active terrorist activity. The COVID-19 pandemic has also raised additional concerns regarding the potential impact of CFT measures on emergency responses. So far, only a few States have adopted dedicated measures in this area (e.g., by strengthening the transparency of licensing and specific exemption measures as well as maintaining focused dialogues with the NPO sector and financial institutions).

10. ABBREVIATIONS AND ACRONYMS

ABF	Australian Border Force
AED	United Arab Emirates dirham
AFP	Australian Federal Police
AML	Anti-Money Laundering
AMLA	Anti-Money Laundering Act
AMLC	Anti- Money Laundering Council
AMLO	Anti-Money Laundering Office (Thailand)
APG	Asia/Pacific Group on Money Laundering
ATM	Automatic Teller Machine
AUSTRAC	Australian Transaction Reports and Analysis Centre
BND	Brunei dollar
CAMLMAC	China Anti-Money Laundering Monitoring and Analysis Center
CDD	Customer Due Diligence
CFATF	Caribbean Financial Action Task Force
CFT	Countering the Financing of Terrorism
CTR	Cash/ Currency Transaction Report
DNFBP	Designated Non-Financial Businesses and Professions
EAG	Eurasian Group
EDD	Enhanced Due Diligence
ERWTF	Extreme Right-Wing Terrorism Financing
EUR	Euro
FATF	Financial Action Task Force
FI	Financial Institution
FIU	Financial Intelligence Unit
FJD	Fijian Dollar
FMU	Financial Monitoring Unit (Pakistan)
FPTBTS	Fictitious tax invoices (Indonesia)
FSRB	FATF-Style Regional Bodies
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
GIF	Financial Intelligence Office (Macao, China)
HKD	Hong Kong Dollar
IDR	Indonesian Rupiah
IFTI	International Funds Transaction Instruction
INTERPOL	International Criminal Police Organisation
IPOA-IUU	International Plan of Action to prevent, deter and eliminate IUU fishing
IUU	Illegal, unreported and unregulated fishing
JAFIC	Japan Financial Intelligence Center
JPY	Japanese Yen
KYC	Know Your Customer
LEA	Law Enforcement Agency
MENAFATF	Middle East and North Africa Financial Action Task Force
MLA	Mutual Legal Assistance
ML	Money Laundering
MNT	Mongolian tögrög, the official currency of Mongolia
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MoJ	Ministry of Justice
MOP	Macao pataka, the currency of Macao, China
MVTS	Money or Value Transfer Services
MYR	Malaysian ringgit

NCC	National Coordination Committee to Counter Money Laundering (Malaysia)
NGO	Non-Government Organisation
NPO	Non-Profit Organisations
NRA	National Risk Assessment
NZD	New Zealand Dollar
OECD	Organisation for Economic Co-operation and Development
PEP	Politically Exposed Person
PF	Proliferation Financing
PHP	Philippine peso
PKR	Pakistan Rupee
PPATK	Indonesian Financial Transaction Reports and Analysis Center
PPP	Public Private Partnerships
RBF	Reserve Bank of Fiji
RFMO	Regional fisheries management organisation
RMB	Chinese Renminbi
RM	Malaysian ringgit
SBD	Solomon Islands dollar
SEC	Securities and Exchange Commission (Philippines)
SGD	Singapore Dollar
SIMP	United States Seafood Import Monitoring Program
STR	Suspicious Transactions Report
STRO	Suspicious Transaction Reporting Office, Singapore's Financial Intelligence Unit
SVF	Stored Value Facilities
TF	Terrorist Financing
THB	Thai Baht
UNCLOS	United Nations Convention on the Law of the Sea
UN CTED	UN Counter-Terrorism Committee Executive Directorate
UNODC	United Nations Office on Drugs and Crime
USD	United States Dollar
VAT	Value Added Tax
VND	Vietnamese dong
WMD	Weapons of mass destruction