APG Yearly Typologies Report 2023

Asia/Pacific Group on Money Laundering

Methods and Trends of Money Laundering and Terrorism Financing

Asia/Pacific Group on Money Laundering

December 2023

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 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 or findings of assessments cannot be shared publicly due to their sensitive nature or due to ongoing investigative/judicial processes.

The 2023 APG typologies report adopts a revised format in response to feedback from APG members. Key changes include:

- An index that allows each case study to be cross-referenced across a number of themes.
- A new section on asset recovery focussed on case studies highlighting successes and challenges involved in effective recovery of proceeds, instruments of crime or equivalent benefits (both domestic and foreign).
- An expanded section for typologies related work undertaken by APG's observer organisations.

Identifying details including names of suspects/offenders, company names, and references to other jurisdictions have been edited throughout the report to sanitise the case studies. Where an APG member has referred to its own jurisdictions and local authorities, these have been left identified. Individuals are primarily referred to as 'Persons' with a distinguishing letter, for example, 'Person A'. Within a single case study, any repeated references to 'Person A' will be the same individual, however multiple case studies may refer to 'Person A', which will mean a different individual in each case study. Likewise with 'Jurisdictions', a reference to 'Jurisdiction X' in one case study, will not mean the same jurisdiction if 'Jurisdiction X' is referenced in another case study. Currency is displayed in the local currency of the submitting APG member, unless United States Dollar (USD) references have been provided. A currency conversion chart has been provided at Section 7 for reference.

The APG Operations Committee has oversight of the typologies research programme and is co-chaired by Samoa and India (2022-2024).

The APG is grateful to AUSTRAC (Australian Government) for providing staff to assist the APG Secretariat, at a critical time, with compilation and editing of this 2023 APG Yearly Typologies Report.

[1] Financial Action Taskforce

1 FOCUS AREA - VIRTUAL ASSETS & VIRTUAL ASSET SERVICE PROVIDERS

1.1 Overview

In October 2018, the FATF amended its Recommendations to explicitly capture financial activities involving virtual assets (VA) and to set standards in relation to the regulation and supervision of virtual asset service providers (VASPs). The relevant requirements are set out in Recommendation 15 (R.15). Since 2018, the FATF and global network have been working to improve implementation of the requirements.

This inclusion of VAs in the FATF Standards is recognition of the possibilities and vulnerabilities of this new technology. VAs and related services have the potential to spur financial innovation and efficiency, but their distinct features also create new opportunities for money launderers, terrorist financiers, and other criminals to launder their proceeds or finance their illicit activities. The ability to transact across borders rapidly not only allows criminals to acquire, move, and store value digitally often outside the regulated financial system, but also to obfuscate the origin or destination of the funds and make it harder for reporting entities to identify suspicious activity in a timely manner.[2]

FATF has identified a number of emerging trends relating to VA and VASPs which are reinforced by the cases and research findings outlined in this report. Recent reports raise serious concerns about the Democratic People Republic of Korea's (DPRK) theft and laundering of hundreds of millions of dollars' worth of VA for financing the proliferation of weapons of mass destruction (PF). Ransomware incidents have grown significantly in recent years, and ransomware payments are almost exclusively demanded in virtual assets. ML trends increasingly show involvement of virtual assets in a range of ML techniques. Terrorist groups, including ISIL, Al Qaeda and their affiliates, as well as extreme-right wing terrorist entities, are increasingly using virtual assets to raise and move funds globally.

This Chapter briefly sets out the FATF framework for AML/CFT controls on VAs, tracks the implementation by APG members, and the threats and trends arising from VAs VASP.

FATF Methodology GLOSSARY

*A **virtual asset** is a digital representation of value that can be digitally traded, or transferred, and can be used for payment or investment purposes. Virtual assets do not include digital representations of fiat currencies, securities and other financial assets that are already covered elsewhere in the FATF Recommendations.*

***Virtual asset service provider** means any natural or legal person who is not covered elsewhere under the Recommendations, and as a business conducts one or more of the following activities or operations for or on behalf of another natural or legal person:*

i. exchange between virtual assets and fiat currencies;
ii. exchange between one or more forms of virtual assets;
iii. transfer of virtual assets;
iv. safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets; and
v. participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.

[2] FATF 2020, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, Introduction https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf

1.2 Threats and Trends

As the VA industry continues to evolve, criminal actors are utilising new methods and trends to profit from their crimes. APG has noted the findings of relevant research presented by blockchain analytics firms, in particular *Chainalysis' Crypto Crime Report 2023* and *TRM Labs Illicit Crypto Ecosystem Report 2023*.

Chainalysis' Crypto Crime Report 2023 reported that illicit cryptocurrency volumes reached an all-time high in 2022, with the illicit transaction volume estimated at USD20.6 billion.[3] Importantly, this represents only 0.24% of the total cryptocurrency transaction volume. ML and predicate offences are the crime types most commonly connected with VAs, however the prevalence of TF and PF through VA is increasing (see sections 1.3 and 1.4 below).

Reports from APG Members, and findings of blockchain analytics firms reveal that fraud, theft, hacking, blackmail and ransomware are the most common illicit activity taking place through VAs. The underlying predicate offences most commonly relate to online gambling, computer crimes, fraud, tax evasion, the sale of illicit or controlled substances (e.g. drugs, firearms), child exploitation and human trafficking. A key area of concern is the use of VAs to evade UN and other sanctions.

Chainalysis Crypto Crime Report 2023: summary of ML activity in 2022

Chainalysis identified that ML through VA typically involves two types of entities and services:

- Intermediary services and wallets, including unhosted wallets, mixers, darknet markets and other services. Criminals utilise these services to temporarily hold funds, obfuscate the movement of funds or to swap between assets.
- Fiat off-ramps, which are services that allow VAs to be exchange for fiat currency. After this occurs, the funds can no longer be traced via the blockchain, and only the service provider (e.g. a VASP) has visibility into the destination of the funds.

With respect to mechanisms to launder funds through VA, centralised exchanges were the biggest recipient of illicit cryptocurrency, with almost half of all funds sent from illicit addresses going directly to centralised exchanges. This is notable given VASPs AML/CFT obligations.

With respect to other mechanisms, there was an increase in the volume of illicit funds sent to DeFi protocols[4]. This is commonly utilised by hackers stealing VAs. Darkweb market ventures and administrators sent their illicit funds primarily to other illicit services (such as other darknet markets) or to high-risk exchanges. Ransomware attackers and fraud criminals sent a large share of funding to mixers.

TRM Labs Illicit Crypto Ecosystem Report 2023 includes the below diagram which maps the use of virtual assets across each stage of the money laundering process; placement, layering and integration. This is a useful tool when considering the risks posed by VA/VASPs, as well as threats and trends.

[3] Chainalysis the 2023 Crypto Crime Report 2023, TRM Illicit Crypto Ecosystem Report 2023
[4] DeFi protocols consist of standards, codes, and procedures that govern decentralized financial applications

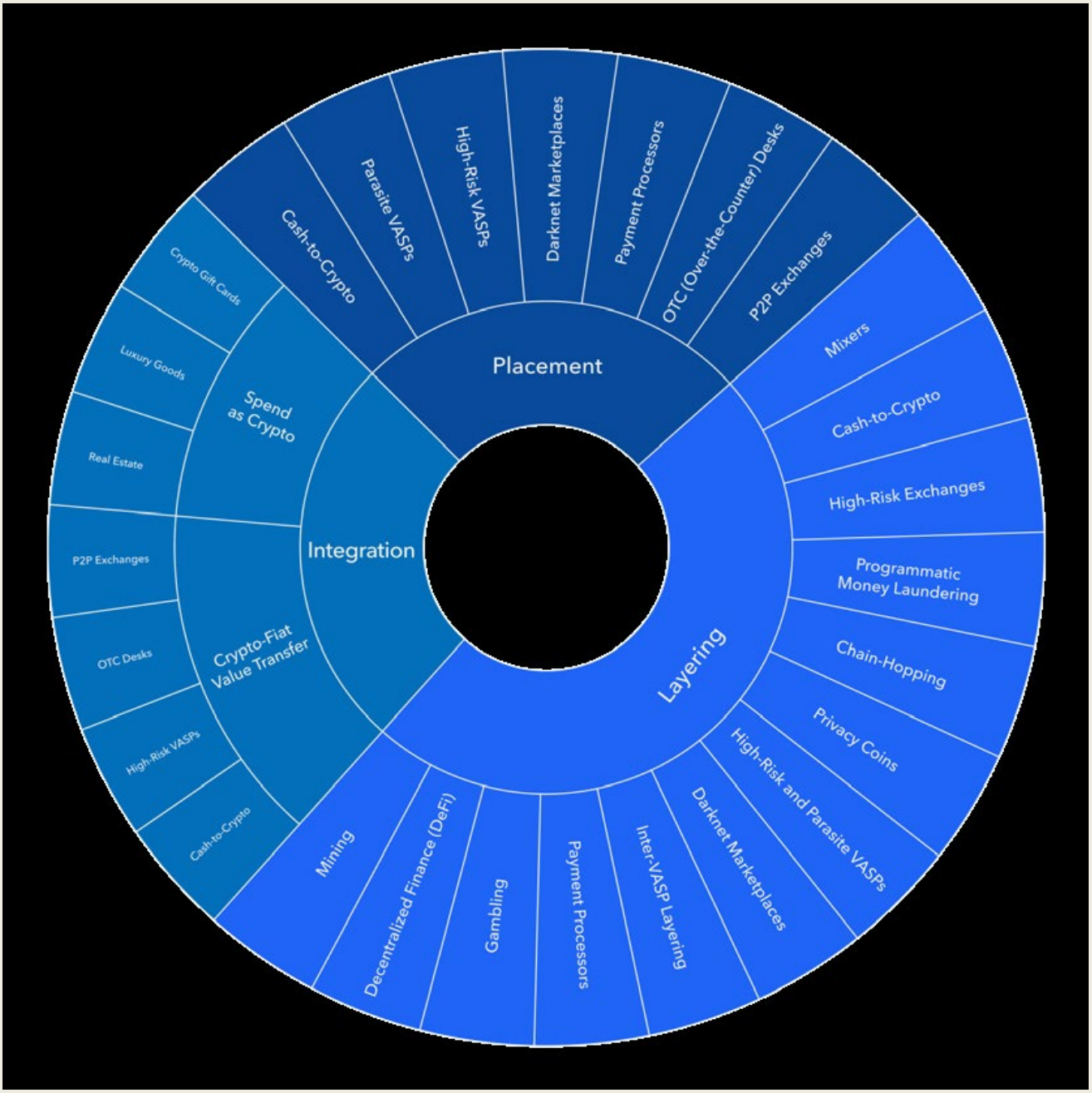


Diagram: TRM Labs Illicit Crypto Ecosystem Report 2023

APG Members reported a number of trends they are seeing in relation to VA/VASPs, the most notable being the increase in money laundering through VAs.

Macao, China

Approximately 100 investigations by law enforcement agencies between 2018 and 2022 related to VA/VASP activities. This trend is observed to be increasing. 98% of cases under investigations were linked to fraud/investment scams, with some scams involving fake websites and applications with no real VA transactions. In a small number of cases VAs (in particular, virtual currencies) were involved, but no local VASP platforms were identified.

Philippines

From February 2022 Philippines regulators expanded transaction reporting requirements when they required all Covered Persons to use VA-specific transaction codes for covered/suspicious transaction report (CTR/STR) filing. Prior to that VASPs registered with the central bank submitted reports using general transaction codes pertaining to remittances, deposits, or foreign currency exchanges.

For large-value VA-specific transactions reported as of mid-October 2022, the majority comprised VA transfers within the same platform (58%), followed by VA transfers to external platforms (17%), fiat-to-VA conversions (15%), and VA-to-fiat conversions (10%). In terms of transaction amount, fiat-to-VA conversions through online bank transfers accounted for the highest percentage (43%), followed by VA transfers to external platforms (39%), and VA transfers within platform (13%).

Most STRs filed pertain to VA transfers to external platforms (93% of total value and 75% of total volume). Fraudulent practices and other violations relating to unregistered investment solicitation emerged as the top reason for suspicion (68% of total transaction amount), followed by suspicious indicators such as lack of underlying purpose or economic justification (14%) and deviations from financial profile or capacity (11%). Other predicate crimes identified were swindling (5%), child exploitation (0.15%), and photo/video voyeurism (0.03%). This is consistent with historical trends, where an AMLC (Philippines FIU) study in March 2020 found that investment fraud-related reasons (e.g., participation in swindling and illegal investment schemes) were the most prevalent triggers prompting VASPs to submit STRs to the AMLC. Some subjects of suspicion were also noted to send remittances (in fiat currency) to VASPs domiciled in foreign jurisdictions. Financial links were likewise uncovered on certain persons of interest (POIs) who were involved in separate cases relating to swindling, drug trafficking, unauthorized investment solicitation, and hacking. Aside from transacting with each other, they were found to provide VAs (specifically cryptocurrency) as a common explanation for their unusually large funds or transaction movement. Some used VA as a front for operations, while others represented that their funds are deposited into or come from gains made off well-known foreign VASPs based in foreign jurisdictions.

While the reports suggest extensive use of foreign VASPs among certain POIs, coupled with domestic VASPs' low utilization of VA-specific transaction codes, the cited statistics only represent a small subset of VA-related transactions passing through the Philippine financial system. Nonetheless, the data indicates that there are significant VA transfers to external platforms (especially for transactions found suspicious), which lends support to suspicions that criminal actors may be moving their funds across VASPs under different regulatory frameworks in a bid to hamper the authorities' detection of their activities and ability to trace their funds.

Hong Kong, China

Given the increasing popularity of VAs, illicit criminal activities related to VAs have become more prevalent. The misuse in VA in a layering process within ML schemes is also on an upward spiral. In 2021, the number of VA-related crime cases reached 1,397, which was a rise of 182.8% from 2020. The financial loss incurred in 2021 was HK$824.1million, a four-fold increase compared to 2020.

Japan
In Japan, VA transactions are assessed as relatively higher ML risk than other products and services of specified business operators, such as deposit taking financial institutions and funds transfer providers. It is believed that the establishment of appropriate internal control systems in response to various risks such as cyber security did not keep up with the operators newly entering the business of crypto asset service providers.
The number of arrests for cybercrime in 2021 was 12,209, the highest number ever. There has been an expansion of ransomware damages, disclosure of information through unauthorized access, and cyberattacks committed by groups having national background.

While the use of blockchain analysis tools to capture transaction histories is cited as one of risk mitigation measures, the FATF's guidance also points out challenges, including technical constraints. Among the crypto-assets used for transactions in Japan by VA exchange service providers, one is known to not disclose transfer records, making it difficult to trace transactions, so it may be more likely to be used for ML/TF. Another is known to be poor at maintaining and updating its transfer records. If wallets used for transactions are acquired or controlled by individuals or VA exchange service providers who exist in countries or areas where they are not obliged to take measures to identify the principal, etc. it becomes difficult to identify the owner of the crypto-assets transferred in a transaction. Since almost all transactions handled by crypto-assets exchange service providers are not conducted in person but over the Internet, they have high anonymity.

The rapidly changing environment surrounding VA transactions needs to be taken into account when identifying and assessing risks. Crypto ATMs change the manner in which VAs are cashed or purchased. For example, there are cases outside Japan in which drug traffickers convert criminal proceeds derived from drug trafficking into bitcoins via crypto ATMs using forged identification documents. Open sources indicate the launch of credit card payments directly using VA (including so-called "stablecoins"). In addition, it has been reported that institutional investors have announced their intention to begin to include VAs in their portfolios.

The existence of DeFi (decentralised finance) services for individuals worldwide that claim to have no central controller, coupled with the fact that there are still jurisdictions that do not regulate VASPs, there is reason to expect a continued increase the inherent risk of VA being used for ML/TF, compared to other financial services.

1.3 Proliferation Financing through Virtual Assets

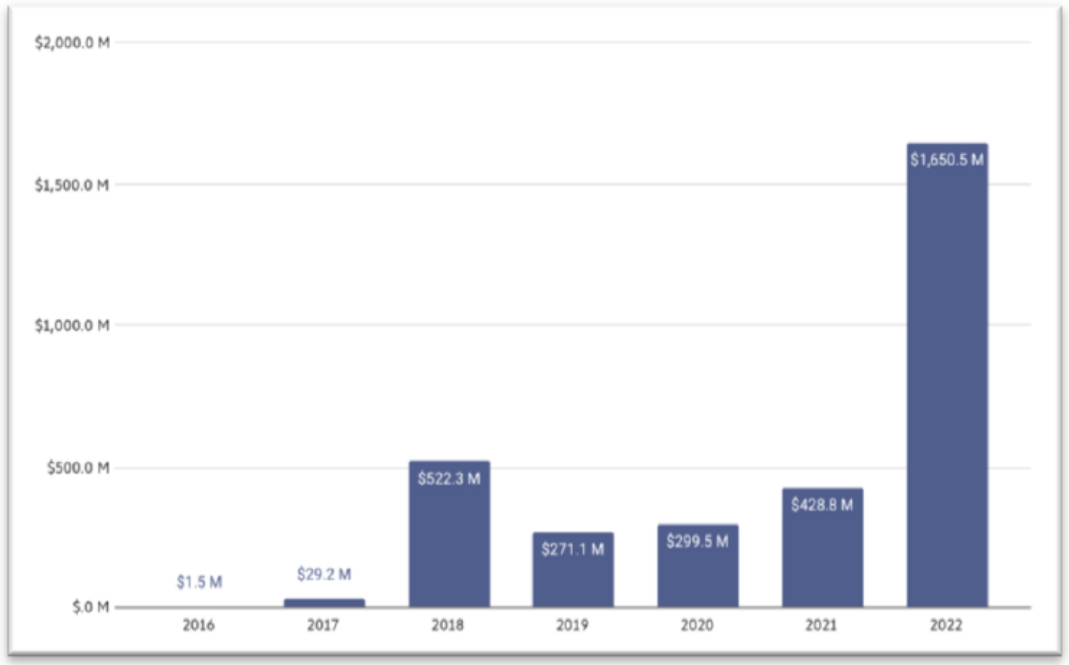
In recent years, there has been a significant increase in the use of VAs to finance the proliferation of weapons of mass destruction (PF), in particular by the DPRK.

The September 2023 report by the UN Panel of Experts on North Korea (UNSCR 1874) (see section 4.1) highlighted reports that DPRK State-sponsored actors were responsible for almost USD 1.7 billion in theft of virtual assets in 2022, more than three times the amount that they stole in 2021.[5] Further, the report notes Chainalysis' finding that DPRK is prioritising cryptocurrency hacks to fund its nuclear weapons program.[6]

[5] UN Panel of Experts UNSCR 1874 Report September 2023
[6] Figure XXVII in the UN Panel of Experts UNSCR 1874 Report September 2023, attributed to Chainalysis.

Yearly total cryptocurrency stolen by Democratic People's Republic of Korea cyberthreat actors, 2016–2022

(Millions of United States dollars)



Source: Chainalysis.

The FATF's 2023 Targeted Update noted the significant threat posed by the DPRK's illicit VA-related activities to finance the proliferation of weapons of mass destruction and called on jurisdictions to take urgent action to implement R.15 in order to mitigate the risk of PF through VAs.[7]

A range of illicit activities, with increasing sophistication, are being utilised for PF through VA. These include:

- Ransomware attacks.
- Hacking.
- Spear-fishing.
- Malware.
- Non-fungible token (NFT) theft.
- Placement of IT workers.

1.4 Terrorism Financing through Virtual Assets

While TF represents a small portion of the illicit transactions occurring through VAs, the use of VAs for TF is increasing.

The February 2023 UNSCR1267 Panel Report highlighted that while ISIL still primarily replies on traditional methods such as hawala and mobile money services to move funds, it is increasingly

[7] FATF (2023), Targeted Upate on Implementation of the FATF Standards on Virtual Assets/VASPs, FATF, Paris, France, https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

using VAs.[8] Further, there is evidence of increased sophistication in the use of VAs by terrorist organisations.

In its 2023 Illicit Crypto Ecosystem Report, TRM Labs reports that it identified a number of ISIS fundraising campaigns that accepted VAs, which raised up to tens of thousands of dollars.[9]

In its 2023 Targeted Update, the FATF identified a typology where VAs are used to finance extreme right-wing terrorism, often through crowdfunding platforms.[10]

1.5 Assessing the risk posed by VA/VASPs

With a rapidly evolving and technologically advanced context, it is evident that assessment of risks posed by VA/VASPs in a jurisdiction is a critical first step.

The FATF standards require jurisdictions to identify and assess the ML/TF risks emerging from VA activities and the activities or operations of VASPs, and apply a risk-based approach to mitigation, commensurate with the identified risks. VASPs are also required to take appropriate steps to identify, assess, manage and mitigate their enterprise and product ML/TF risks.

A number of technical assistance providers have prepared materials to support the conduct of risk assessments. For example, the World Bank has released a "*Virtual Asset and Virtual Asset Service Providers ML/TF Risk Assessment Tool*" which is chiefly aimed at competent authorities.[11] The Royal United Services Institute (RUSI) issued an "*Institutional Virtual Asset Service Providers and Virtual Assets Risk Assessment Guide*",[12] designed to assist VASPs to identify and assess their enterprise ML/TF risks. Tools such as these provide support for jurisdictions and individual VASPs to meet their risk assessment obligations.

Many APG members have conducted risk assessments to identify the ML/TF risks relating to VA activities and the operations of VASPs. Below are some examples reported by members:

Hong Kong, China

The Financial Intelligence and Investigation Bureau of Hong Kong Police Force has an ongoing thematic analysis on ML trends relating to VASPs. Holistic reviews on selected STRs, FIU to FIU exchanged information and other information from various sources on prevalent crime trends will be conducted with reference to the overall ML/TF threat and vulnerability in Hong Kong, China. Findings are scheduled to be published in 2023.

[8] UNSCR1267 Panel Report Feb 2023 – Pg 82
[9] TRM Labs Illicit Crypto Ecosystem Report June 2023.
[10] FATF Targeted Update 2023.
[11] https://www.worldbank.org/en/topic/financialmarketintegrity/brief/national-money-laundering-and-terrorist-financing-risk-assessment-toolkit-disclaimer-and-terms-of-use
[12] https://static.rusi.org/Institutional-VASP-VARAG-web-final.pdf

Japan

Japan's *National Risk Assessment-Follow up Report 2022*, which includes assessment of VA/VASPs, was published on 1 December 2022[13],

In addition, Japan's Financial Services Authority published the *Research Report of JFSA Multilateral Joint Research on the Chain of Trust of Decentralized Finance* was published in June 2023 [14]. This research was conducted to analyse case studies of representative DeFi (Decentralised Finance) projects, based on the assumption that current major DeFi projects have certain trust points, centralized elements which may be subject to regulation. The research found that (i) a variety of trust points/centralized aspects exist in most DeFi and that (ii) in-depth analysis on each DeFi is required to identify objects which should be regulated, since references to "DAO[15]" or "Governance token" are significantly different by projects.

Macao, China

Macao, China has carried out a series of actions to assess the risk of VA/VASPs. The inter-departmental AML/CFT Working Group, comprising of 15 government agencies, conducted a review on VA and VASPs in July 2020. The Financial Intelligence Office (GIF), as the coordinator of the Working Group, and the supervisor of FI, and the Monetary Authority of Macao (AMCM), worked together to prepare and analyse a VA/VASPs-related survey for the Working Group members.

The survey assessed risks from the following perspectives:

- An overview of any VA and VASPs operations in Macao, China (listing 18 choices of operations);
- Legal status of the statutory framework of respective competent agencies on VAs and VASPs;
- Any cases identified (both civil and criminal) which related to VAs/ VASPs; and
- An overview of companies which had business related to VAs and VASPs.

Overall, the risk of VAs and VASPs in Macao, China is assessed as low. No trading platforms have been identified to be in operation and criminal cases related to VA/VASPs are more closely associated with fraud and scams. The majority of STRs reported in relation to VA/VASPs relate to personal investments, with only a handful on the suspected use of personal accounts to transfers funds to overseas VA platforms. No actual exchange of VAs were identified in these STRs.

Despite the low risk identified, Macao, China continues to implement a number of measures to mitigate the risk of VAs and VASPs:

- All banks and payment service institutions in Macao, China are required to not participate in or provide, directly or indirectly, any financial services for VA activities.
- Insurance companies are required to not accept or use VAs as the means of payment for premium or claims, and should evaluate whether current or planned business and operation comply with regulations.
- Authorities will identify any VASPs established/operating in Macao, China and to carry out any necessary follow-up actions.
- Authorities will stay vigilant to emerging risks related to new technologies.

[13] https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/nenzihokoku_e.htm
[14] https://www.fsa.go.jp/policy/bgin/ResearchPaper_qunie_en.pdf
[15] Decentralised autonomous organisation

- Share and alert the risk of VA activities and VASPs to banks through public-private partnership meetings. A list of VASP platforms collected from various sources will be periodically shared to banks for their internal risk analysis purpose and application of relevant preventive measures.
- VA are not permitted by law to be a legal payment method in the casinos. The Gaming Inspection and Coordination Bureau (DICJ) have on-going monitoring in place to prevent casinos from dealing transactions with VA and engage with VASPs.

Thailand

AMLO published NRA 2022 which covered VA and VASP.[16] In addition, AMLO conducted a sectoral risk assessment on the VASP sector for each service provider. This report is classified.

Philippines

The Bangko Sentral ng Pilipinas' (BSP) March 2021 *3rd Sectoral Risk Assessment (SRA) of Banks and other BSP-Supervised Financial Institutions (BSFIs)* included a risk assessment on VASPs.

The SRA identified that the overall vulnerability for the VASP sector is medium. This is due to the inherent vulnerability of VAs to ML, TF and PF due to its unique features such as cross-border nature of transactions, capacity for fast settlement, potential for increased anonymity, among others. Meanwhile, the quality of general AML/CFT controls of VASP is assessed as medium. The AML/CTF legal, regulatory and institutional framework of VASP are in place and generally consistent with international AML/CFT standards.

In addition to the SRA, BSP also conducts various supervisory activities to further inform risk understanding for this sector. This includes, among other things, conduct of examinations and thematic reviews to assess the level of risk and quality of risk management framework, and surveillance activities to identify and monitor trends and typologies.

1.6 APG Member Implementation of FATF VA Requirements

As at October 2023, six joint FATF/APG members and 14 APG-only members have been assessed against the revised requirements in R.15, either through a mutual evaluation or follow-up report. Of these, only one is from the Pacific sub-region.

All six of the joint FATF/APG members received a rating of largely compliant (i.e. a 'passing mark'). Of the 14 APG-only members, only two (Mongolia and Thailand) received a rating of largely compliant, with four rated non-compliant and five rated partially compliant. This equates to 86% of APG-only members, assessed against the revised requirements, not having an adequate underlying framework in place for VA/VASPs.

[16] https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NRAYThailandYforYPublicationYEnglish_6112.pd

Common deficiencies identified in relation to APG-only members failing to meet the requirements of R.15 include:

- The selection of a prohibition framework with an inadequate underlying prohibition.
- Gaps in the scope of coverage of virtual assets as the five limbs of the FATF definition are not adequately covered.
- A lack of risk assessment.
- No supervision conducted on VASPs.
- A lack of identification of illegal operations occurring and no sanctions being applied.
- Limitations in the ability to conduct international cooperation relating to VA/VASPs.

Conducting VA/VASP risk assessments and establishing legal and institutional frameworks for regulation and supervision of VASPs remains a significant challenge for many APG members.

The APG Donors and Providers (DAP) Group is working to enhance support for APG members with this priority topic. Technical assistance with implementation of VA requirements was the most common request by technical assistance recipient jurisdictions at the APG's 2022 and 2023 Technical Assistance Forums.

Selection of a prohibition framework with an inadequate underlying prohibition

While many APG members have indicated a preference for prohibit VASPs, frameworks for effectively prohibiting VASPs are challenging to establish and implement. None of the APG-only jurisdictions who have chosen to prohibit VA/VASPs have obtained a largely compliant rating (i.e. a 'passing mark') for R.15. In fact, as at October 2023, only one jurisdiction globally using a prohibition framework has obtained a largely compliant rating for R.15.[17]

The FATF's June 2023 Targeted Update on the Implementation of the FATF Standards on VA/VASPs (FATF 2023 Targeted Update) found that, based on a survey, the global percentage of jurisdictions which have opted to prohibit VASPs was 11%.[18] Within the group of APG members who have been assessed against the revised requirements, seven have selected a prohibition regime, three a regulation regime and one had yet to select a framework. This equates to 64% of these jurisdictions choosing to prohibit VASPs, which is far higher than the global average.

The key deficiency identified with respect to implementing a prohibition framework is that the jurisdiction chooses this framework without an enforceable, underlying prohibition. For example, some jurisdictions have issued advice to the public not to trade in cryptocurrency, or a notice advising that cryptocurrencies are not recognised, but these have no legal basis.

A further common deficiency relating to the selection of a prohibition framework is the misconception that choosing to prohibit VA/VASPs removes all R.15 obligations from the jurisdiction.

Jurisdictions which select a prohibition framework are required to:

(i) on an ongoing basis, assess the risks posed by VA/VASPs and apply a risk-based approach to ensure that measures to prevent or mitigate ML/TF risks are commensurate with the risks identified;
(ii) take action to identify natural or legal persons that carry out VASP activities, and
(iii) apply appropriate sanctions, and provide the widest possible range of international

[17] FATF (2020), Anti-money laundering and counter-terrorist financing measures – People's Republic of China, *1st Enhanced Follow-up Report & Technical Compliance Re-Rating*, FATF, Paris http://www.fatf-gafi.org/publications/mutualevaluations/documents/fur-china-2020.htm
[18] FATF Targeted Update 2023

cooperation in relation to ML/TF and predicate offences related to virtual assets.

Elements of Effective Policies for Crypto Asset: IMF

The IMF recently published the Paper on Elements of Effective Policies for Crypto Assets, which aims to address questions by Fund members on how to respond to the rise of crypto assets and the associated risks. The paper presents the following observations regarding VA prohibitions:

- Prohibition frameworks which make all VA activities illegal may stifle innovation and drive illicit activities underground.
- Prohibition can be costly to enforce and increase the incentive for circumvention due to the inherent borderless nature of VAs, resulting in potential heightened financial integrity risks and inefficiencies.
- When substitute assets are not widely available in the legal market, users may be more motivated to access illegal markets and willing to pay higher prices for those assets, due to the stronger incentives to obtain them.
- VAs that escape prohibitions may generate additional negative externalities (e.g. more virtual asset activity may become linked to the dark web).
- Targeted restrictions could be justified to manage specific risks.
- Restrictions/prohibitions should not substitute for robust macroeconomic policies and credible institutional frameworks, which are the first line of defence against the macroeconomic and financial risks posed by VAs.

www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092

1.7 Red Flag Indicators

Based on more than one hundred case studies contributed by jurisdictions from 2017-2020, the FATF issued a report on *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing* in September 2020[19]. The report is designed to assist VASPs, Financial Institutions (FIs) and Designated Non-Financial Business and Professionals (DNFBPs) in identifying and reporting potential ML and TF activity involving VAs. The red flag indicators set out in the report relate to transactions, transaction patterns, anonymity, senders or recipients, source of funds or wealth and geographical risks.

[19] FATF 2020, *Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing*, Introduction https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Virtual-Assets-Red-Flag-Indicators.pdf, Paragraph 6.

Key red flags indicators relating to VA/VASP transactions include:

- Incomplete KYC information, including potential unwillingness of customer to provide KYC information.
- Structuring of VA transactions into small amounts or amounts just below a threshold.
- Transactions that don't align with customer profile and expected account usage.
- Transferring VAs to VASPs in another jurisdiction where there doesn't appear to be a relationship.
- Depositing VAs and then immediately withdrawing or converting the VA.
- Transactions that involve the use of multiple VAs without logical business rationale.
- The conduct of VA-fiat currency exchange at a potential loss with without logical business rationale.
- Transactions whose purpose appears to be to obscure the flow of funds, for example through the use of mixing and tumbling services.
- The use of IP addresses associated with criminal activity.
- The use of the same IP-address for a large number of seemingly unrelated VA wallets.
- Frequent transactions with VASPs in jurisdictions known to have weak AML controls.

Source: FATF Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, 2020

1.8 The importance of International Cooperation

A key facet of the FATF Standards is for jurisdictions to have a legal basis for international cooperation, and to provide it in order to deliver appropriate information, financial intelligence, and evidence and facilitate action against criminals and their assets. With respect to VA, R.15 requires jurisdictions to rapidly provide the widest possible range of international cooperation in relation to ML, predicate offences, and TF relating to VA and VASPs. In particular, supervisors of VASPs should have a legal basis for exchanging information with their foreign counterparts, regardless of their supervisors' nature or status and differences in the nomenclature or status of VASPs.

The borderless nature of blockchains and the purpose-built ease and speed of transfer of value through VAs means that it is essential for jurisdictions to utilise international cooperation to effectively supervise VASPs, and successfully investigation and prosecute offences involving VAs. The importance of international cooperation is emphasised in the March 2023 Report of the UN Panel of Experts for North Korea (UNSCR 1874), where, with respect to illicit generation of revenue through VAs and other cyber-activities, the Panel recommends jurisdictions "strengthen cooperation, facilitate dialogue and enhance information sharing[20]".

1.9 Conclusion

The information set out in this Chapter emphasises the need for jurisdictions globally to implement the VA/VASP requirements set out in R.15. As the sector and criminality continue to evolve, APG members need to ensure their regulatory and supervision frameworks and their law enforcement capabilities remain sufficient to address the growing risks and challenges.

[20] DPRK UN Panel of Experts Report March 2023, page 77.

2 MONEY LAUNDERING AND TERRORISM FINANCING CASE STUDIES

Case studies provided by APG members have been set out in alphabetical order by reference to the source jurisdiction. Under the title of each case study, relevant accepted terms referring to predicate offences, methods of payment or other context, are included. These terms are referenced in the index in section 8 of the report.

2.1 Australia

Case study # 1 - Valuable diamond alleged to be proceeds of drug crimes

drug-related crimes; trade in precious metals and stones

The Australian Border Force (ABF) received an industry referral raising concerns about the re-importation into Australia of a 15-carat diamond valued at AUD24 million and declared as 'returned goods'.

Intelligence checks revealed the importer (Person A) had a lengthy criminal history and had recently served a term of imprisonment following a guilty plea to two counts of "manufacturing a prohibited drug" contrary to s 24(1) of the Drug Misuse and Trafficking Act 1985.

Further analysis identified the diamond had been exported 12 months earlier, when charges were first laid against Person A. Subsequent physical examination of the diamond confirmed its value and a hold was placed on the consignment.

This information was referred to a partner agency, which obtained a warrant to seize the diamond as 'proceeds of crime'. It was determined Person A had laundered the proceeds of their drug crimes by purchasing the diamond and sought to evade confiscation by transferring the stone to another jurisdiction under the guise of seeking a specialist valuation.

Source - Australia

Case study # 2 - Multiple cash withdrawals

tax crimes

In January 2021, a joint operation was undertaken between several law enforcement and government agencies in Australia following receipt of intelligence reporting. The investigation revealed money mules were conducting cash withdrawals through a bank branch and delivering the funds to a cash coordination point. The criminal activity was associated with companies within the construction industry suspected to be evading tax. Four individuals were arrested for dealing with property suspected of being proceeds and/or the instrument of crime. Cash and assets valued at AUD4 million were seized.

Source - Australia

Case study # 3 - International money laundering syndicate – restraint action

standalone ML; use of virtual assets; purchase of real estate; abuse of legal persons and arrangements; wire transfer; financial institutions; professional facilitators; transnational organised crime group; suspicious transaction reporting; international cooperation

In 2023, nine Persons were arrested in connection with a suspected AUD10 billion money laundering organisation (MLO). The investigation commenced as a result of the previous arrest of suspects carrying large amounts of cash and extensive tracing of the proceeds of crime. The nine Persons are alleged to have dealt in the proceeds of crime, used foreign and domestic shelf companies to launder funds, and submitted fraudulent bank loan applications. The MLO was connected to significant suspicious incoming international transfers and suspected of using professional facilitators including accountants and bank staff to apply for loans with domestic

banks and using the proceeds to fund acquisitions of real properties and make mortgage payments?

Significant domestic cooperation included the Criminal Asset Confiscation Taskforce (CACT), Australian Federal Police (AFP) money laundering taskforce AVARUS, AUSTRAC, the Australian Taxation Office (ATO), the Australian Securities and Investments Commission (ASIC), and the Department of Home Affairs. International cooperation with foreign law enforcement agencies was also undertaken via the AFP's international police network.

The AFP has restrained property over the value of AUD200 million. The restraint included AUD30 million of cryptocurrency, 18 designer watches, 17 designer handbags, at least 46 items of luxury jewellery, 20 real properties, 66 bank accounts, and five luxury vehicles.

Nine Persons have been charged with money laundering offences under the *Criminal Code 1995* and the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006.* The confiscation proceedings under the *Proceeds of Crime Act 2002 (Cth)* are ongoing.

Source - Australia

2.2 Bangladesh

Case study # 4 - Use of the internet to hack bank accounts

theft; fraud; use of the internet

Person A allegedly used the internet to hack victims' bank accounts and mobile financial services with the intent to steal funds from their accounts. Person A sent messages with a 'one-time password' to victims' mobile numbers to acquire their account credentials and gain control of their accounts. Person A misused internet banking services by using fake IP addresses similar to those of the victims' banks.

Further investigation revealed that Person A had opened several bank accounts and MFS accounts by introducing himself as a 'freelancer' and without producing any supporting documentation. Transactions on these accounts were similar in nature, involving peer-to-peer transfers of small amounts. A total of BDT3.59 million (approx. USD32,404) was stolen from numerous victims' accounts held at a number of FIs and then withdrawn from Person A's accounts in cash.

An intelligence report was prepared by the FIU and disseminated to the relevant LEA. Investigation into the case is ongoing.

Source - Bangladesh

Case study # 5 - Theft of customers' funds using E-commerce platform

theft; fraud; forgery; use of the internet; abuse of legal persons and arrangements

An e-commerce company collected money from customers by offering 'Double Taka' and Summer Vouchers, which offered discounts of 50-60% on products including televisions, motorcycles, freezers, and mobile phones. The company failed to deliver the products ordered by customers. Instead, the funds received were transferred to the personal accounts of the e-commerce company owner to purchase fixed assets.

A total of BDT 11,666.79 million (approx. USD105.31 million) was collected in the accounts of the e-commerce company, its associated companies, and the personal accounts of the owner. A significant amount of the money was found to be diverted through the accounts of different affiliated companies and associated persons.

Based on the FIU's analysis, an intelligence report was disseminated to the relevant LEA for further action. The investigation into the case remains ongoing.

Source - Bangladesh

Case study # 6 - Fraudulent importation of software and ML via acquisition of online gaming coins

smuggling; fraud; abuse of legal persons and arrangements; gaming

A Bangladeshi company, Company A, was suspected of siphoning off funds by making false declarations about importations of software from an offshore company, Company B. A financial analysis revealed the funds were channelled to a gaming company to purchase online gaming coins. The beneficial owner of company B is Bangladeshi, and they received approximately USD590,000 within a six-month period from purportedly exporting the software to Bangladesh.

Further investigations revealed customers deposited small amounts into the mobile banking accounts of Company A to purchase the online gaming coins. The funds were then layered through several other accounts of the company, and its associates. These companies had a total of 23 mobile financial services accounts, and a total of BDT2,195 billion (approx. USD19,828 million)was deposited via 13.2 million transactions, with an average deposit amount of BDT 167 (USD 1.50).

An intelligence report was disseminated to the relevant LEA for action. The investigation into the case remains ongoing.

Source - Bangladesh

2.3 China

Case study # 7 - Money laundering proceeds of cyber-enabled fraud

fraud; use of the internet; abuse of legal persons

On 12 February 2023, local police in province L arrested 11 suspects including Person A. Since September 2022, Person A and others recruited subordinates through the introduction of relatives and friends with a 'high profit' gimmick. They registered more than 40 shell companies and opened several corporate accounts using these subordinates' identities, which were then used to launder illicit proceeds from overseas cyber-enabled fraud gangs.

In the lead up to Person A's arrest, the investigation revealed Person A and their criminal companions were associated with more than 3000 cyber-enabled fraud cases nationwide and internationally, totalling approximately RMB1 billion (USD137 million).

Source - China

Case study # 8 - International asset recovery of the proceeds of corruption and bribery

bribery and corruption; underground banking; international business companies

Person A is suspected of corruption and accepting bribes and fled abroad in May 2014. In April 2016, Interpol issued a red notice. Authorities cooperated with foreign LEAs to seize and freeze illicit assets acquired in foreign jurisdictions according to domestic laws and international conventions. Proceeds of the corruption and bribery offences were moved to foreign jurisdictions via underground banking services and international business companies providing real estate investment services. The case is ongoing in the foreign jurisdiction.

Source - China

2.4 Cook Islands

Case study # 9 - Disruption of international cannabis and ML syndicate

drug-related crimes; cash; structuring; suspicious transaction reporting; international cooperation

A joint drug and financial investigation, named 'Operation Kotaa – Police, Operation Falcon – FIU', was initiated in response to intelligence provided by the community and law enforcement partners about the presence of a drug syndicate operating in the Cook Islands. The joint operation was supported by New Zealand Police, New Zealand Customs and the New Zealand Transnational Crime Unit.

Intelligence identified two primary Persons (referred to as 'Person A' and 'Person B'), together with their associates, operating a drug syndicate importing cannabis to the Cook Islands via sea freight from Jurisdiction B.

Proceeds from the sale of the cannabis in the Cook Islands were then deposited by multiple individuals into two separate bank accounts and subsequently the funds were withdrawn using a Cook Islands debit card at ATMs located in Jurisdiction B. An estimated total amount of NZD400,000 was transferred in this way.

Person A is a resident of the Cook Islands and operated a small lawn mowing business. Person B has ancestral ties to the Cook Islands, but is a resident of Jurisdiction B, and owns and operates multiple small businesses and is associated with an organised criminal group. Person B travelled frequently to the Cook Islands and came to the attention of local law enforcement through intelligence gathered from the community. Community members had observed Person B spending conspicuously large amounts at a local bar and financially sponsoring a domestic rugby league team.

Persons A and B jointly registered a small business in the Cook Islands to create a front to legitimise their criminal activities. Investigations revealed the business had remained dormant from the day of registration. Person A coordinated the sale and distribution of drugs to multiple dealers in the Cook Islands, and deposited the funds into accounts of Person B located in the Cook Islands. Person B accessed the accounts through ATMs in Jurisdiction B and was identified to be the main supplier of cannabis to the Cook Islands.

In 2019, a suspicious activity report was filed in relation to a large cash deposit made into an account of Person B. Financial investigation revealed Person A coordinated a 'structuring' operation involving multiple third-party individuals depositing cash amounts that ranged from NZD300 to NZD9,000 (being less than the reporting threshold of NZD10,000). Text message communication also identified a link between Person A, Person B and multiple individuals involved in the drug syndicate, including two associates who had existing criminal records for drug offences. These two associates were identified as Person A's main drug distributors or drug dealers in the Cook Islands.

The joint drug and financial investigation involved authorities from Jurisdiction B to focus efforts on Person B in that jurisdiction and authorities in the Cook Islands to focus efforts on Person A. Person A was prosecuted in September 2022 and sentenced to seven years imprisonment on charges of conspiracy to sell/distribute class C (Cannabis) drugs and contempt of court. Evidence for ML was presented during the court case but no charge of ML was imposed. The two associates gave evidence against Person A and were each convicted and sentenced to four years imprisonment.

Source – Cook Islands

Case study # 10 - Renewable Energy Investment scam

fraud; use of the internet; suspicious transaction report; abuse of legal persons and arrangements; international cooperation

A phishing website targeted investors in foreign Jurisdiction A. The investment scheme into renewable energy initiatives was purportedly being offered by the Cook Islands government.

A suspicious activity report was made by reporting institution (Bank A). Bank A was asked by a bank overseas (Bank B) to stop an incoming transaction of NZD100,000 to an account at Bank A from a customer of Bank B. The purpose of the transaction was to invest in the fraudulent scheme that was also falsely represented as being offered by Bank B. Bank A acted upon the request from Bank B to stop the transaction.

It is unknown if the account at Bank A belongs to the perpetrators of the investment scam. The account holder at Bank A is an international trust company. The company offered digital automation and consulting services for various businesses located in multiple jurisdictions. The founders/ultimate beneficial owners of the company's account are two male individuals.

Bank B promptly took action to notify the relevant internet service providers hosting the fraudulent investment scheme as well as the financial regulator and cyber security authorities. Bank B also ensured its own website was made aware of the situation. In addition, the Cook Islands Government issued a media statement to inform the public about the scam. Four potential investors had shown interest in the investment scheme and were informed it was fraudulent.

The perpetrators of the investment scam changed their approach to use Bank A to falsely promote their fraudulent scheme. Bank A performed a risk assessment of the account holders and terminated their relationship.

Assistance from law enforcement and Bank B led to the identification of a third individual who may be related to the investment scam. However, no clear link was established between this individual and the two previously mentioned individuals or to the scam itself. No additional incidents have occurred or been reported and no further action has been taken.

Source – Cook Islands

2.5 Hong Kong, China

Case study # 11 - Transnational ML syndicate using unlicensed Money Service Operators and family members

organised crime; money laundering; transnational organised crime group; underground banking

Police in Hong Kong, China received information from Jurisdiction X that HKD32 million in criminal proceeds laundered by an organised crime syndicate, (syndicate members were arrested in Jurisdiction X), was transferred to the bank account of Person A in Hong Kong, China. Investigation revealed that Person A received the tainted money through unlicensed money service operators, and the funds were then transferred to the bank accounts of Person A's wife, daughter and associates. Person A's wife and an associate were arrested for money laundering in 2022 and funds totalling HKD13 million were seized. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 12 - Laundering proceeds of Sexual Exploitation through use of Stored Value Accounts

sexual exploitation;/new payment method; third party ML

In 2022, an investigation into a local vice syndicate, that arranged women to provide illegal sex services, found that the syndicate received service charges from patrons in cash, and the cash funds of approximately USD35,000 were then deposited into stored value facilities accounts held by the syndicate's money mules, prior to being transferred to the syndicate. Two syndicate members were arrested in late 2022 for vice offences by law enforcement agencies. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 13 - Laundering Illicit Gambling proceeds via Virtual Bank Accounts

gambling; use of the Internet; third party laundering; suspicious transaction reporting

Analysis by the JFIU of Hong Kong, China suggested that eleven virtual bank accounts were used for receiving and laundering HKD38 million generated from illegal online gambling activities. The illicit funds were then transferred to several bank accounts controlled by a gambling syndicate. In 2022, the syndicate's operation centre was raided and five people including the ringleader were arrested for gambling and money laundering offences. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 14 - Exploitation of Futures Company

fraud; use of capital markets; purchase of valuable or cultural assets; third party ML; suspicious transaction reporting

Through proactive analysis of reported telephone deception cases which involved soliciting investment from victims, the JFIU of Hong Kong, China uncovered a criminal syndicate responsible for laundering HKD345 million (US44 million) between 2020 and 2021. The syndicate controlled a local licensed futures company to launder the funds (Company A). Ten money mules were recruited and set up with bank accounts and securities accounts with Company A. Once tainted funds were deposited into the bank accounts of the money mules, the funds were then transferred to the money mules' securities accounts held with Company A. This resulted in high-frequency and large-volume trading in the futures markets resulting in total loss of the investments but high transaction charges paid to Company A. In 2022, seven of the money mules were arrested by Hong Kong, China Police. Police seized HKD3.3 million and luxury watches worth HKD800,000 (USD102,000) at the residence of the leaders of the syndicate. Furthermore, a total of HKD17 million (USD2.2 million) across 26 accounts used by the syndicate was also seized. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 15 - Laundering proceeds of 'Loco-London' gold fraud via casino accounts

fraud; casinos; money value transfer services

Between May 2016 and July 2018, a fraud syndicate perpetrated a series of Loco-London Gold ("LLG") investment scams by operating two bogus LLG trading companies to deceive victims around the world, and received benefits amounting to a total of HKD628 million (USD80 million). Once funds were received from victims, the money was remitted to several accounts in Hong Kong and Jurisdiction B. Owners of a licensed money remittance business, participated in the scam by remitting HKD192 million to casino accounts in Jurisdiction C. The LLG scam was reported to law enforcement agencies and led to the arrest of four people, including the business owners of the money remittance business. In 2023, all four were

charged with conspiracy to defraud and money laundering. A total of HKD160 million (USD20.4 million) was seized from several bank accounts held by the syndicate, and a further HKD130,000 was prevented from being dissipated. This result was achieved with the assistance of Jurisdiction B to trace the proceeds of crime. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 16 - Covid-19 Government loan fraud

fraud; financial institutions; COVID-19; third party ML

To alleviate the financial burden of small and medium-sized enterprises during the COVID-19 pandemic, the Government of Hong Kong, China launched a "Special 100% Loan Guarantee Scheme ("PLGS")" for eligible enterprises to borrow a maximum of HKD6 million. In 2022, Hong Kong Police neutralised two fraud syndicates which had recruited money mules to apply for loans worth HKD295 million using false employment and account documentation. For the loans that were approved, the funds were deposited into the money mules' bank accounts and immediately transferred to banks accounts of the leaders of the syndicate. Thirty-eight people have been arrested across two criminal syndicates and charged with conspiracy to defraud. Approximately HKD7 million in proceeds has been seized. The investigation into the case remains ongoing.

Source – Hong Kong, China

Case study # 17 Embezzlement of cryptocurrencies

theft; use of virtual assets; purchase of real estate; purchase of valuable or cultural assets

Person A was the financial operator of a FinTech company and his duties included handling the company's crypto-accounts. Person A took advantage of his position and transferred USD3.2 million (amounting to HKD25.6 million (USD3.3 million)) to his and his relatives' personal crypto-wallets. The stolen cryptocurrencies were subsequently exchanged for other cryptocurrencies, and were transferred back-and-forth between Person A and his associates.

Ultimately, cryptocurrencies worth around HKD18 million were converted to fiat currency and deposited into Person A's personal bank accounts, while the remaining cryptocurrencies were transferred to another crypto-wallet. Person A and his associates then purchased two residential properties and a brand-new vehicle. In mid-2022, the FinTech company conducted an internal audit check and uncovered Person A's embezzlement. Person A and two associates were arrested by the Hong Kong Police and charged with theft. HKD2 million in Person A's bank accounts and HKD 6 million virtual assets with a value of HKD 6 million were seized. The Investigation is ongoing.

Source: Hong Kong, China

Case study # 18 - Disguising ML Activities as Crypto transactions

fraud; use of virtual assets; third party ML

Investigation by Hong Kong Police revealed that a scam syndicate had exploited 136 bank accounts belonging to themselves or money mules to launder HK27M proceeds generated from various types of scams. The tainted monies were intermingled within these accounts or used in cryptocurrency trading before they were eventually withdrawn in cash from ATMs. In mid-2022, 16 persons, including the core syndicate members were arrested for money laundering and HKD 5.5 million was withheld from dissipation. The investigation is ongoing.

Source: Hong Kong, China

2.6 Indonesia

Case study # 19 - Terrorism Financing disguised as donations and legitimate business income

terrorism financing; financial institutions; abuse of legal persons; illicit arms trafficking

From 1998 to 2006 Person A was involved with the Negara Islam group. In 2005, Person A became acquainted with Jamaah Islamiyah (JI) by invitation of an ustad (teacher). In 2007, Person A performed an oath of allegiance in Rangkasbitung to join Jamaah Islamiyah, following an invitation from the teacher.

After the oath, Person A was appointed as an amir of Ribabah (the bottom of Jamaah Islamiyah organizational structure with only two members). Person A had a background as an entrepreneur (owning a successful car repair shop business in Pandeglang with several branches in other cities), and was appointed as a member of Iqtishod sub division which is part of Tajhiz division which focuses on the economy/business structure of Jamaah Islamiyah.

During this tenure, Person A made a deal with other JI members (under the leadership of Subject B, the owner of Company B) to plan terrorism acts targeting Chinese citizens in Banten. They also made preparations for amaliyah (terrorist attack) with the aim of taking over the government of the Republic of Indonesia, and implementing Islamic Sharia Law.

Person A and other JI group members planned to fund the purchase of firearms to carry out the attacks. Person A sent a sum of IDR76,000,000 (USD4,860) in six phases gradually. He used banking methods four times, each amounting to Rp 5,000,000 (USD319), and cash method twice in the amounts of IDR6,000,000 (USD383) and IDR50,000,000 (USD3,197).These payments were described as donations and combined with business income from Company B, totalling IDR286,000,000 (USD18,291).

Subject C, an employee at Company B, and the younger brother of the owner of Company B then collected the funds. Subject C then handed over the funds to Subject D, a JI member from East Java region, who was assigned to buy illegal firearms. Subject D managed to buy 1 revolver, 2 modified soft gun revolvers, 2 FNs with magazines, 1 SS1 with 2 magazines, 3 boxes of 9 mm calibre bullets, 2 boxes of 22 calibre bullets, and hundreds of SS1 bullets of calibre 5.56 mm before being arrested.

In 2021, Person A received a four-year imprisonment sentence and a fine of IDR50,000,000 (USD3,197), while the evidence (the firearms and ammunition) have been confiscated.

Source - Indonesia

Case study # 20 - Charity Box for Terrorism Financing

terrorism financing; abuse of NPO; cash

Person A, along with two other individuals, established Foundation X to support activity of JI particularly in the West Sumatra Region. Person A served as the founder of and advisor to Foundation X with overarching responsibility for its operations.

To conduct their activities, Foundation X sourced funds from:

- 40 money boxes / piggy banks disseminated to houses of donors.
- 25 glass boxes / charity boxes around the Payakumbuh city area.
- An account used to fund its 'activities program'.

Activities conducted by Foundation X included:

2017: Ramadhan Humanity Care (this activity was in cooperation with Z foundation (a legitimate NPO) and generated donations valued at INR260,000,000 (USD16,628). Funds were transferred to a bank account owned by Z foundation.

2018: Walk for Care to Rohingya (generated donations valued at IDR20,000,000 (USD1,279). Funds were transferred to foundation Z.

Foundation X agreed to support Foundation Z on the understanding that Person A would be sent as a volunteer to foreign jurisdiction A to deliver funds received from the fundraising activities.

Person A knowingly intended to deliver the funds to JI a prescribed terrorist organization. On 8 June 2022, Person A was convicted by East Jakarta Court to six years imprisonment and fined INR50,000,000 (USD3,197).

Source - Indonesia

Case study # 21 - Legal Charitable Foundation abused for Terrorism Financing

terrorism financing; abuse of NPO; new payment methods

Person A became a member of JI in 2006 and was active in the region of North Sumatra. At the end of 2014, Person A became the Chief of Charity Foundation X, a legal charitable foundation recognised by the Indonesian government.

After his appointment, Person A conducted several programs such as Donations for Gerakan Sedekah Seribu Sehari (IDR1,000 per day); Zakat; Social Donations including foods for poor people as well as charity boxes. 1,800 charity boxes were disseminated until 2020. Funds collected Charity Foundation X between 2014 and 2020 amounted to IDR1.2 billion (approx. USD77,297). In 2016, Person A started to learn digital fundraising.

The funds raised by Charity Foundation X were used for external programs, such as da'wah, education, social donation, Islamic solidarity world, enhancement of economic society, disaster response and internal programs such as legal / advocacy advice to arrested members of JI and their families. Charity Foundation X also made money transfers directly to JI.

Every year Charity Foundation X manipulated its reports to Baznas (National of Zakat Infaq and Sadaqah) and Ministry of Religion Affairs to conceal that it was a foundation created under JI.

While Person A held the position of Chief of Charity Foundation X in North Sumatra, he joined its National Conference and Board of Directors and discussed reports of programs conducted by each region and upcoming programs. At the same time Person A was receiving direction from Jamaah Islamiah JI, including how to transfer funds from the regional branch of Charity Foundation X to JI.

On December 2021, Person A was convicted on charges of terrorism and terrorism financing by judges, and received a sentence of five years imprisonment and fines of IDR100,000,000 (USD6,395).

Source - Indonesia

Case study # 22 - Multi Jurisdiction NPO exploited for Terrorism Financing

terrorism financing; abuse of NPO

In April to May 2020, Indonesia's FIU, PPATK, together with a counterpart FIU (FIU B), exchanged information within the framework of a joint analysis of alleged terrorism financing through the collection and distribution of donations carried out by several Non-Profit Organizations (NPOs), with global operational activities, and located in Indonesia and FIU B's jurisdiction (Jurisdiction B). One of these NPOs is Charity Foundation B which is registered in

Jurisdiction B. Within the period of 6 May 2019 to 23 July 2021, Charity Foundation B was identified as having conducted international wire transfers worth a total of AUD375,915 (USD240,873) to jurisdictions of interest.

Three parties in Indonesia were identified as receiving funds from Charity Foundation B, namely Person A (total IDR 133,213,091), Person B (total IDR 71,665,605) and Person C (total IDR 76,743,325). One of the administrators of Charity Foundation B, Person D, also wired funds to persons of interest to law enforcement in Jurisdiction C.

In addition, in May 2020, Person D was identified as transferring funds amounting to IDR 13,710,540 to Person D.

On July 27, 2021, PPATK coordinated with Densus 88 AT Indonesian National Police (INP), in which the Detachment 88 AT conveyed indications of terrorism financing supporting the terrorist group MUJAHIDIN INDONESIA TIMUR (affiliated with ISIS) by Person A, where it was suspected that the funds were derived from NPOs and individuals in Jurisdiction B (Person A was one of the entities who had received wire transfers from Charity Foundation B).

Furthermore, PPATK provided intelligence information based on the results of a joint analysis with FIU B. On July 29, 2021, Person A was named a suspect in Terrorism Financing and was arrested in Makassar, South Sulawesi. The investigation revealed that Person A made transfers to support the activities of the East Indonesia Mujahidin Group at the direction of Person N. In March 2022 the Indonesian Attorney General's Office advised that the case against Person A would go to trial.

PPATK conducted financial analysis of parties in Indonesia who received wire transfers from Charity Foundation B and Person D. PPATK also monitored social media for affiliated parties in Indonesia. Several additional entities of interest were identified and the analysis results were submitted to Detachment 88 AT.

PPATK also initiated trilateral joint financial analysis with FIU B and another counterpart FIU (FIU C) from Jurisdiction C (which had been identified in earlier analysis as receiving wire transfers from Charity Foundation B and Person N). The three FIUs also submitted a request to the FIU of Jurisdiction D to obtain information regarding donors and possible indications of involvement with terrorist groups in that jurisdiction.

In addition, PPATK worked hand in hand with the Directorate General of Customs and Excise (DGCE) in exchanging information. On 11 February 2022, the DGCE submitted data on Passenger Risk Management that confirmed that Person D had made two trips to Indonesia. Investigations revealed that the purpose of Person D's travel was to meet with Person A and distribute funding in Indonesia. As a result, incoming passenger alerts have been placed on Person D.

Source - Indonesia

Case study # 23 - Use of money-changer to obtain US dollars for travel to join terrorist organisation

terrorism financing; financial institutions; currency exchange

Person A was arrested in 2019 and subsequently convicted of committing a criminal act of terrorism and sentenced to six years of imprisonment.

Person A, together with several of his colleagues, routinely developed strategies to travel internationally to join a foreign terrorist organisation. In preparation, he made a bank cash withdrawal of IDR50,000,000 (USD3,197) with the intention that it would be exchanged for

USD at one of the money changers in Aceh. In addition, Person A also received a money transfer of IDR100,000,000 through a bank account which was exchanged for approximately USD6,950.

The USD and bank transfers were used, to fund the purchase of flights to a conflict areas. One of the bank transfers was affected through the account of the wife of one of the colleagues of Person A.

Source - Indonesia

Case study # 24 – Standalone Terrorism Financing from legitimate business funds

terrorism financing; cash

Person A owned a bread factory. He was not a member of JI but knew some of the senior member of the terrorist organisation and provided financial assistance to an Islamic boarding school affiliated to JI by providing rice and IDR350 million (USD22,384). Indonesian authorities conducted investigation into the financial flows, which indicated that the money was given to an intermediary to be handed to the school. The intermediary was the treasurer of JI. Person A was convicted of TF and sentenced to four years and six months imprisonment and fined IDR100 million (USD6,395) in 2021.

Source - Indonesia

Case study # 25 - Third Party Money Laundering from Narcotics

drug-related crime; third party ML

Person A acts as the recipient of funds from a foreign narcotics network on behalf of prisoners in three locations of the High-Risk Narcotics Correctional Institution in Indonesia. Person A has registered twelve companies, including companies purporting to run businesses such as import/export, tour and travel, IT and E-Commerce services and money exchanges through which the proceeds of the drug trafficking are laundered. The proceeds are estimated to be IDR390.2 billion (USD25 million).

Person A was sentenced to imprisonment for six years and received a criminal fine of Rp. 5,000,000,000 (approx. USD319,780). Assets confiscated to the state included three houses, one car and related bank accounts.

Source - Indonesia

Case study # 26 - Self Laundering in insurance business

fraud; market manipulation; standalone ML

Person A controlled the investments of Company A (an insurance company) together with six others. Person A served as Director of Investment and Finance from 2012-2014.

Between 2012 and 2019, Person A and others held shares in other entities which they manipulated to increase in value in the regular market and then sold them to Company A (via Person A's position in Company A).

The purchase of these shares and other investment instruments was risky because no fundamental and technical aspects had been conducted, where the analysis made is only for administrative completeness regarding the purchase of shares according to the agreement.

Person A spent the proceeds from the sale of his shares to Company A by buying land and buildings with the aim of disguising the origin, source, location, designation, or actual ownership of assets on behalf of himself and his family.

Mr. J was sentenced to 15 years of imprisonment and criminally fined IDR 750,000,000 (approx. USD48,000). Mr J was also ordered to pay the state IDR 314,868,567,350 (approx. USD20 million) representing the benefits he received from his illegal activity and assets including one car and seven apartments have been confiscated.

Source - Indonesia

Case study # 27 - Standalone Money Laundering using Legal Persons

standalone ML; abuse of legal persons

In mid-2017, Person B contacted Person A (the defendant) and asked him to open a company account for Company X. Person A then contacted Persons C and D to prepare an account for receiving funds from abroad.

On 5 January 5 2018, there was an inflow of Rp. 43,953,170,300 (approx. USD4,938) to Company Y from overseas transfers. The defendant, played an active role in transferring the money in the account of Company Y to the account of Company X by breaking up the transfer value and using the underlying as a land purchase, disguising the source of funds from Person B.

The court sentenced Person A with imprisonment for 3 (three) years and a fine of Rp. 1,000,000,000, or USD66,938.

Assets confiscated include:

- Money of Rp. 20,009,571,418 - (approx. USD1.3 million).
- Money of Rp. 19,896,963,138,- (approx. USD1.3 million) in the Bank M account in the name of Company Y.
- Money of Rp. 100,444,759,- (approx. USD6,720) - Cash Rp. 61,410,913 (approx. USD4,150).

Source - Indonesia

Case study # 28 - Proceeds from illegal Online Gambling used to purchase real estate and goods

gambling activities; purchase of real estate and goods

Offline and online gambling are crimes in Indonesia. In March 2021, police arrested 13 people in Jambi, Sumatra in premises suspected of being used for online gambling.

Investigations revealed that Person A was the owner and manager of the lottery gambling business. Proceeds of the illegal gambling activity were sent via bank accounts and used by Person A to purchase real estate and motorcycles.

Source - Indonesia

2.7 Japan

Case study # 29 - Proceeds of drug trafficking online - laundered using false names

drug-related crime; use of the internet; financial institutions

Person A was arrested on charges of violation of the *Act on securing Quality, Efficacy and Safety of Products including Pharmaceuticals and Medical Devices* and the *Act on Punishment of Organised Crimes* for selling illegally smuggled dangerous drugs and concealing proceeds of crime.

Person A made a profit by importing raw materials from Jurisdiction B and mixing them with other precursors to create and sell an illegal drug online. The criminal proceeds from these internet sales were deposited by Person A's mother who made 54 remittance transactions to her bank account via an ATM. Person A's mother was not implicated in any offending and was unaware that the funds were criminal proceeds. The total value deposited to the mother's account was JPY15,709,000 (approx. USD104,000). A further JPY8,755,000 (approx. USD58,000) was remitted by Person A using false names to his bank account via 15 transactions.

Source - Japan

Case study # 30 - Drug trafficking proceeds from Organised Crime Group

organised crime; drug-related crime; financial institutions

Person A, a member of a Japanese Organised Crime Group laundered the proceeds of trafficking in stimulants by depositing cash into three bank accounts held in a third person's name. Person A made 56 transactions on the accounts totalling JPY2.78 million (approx. USD18,000) in cash during the period August 2020 to June 2021.

The case is proceeding on the basis of an offence of disguising facts with respect to the acquisition of the proceeds of violation of the Anti-Drug special provisions law.

Source - Japan

Case study # 31 - Securities Company employee defrauds customers by creating false accounts

theft; fraud; use of the internet; financial institutions

Person A was employed by a securities company to develop and maintain its online securities trading system. Person A opened bank accounts in the names of the company's customers and transferred a total of JPY160 million (approx. USD1.06 million) from their securities accounts to the false accounts, from June 2017 to November 2019. Person A was prosecuted and convicted of Computer Fraud and violation of the *Act on Punishment of Organised Crimes*. Person A was sentenced to four years and six months imprisonment.

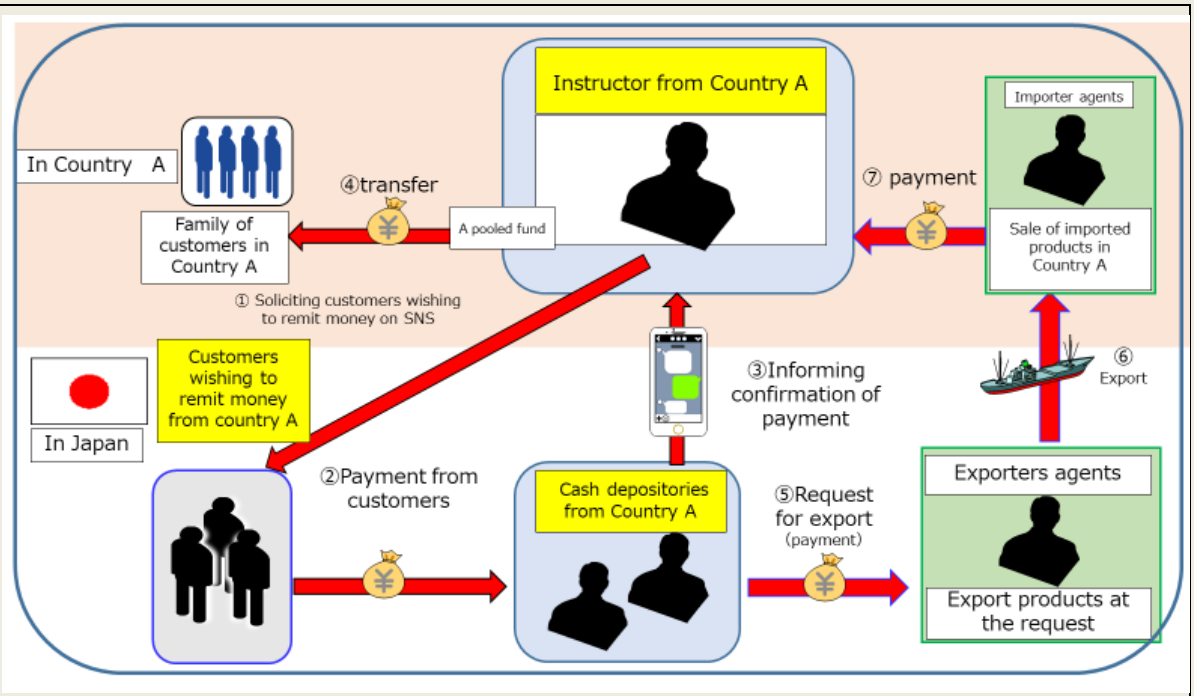
Source - Japan

Case study # 32- Underground banking intersection with import/export business

underground banking

An instructor in Jurisdiction A sought customers wishing to remit money from Japan on SNS, then instructed cash depositories in Japan to determine the transaction rates and designate bank accounts. Following the instructions, cash depositories confirmed payment from remitters. Then, upon payment, cash depositories asked export agents to export products under the guise of legitimate trade. In this way, cash in Japan was exchanged in Jurisdiction A's currency and deposited in bank accounts in Jurisdiction A. The commissions made on these transactions are relatively low, but the suspects have likely made profit from the commissions paid by the customers.

Source - Japan



Case study # 33: cryptocurrency scam where investor targeted through dating website

fraud; use of virtual assets

Person A and his group of associates developed a worthless crypto asset as a token for raising funds to invest in a fictitious overseas business. A victim was deceived into investing in the crypto assets by the group impersonating a female investor on a dating website. The victim used 42 Bitcoin and 1.4 million Ripple to purchase the fake crypto assets.

The group then transferred the fraudulently obtained virtual assets through two further coin wallets and a crypto broker before converting the cryptocurrencies to cash.

Source - Japan

Case study # 34 Proceeds from computer fraud concealed via transfer of Virtual Assets

fraud; use of virtual assets; third party ML

Person B conducted computer fraud and moved bitcoin to Person C, a person under his control. Person C transferred the Bitcoin to Person A, in exchange for a cash payment of JPY209 million (approx. USD1.4 million). Person A concealed the 41.28 Bitcoin in March 2021, by holding it in a wallet in the name of Person D but controlled by Person A.

Person A was arrested and prosecuted for violating the *Act on Punishment of Organised Crime (Concealment of Criminal Proceeds)*.

Source - Japan

2.8 Korea

Case study # 35 - "Omnis Gold" Internet fraud

fraud; phone fraud; use of the internet; use of virtual assets

This is a fraud case where the perpetrators swindled 141 victims of approximately KRW35.9 billion (approx. USD26.46 million). The fraud involved deceiving victims to charge points through a smartphone application and buy "Omnis Gold" coins with the promise of receiving a 4% return on their investment. The FIU facilitated the investigation by providing financial transaction reports to the investigating police office. By conducting a prompt and compulsory investigation, the prosecutors and police substantiated the perpetrators' offending and successfully arrested them all. The prosecutors and related relevant authorities identified the financial benefits obtained by the perpetrators and the Court approved a preservation order for forfeiture, before the prosecution on general property (not associated with the crime), owned by the perpetrators, consequently contributing to recovery of funds on behalf of the victims.

Source - Korea

2.9 Macao, China

Case study # 36 – Standalone Money laundering of foreign proceeds

standalone ML; financial institutions; wire transfer

Between December 2021 and March 2022, four Persons in Macao, China received a total of 125 remittances from three individuals in Jurisdiction A totalling USD2.8 million. Once funds were received into the accounts of the four Persons, the money was withdrawn in cash. During a CDD procedural check, the financial institution requested information as to what the cash was being used for and the four Persons advised it was to purchase goods, but could not produce sufficient documentation to support their claims. At the same time, the FIU of Macao, China received intelligence from overseas authorities that the three individuals in Jurisdiction A had previously used their bank accounts to collect fraudulent funds. The four Persons in Macao, China were suspected of assisting in the laundering of illegal funds from cross-border transfers, and the STR case was passed onto the Public Prosecutions Office by the FIU of Macao, China.

Source –Macao, China

Case study # 37 - Nine local men and women operating money laundering syndicate using debit cards to purchase gold

transnational organised crime group; fraud; dealers in precious metals and stones; third party ML; use of debit cards

In March 2022, the Judiciary Police received a crime report from the person-in-charge of a goldsmith shop regarding overseas customers conducting large transactions with debit cards. Payments for the transactions were suspended by the respective financial institutions as they were suspected to be proceeds of crime.

An investigation revealed a cross-border criminal syndicate was receiving proceeds of an overseas fraud via overseas bank accounts, and then deploying card holders to Macao, China to purchase gold with their cards. The debit cards and gold would then be given to the syndicate members, who would subsequently take the gold to a liquor shop after a number of layering transactions carried out by multiple syndicate members.

On one day, four overseas card holders visited two goldsmith shops five times, and used five different debit cards, to purchase gold valued at USD740,000.

Approximately USD370,000, of the total amount used to purchase the gold, were proceeds of crime from a telecom 'brushing' scam involving 55 victims.

On 19 October 2022, nine people were arrested across multiple locations. Items seized included 1 gold grain, cash in different currencies equivalent to more than USD125,000 and

four cars. Some of the involved individuals admitted to acting under the instructions of the criminal syndicate to assist in transferring and laundering the illicit proceeds by the method of purchasing gold with bank cards, for which they received around USD430 for every successful transaction. The investigation into the case is ongoing.

Source –Macao, China

Case study # 38 - Money laundering through casinos and trade in precious metals and stones

organized crime; bribery; extortion; standalone ML; foreign predicate offence; casinos; cash; trade in precious metals and stones; suspicious transaction reporting; use of debit cards

In 2021, the Public Prosecutions Office opened an investigation into suspicious activities reported by the FIU. In this case, Person A organized a criminal group (triad) in Jurisdiction X, arranging for others to conduct criminal acts such as bribery, control and embezzlement of state-own assets through violence, procuring of prostitution, extortion and blackmail. The total value of the proceeds of crime from these activities was estimated to be USD290 million. Person A received a life sentence in 2020 in Jurisdiction X.

The investigation revealed the proceeds of crime from Jurisdiction X, were concealed by being brought to Macao, China and gambled in several casinos by Person A. Between 2012 and 2017 Person A travelled to Macao, China and gambled, he also withdrew cash using credit and debit cards. Person A deposited a sum of USD2.9 million into his gambling account and purchased gold bars valued at USD583,000.

Person A was charged by the Public Prosecutions Office of Macao, China with money laundering in 2022.

Source –Macao, China

Case study # 39 - Detection of a cross-border drug trafficking case alongside with money laundering charges

standalone ML; use of debit cards; cash

In May 2020, the Judiciary Police and the police of Jurisdiction Y conducted a joint anti-drug trafficking operation and detected a cross-border drug trafficking case. Later, the police of Jurisdiction Y found four debit cards belonging to persons from Macao, China. It is alleged the bank accounts, which the debit cards were connected to, held the proceeds of drug trafficking. It was discovered the bank accounts belonged to two people from Macao, China. The two accounts were used to launder about USD198,000 between January 2020 and May 2020. The suspects involved in the case indicated they had withdrawn the proceeds of crime in cash using an ATM overseas.

In January 2022, 29 suspects were questioned in relation to the crime, and nine people made admissions in relation to purchasing drugs and depositing payment for drugs into the two accounts. It was uncovered the bank account holders provided ATM cards and passwords for others to use, in an effort to conceal the proceeds of crime. Two suspects were charged with aggravated money laundering and referred to respective prosecution authorities for action.

Source –Macao, China

Case study # 40 Using proceeds from telecommunications network fraud to purchase virtual currency

transnational organised crime group; fraud; third party ML; use of virtual assets; use of debit cards; foreign predicate offence; international cooperation

At the end of March 2022, the Judiciary Police of Macao, China received a notification from a counterpart in a foreign jurisdiction that a criminal syndicate was involved in cross-border virtual currency money laundering activities. After in-depth investigation, it was found that the syndicate used part of the proceeds of telecom internet fraud to purchase virtual currencies and laundered the money through a local telecommunication store.

According to the investigation, the criminal syndicate commenced its operation in October 2020. The syndicate instructed its underling members to open about 180 bank accounts in Jurisdiction A, which specialized in receiving and handling illegal proceeds derived from telecom frauds taking place locally and in several other jurisdictions, as well as receiving huge number of deposits of unknown origin. Since July 2021, the criminal syndicate ordered a number of members to travel to Macao, China to withdraw money from ATMs using bank cards issued by Jurisdiction A. Subsequently, virtual currencies were purchased via a telecom store and were resold on an overseas VASP trading platform. Money gained from VA sale transactions would then be withdrawn in cash in Macao, China thereby attaining the purpose of money laundering. Bank accounts in different jurisdictions held by the criminal syndicate were used for handling suspicious funds of approximately USD141 million in total, while syndicate members in Jurisdiction A and Macao, China withdrew a sum of USD46 million in total.

A joint operation by the Judiciary Police and the LEAs of Jurisdiction A was carried out. Judiciary Police officers intercepted two suspects from Jurisdiction A in a hotel, while intercepting two Macao, Chinese suspects and other suspects from Jurisdiction B in an apartment and at a telecom store respectively.

The Judiciary Police investigated and learnt that the two involved suspects from Jurisdiction A had withdrawn money approximately 1,000 times from ATMs in Macao, China since December 2021, with a total of USD3.6 million in cash being withdrawn. The bank accounts of the duo received a total of USD242 thousand derived from 12 scam cases in total.

The duo confessed at the same time that they used their own bank cards and those of their relatives and friends to withdraw money, and assisted the criminals from Jurisdiction A to conduct virtual currency transactions via overseas VA platforms. One of the Macao, China suspects and the other suspects from Jurisdiction B were staff members of the telecom store.

The Judiciary Police arrested and transferred the above suspects to the Public Prosecutions Office for charges of criminal association and money laundering, while continuing to pursue other involved individuals.

Source: Macao, China

2.10 Malaysia

Case study # 41 - Traffic Summons Discount Syndicate

bribery and corruption; suspicious transaction reporting

The FIU of Malaysia received Suspicious Transaction Reports from multiple financial institutions regarding law enforcement officers who were suspected of receiving and transacting sums above their income. Based on the FIU's analysis of the STRs, the law enforcement officers had received funds ranging between MYR30 (approx. USD7) and MYR20,000 (approx. USD4,270) from parties referencing summons payments and vehicle plate numbers. The FIU identified the recipients as law enforcement officers, and that they subsequently withdrew these funds in cash. The FIU referred the suspects to the Malaysian Anti-Corruption Commission (MACC) for investigation.

The MACC investigation revealed that there were two separate syndicates with similar modus operandi, the law enforcement officers identified individuals via social media who were interested in settling their traffic fines for a lower amount than charged. Once funds were received by the syndicate members, they were withdrawn in cash and a portion used to clear the summons at a discounted amount via a summons payment system which the law enforcement officers have access to, and the balance of the cash was then shared among syndicate members.

As a result of the investigation by the MACC, 60 accounts were frozen while 11 suspects were detained on suspicion of being members of the syndicates, which involved transactions worth more than MYR5 million (approx. USD1.06 million) since 2016.

Source - Malaysia

2.11 Mongolia

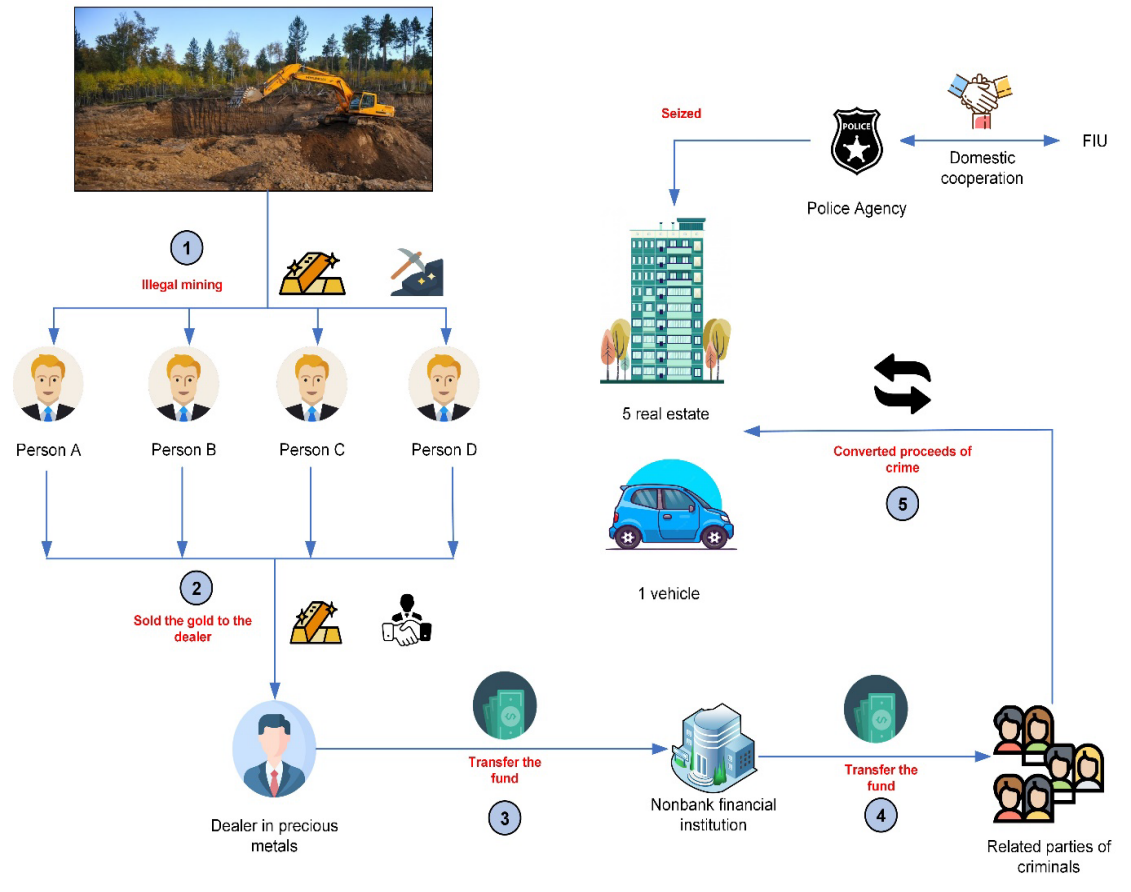
Case study # 42 - Money Laundering proceeds from Illegal mining

environmental crime; use of real estate; dealers in precious metals and stones

Persons A, B, C and D illegally mined gold under a licence for land restoration and sold it to dealers in precious metals. The perpetrators used non-bank financial institutions to receive the payment to their related parties' bank accounts to conceal the proceeds of the crime and then bought numerous pieces of real estate and vehicles. The dissemination by the FIU of financial information about the perpetrators, following a request from a law enforcement agency, has been a great 'value add' in the detection of the illegal activity. In addition, the law enforcement agency confiscated five apartments and one vehicle. In total, criminal proceeds worth MNT 657 million (approximately USD190,629) were seized in the course of the investigation.

The investigation started in May 2022 and legal proceedings commenced in January 2023.

Source - Mongolia



Case study # 43 - Laundering proceeds of drug trafficking through gambling accounts

drug-related crimes; gambling activities; international cooperation

Person A runs a criminal organisation involved in drug trafficking. Person A received narcotic drugs from two foreign countries through international mail addressed to his associates. Person A sold the drugs through his dealers who deposited the proceeds into international gambling accounts which Person A was then able to withdraw. Person A used these proceeds to purchase movable and immovable properties such as motor vehicles and real properties.

The investigation into the case has been ongoing since May 2022. Vehicles and real estate worth MNT 1.6 billion (approx. USD464,000) have been seized.

Mongolia's Narcotics Control Department cooperated with several national and international law enforcement agencies, including Customs, foreign police agencies, Interpol and the International Criminal Police Organisation.

Source - Mongolia

Case Study # 44 - Social Media Fraud – inheritance scam

fraud including identity fraud; use of the internet; cash; debit cards; international cooperation

Person A, a citizen of foreign Jurisdiction B, established relations with Mongolian citizens using social networks such as Facebook and Instagram. Person A created a scam claiming that the Mongolian citizens were entitled to inherit a large sum of US dollars by paying a transaction fee. The victims were instructed to transfer the fees into accounts of citizens who had had their internet banking information compromised. Person A also requested one of the victims to order an international bank card and send it to them via international mail. Person A then withdrew the funds from ATMs in Jurisdiction B.

The investigation into the case has been ongoing since January 2022, as Mongolia continues to work with the Economic Crime Department and the Fraud Investigation Department. Exchange of information through the Egmont Group, Interpol and the International Criminal Police Organisation has been integral to the investigation. The value of the fraud is estimated to be around MNT 158 million (approx. USD 45,843) in total).

Source - Mongolia

Case study # 45 – Theft of personal items and conversion of cash

robbery or theft/third party ML/currency exchange

In August 2022, Persons A and B broke into an apartment and stole USD 120,000 in cash, a middle-sized jasper snuff bottle, a horse saddle, gold bullion, a wristwatch, a diamond-encrusted ring and other jewellery. Person A's wife and mother-in-law exchanged a portion of the US dollars at a non-bank financial institution and purchased a motor vehicle.

USD 89,000 in cash and one vehicle were seized during the investigation.

The trial is scheduled for March 2023.

Source - Mongolia

Case study # 46 Transferring virtual assets from other people's wallets using malicious program

use of the internet; third party ML; use of virtual assets; money laundering

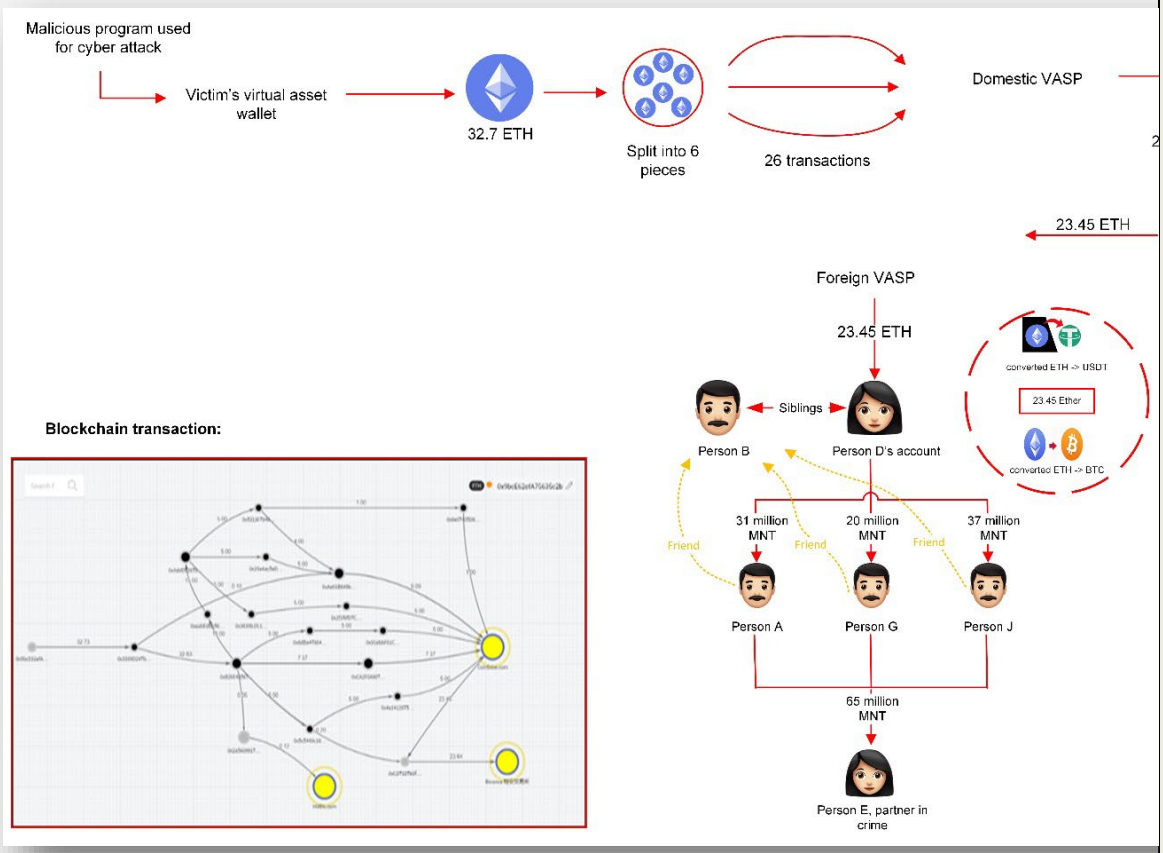
On July 2021, Person B hacked a victim's personal computer using a malicious program and stole 32.7 Ethereum from his virtual asset wallet. Then 32.7 Ethereum was transferred to a domestic VASP in 26 blockchain transactions divided into 6 pieces. Further, 23.45 Ethereum was transferred to the blockchain wallet and then transferred to Person D's account at a foreign VASP.

Person D is the younger sister of Person B, the above-mentioned cyber-attacker, and Person B converted Ethereum he hacked into Bitcoin and other cryptocurrencies to conceal the illicit origin using his sister's account. Next, he transferred cryptocurrencies to Person M, N and O, who were friends of Person B. After that, MNT 65 million was transferred to Person E who committed the crime together.

During the investigation, investigators found 0.5 Bitcoin in Person D's account at the foreign VASP, which was the remaining amount of cryptocurrency from the conversion of the stolen Ethereum, and then froze Person D's account at the foreign VASP.

Person B paid full restitution at the court stage; in October 2022, he was sentenced to 2 years and 6 months in prison under Articles "Illegal invasion to electronic information", "Developing and selling program and device for illegal invasion to electronic information network", "Money laundering" of the Criminal Code of Mongolia.

In January 2023, the Criminal Court of Appeal upheld the sentence of Person B.



Source - Mongolia

2.12 New Zealand

Case study # 47 Bitcoin trader facilitates fraud

fraud; use of virtual assets

A peer-to-peer bitcoin trader operating on localbitcoins.com facilitated the conversion of fraudulently obtained fiat currency into bitcoin on behalf of international fraudsters operating offshore. The overseas fraudsters would contact NZ-based victims and engage in deceptive practices (primarily romance and 'advance fee' scams) to convince the victims to provide them with money. The scammers instructed their victims to meet with their local 'associate' (the bitcoin trader) to conduct a cash handover, providing the victims with a time and place to meet the associate.

Meanwhile, the scammers also contacted the bitcoin trader advising they wished to purchase bitcoin with NZD, instructing the trader to meet with their 'associate' (who was actually the scam victim) at a specific time and place to conduct the handover. The scammers provided the trader with their bitcoin wallet address to which he was to credit bitcoin to the value of the cash handed to him by the victim. The bitcoin trader did not undertake any forms of CDD when facilitating these trades, accepting the cash from the victim, and crediting the value in bitcoin to the fraudster on a 'no questions asked' basis.

Source - New Zealand

2.13 Pakistan

Case study # 48 - Money Laundering through Fake Companies/Entities across Borders

trade based money laundering; underground banking; smuggling; tax crime; suspicious transaction reporting

Multiple STRs were reported by several currency exchange companies and a bank to Pakistan's FIU, the Financial Monitoring Unit (FMU) in relation to Person A, the owner of Company A operating in a provincial capital city.

Company A was exporting different types of goods to Company B, located in a foreign jurisdiction. The classification code for the goods to be exported was altered by Company A several times which triggered an alert at the bank. In parallel with this activity, different Currency exchange companies reported that Person A was also involved in purchasing high value foreign currencies (equivalent to USD2 million).

A follow up investigation by the reporting bank revealed that Company B was a fake company that did not exist in the foreign jurisdiction, and no actual goods were being exported in settlement of other payments to be routed to Pakistan. The funds received via encashment of dollars from cross border transactions were lodged against four advance payments for the export of goods to the foreign jurisdiction amounting to USD780,000. The dollars were purchased via structuring from different exchange companies by Company A in Pakistan.

Further, Person A routed approximately PKR1.5 billion through different accounts maintained with different banks by him via transactions with unrelated counter parties.

The tax records of previous years showed that Person A had paid a meagre amount of tax amounting to PKR365,000 (approx. USD1.3 million), in 2018 only. Person A was suspected of involvement in Trade Based Money Laundering, Tax Evasion and Hawala/Hundi. The FMU disseminated the financial intelligence to relevant Law Enforcement Agencies and also the Regulator. A raid was conducted on the basis of FMU's financial intelligence at the place of business of Company A. During the raid it was found that no actual business was carried on at the declared business premises and further investigation revealed an element of Trade Based Money Laundering (TBML). Several arrests were made and a case was registered against the relevant persons and the matter is under trial before the court of law.

Source - Pakistan

Case study # 49 – Terrorism Financing by small business

terrorism financing; underground banks & hawala; suspicious transaction reporting

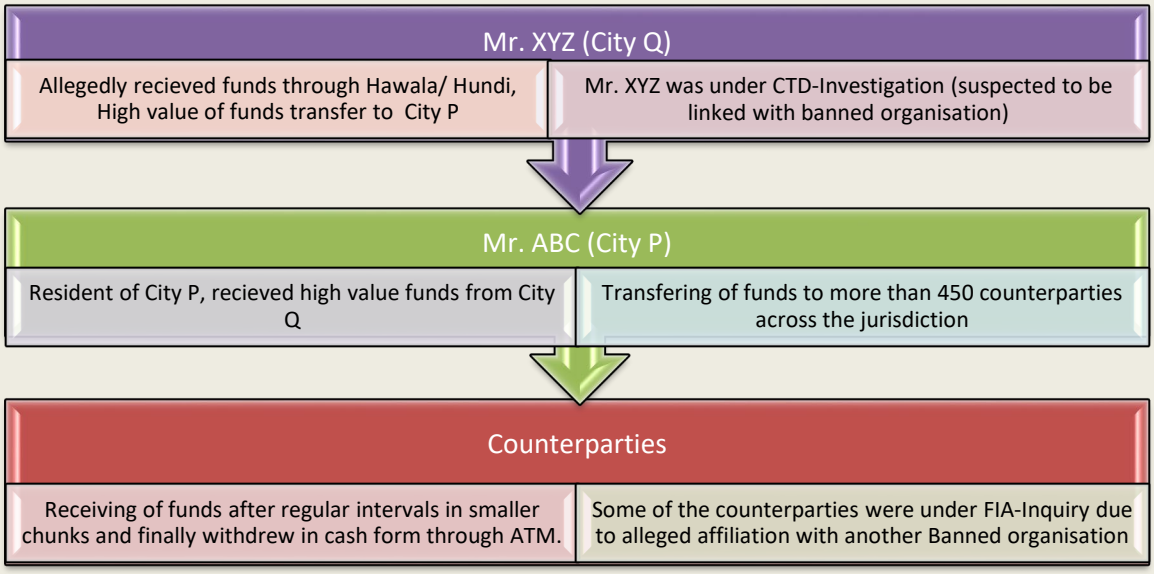
An STR was made about Person A due to unusual financial activity which did not match with their declared profile. Person A was a resident of City P and was running a small cloth shop, however, he was receiving funds from unrelated counterparties based in remote areas including City Q. It was found that Person A was maintaining seven bank accounts with three different banks with a combined credit turnover of PKR474 million (approx. USD1.65 million) over the past three years.

Analysis of inflow of funds revealed that individual was mostly receiving funds from Person B based in City Q. Person B was searched in the FIU's internal database and it was found that the FMU had already disseminated financial intelligence to the Counterterrorism Department (CTD) and Federal Investigation Agency (FIA) in relation to Person B's involvement in the illegal business of hawala/ hundi and possible links with a domestic banned organization. During this analysis, it was found that both Persons A and B were under investigation with CTD.

Analysis of the outward flow of funds from Person A revealed that the funds were being remitted to around 450 counterparties across the jurisdiction in small amounts at regular intervals. Further, analysis of those counterparties found that multiple individuals who were receiving funds were already under investigation by the FIA for their alleged involvement with a banned organization.

The FIU's analysis was shared with the CTD and FIA for further investigation. Pictorial presentation of the flow of funds is provided below.

Source - Pakistan



Case study # 50 – Terrorism Financing of Vehicle-borne Improvised Explosive Device

terrorism financing; money value transfer services; international cooperation

A vehicle-borne improvised explosive device (VBIED) exploded in 2021, in a large city in Pakistan, resulting in several casualties. Initial investigation revealed that Person A was the key suspect and the owner of the vehicle used in the attack. CTD registered a case against Person A along with his facilitators, including Persons B, C and D. CTD also asked the FMU to provide details of STRs/CTRs and Banks accounts/financial transactions of the suspects.

The FMU conducted a search of its internal database and also circulated the Computerized National Identification Numbers (CNICs) amongst its reporting entities. The details received from the reporting entities identified individuals linked to the suspects including the wife and son of Person A, the account introducer of Person A, the financers of Persons A and D, and the brother of Person C (and a proscribed person).

The FMU disseminated its financial intelligence to the CTD and at a later stage, it shared a detailed analysis that found that Person A, a resident of the biggest city of Pakistan visited another large city of Pakistan where he reactivated a dormant account, conducted a cash withdrawal transaction and then closed the account. The withdrawn funds were then allegedly used to purchase the vehicle which was used in the terror attack. Person C provided logistics to Person A and is a brother of a proscribed person. Person C was later identified as key suspect in the attack. The detailed analysis found that the financier of Person A had also conducted transactions with Person D apparently for terror financing. Further investigation by CTD, identified that Person A's financier was the mastermind behind the terror attack. Frequent travel abroad by the suspects was also observed.

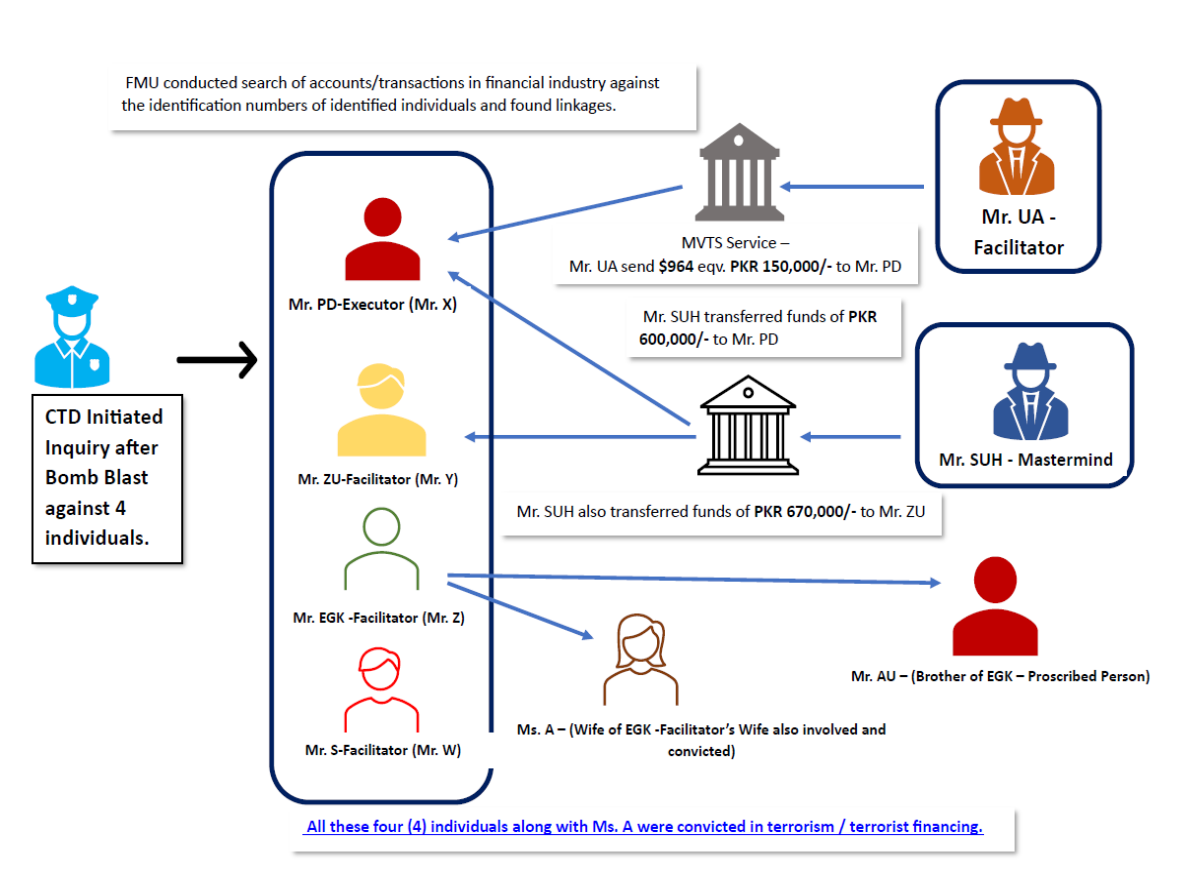
The FMU identified that Person A had received some remittances from a foreign jurisdiction. Therefore, the FMU sought international co-operation from the relevant foreign FIU in respect of the remittances received. The foreign FIU provided the requested information to the FMU which was passed on to CTD.

The mastermind/financer, executor and facilitators (and Person A) were arrested and convicted under the *Anti-Terrorism Act* 1997 and other relevant laws. However, two individuals were convicted of terror financing and received punishment of five and seven years'

rigorous imprisonment along with a fine of PRK 50,000- and PRK100,000 respectively (approx. USD174-348)

Furthermore, orders for confiscations/forfeiture in the sum of PKR3,144,000 (approx. USD10,956) were made although the value of assets seized/frozen initially was PKR4,025,000.

Source - Pakistan



Case study # 51 – Tax evasion by a group of family members

tax crime; suspicious transaction reporting; abuse of legal persons and arrangements

An STR was made against Company A for suspected of tax evasion. Analysis by the FMU found that Company A was registered with Securities and Exchange Commission of Pakistan (SECP) by four members of the same family. Fifteen other entities were also registered with SECP by the same family members.

The family members were maintaining a number of personal and business accounts with different banks. Huge credit turnovers in the accounts were noted. The legal persons/entities were also conducting a large number of currency transactions. The funds were being routed through different bank accounts of the entities making the flow of funds complex. It was suspected that this was a strategy to conceal the origin of the funds.

The Federal Board of Revenue (FBR) database showed that despite the huge turnovers of the accounts, minimal amounts of tax had been paid to the government by Company A and the family members. Public domain searches revealed that the reported individuals were allegedly involved in mis-declaration, stealing and tax evasion. The case was referred to the FBR-Inland Revenue for further investigation in February 2021 and is currently under trial.

Source - Pakistan

Case study # 52 – Luxury Motor Vehicle Fraud

fraud

Company A was registered with the Securities and Exchange Commission of Pakistan (SECP). The company was an authorized dealer of a renowned foreign automobile manufacturer (Company B) specializing in high-performance sports cars, SUVs and sedans.

The owner of Company A, Person X, maintained a number of personal and business accounts with different banks with significant credit turnovers. Review of statement of accounts revealed that Company A made their last consignment payment to Company B in 2017. Further, it was found that no vehicles had been delivered to Company A over the last two years by Company B due to a legal issue. Despite this, Person X was falsely claiming that vehicles were available for booking and was collecting advance payments from the public. Analysis revealed that a number cheques purporting to be refunds were dishonoured.

Analysis showed that Person X was fraudulently collecting the funds from the general public for the delivery of luxury cars but no vehicles were delivered, nor were the advance payments refunded. It is estimated that Person X made PKR800 million (approx. USD 2.8 million) from this activity.

Person X departed to a foreign jurisdiction after conducting the fraudulent activity. The FMU shared its financial intelligence with the relevant LEA for further investigation and a case was filed against Person X.

Source - Pakistan

Case study # 53 - Ponzi Scheme, defrauding public by offering lucrative investment packages

fraud; organised crime; abuse of legal persons and arrangements; use of the internet

Person A declared himself proprietor of Business A, engaged in IT services, E-commerce and online advertisement services. Person A opened five accounts in the name of Business A at different banks in the year 2019. The transactional activity in the accounts was comprised of online transfers (IBFTs, Internet Banking, Mobile applications) and cash deposits from a large pool of individuals all over Pakistan. The credit transactions were in small amounts, but the frequency of credit transactions was very high, while debits were less in number but high in value.

Simultaneously, Person A registered a private limited company with SECP in the same business name, which was involved in the business of online shopping and E-Commerce. As per the company registration form, it had three directors, namely Person A (51% shareholding), Director 2 (25% shareholding) and Director 3 (24% shareholding). The individuals opened company bank accounts with different banks in Pakistan at the start of 2021, however, Person A was the only authorized signatory for each of the company accounts.

Activity on the accounts mostly comprised of online transfers (IBFTs, Internet Banking, Mobile applications) and cash deposits from different individuals for investment. Analysis identified that the accounts were used to raise funds from the general public all over Pakistan for the purpose of investment for lucrative profits, which was against the mandate of the company.

The private limited company with the same name as Business A was working as an agent of a foreign forex trading entity in Pakistan and various social media platforms were used to demonstrate the process to make payments to the foreign forex trading app through the company accounts. The central bank has declared the online forex trading platforms illegal and barred Authorized Dealers from facilitating forex trading activity on these platforms.

The financial institutions, regulatory bodies and law enforcement agencies received complaints against the company from the general public regarding frauds and cheating the public at large. Upon inquiries by the banks, the individuals including Person A withdrew all funds from the accounts via cash and digital transfers. Later, all the accounts were either closed or blocked by the banks, upon instruction from the Law Enforcement Agency.

The financial intelligence was shared with the relevant law enforcement agency which started investigating Company A and its directors. The intelligence was also shared with the regulators for sensitizing the financial institution and for taking appropriate regulatory action.

The SECP has included Company A in the list of companies that have indulged in unauthorized activities of leasing/financing facility, Multi-level Marketing (MLM), pyramid/Ponzi schemes, seeking deposits from the general public in the name of jobs, investment and trading etc. Further, the FIA has registered a case against Company A and its directors, including Person A.

Source - Pakistan

Case study # 54 - Use of family members' personal accounts for business transactions

tax crime; hawala

Several STRs were made by different banks in relation to four individuals who were depositing cash in their respective bank accounts in a structured manner in order to avoid the reporting threshold. These individuals were engaged in sugar brokerage and dry fruit businesses and were conducting transactions with unrelated counterparties located in different geographical locations in the jurisdiction which was suggestive of a hawala business.

During the analysis of the STRs received by the FMU it was also noted the reported individuals had conducted transactions with sugar mills. As per media news at the time, an inquiry commission was investigating various sugar mills in relation to allegations of sugar hoarding, which presented another avenue of further enquiry to determine whether the four individuals were involved in this activity.

The FMU's analysis was shared with the relevant LEA for investigation in relation to tax evasion and hawala, respectively. The case is now at the prosecution stage, however, four assets have already been seized.

Source - Pakistan

Case study # 55 – Dealer in Precious Metals and Stones prosecuted for Money Laundering

standalone ML; trade in precious metals and stones

An individual engaged in the business of gems and mineral specimens was identified as maintaining multiple accounts at different branches of the same bank located in three different cities. Significant credit turnover was noticed across the accounts, with credits mainly sourced from foreign remittances. Upon inquiry, the individual declared to the bank that these were payments for his gems and mineral exports, however, no documents were provided in support of these claims. The individual was also reported in some CTRs conducted in high-risk border areas of Pakistan.

Based on the financial intelligence shared by the FMU, the relevant law enforcement agency initiated an investigation and are prosecuting the individual for money laundering based upon the difference identified between their declared import & export data and accounts turnovers.

Source - Pakistan

Case study # 56 – Bank fraud laundered through Company

abuse of legal persons and arrangements; international business companies; fraud; foreign predicate offence; international cooperation

An STR was received by the FMU from a local bank in relation to Pakistani citizen Person A. The STR referred to an adverse media report about Person A and his family for alleged involvement in a significant banking fraud in a foreign jurisdiction. The media report stated that Person A received proceeds of over GBP100 million (approx. USD123 million) through this fraud.

In 2000, Person A formed Company C to provide finance to MPs, footballers and entrepreneurs. In 2004 Person A was named Young Entrepreneur of the Year in the foreign jurisdiction.

Analysis of open-source media identified that Company C collapsed in 2007 with massive debts, however, by falsifying accounts, Person A was able to obtain massive loans from a foreign bank and managed to funnel the loan funds into family bank accounts in Pakistan. Reportedly, Person A has been jailed in the foreign jurisdiction.

Analysis of the STR and currency transactions reports (CTRs) by the FMU uncovered multiple accounts being maintained by Person A and his family members with different banks in Pakistan. Analysis of KYC/CDD documents reported in a STR revealed that Person A changed his name on his national identity card in Pakistan. The analysis of STRs/CTRs also showed that accounts were being maintained by Person A and his family members mostly in their personal names and Person A also controlled family members' accounts. The accounts contained different currencies including USD, GBP, EUR and PKR. Huge funds were routed through Person A and his family's accounts via different modes of transaction.

Additional open-source analysis revealed family members of Person A were appearing in a local court in Pakistan for alleged involvement in a property fraud. Person A was also identified as having formed a real estate business and a fashion brand business in Pakistan.

Based on the available information and analysis, the financial intelligence was shared by the FMU with the law enforcement agencies (LEAs). The inquiry and investigation by the LEAs revealed that Person A was involved in the offence of money laundering and has concealed his taxable income and assets and evaded tax thereon. The LEAs also obtained international cooperation from the foreign- FIU through Pakistan's FMU during the investigation process.

Source - Pakistan

Case study # 57 – Ponzi scheme using online platform

fraud; use of the internet; use of virtual assets; abuse of legal persons and arrangements; international cooperation

Origin of POC/ML

This complex online fraud offence was discovered by law enforcement in January 2021.

The FMU also received an STR and disseminated their analysis in relation to the group referenced below (A&B Group) in early 2021 highlighting concerns in relation to the operations of their companies and accounts.

Persons A and B are the principal suspects involved in a Ponzi scheme responsible for cheating members of the public of PKR17 billion (USD94.4 million) between January 2019 and February 2021. They developed the A&B Group and with the help of another individual maintained a web portal purporting to offer investment opportunities with a return of 7% to 20% per month.

The companies solicited investment by claiming business in property deals; Crypto Exchange; Information Technologies, Transport Services and Trading, however, no such investments were ever made and the investment from new customers was used to finance the interest payments made to current 'investors' creating a Ponzi scheme. It is assessed that 50% of new deposits were diverted to pay current investor interest and agents who were employed to establish new investors. Payments from this online platform were funneled through the A&B company group.

Highlights of ML investigation

The A&B Group was made up of 26 companies established by Person A and registered in the names of his family members including his son, his cousin, and two wives in the family group.

Investigation with SECP revealed that these companies held no legal license to solicit deposits from the public and as such their actions were illegal.

Investigation linked 70 bank accounts of the accused, his relatives, un-registered companies and SECP registered companies, maintained in several commercial banks throughout Pakistan since 2019. Analysis of these accounts was undertaken utilizing banking experts and established how the scheme laundered the proceeds of crime through these accounts and into

the private accounts and investments of Person A and his accomplices. Details of these accounts were obtained from the Central bank and in excess of 50,000 transactions were analysed.

An asset discovery investigation established that the POC had been used to purchase 31 immoveable properties and 30 moveable properties with an estimated value of PKR 6.7 billion (USD 37.2 million)

Interagency and International cooperation

The LEA formed an investigation team in September 2021 led by the AML/CFT Directorate, Islamabad with a senior investigator and lead investigator appointed. Expert forensic computer investigators facilitated the recovery and analysis of a complex database which enabled investments to be transacted though a multilevel fake referral scheme. This database was held in the cloud and required expert assistance to recover. The database contained in excess of 1,000,000 transactions which were reconciled against payments into the A&B accounts.

Family tree and related data was collected Database and Registration Authority and the travel history of the accused was obtained to aid the investigation. Information / evidence shared by Financial Monitoring Unit (FMU) and Securities and Exchange Commission of Pakistan (SECP) and record from different commercial banks through regulator (SBP) also helped in the investigation.

Interpretation of the data retrieved from the website of the accused suggested that the accused have been doing same fraudulent business in Jurisdictions B and C. Financial investigation has also suggested that the POC was transferred to Jurisdiction D for which international cooperation request has been sent. International cooperation is also underway to trace the assets in jurisdictions B and C and tracing the accomplices of the accused there.

Use of Modern Investigative Techniques

Investigation techniques utilized during the ML Investigation included forensic accounting, digital forensics, social engineering of social media profiles, analysis of banking records, interviews and seeking assistance from international jurisdictions.

Attachments / Seizures

- 41x accounts with deposit of PKR. 3 billion (16.6 million USD) were frozen under S12 of National Accountability Ordinance ('NAO'),1999 during May-July 2021.
- 17 properties were identified and frozen under S12 of NAO 1999 in May-July 2021 with an estimated value of PKR 2.5 billion (13.8 million USD).
- 13 properties valued at PKR 700 million (3.5 million USD) frozen under S12 of NAO 1999 in January 2022.
- 30 vehicles valued at PKR 500 million (2.5 million USD) frozen in under S12 of NAO 1999 March 2022
- All identified assets have been attached to the court case and remain frozen.
- Total attachment / seizures of bank accounts, 31 immoveable and 30 moveable properties is PKR 6.7 billion (USD 37.2 million)

The Securities and Exchange Commission of Pakistan has also concluded adjudication proceedings against the Group and its sponsors for raising illegal deposits from the public and operating pyramid schemes, in violation of the Companies Act, 2017. The Group comprises of 18 companies incorporated under the Companies Act, 2017 as well as five unincorporated business setups. The main sponsor of Group is Person A, along with his immediate family members. SECP, after completing the due process of law, has disqualified the sponsors of the Group from becoming directors of any company for a period of 5 years and has also imposed a penalty of Rs.100 million on each of its sponsors. Further, the sponsors shall not be allowed to incorporate any new company under the Companies Act, 2017.

Element of Complexity / Multiple Parties / Criminal network

As detailed above, the perpetrators acted as an organized network in creating an online platform and controlling payments into the A&B Group of companies for an unlawful Ponzi

scheme. This multilevel referral fake scheme rewarded agents who introduced new clients and used the income from new investors to pay out existing liabilities and keep the scheme afloat.

Investigation involved analysis of huge number of transactions (over 1,000,000 transactions were recorded between, 2019 and 2021), on the platform resulting in the collection of PKR 17 billion (USD94.4 million) which flowed through the shell companies set up by Person A and his accomplices.

Use of shell companies as multiple parties having complex structures, multiple bank accounts, online transactions, online investment platform contributed to the complexity of investigation which also involved a complex money trail and forensic bank accounting of more than 70 bank accounts in which the POC was collected and routed through.

Tracing and accounts analysis of 26 shell companies having bank accounts in various parts of the jurisdiction was also a challenge. The investigators are able to crack the entire computer and internet-based system and database to access the records and ascertain the exact amount of POC collected.

Source - Pakistan

Case study # 58 - Drug Trafficking patronized by a political exposed person

drug-related crime; politically exposed person

Person A was arrested in 2022 after LEA intercepted a motorcycle and discovered 0.5 kg of Hashish. During the investigation, LEA requested information from financial institutions to trace Person A's assets and financial linkages.

On the basis of these inquiries the FMU received a STR from a savings bank advising that Person A purchased a savings certificate valued at PKR300,000 (approx. USD1,045) in 2020, which was blocked on the basis of the LEA's asset inquiry letter. During the analysis by the FMU, it was found that Person A visited a bank branch in 2022 and deposited a large sum of cash in the form of five cash transactions into the account of Person B. Upon probing, it was revealed that Person B was a political exposed person. Further analysis of transactional activity in the bank account of Person B revealed that they authorised pay orders – in the same amount received from Person A - to a third party for the purchase of a property The FMU's financial intelligence was shared with the relevant law enforcement agency.

Person A has been charged under the Control of Narcotics Substance Act 1997.

Source - Pakistan

Case study# 59 Bitcoin trader facilitates fraud

Drug related crime; use of virtual assets

An STR was reported by Bank A on the account of Person A upon suspicion of his involvement in unauthorised dealings in VA. Activity on a VA trading platform revealed that Person A was involved in the sale/purchase of Bitcoins, which is not legal in Pakistan as per the Central Bank's instructions. Bank A investigated Person A's account because transactional activity was reportedly unusual due to high turnovers in the account and transactions with unrelated counterparties. During the analysis of transactional activity, it became clear that the individual was involved in the trading of virtual assets.

Further, Person A was conducting high value transactions with various unrelated counterparties, most of whom were suspected of being involved in Hawala or other criminal activity. Pakistan FIU's databases, identified one of Person A's counterparties, Person B, a proprietor of X business which was found during an investigation by the Anti-Narcotic Force to have acquired proceeds from the sale of drugs. The account of Person B was credited with a substantial volume of funds from the account of Person A with no clear purpose.

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

Source - Pakistan

2.14 Philippines

Case study # 60 – Fraud by employees

suspicious transaction reporting; theft; wire fraud

Company A had 174 STRs on its account - between 4 November 2019 and 12 December 2019 - funds with an approximate total value of USD226 million were transferred from the company's account to 69 recipient-accounts in 14 countries, including an individual in Jurisdiction B. Company A's account was a common account for numerous affiliated companies within a group. The recipients were not suppliers of Company A and had no business transactions with them. It was revealed the remittances to the bank accounts were facilitated by key employees of Company A, Worker 1 and Worker 2 who were authorised to operate the accounts, but not authorised to make those specific transfers. Worker 1 claimed to be the victim in the romance scam and had stolen funds from Company A to pay the scammer.

The individual located in Jurisdiction B, received two deposits of USD500,000 each from Company A, into two domestic bank accounts, on the same day. The FIU of Jurisdiction B assisted with information about this individual which led to recovery of USD999,464 between 10-16 December 2019.

The FIU of Jurisdiction B also coordinated with the FIU of Jurisdiction C to determine other possible cohorts.

Source - Philippines

Case study # 61 – Proceeds from sale of child abuse material

sexual exploitation; money value transfer services

Person A, a foreign male national was arrested by authorities in Jurisdiction A for child sex offences. Person A sent money via mobile wallets to a suspected national of Jurisdiction B, facilitating the purchase of child abuse materials. Investigation into Person A's devices revealed screenshots between 29 December 2022 and 2 January 2023, showing funds transfers via mobile wallets totalling PHP1,300.

Currently, the FIU of Jurisdiction B is conducting a parallel investigation on the case.

Source - Philippines

Case study # 62 – African Drug Syndicate

organised crime; transnational organised crime group; drug-related crime

Five Persons were identified through 158 suspicious transaction reports totalling PHP3.8 million (USD317000). It was suspected that the Persons are part of the African drug syndicate (ADS). Person A and Person B were arrested by the LEA in province X on 8 November 2017 for allegedly supplying "shabu" (crystal meth) in the region.

Bank information revealed Person A operated a beauty salon and was in relationship with Person C, who was also suspected to be involved in the STRs. The accounts of Person A were

frozen pursuant to a freezing order dated 22 October 2020 for alleged involvement in illegal drugs although this did not result in forfeiture due to inadequate asset value.

Person B had suspicious dealings with Person D.

Person E was arrested, together with a citizen from a foreign jurisdiction on 10 March 2018. Intelligence reports indicated they were engaged in the extensive distribution of shabu in province X and the region. The diagram below shows the interrelationship of the suspected individuals who are all members of ADS.

Volume-wise, inward (international) remittances related to ADS dominated STRs (45 instances out of 158). In terms of PHP value, outward transfers (international) related to ADS amounted to PHP1.4 million (or 38% of the total outward STRs). The year 2017 seems to be the most active year for the group both in terms of volume of transactions and corresponding peso-equivalence due to the contributions of Persons A and D. Reported transactions tapered off in the succeeding years, following the arrest of Persons A, B and E.

Source - Philippines

Case study # 63 – Successive Deposits and Withdrawals

suspicious transaction reporting; casinos

In 2014 Person A opened a regular savings account with Bank ABC with an initial deposit of PHP449,000 (USD7,913). Person A declared having a consultancy business, from which he generates his funds.

From 27 March 2017 to 20 April 2017, several cash and cheque deposits (ranging from PHP357,000 to PHP4.90 million (USD 86,000)) were made into Person A's account, followed by large-value withdrawals (ranging from PHP605,600 to PHP7.08 million).

In the conduct of enhanced due diligence, Bank ABC discovered that Person A acts as a money mule who carries cash to casinos. Person A himself disclosed to the branch that his friends deposit funds to his accounts, which he then delivers to them should they need cash at the Casino. Upon inquiry by the branch on the nature of these transactions, Person A stopped using his personal account.

Meanwhile, Bank ABC also filed STRs on Entity A, which appeared to be Person A's consultancy business. Between 20 June 2014 when Entity A's account was opened and April 2017, there were no significant transactions observed. However, between 3 April 2017 and 24 January 2018, the branch noted 853 transactions, ranging from PHP126,500 to PHP10.09 million (USD2,200 to 178,000). Additional 132 transactions with amounts ranging from PHP17,000 to PHP13 million were recorded from 23 March 2018 to 8 November 2018. The covered person deemed the transactions of Person A and Entity A as having no underlying legal or trade obligation, purpose, or economic justification.

Source – Philippines

Case study # 64 – Citizen fraudsters

suspicious transaction reporting; abuse of legal persons and arrangements

Two STRs corresponding to suspicious transactions dated 31 March 2016 were filed by Bank ABC on two individuals—a Filipino and a Jurisdiction X Citizen—for their alleged involvement in a modus operandi of Jurisdiction X Citizen fraudsters. Based on Bank ABC's disclosure, the modus operandi involved Filipino women who are being used by Jurisdiction X Citizen fraudsters to facilitate the opening of their fly-by-night businesses. These businesses are supported by business registration certificates from the Department of Trade and Industry which in turn are presented by Jurisdiction X Citizen as supporting documents when opening accounts.

As observed by the reporting covered person, the accounts owned by the alleged Jurisdiction X Citizen fraudsters would have a minimum balance upon opening. The accounts would remain inactive for a year and then a highly suspicious, questionable amount of money would be transferred/credited thereto.

Source - Philippines

Case study # 65 – Romance Scam

use of the internet; fraud

A reporting covered person discovered multiple online posts involving an account allegedly used in a romance scam. Romance scams involve a person/or persons feigning romantic intentions towards a victim, who will later be defrauded once the former gains the latter's trust and confidence.

The reporting covered person narrated that the social media posts identified the scammer as Person A. Person A would introduce himself to his victims as a member of the Marine Corps. Thereafter, Person A would send a message supposedly from his superiors, asking for money to fund his flight, to be booked by a military agent. Person A would ask the victim to send funds to an alleged Bank X mule account under another name.

Source – Philippines

Case study # 66 – Flipping funds

suspicious transaction reporting; Use of the internet; new payment method

A total of 74 STRs were filed by covered person PQR on Person A for wallet-to-wallet transfers in October 2021that were deemed to be not commensurate with the business or financial capacity of Person A, whom PQR profiled as a driver.

Person A's transaction-level data displayed indicators of being a possible mule account. The chain of transactions involving Person A begins with a single sender, transmitting funds exactly amounting to PHP10,000 (USD176). Thereafter, the money would be passed to another person who would then send the money back to Person A.

Upon closer inspection of the transaction-level data submitted by PQR, it was noted that Person A's transactions coincided with PQR's promo gaming activity called the "Send Money Challenge." Said promo allows PQR's consumer accountholders residing in the Philippines to earn a voucher when they send a minimum of PHP10,000 to a unique verified client of PQR, through PQR's Send Money feature. Each user can participate up to 10 times to get the maximum reward.

Person A transacted with at least two sets of PQR account holders on each of the indicated transaction dates. Person A transacted with their counterparts in various geographical regions across the jurisdiction.

Source – Philippines

Case study # 67 – Possible pass-through accounts

suspicious transaction reporting

Person A was the subject of 23 STRs filed by Bank X on 13 December 2018 due to unusually frequent transactions associated with his account. Based on the STR narratives, Person A's account recorded 97 transactions with an aggregate amount of PHP2.9 million (USD51,000), in a span of 35 days. These transactions comprised 17 cash deposits, totaling PHP1.1 million;

23 online fund transfers, totaling PHP0.4 million; 10 over-the-counter withdrawals, totaling PHP1.1 million; and 37 ATM withdrawals, totaling PHP0.3 million.

During the probing process, Person A claimed that most of the fund inflows were given by a relative as an allowance and for payment of tuition fees. Person A, however, did not disclose the name and profile of the relative. In addition, Person A admitted that their unnamed friends were also using the account to receive funds in their favour. The account behaviour is indicative of a pass-through pattern, where the total fund inflows stood at PHP1.5 million and fund outflows at PHP1.4 million.

Meanwhile, two other CPs filed STRs in relation to Person A on the basis of an AML investigation being conducted on Jurisdiction X students and Person A's outward transfers were deemed as not commensurate with their declared profile. These two CPs stated that Person A was sending large amounts of money without familial relationship or an underlying legal trade obligation. Further, no supporting documents were presented to establish legitimacy of relations.

Source – Philippines

Case study # 68 – Alleged association with bank hacking incident

use of the internet; fraud

Eleven individuals and three entities figured in 56 STRs valued at PHP24.7 million (USD435,000), linked to alleged involvement in the 2021 Bank ABC hacking incident. Person A is one of the five suspects arrested by the NBI, and suspected to behind the unauthorized transfer of money from more than 700 Bank ABC customers in January 2022 to Bank XYZ accounts. A law enforcement agency informant revealed that while a person offered phishing websites to perpetrators and used e-mails to send links of phishing websites to victims, persons in Jurisdiction B provided devices to anyone looking for options to cash out illegally obtained funds. In addition, two local persons served as the web developers tasked to scout for vulnerabilities in bank websites.

Based on a news article, alleged cybercriminals were able to access the victims' accounts at Bank ABC, despite the victims not clicking any suspicious links. Clients of Bank ABC were surprised to receive emails, as well as text communications, notifying them of the bank transfer. Also, there were instances when the hackers were able to get past the one-time PIN (OTP) security feature of the bank.

An AMLC financial intelligence report identified that the Bank XYZ accounts of four local persons, B, C, D and E, were found to be recipients of funds from Bank ABC and apparently were used by a certain Person J who is not an account holder of Bank XYZ. The value of the suspicious transactions was PHP7.7 million (USD135,711).

Person F generated the highest number of STRs from the dataset related to this case valued at PHP9.3 million. The STRs narrated that the subject's account was identified as one (1) of the recipients of funds from the hacked Bank ABC accounts as well as the first to third level beneficiary of the earlier mentioned accounts of persons B and D. Person F was asked for supporting documents to establish the legitimacy of the various online bank transactions given their declared source of funds as a medical student. The subject disclosed involvement with cryptocurrency exchange trading.

The Bank ABC related hacking transactions occurred mainly in 2021 and were found to be mostly inter-account transfers with 41 counts valued at PHP22.3 million (USD393,000) and cash deposits valued at PHP1.5 million (USD26,436).

Source – Philippines

Case study # 69 – Recruitment of money mules

use of the internet; fraud

Money mules are recruited via face-to-face, online job scams, social media networks, and romance scams. Some were duped into believing that they would be involved in legitimate transactions and were attracted with the lucrative return.

For instance, Person A has a legitimate convenience store and was recruited by Person B into what Person A believed was a legitimate money scheme. Person B promised Person A a portion for every bank transaction they undertook. Person B is a national of foreign jurisdiction X and was arrested in 2019 for allegedly operating a multimillion PHP online scam. It is alleged that Person B entered the Philippines on a student visa and created a romance scam through which he swindled women of approximately PHP8 million (USD141,000).

Person A assisted Police with their investigation. It was found that Person A had made 83 transactions valued at PHP3.6 million (USD63,500) during a six-month period in 2019. All transactions were purely cash-based (i.e., cash deposits, and withdrawals via ATM, and over-the –counter) obscuring the ultimate source (deposits) and destination (withdrawals) of funds.

Source – Philippines

Case study # 70 – Package Scam

fraud; new payment method

Person A, a Jurisdiction X national, is included in the list of customers provided by a covered person (an EMI), in relation to possible involvement in suspicious activities through the use of mobtels (mobile telephones). Person A's account posted significant deviations on transaction amounts over the years. He had one (1) transaction involving mobtels (electronic cash card/gift card/debit card – withdrawal), amounting to PHP2,298. Person A received a total of PHP0.2 million in 2018 via six remittance transactions from Person B. Person A received 104 remittance transactions from Person C, amounting to PHP3.7 million (approx. USD65,209).

Person C received transactions coming from various individuals who are possibly victims of their deceitful acts where the declared purpose was mainly for business while the relationship to sender is either a client or a friend. The reporting entity specified that Person C had a total of 104 outward remittances, amounting to PHP3.7 million and 78 inward remittances, amounting to PHP2.7 million.

In addition, Person C is suspected of being an associate of Person D. A customer of said pawnshop requested pertinent documents concerning Person D and Person C who are allegedly involved in swindling activities. Said customer went to a branch of the pawnshop to send remittances with aggregate amount of PHP78,000 to Person D, where the purpose was payment for a package and the stated relationship to the receiver as "company representative of EG," a global courier. The remittances were released on the same day by one of the pawnshop's authorized agents and the declared purpose was payment, while the relationship indicated was as "a friend." In the pawnshop's conduct of due diligence, it was learned from the customer (sender) that the foregoing remittances were payment for her anticipated package coming from her son-in-law. Purportedly, the customer received a call from a representative of EG informing that her package has arrived at the airport, but she needs to pay PHP78,000 for its release to be coursed through Person D who is referred to as an agent. The fraudulent act was only discovered when the customer's daughter informed her that there is no package being sent by her husband (the victim's son-in-law). Moreover, the customer tried to communicate with the alleged agent, who, unfortunately, can no longer be contacted. Relative to this, a copy of the CCTV footage and other necessary documents of Person D and Person C were requested, and said incident was also reported for blotter to the

police. The pawnshop deemed the transactions of Person D and Person C suspicious due to the swindling complaint filed by the package scam victim.

Source – Philippines

Case study # 71 - International inward remittances received on behalf of a person by a group of people possibly related to each other

new payment method

A group of males from three foreign jurisdictions were reported as potentially engaged in an illegal activity. The group were receiving remittances on behalf of an unidentified female customer with whom they declared a family relationship. Most of the transactions were claimed simultaneously on the same day at MSB A Branch, while other transactions were collected using the MSB A Service App. It was also noted that these customers have suspicious e-mail addresses in their records and are apparently related to each other because of their similar family names, residential location, and occupation. According to the report, these individuals are potentially linked to hacking and blackmailing activities.

Source – Philippines

Case study # 72 - Client's withdrawal in cash, leaving no audit trail

fraud; use of the internet

Person A's account was a subject of an investigation because of a remittance cancellation due to an alleged e-mail hacking. The remittance came from a company and was allowed to be credited to Person A's account, as they had previously provided documents, such as a condominium reservation agreement and price table, and a franchise agreement with an accredited remittance partner. Person A had received three remittances from Person B, totalling PHP16.6 million (USD292,000). Correspondingly, cash withdrawals ranging from PHP90,000 to PHP5 million, totalling PHP16.34 million were likewise transacted. Person A claimed that person B is a friend, and the remittances were intended for financial assistance on the proposed franchise of an MSB B outlet and for the purchase of two condominium units. The transactions on the account and business papers, however, did not reveal other transactions pertaining to her remittance agent business or trading. Given this information, Person A's transactions were reported on the basis of the recalled remittance allegedly due to e-mail hacking fraud and questionable remittances with significant amounts that were all withdrawn over the counter in cash, leaving no audit trail.

Source – Philippines

Case study # 73 - Suspicious Indicators: Not commensurate with the financial capacity of the client (4 examples)

suspicious transaction reporting

A reporting entity received a report from Bank C regarding unauthorized fund transfers related to a confirmed phishing incident, involving the account of their client, Person A. The funds credited to Person A's account were either subsequently withdrawn via ATM or transferred to other accounts. Historical review of the account showed inflows of cash deposits and online transfers (unknown senders/recipients for remittance transactions) that ranged from PHP300.00 to PHP100,000 (USD1,762), which exceed the declared profile of Person A. Person A had declared an online business and a grocery store (unregistered business) as the source of their funds with a monthly income of PHP50,000.

A bank noted three transactions of a construction company, Company B, that were deemed not commensurate with its business or financial capacity. The transactions consist of an inward remittance of USD34,276 (EUR24,914) from a foreign Non-Governmental

Organization (NGO); a check deposit of PHP100 million (USD1.76 million) that was subsequently returned the next banking day; and an attempt to deposit a bogus EUR50 million bank draft, purportedly issued by a Foreign Bank. It was also disclosed that the inward remittance of USD34,276 is the subject of a complaint due to an alleged fraud. The complainant claimed that this this remittance was supposed to benefit a domestic NGO. Online search revealed that a case of estafa (fraud) was filed against Company B and its president, Person X. Person X, along with another individual, was arrested by the National Bureau of Investigation for allegedly stealing PHP6 million (USD105,745) from the funds provided for Typhoon Yolanda aid. Both were accused of hacking into the e-mail addresses of a domestic NGO and a foreign NGO so that the money was not deposited into the bank account of the domestic NGO but the account of the construction company.

Person A works as a team leader and "code stockist" at Marketing Company X. Person A's account, included 138 cash deposits, 356 Internet fund transfer credits, 11 international and domestic inward remittances, and 143 bills payment credits. Person A's customers buy codes for the activation of their Marketing Company X account to become an official member. Based on the report of the CP, Marketing Company X's business model looks like a pyramid scheme as the company does not have products to sell and the business relies on the recruitment of people. There were two ways to earn: firstly, through captcha encode (This does not require a software installation and is mostly used by websites to prevent hackers and spammers from immediately doing a particular action, using script or bots. Criminals prefer bots to hack passwords in various accounts and spam comments in blogs); and secondly, by inviting people. The volume of the transactions noted are suggestive that the account is being used as a conduit to facilitate pyramid activity by Company X. Likewise, the transactions were grossly incommensurate with Person A's declared economic profile.

Bank A received a report against their client, Person A, regarding unauthorized fund transfers due to a confirmed phishing incident, involving a savings account owned by a client of Bank B. Review of the Bank B client's account disclosed that there were 13 online fund transfers, ranging from PHP2,500 to PHP50,000 to the savings account of Person C. Examination of the account of Person C showed several transaction inflows composed of cash deposits, online payments, and fund transfers that were not consistent with the declared profile and source of funds of the client, while transaction outflows consist of withdrawals via OTC and ATM, and transfers to other deposit accounts. Upon inquiry about the source of funds credited to his account, Person C claimed that they were from his parents. He also denied connections with or knowledge of the Bank D client and admitted sharing his account number to his family and friends.

Source – Philippines

Case study # 74 – Account takeover involving electronic money issuer (EMI) wallets (2 examples)

fraud; new payment method

EMI 1 reported 8,847 transactions in 2019, following its investigation of complaints raised by some banks involving account takeover, where some bank accounts maintained by these banks were compromised and proceeds of the activities were transferred to various EMI 1A wallets. The accounts were compromised through hacking, using phishing methods to capture details necessary for the transactions.

In 2021, EMI 1 reported 13,116 transactions, involving various EMI 1A customers who are victims of account takeover. These include incidents of EMI 1A customers falling victim to phishing through calls, SMS, e-mails, phishing links, fake EMI 1A pages, other fake pages via social media platform chat or through an e-commerce platform app, lost/stolen phones, and other means.

Source – Philippines

Case study # 75 – Hacking of user account in social media platform

use of the internet

Reports were submitted regarding the client, Person A, where her account was used to illegally transfer funds by hacking the social media user account of a male victim and defrauding the victim's wife to remit PHP130,000 (approx. USD2,324) via a convenience store. This involved six STRs and were reported by two covered persons.

Source – Philippines

Case study # 76 - No underlying legal or trade obligation, purpose, or economic justification (2 cases)

suspicious transaction reporting

(1) In the case of Person A, the bank reported that based on Person A's submitted accreditation certificate, it was authorized to operate in a property in Pasay City. Person A's customer information record with the bank, however, contained a Pasig City address. Further, the branch manager visited the declared business address, but the place was empty. Person A made significant cash deposits, totalling PHP10.56 million (approx. USD189,000) from October to December 2018. Cash transactions range from PHP1 million to PHP3 million. The bank requested supporting documents, but person A failed to provide any.

(2) In another case, Person B received various remittances, totalling USD14.99 million (PHP714.51 million) from 24 August 2015 to 14 November 2016. The reporting entity views the remittances as having no economic justification and noted unvalidated claims by Person B that the remittances came from authorized payment service providers. Person B's account was also noted to have the same signatories as Person C, who was also a subject of several STRs for having the same transaction pattern as Person B. Both Persons B and C are Service Providers.

Source – Philippines

Case study # 77 - Amount involved is not commensurate with the business or financial capacity of the client

suspicious transaction reporting

In 2018, Person A, an SP, was the subject of several STRs involving various transactions from 2017 to 2018, particularly eight (8) check in-clearing transactions (PHP30.74 million), 122 cash deposits (PHP431.06 million), 58 check deposits (PHP247.15 million), 13 inter-account transfers (PHP119.75 million), and 1 generic-coded STR (approx. total USD14.7 million). The bank narrated that it was closely monitoring the transactions of Person A due to the large transactions being made, which range from PHP256,000 to PHP89 million. The bank further narrated that the client advised that the transactions are lease payments of various individuals and entities. The client, however, was unable to present supporting documents to justify the disclosed reason. The transactions were perceived as not commensurate with the client's declared source of funds.

Source – Philippines

Case study # 78 –Unusually Frequent trips

suspicious transaction reporting; cash; casinos

Between December 2019 and March 2020, Individual Carrier J landed in Manila 33 times from either of two foreign jurisdictions A and B. Except for two trips, Individual Carrier J brought cash from Jurisdiction A (with equivalent values between USD132,632 and USD3.6 million). On two occasions, Carrier J brought US dollars, amounting to USD250,000 and USD11.8 million, respectively. Individual Carrier J declared in the FX declaration forms that he was involved in sales international trading. In some of these, he also named himself as the owner of the foreign currencies in his possession and Person A as the intended recipient.

Investigation into Person A indicated that A received foreign currencies not only from Individual Carrier J but also from Individual Carriers K and L, both nationals of Jurisdiction C and Individual Carriers M and N, both from Jurisdiction A. The five named carriers had a total of 38 inbound trips from December 2019 to March 2020 and their disclosures stated that the funds were for Person A for casino gambling. In a span of about four months, Person A received a combined amount of about USD60.9 million from these five carriers.

Among the five identified carriers (Carriers J, K, L, M, and N), only one yielded a positive match in the Philippines FIU database. Information received by the AMLC on 07 July 2020 revealed that Individual Carrier L has been previously flagged by the local-level police authority in Individual Carrier L's in Jurisdiction C for alleged involvement in an organized crime. A suspicious transaction bearing the same date showed that upon the request of the Philippine Casino regulator, Individual Carrier L has been put under review after being identified to have been transporting bulk currencies into the Philippines.

Source – Philippines

Case Study # 79 – Cryptocurrency heist

use of virtual assets; terrorist financing; abuse of non-profit organisation

Person A is a project director of a non-profit organization that was suspected by law enforcement agencies to be involved in TF by supporting activities of a group in the southernmost part of the Philippines. The Crypto account in VASP C of Person A was receiving cryptocurrencies (mostly bitcoin) from more than 300 external crypto wallets and other crypto accounts in VASP C accumulating to around P856,000 (approx. USD15,309). Funds were accumulated in Person A's account in VASP C and eventually transferred to crypto wallets with unknown addresses.

Source – Philippines

Case Study # 80 – Funds from donations scam converted to cryptocurrency

use of virtual assets; terrorist financing

Ms. H, a female college student in a location high risk for TF, is under investigation for alleged involvement in TF activities of a designated group. There were donations from various senders coursed through EMI X and MSB Z (in small amounts not exceeding P2,000) for four months aggregated to around P92,000. Ms. H also received funds from various bank transfers that accumulated to around P263,000 (approx. USD4,703). It appeared that the accumulated funds were not used for the advertised purposes but were used to purchase cell phone load and were withdrawn by Ms. H. A part of the funds was used to purchase fraction of bitcoin which was eventually transferred to crypto wallet with unknown address.

The case was referred to the AMLC Secretariat by a law enforcement agency requesting the conduct of a financial investigation on Ms. H and bank accounts (with Ms. H as the account owner) posted in various social media accounts for donations for affected areas of the super

typhoon which may have been used to finance terrorism in the Philippines. The investigation is still ongoing.

Source – Philippines

Case study # 81 - Funds from donation scam converted to cryptocurrency

use of virtual assets; terrorist financing

In 2022, AMLC received a report from a VASP who disclosed that an account holder had cashed in funds through a Money Service Business (MSB) and converted them to bitcoin. These funds were then sent to an unlabelled wallet address. Further analysis on the blockchain platform reveals that the bitcoin from the said wallet address was eventually forwarded to another wallet address associated with transfers which had links/associated with terrorist organization.

This matter has been referred to domestic law enforcement and international counterparts.

Source – Philippines

Case study # 82 - Funds from Organized Crime converted to cryptocurrency

organised crime; money laundering; use of virtual assets

Mr. I and Mr. O posed as Jurisdiction X students in the Philippines and enrolled in provincial colleges. Mr. R is a 29-year-old Filipino crypto trader with fund transfers from Jurisdiction X Citizens suspected to be involved in a hacking incident. Mr. R and his counterpart Jurisdiction X Citizens used a common law firm based on their transaction patterns in Bank Y. Mr. I was noted to have high volume cash in transactions in VASP C via his bank account in Bank Y ranging from PhP11,000 to PhP2.2 million. Similarly, Mr. O has high-volume cash in transactions in VASP C.

Meanwhile, Mr. R had sale transactions of a cryptocurrency (a form of cash out) with VASP B totalling PhP5.5 million after Mr. I sent fund transfers to his accounts. Mr. R also sent two outward remittance transactions totalling PhP1.8 million to a foreign politically exposed person of Jurisdiction S which was high risk for TF and hacking. Based on initial investigation of the Anti-Money Laundering Council, significant part of the proceeds of a hacking incident allegedly ended up in unidentified crypto wallets as planned, coordinated, and processed by Mr. I, O and other anonymous members of the group involved in the hacking. In addition, Mr. I and Mr. O were reported to have been recruiting Filipinos across the jurisdiction as money mules.

This information was shared with the National Bureau of Investigation on 29 September 2020.

A separate investigation revealed Mr. R to be a related party of an incidental subject in a drug-related case. The information was shared with a law enforcement agency during a Target Intelligence Packaging workshop held in April 2021.

In a recent study titled "Environmental Scanning: Cybercrime Threats and Perpetrators" (Environmental Scanning Study), the AMLC likewise identified Mr. I, Mr. O, and Mr. R as among the thirteen individuals who were related parties in the hacking incited that transpired between in June 2020. Several banks, pawnshops, and EMIs reported 801 questionable transactions totalling PHP162.3 million (approx. USD2.9 million) involving these thirteen individuals and one (1) corporate entity. The Environmental Scanning Study was disseminated to various AMLC stakeholders, including law enforcement agencies, in November and December 2022.

Source – Philippines

2.15 Singapore

Case study # 83 - Case of terrorism financing through online platforms

terrorism financing

In 2022, a foreign national working in Jurisdiction A was convicted and sentenced to two years and eight months' imprisonment, under the Terrorism (Suppression of Financing) Act 2002, for providing monies to benefit a terrorist entity. The individual worker was self-radicalised and attracted to the Islamic State of Iraq and Syria's goal of establishing an Islamic caliphate in Syria. In 2020, Person A transferred monies of up to SGD 891 (USD654) on 15 occasions through online platforms, to fundraising campaigns for Syria-based organisations. Person A was aware the funds could either entirely or in part, be used to benefit the causes of Hayat Tahrir Al-Sham, an entity designated under the ISIL (Da'esh) and Al-Qaida Sanctions List.

Source - Singapore

Case study # 84 - Case of international cooperation in ML investigations

fraud; foreign predicate offence; third party ML; currency exchange; cash; international cooperation

Between 2019 and 2020, the Commercial Affairs Department (CAD) of the Singapore Police Force received reports stating victims were deceived into transferring monies totalling SGD54,940 (USD40,314) to two bank accounts in Jurisdiction A for fictitious investments. These transfers were made to a bank account maintained in Jurisdiction A in the name of an incorporated company (Company A), and a bank account maintained in Jurisdiction A in the name of a foreign national from Jurisdiction B, (Person B).

Within a span of four days following the receipt of the monies, the funds were transferred from Company A and Person B's bank accounts into a personal bank account maintained in Singapore by another foreign national from Jurisdiction B, Person C. Investigations subsequently revealed the transfers from Company A were made pursuant to an unlicensed cross-border money-changing and remittance transaction operated by Person C in Jurisdiction B, and the transfer from Person B was purportedly for the purchase of luxury watches from Person C.

In August 2020, Person C was charged for carrying out an illegal remittance business in Jurisdiction A and money laundering offences committed under the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act*. Person C was granted permission to leave Jurisdiction A and failed to return. The Court issued an arrest warrant against and CAD sought Jurisdiction B's assistance to locate and repatriate Person C. In October 2022, Person C was arrested by the authorities in Jurisdiction B while attempting to depart for another jurisdiction. Person C was brought to Jurisdiction A where they made full restitution to the victims and was convicted and sentenced to 12 weeks' imprisonment. The successful cooperation between Jurisdiction B and authorities from Jurisdiction A proved invaluable in the prosecution of money laundering offences committed through a bank account in Jurisdiction A and repatriation of Person C to be charged and prosecuted with the relevant offences.

Source - Singapore

Case study # 85 - Case of STR- initiated ML investigations arising from investment scams

fraud; foreign predicate offence; third party ML; abuse of legal persons and arrangements

In 2018, Singapore's Financial Intelligence Unit, the Suspicious Transactions Reporting Office (STRO), received information regarding bank accounts maintained in Singapore belonging to a Singapore-incorporated entity (Company A). The company had received proceeds of an investment scam from victims in Jurisdiction B. Working closely on the financial intelligence disseminated by the STRO, the CAD of the Singapore Police Force initiated money laundering investigations.

Investigations revealed that Company A was incorporated by Person A. Sometime in 2017, Person A entered into an arrangement with their friend, Person B. Under this arrangement, Person A would assist by facilitating transactions in Company A's corporate bank accounts on instructions from Person B. Person A would receive a commission for each amount transacted. Investigations found that Person A maintained a total of three corporate accounts for this purpose. Between December 2017 and November 2018, these corporate accounts received a total of USD1,960,478 and SGD1,606,191(USD1.18 million) across 307 inward transfers, of which USD331,822 and SGD4,250 were confirmed to be the benefits of criminal conduct arising from investment scams with victims located in both Jurisdiction B and Singapore.

Person A was prosecuted and charged for money laundering offences committed under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act in Singapore. For recruiting Person A into the arrangement, Person B was convicted and sentenced to 26 months' imprisonment and fined SGD 70,000 (approx. USD51,000) for money laundering offences under the CDSA. The swift conveyance of financial intelligence ensured that the Singapore authorities could take immediate and decisive action – thus preventing the further misuse of Company A and its bank accounts from receiving proceeds of crime.

Source - Singapore

Case study # 86 - Case of ML investigation involving illegal wildlife trafficking activities

environmental crime; organised crime; third party ML; foreign predicate offence; transnational organised crime group

The CAD and the National Parks Board commenced joint investigations into a case of illegal wildlife trafficking of rhinoceros horns, involving proceeds of crime of about SGD1.2 million (USD880,000). The agencies collaborated closely in a multi-pronged approach, which included enforcement action against the illegal wildlife trade, and investigating the financial flows, to identify the syndicate members (e.g. in poaching, transport and middlemen) and the financier behind the illicit activities based overseas. Information exchange was facilitated by INTERPOL, the FIU and direct agency-to-agency channels with the source, transit and destination countries. INTERPOL provided valuable inputs on trends and its experience in multilateral liaison efforts.

Recognising that international co-operation amongst the source, transit and destination countries was essential to halt the illicit trade, the agencies participated in an INTERPOL Operational Support Team (OST) deployed to Jurisdiction A to assist the foreign authorities in their wildlife trafficking investigations against the syndicate. The INTERPOL OST focused on the exchange of information between the authorities and fostered bilateral relationships to facilitate future co-operation. It also aimed to set a model to promote collaborative information sharing and exchange, which is vital to peel back the layers involved in illegal wildlife trafficking syndicates.

Person A from Jurisdiction A was prosecuted as the trafficker with two charges under the *Endangered Species (Import and Export) Act* for bringing 18 pieces of white rhinoceros horn and two pieces of black rhinoceros horn into Singapore without a valid CITES export or re-export permit. Person A was also charges with one count under the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992* for assisting Person B, whom Person A knew to be involved in the illegal trade, to retain his benefits from the criminal conduct.

Source - Singapore

Case study # 87 - Case of money laundering involving VAT fraud proceeds

tax crime; smuggling; fraud; third party ML; foreign predicate offence; cash

In March 2021, Singapore's Customs and the CAD conducted joint investigations following information received of an unsuccessful attempt to make Value-Added Tax (VAT) refund claims in foreign Jurisdiction B by persons travelling to a city in Jurisdiction B for the purpose of claiming fraudulent VAT refunds at its airport. The travellers were allegedly not entitled to claim such VAT refunds as they did not purchase the jewellery pieces in question from Jurisdiction B. It is alleged the invoices used to claim the refunds were fictitious. In total, these travellers received EUR42,975(USD45,700) in VAT refunds. After obtaining the refunds in cash, the travellers returned to Singapore.

Extensive information exchange was conducted via INTERPOL, the FIU and direct agency-to-agency channels of Singapore and Jurisdiction B. Competent authorities on MLA in both countries were also in close contact to provide advice and expedite the investigation to obtain the necessary evidence for successful ML prosecution.

In December 2022, Person A and the travellers were charged for engaging in a conspiracy to possess the fraudulently obtained VAT refunds under section 47(1)(c) of the CDSA (2000 edition) read with section 109 of the Penal Code. The travellers were also charged for failing to declare the cash they were carrying into Singapore which exceeded the prescribed amount under section 48C(2) of the CDSA (2000 edition). Person B allegedly returned to Singapore with jewellery pieces in question without making the necessary declaration under the Customs Act. Person B was also charged with failing to declare goods imported into Singapore under section 128B(1)(a) of the Customs Act. Person A was also charged with abetting the travellers to breach their cash reporting obligations and abetting Person B in the commission of the offence under the Customs Act. The case is currently in court.

Source - Singapore

Case study # 88 - Case of Company director convicted of Tax Evasion, ML and Cheating Offences

tax crime; fraud; standalone ML; financial institutions; purchase of real estate; purchase of valuable or cultural assets

Person A is a director of Company A, a Goods and Services Tax (GST) registered company. Despite Company A being GST-registered, Person A conducted cash sales with customers without accounting for the sales in both income tax and GST returns of Company A. This resulted in an undercharge of SGD110,119 (USD81,000) of GST between 1 May 2011 and 31 October 2017, and SGD69,391 (USD51,000) of corporate income taxes underpaid between the years of assessment 2013 and 2017. Sometime in 2013, Person A influenced his staff to alter inventory figures to inflate the profits of Company A in an attempt to dishonestly induce a financial institution into approving Company A's loan application.

Person A was also found to have used the under-declared sales of Company A to pay for his deposit and housing loan for a condominium and vehicle, totalling more than SGD400,000 (USD294,000.)

This case was identified by an officer situated at the CAD Satellite office for parallel ML investigations and allowed for information sharing, and close cooperation between the tax and ML agencies. In May 2022, Person A was convicted for tax offences, cheating and money laundering offences under section 47(1)(c) of the CDSA. In June 2022, he was sentenced to nine months imprisonment and ordered to pay penalties totalling SGD253,195 (USD186,000).

Source - Singapore

Case study # 89 - Case of Professional Enabler who facilitated dealing with proceeds of crime

fraud; foreign predicate offence; professional facilitators

This is a case of a professional enabler who facilitated the use of shell companies to deal with scam proceeds.

Person A was appointed as the local resident director of four companies incorporated by foreign directors. Person A failed to conduct the relevant due diligence and did not make contact with the foreign directors of the companies. The corporate service provider couriered bank documents and tokens to unknown overseas addresses when instructed by an unverified party. As a result, the four companies' bank accounts received criminal proceeds of over USD550,000. Through collaboration with foreign authorities, it was established that the criminal proceeds were linked to business email compromise scams and internet love scams, involving multiple local and overseas victims. Person A was convicted in late 2021 of offences under the *Companies Act*, an alternative criminal justice measure to ML, and sentenced to imprisonment of six weeks and disqualified from being a company director for five years.

Source - Singapore

Case study # 90 - Case of criminal syndicate engaged in complex ML

fraud, third party ML; financial institutions; dealers in precious metals and stones; cash

An investigation revealed that a criminal syndicate used nine dormant business entities to defraud close to SGD40 million (USD29.4 million) in training grants from a government agency. The business entities were set up by Person A and Person B, who are husband and wife. With the assistance of another person, Person C, the syndicate recruited Person D and several others, who agreed to be appointed as nominee directors of the business entities and to relinquish control over the business entities to the syndicate. Person A engaged three runners to cash cheques issued from bank accounts of the business entities. Person A or another member in the syndicate accompanied the three runners to the bank, handed the cheques to them and waited near the banks to collect the cash. The three runners received commissions in return.

Person C assisted the syndicate to launder the criminal proceeds by accompanying the nominee directors to cash cheques issued from bank accounts of the business entities and bank accounts controlled by members in the syndicate, including the personal bank accounts of Person D. Person A instructed the nominee directors who were the authorised signatories of the bank accounts to issue cheques and help cash some of the cheques and handed the monies to Person C.

The cash withdrawals made by Person D were also handed to Person C. Person C would hand the monies to Person A or another member in the syndicate as directed by Person A. Person C

received part of the cash as commission to be shared with the nominee directors and Person D.

On several occasions, Person B was handed a portion of the withdrawn criminal proceeds by various members in the syndicate. Person B would place some of the cash in a safe located in their brother's flat. The safe was purchased by Person B under the instruction of Person A.

In late 2017, Person A, Person C, Person D and several nominee directors fled before the investigation commenced. Person C took cash with him and left the jurisdiction with Person D. Person D purchased jewellery using the criminal proceeds before he left the jurisdiction. While Person A was away, Person B used the criminal proceeds to purchase gold as directed by Person A. Further, to avoid detection, Person B told their brother to empty the contents of the safe and pass them to someone else for safekeeping, on Person A's instruction.

With the close cooperation and assistance of authorities in Jurisdiction's A, B and C, all absconded persons were arrested. The key operatives, Persons A, B, C and D were convicted for engaging in a conspiracy to cheat the government agency and various money laundering offences which included concealing, converting, transferring, acquiring benefits from criminal conduct and removing criminal proceeds from jurisdiction. They received sentences of between 80 months and 110 months for the money laundering offences.

Furthermore, the investigation revealed three Precious Stones and Precious Metals Dealers (PSMDs) sold gold and jewellery to Persons B and D. The purchases were mainly made in cash. The PSMDs failed to conduct the requisite customer due diligence and/or submit cash transaction reports for single cash transactions exceeding SGD20,000 and were prosecuted, receiving fines ranging from SGD9,000 to SGD40,000 (USD6,600 to USD29,000).

Source - Singapore

Case study # 91 - Use of money couriers by overseas-based drug syndicate

drug-related crime

Between January to May 2021, Singapore's Central Narcotics Bureau (CNB) investigated an overseas-based syndicate that was supplying heroin, cannabis and methamphetamine to local traffickers. This syndicate made use of legitimate vehicles ferrying goods to smuggle drugs into Singapore.

To mitigate risk and prevent a situation where the syndicate would lose both the drugs and proceeds of crime, this syndicate devised a multilayered network and made use of drug couriers and money couriers to deliver the drugs and collect the drug proceeds respectively.

Besides using local storekeepers to collect money from local drug clients and passing it back directly to the supplying syndicate members, the syndicate also made use of other money couriers to remit drug proceeds collected from his local drug runners. The remittance services were believed to be licensed moneychangers-cum-remittance service providers who were not involved with the drug trafficking activities, and unsuspectingly allowed their services to be used by drug traffickers.

Three of the storekeepers who assisted to pass money to the syndicate's money couriers or remit using remittance services have since been arrested and investigated concurrently under the *Misuse of Drug Act (MDA) and Corruption, Drug Trafficking, and other Serious Crimes (Confiscation of Benefits) Act (CDSA).*

Source - Singapore

2.16 Solomon Islands

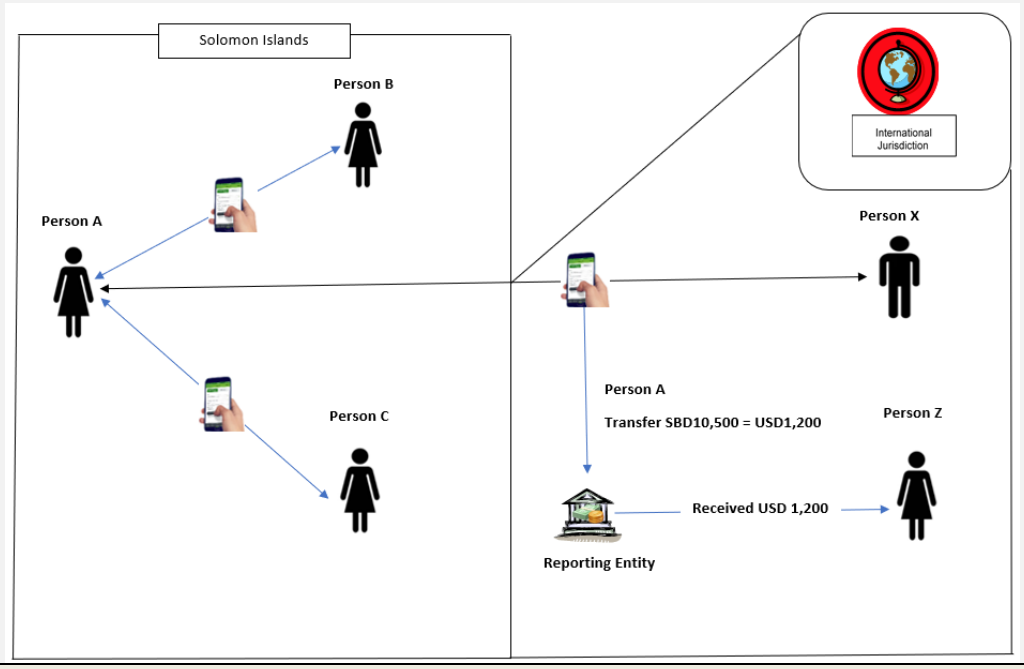
Case study # 92 – Package Fraud

fraud; identity theft

Between July and August 2022, Person A came across two individuals, Person B and Person C on Facebook, who both claimed to be residents of Solomon Islands. Person B introduced Person A online to an organisation responsible for helping disabled people throughout the world. Person B told Person A that if they were interested in joining the organisation, they would connect them to the bosses of the organisation, and register them to become a full-time member. Person A was then referred to Person C who claimed that their system showed Person A had won USD90,000.

Person A was required to pay SBD5000 (USD600) upfront in order for the winning prize to be released to them. Person A was instructed to pay this amount via FEDEX, and a package would be sent to them. Person A then had to liaise with Person X, who was assigned to deal with the prize. On 29th July 2022, Person A transferred the funds requested via a reporting entity, and on 1 August 2022, Person A received a further request from Person X for SBD5,000 (USD600) to enable the clearance of the package. Person A sent a total of SBD10,500 (USD1,200), however no package was received. Person X contacted Person A and demanded more payments for the purposes of shipping fees/charges. The issue was reported to a reporting entity that confirmed an initial analysis showing the transaction fits a profile of a possible consumer fraud. The reporting entity interdicted Person Z in Jurisdiction B from using its services.

Source – Solomon Islands



Case study # 93 – Fraud involving citizens sending their debit cards overseas

fraud; structuring; cash; suspicious transaction reporting; debit cards

A local bank account received large deposits and multiple mobile transfers from within the Solomon Islands (approximately SBD20,000 (USD2,400) over course of three months), which were followed by immediate cash withdrawals carried out from the Solomon Islands and jurisdiction B.

The Solomon Islands FIU received a suspicious transaction report from a reporting entity concerning several bank accounts that showed similar activity. Preliminary investigations carried out by the FIU revealed that local account owners are also sending their debit cards overseas to foreigners they met online, who promised them prosperous business opportunities. The large deposits and mobile transfers in the Solomon Islands are from various individuals who were scammed by the foreigners.

The scam targets the elderly populace via online platforms and social media and convinces them to send their visa debit cards to the perpetrators. The perpetrators also scam others via social media to deposit funds into accounts which they can access from their foreign jurisdictions.

The FIU is looking into the suspicious transaction reports and will be disseminating its reports to relevant law enforcement agencies. The investigation into the case remains ongoing.

Source – Solomon Islands

Case study # 94 – Tax Crime across jurisdictions–

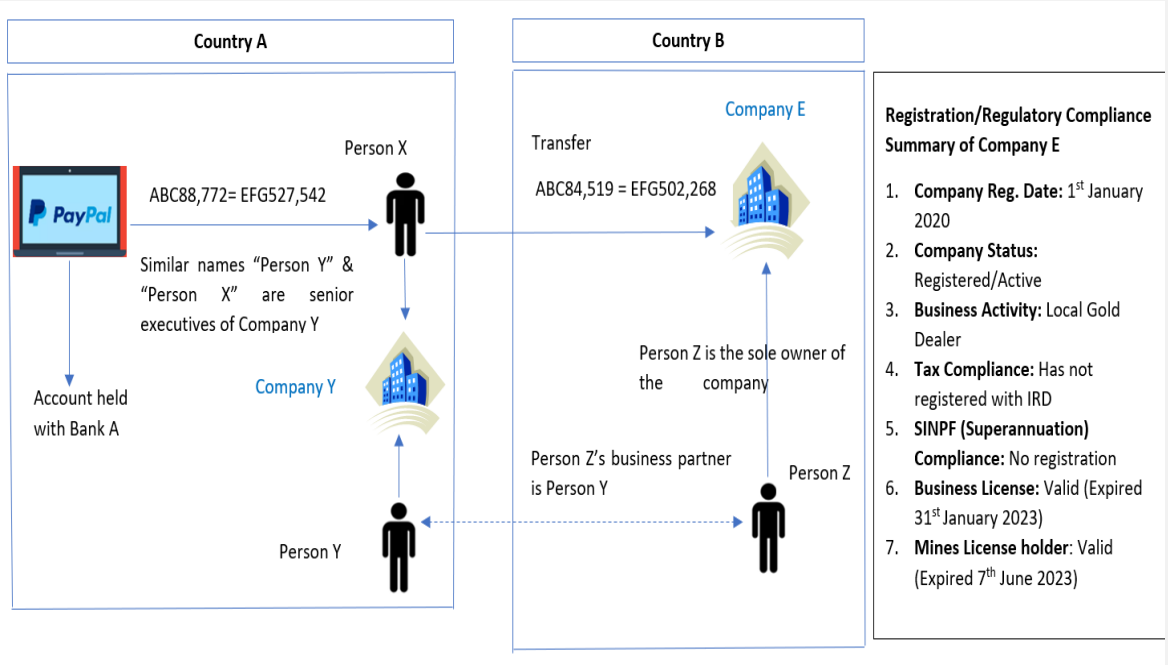
tax crime; abuse of legal persons and arrangements

The FIU received a suspicious transaction report from foreign Jurisdiction A concerning Person X (a Solomon Islands citizen residing in Jurisdiction A), who was sending multiple large amounts of funds from their personal account to Company E in the Solomon Islands, claiming to be for renovations to their home (approximately SBD502,268 (USD60,000)). The claimed purpose for the funds transfers does not match the reasons stated in the electronic transfer form, as Company E, the receiver of the funds, is a mineral extracting company (gold) owned by Person Z.

Further checks revealed Company E has a business agreement with Company Y in Jurisdiction A. Person X is a senior executive along with Person Y in Company Y. Multiple transactions with the same narratives (claims for home renovation) were being carried out between Person X and Company E. The funds transferred by Person X to Company E is for buying gold to export (as is stated in the agreement), and not for home renovation as it is claimed in the narrative for the funds transfers. It is suspected that this is a form of tax evasion relating to business income.

The FIU has disseminated the report to IRD for further investigations.

Source – Solomon Islands



2.17 Chinese Taipei

Case study # 95 - Virtual Pets Fraud

fraud; use of the internet

In 2020 the Criminal Investigation Bureau of Chinese Taipei received a report about a group of suspects setting up an app, and taking on the roles of platform manager, LINE investment chatroom moderator (LINE is an app for electronic communications), and event seminar hosts. The platform attracted members to join by advertising an investment of virtual pets. Members who purchased virtual pets were promised to receive an average daily profit of 2% of the value of the adopted (purchased) pets, and an additional profit of 5 to 10% of the value of the pets if they referred downline members to join the scheme.

Members were asked to link their own phone numbers to their personal bank accounts for trading virtual pets among members and purchasing virtual pets from the app platform, as well as for receiving and remitting funds. The group made a profit by sporadically posting new virtual pets on the trading platform and selling them to the members. The trading platform was closed without warning in April 2020, causing many members to lose their money.

After nearly a year of surveillance, it was discovered that the criminal group was led by Person A, who purchased the platform app from a foreign jurisdiction. Shareholders, Person B and others set up five LINE investment chatrooms and served as moderators. Other members of the group were responsible for responding to members' inquiries, organising investment promotion seminars and promoting investment speculation in the LINE investment chatroom group.

After the evidence collection was completed, two waves of arrests were conducted on 16 November 2021 and 23 February 2022. A total of 16 suspects were apprehended and their premises were searched. Upon further investigation, it was discovered that 56 victims were defrauded NTD 20 million (approx. USD620,000) during the period from the establishment of the investment platform in August 2019 to its sudden closure on 2 April 2020. The group used several bank accounts for receiving the funds from members, and some of the accounts were found to be dummy accounts.

Six of the 16 are being prosecuted for violating the Banking Act and are currently at trial. No assets have been seized.

Source – Chinese Taipei

Case study # 96 – Two jurisdictions Joint Collaboration to Break Counterfeit Card Syndicate Laundering Money by Stealing Points from Coffee Chain Stores

fraud; forgery; organised crime; use of the internet; credit cards/stored value cards

The Criminal Investigation Bureau (CIB) received a notification from Jurisdiction B's LEA regarding victims in Jurisdiction B receiving emails from a fake post office, claiming the delivery of a package had failed, and that pre-payment was required before the next delivery attempt. The victims clicked on the phishing link and followed the website's instructions to enter their credit card numbers and OTP passwords, then found that their credit cards were tied to "Apple Pay" and immediately afterwards, the credit cards were used to buy stored value points from a Chinese Taipei coffee chain.

A joint investigation between Chinese Taipei and Jurisdiction B assisted the prosecutor's office to commence an investigation into the case. The Prosecutor's office found that Person A recruited members and set up a phishing website to send emails or text messages to scam victims. Once the victims clicked on the link and entered their credit card/UnionPay card numbers and OTP passwords, the victims' credit card/UnionPay card information was stolen, and counterfeit cards were created.

The members of the criminal group would then bind the cards with mobile payment platforms such as "Apple Pay" and proceed to the physical stores of the coffee chain, where they would purchase stored value cards with the counterfeit credit card/UnionPay cards, and then sell the stored value cards to third parties at a discount in exchange for cash.

The scam group took advantage of the coffee chain's occasional promotions and racked up additional purchases with counterfeit cards. A total value of NTD1 million (USD31,000) was made in one week during the promotional period. The stored value cards were then sold at a discount downstream for profit. Because the points on the stored value cards were equivalent to cash, the method used was able to launder money across borders. Within a year, the criminal group made a profit of nearly NTD10 million (USD310,000), with victims spread throughout the world. On 29 March 2022, the police arrested five suspects, including the ringleader and seized card printing machines, blank chip cards, UnionPay cards and stored value cards. The suspects are being prosecuted however the ringleader absconded overseas.

Source – Chinese Taipei

Case study # 97 - Suspected Corruption by head of Local Government Agency

bribery and corruption; purchase of real estate; politically exposed person

Person A was the head of a local government agency and had been receiving income from bribes given to them from several companies over the years. Person A evaded investigation, prosecution and punishment by the judicial authorities of Jurisdiction A. In order to evade investigation, prosecution and punishment by the judicial authorities of Chinese Taipei, Person A Laundered the proceeds of this bribery and corruption by using bank accounts under the names of their relative of first-degree kinship and kept the passbooks and personal stamps of the accounts to deposit the funds from the bribes. Person A occasionally instructed government agency employees to use the borrowed accounts for depositing and withdrawing cash. The funds were also used to purchase land with friends, under the name of their relative.

Person A has been prosecuted for violating the Anti-Corruption Act and the Money Laundering Control Act, and is currently on trial. He received a total of about NTD 10 million (USD 310,000) in bribes.

Source – Chinese Taipei

Case study # 98 - Suspected Money Laundering

bribery and corruption; use of credit cards; cheques; cash; politically exposed person; structuring

Person A was the magistrate of County I. Since 2000, with the intent to conceal cash from unidentified sources and avoid confiscation, Person A proposed an arrangement with Person B, the director general of the Farmers' Association. The arrangement involved each of them issuing and exchanging bearer cheques of the same date and same value. When Person A received NTD 1 million (USD31,000) in cash, they would then issue a bearer cheque of NTD 1 million to Person B via their secretary Person C and Person B would in return issue a bearer cheque of the same amount with a maturity date of the next day to Person A.

Person A would then deposit the bearer cheque to accounts under the names of Person D and Person E, who were friends of Person A. The accounts remained under Person A's control and were used by Person A. When Person A's cheques expired, the cash value of NTD 1 million from unidentified sources would be cashed into Person B's account, and the same amount would be exchanged from the bearer cheques issued by Person B the next day. Person C used the passbooks and personal seals of Person D and Person E to withdraw the money from their accounts and gave it to Person A. Person A paid Persons D and E 1% to 3% of the amount of cash for borrowing the accounts. Person C used the passbooks, seals or stamped withdrawal slips to withdraw the money from these accounts over the counter of the financial institution, and the amount withdrawn each time would not exceed NTD 500,000 to avoid threshold currency transaction reports.

The withdrawn funds were given to the son of Person A, who rented a small suite to hide the money in a safe. By issuing cheques purportedly for loans and circulating the cash flow, an illusion was created that there would always be only NTD 259 remaining in the accounts. The above-mentioned approach of exchanging cheques, cashing by deduction, using bank accounts of others, over-the-counter cash withdrawals, and making and issuing cheques as evidence for creating new debts to repay the old ones created an illusion of repayment of loans, to prevent the cash from being seized.

Person A was charged with the crime of holding property of unidentified sources.

Source – Chinese Taipei

Case study # 99 - The Bribery Case of Mayor A

bribery and corruption; use of real estate; politically exposed person

In 2020, Person A, the mayor of Township S received bribes from Persons B, C and D during an employment recruitment and selection process. Person C gave Person A a bribe of NTD 600,000(USD18,600) through Person E, and Person C and Person D gave their bribes of NTD 450,000 (USD14,000) directly to Person A.

In order to conceal the origin of the funds, Person A used their mother's bank account and instructed their assistant at the mayor's office, Person F, to deposit and withdraw cash on their behalf. Between April and May 2021, Person A mixed the funds from bribes together with other funds, and made an investment in the name of their son by contributing NTD 1.9 million

(USD59,000) to a joint venture with a friend to purchase land with a value of NTD 5.7 million (USD177,000).

Person A was prosecuted in 2022, for violating the Anti-Corruption Act and Money Laundering Control Act. He handed over all the proceeds of crime to the prosecutor's office.

Source – Chinese Taipei

Case study # 100 - Investment Fraud and Violation of the Banking Act

fraud; purchase of real estate

Person A was the beneficial owner of Company A in foreign Jurisdiction B, claiming to have many years of experience in futures investment. From April 2013 to July 2021, Person A designed futures investment and overseas monetary fund investment plans, and recruited investors.

Person A and their accomplices promised to give the investors back their funds along with profits in an excessive amount, after managing futures investment on behalf of them for a certain period of time. In the investment contracts signed by Person A and the investors, the funds given to Person A were in the name of investment funds or borrowed money. Person A asked the investors to open a futures account with one of their accomplices who worked at a futures commission merchant.

After the accounts were opened, Person A then asked the investors to provide their online trading account passwords. However, only a small portion of the funds were used in futures investment. Person A withdrew most of the funds and used it to pay profits to the investor and continued to attract investors with fake overseas funds investments and overseas futures trading platform investment plans.

Person A deceived the investors into putting in more funds by suggesting the investment funds could be returned only if a certain amount of money were remitted to an overseas account. From 2013 to 2021, Mr. Person A defrauded a total of NTD 873,154,028 (approx. USD27million) from the investors.

In order to disguise and conceal the origin of the proceeds, Person A and their accomplices used the proceeds to buy real estate and life insurance policies. During the investigation, bank accounts, securities and real estate were seized. Person A and their accomplices are currently at trial, being prosecuted for violating the *Banking Act, Criminal Code, Futures Trading Act, Securities Investment Trust and Consulting Act, and Money Laundering Control Act.*

One real property, 27 bank accounts and four securities accounts have been confiscated, with the value of NTD 28.8 million in total.

Source – Chinese Taipei

Case study # 101 - Gambling and Money Laundering through Third-Party Payment Enterprises

gambling activities; new payment method; tax crime; use of the internet

In August 2018, Person A set up a company with accomplices and started an online gambling platform aiming for gamblers from foreign Jurisdiction A. A total of three server rooms were set up in Chinese Taipei. Person B was the manager of the server rooms and several customer service agents were hired. The gamblers would apply for an account, and login to the platform with their usernames and passwords. Gamblers could use Jurisdiction A currency to exchange gambling credits and use the credits to bet in electronic games and sports games such as soccer and basketball. If the gamblers won, the bets would be paid through third-party payment

enterprises in Jurisdiction A. The top-ups of gambling credits were also handled through third-party payment enterprises.

The money laundering scheme was managed by linking up the content management system of the gambling platform with the system of third-party payment enterprises. Gamblers could top up using convenience store payment, credit cards, and virtual accounts. The funds were first remitted to dummy accounts through third-party payment enterprises, and the customer service agents would use online banking to move the funds between several accounts, then eventually transfer the funds to the account of the company. When gamblers asked to change the gambling credits back to Jurisdiction A currency, it was done through third-party payment enterprises, and the funds were remitted to the gamblers account from the dummy accounts in Jurisdiction A by using online banking. The origin of the money from gambling was thus disguised and concealed.

Person A and their accomplices were charged with tax crime and money laundering. In exchange for probation, they returned the illicit proceeds of NTD 200 million (USD6.2 million), agreed to pay a fine of NTD 850 million (approx. USD26.4 million), and promised to donate NTD 10 million (approx. USD31,000) each year to the Association for Victims Support for two years.

Source – Chinese Taipei

Case study # 102 Platform G's Alleged Violation of the *Money Laundering Control Act*

fraud; use of the internet; use of virtual assets

A fraud ring used online social media to promote investment in virtual asset F coins, which were issued by Platform G. To attract investors, the value of F coin was claimed to increase steadily. The fraud ring fabricated false investment return data on its website and reached out to Internet users through communication software such as LINE. They first solicited small investments and made payments for returns to gain trust. They then persuaded investors to invest more money. However, Platform G informed investors in January 2020 that their accounts are blocked and suspended any withdrawals.

The fraud ring consisted of Person A and his accomplices. They provided all their financial account information to the fraud ring for receiving payment and transferring payments to victims' investment accounts, and served as the "money mules" for the ring. They then used their virtual asset wallets in multiple VASPs to buy Tether (USDT) and other cryptocurrencies, then transferred the cryptocurrencies to cold wallets controlled by unknown persons. They also used third-party payments to assist in the transfer of criminal proceeds. The total amount of criminal proceeds was NTD 111,291,972 (approx. USD3.45 million).

Source – Chinese Taipei

Case study # 103 Cryptocurrency heist

theft; use of virtual assets

The members of a criminal group applied for 4 accounts with a VASP, used the time difference loophole that cannot be updated in real time on the platform, and repeated the exchange, sale and withdrawal of cryptocurrencies. From the end of 2020 to January 2021, the group overtook 300,000 USDT and 217 ETH with a market value of more than NTD 25 million (approx. USD775,000), and then transferred the withdrawn cryptocurrencies to accounts of other VASPs to hide the proceeds of crime.

Source – Chinese Taipei

Case study # 104 - International cooperation on a cryptocurrency robbery case

theft; international cooperation

The Criminal Investigation Bureau (CIB) received reports from the LEAs in Jurisdiction A that suspect Person A (dual national) was involved in the robbery and theft of approximately USD3 million worth of various types of cryptocurrency from a victim on March 16, 2022. Courts of Jurisdiction A issued a warrant for person A's arrest on March 23rd.

After investigation, it was discovered that person A had entered Chinese Taipei before the warrant was issued. In order to investigate whether or not the suspect came to Chinese Taipei with the intent to conceal the illicit gains of the abovementioned robbery and whether the suspect had committed a crime in Chinese Taipei, Jurisdiction A and Chinese Taipei conducted a joint cooperation on criminal investigations.

Person A was a fugitive wanted by a Jurisdiction A court for involvement in a major criminal felony in Jurisdiction A and Jurisdiction A had cancelled his passport, so person A was not legally permitted to be in Chinese Taipei. Furthermore, he was involved in armed robbery, intimidation, kidnapping, illegal detention and other violent crimes in the Jurisdiction A, endangering Chinese Taipei's public safety and public order, thus he was actively pursued through multiple channels by CIB. On May 31, Person A was arrested with a detention warrant issued by the prosecutor, and on June 3, he was deported from Chinese Taipei under immigration law.

This case involved intelligence sharing and integration. In accordance with the Agreement on Mutual Legal Assistance in Criminal Matters signed by Chinese Taipei and Jurisdiction A Person A was successfully apprehended and extradited.

Source – Chinese Taipei

2.18 Thailand

Case study # 105 - Medical device, equipment, and rubber gloves Scam

fraud; standalone ML; wire transfer; purchase of valuable or cultural assets

AMLO, in cooperation with the Economic Crime Suppression Division of the Royal Thai Police investigated a fraud by Company A, who claimed to be a distributor of medical devices and equipment and rubber gloves under the trademark of Company M in Switzerland. Company A made a trade contract with Company B in the amount of USD2.6 million. On the due date, the goods were not delivered as agreed. The investigation concluded that the beneficial owners of Company A used the proceeds of the fraud to purchase assets. The assets including cars and bank accounts were temporarily seized and frozen by AMLO.

Source – Thailand

Case study # 106 - Terrorism Financing Through ATM Transaction

suspicious transaction reporting; terrorism financing; cash

According to a STR filed by bank B, Person A had been conducting transactions not in line with their expected income. Person A's expected monthly income was 8,000 baht however he conducted several transactions through an ATM totalling more than 600,000 baht (USD16,500) over a short period. AMLO investigated and found a link between Person A and several cases involving improvised explosive devices. As a result Person A was listed as a designated person. Person A's assets were frozen and he is currently a Person in a TF case.

Source – Thailand

Case study # 107 - Transnational Human trafficking

trafficking in human beings; cash; wire transfer

Thai police officers arrested Person A, who was subject of an Interpol red notice warrant. Person A was extradited to their home jurisdiction, Jurisdiction B. The court in Jurisdiction B later convicted Person A of human trafficking and migrant smuggling under their criminal law - Person A was threatening, procuring, and extorting foreign women for prostitution. The AMLO investigated and seized 21 assets owned by Person A and their associates valued at approximately THB23 million (USD632,000), consisting of cash and bank accounts. The confiscation case is currently subject of legal proceedings.

Source – Thailand

Case study # 108 - Public Fraud: the bargain travel packages.

fraud; racketeering; use of real estate; use of capital markets; financial institutions

A tour company advertised international travel packages at a low price on social media and several people purchased the packages. The customers were not able to travel on the packages purchased as the tour company claimed to have difficulties in visa issuance and financial liquidity, and refused to provide refunds.

AMLO's investigation into the case revealed the tour company conducted complex financial transactions through various other businesses and acquired assets worth THB 75 million (USD2 million) consisting of bank accounts, bank lottery, real estate, shares, warrants, and derivative warrants. AMLO seized and froze the assets and the case is currently subject of legal proceedings.

Source – Thailand

Case study # 109 - Illegal Online Casino Case

gambling activities; use of virtual assets; purchase of valuable or cultural assets

Person A was investigated by the Thai Police, and it was found that Person A owned an online gambling website. AMLO initiated a financial investigation for illegal gambling, which resulted in various assets including four super cars, a luxury car, bank accounts and VA trading accounts being seized and frozen. It is estimated the total value from the proceeds of crime was over THB200 million (USD5.5 million). The case is currently subject of legal proceedings.

Source – Thailand

Case study # 110 – Financing improvised explosive devices

terrorism financing; suspicious transaction reporting

According to a STR filed by bank B that Mr. A had been conducting transaction not in line with expected income in particular Mr. A expected monthly income was 8,000 baht while he conducted several transactions through ATM over 600,000 in total over a short period, AMLO then investigated and found the link between Mr. A and several cases involving improvised explosive devices (IED) and finally listed him as a designated person. His assets were frozen and currently a subject in a TF case.

Source – Thailand

Case study # 111 The cryptocurrency wizard

fraud; use of virtual assets

Person A, a self-acclaimed "cryptocurrency wizard", deceived numerous victims into investing in a Bitcoin portfolio while using Facebook and streaming games. Person A claimed that investors would receive high returns of around 30 percent on their investment and posted pictures of money transfers. Victims received returns initially, but then Person A claimed that the bank had a problem with money transfers so the returns might be delayed and then Person A closed his Facebook account and his portfolio. Victims claim to have lost around 22 billion baht (approx. USD 643,881,741) to the scheme and filed complaints with the Royal Thai Police. Person A was arrested in January 2019.

Source – Thailand

3 MONEY LAUNDERING & TERRORISM FINANCING TRENDS

This section of the Typologies Report includes information from Members about research and studies being undertaken in part 3.1, members' reports about any ML and TF trends observed over the 2022-2023 period in part 3.2 and their observations about the effectiveness of anti-money laundering and counter financing of terrorism measures in part 3.3.

3.1 Recent research or studies on ML/TF methods and trends

3.1.1 Hong Kong, China

The 2nd Hong Kong Money Laundering and Terrorist Financing Risk Assessment was conducted and its report published in July 2022. The report contains the assessment of ML/TF trends taking into account updated statistics between 2016 and 2020.
(https://www.fstb.gov.hk/fsb/aml/en/risk-assessment.htm)

The Financial Intelligence and Investigation Bureau of Hong Kong Police Force is currently conducting strategic analyses on ML trends relating to Shell and Shelf Companies and Unlicensed Money Services Operators.

3.1.2 Japan

Japan's National Risk Assessment-Follow up Report 2022 was published on 1 Dec 2022. English version is expected to be published shortly.

Japanese Website:
https://www.npa.go.jp/sosikihanzai/jafic/nenzihokoku/nenzihokoku.htm

English Website:
https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/nenzihokoku_e.htm

3.1.3 Lao People's Democratic Republic

Lao PDR reviewed its National Risk Assessment in 2022. The review noted the following prevalent trends: fraud, drugs, falsifying documents or the use of fake documents, theft, producing or using counterfeit currency, producing or using counterfeit cheques or other currencies illegally, and environmental crime.

3.1.4 Macao, China

During the period from January to December 2022, a total of 2,199 STRs were received by the Financial Intelligence Office of Macao (GIF), with 1,177 STRs from the gaming sector, 765 STRs from the financial sector (including banking, insurance and financial intermediaries) and 257 STRs from other sectors.

During the same period, 162 STRs were disseminated to the Public Prosecutions Office for further investigation by Law Enforcement Agencies. These cases were mainly related to crime syndicates and fraud.

Common Money Laundering and Terrorism Financing trends detected from Macao, China's STRs were:

- Irregular large cash withdrawals;

- Significant cash deposits with non-verifiable source of funds;
- Use of ATM, phone banking, cash deposit machines;
- Use of cheques/account transfer etc. to transfer funds;
- Chips conversion with minimal or no gambling activities;
- Suspicious wire transfers;
- Use of online banking/internet;
- Possible match with screening system watch-list or other black list;
- Suspected to be engaged in illegal financial activities.

3.1.5 **Malaysia**

Labuan Risk Assessment

The Labuan Financial Services Authority (LFSA) of Malaysia has taken a number of measures to identify and assess its money laundering and terrorism financing threats, by conducting a risk assessment of the entities in the offshore financial centre.

The Labuan Risk Assessment (LRA) which was conducted in 2021 and completed in 2022 aims to:

- Identify general and specific risks to further improve financial crime risk management
- Determine level of effectiveness of control measures
- Establish the residual risks of the sector
- Provide guidance and apply appropriate strategies and measures to address key risks identified and improve policy documents.

The risk assessment covered:

- Assessment of the vulnerabilities and threats in determining the sector's inherent risk
- Licensed and Non-Licensed Entities

Based on the assessment's outcome, the Labuan sector was rated as a low-risk sector attributed to its enhanced internal controls by Labuan reporting institutions and intensified supervisory activities. It was recommended that financial technology (fintech) be adopted to optimize supervisory actions and manage key risks and improve stakeholder engagement and improve the reporting institutions' capabilities. The report was endorsed by the National Coordination Committee to Counter Money Laundering (NCC) in April 2022 and shared with relevant stakeholders including the NCC members and reporting institutions in Labuan.

Advisory

Bank Negara Malaysia (BNM) continued to produce an advisory in 2022 for selected reporting institutions on cybercrime, in particular on ransomware and fraud, ML/TF trends and red flags to assist them in the detection and submission of suspicious transactions reports. The advisory serves as a response to the evolving modus operandi on cyber-related extortion in both the domestic and international landscape.

3.1.6 **Philippines**

Philippines - Money Mules Typologies Brief
http://www.amlc.gov.ph/images/PDFs/PR2023/2022%20DEC%20TYPOLOGIES%20BRIEF%20MONEY%20MULES_For%20Publication.pdf
This study was derived from a total of 821,979 money mule related suspicious transaction reports (STRs) received by the AMLC between the first quarters of 2016 and 2022. The STRs had an

aggregate value of PHP510.17 billion. As observed in this report, the suspected money mules are involved in the following activities:

- **Transactions Made Using Self-Service Kiosks:** Between 1 February 2019 and 4 September 2020, a total of 91,726 STRs with an aggregate value of PHP593.96 million (USD10.74 million) were filed by covered person PQR on 2,508 individuals, whose accounts showed unusual inflow and outflow transactions completed using self-service kiosks found in a convenience store chain. The rapid movement of funds through a digital payment platform (inflows) and an online transfer facility (outflows) suggests that the accounts involved are possibly used as pass- through accounts.

- **Transactions by Individuals with Sequential MINs (mobile identification numbers):** Covered person PQR flagged 308 individual clients who are involved in multiple fund transfers that amounted to PHP63.195 million (USD1.1 million) in less than seven months. These transactions were made in favor of Person A, who has an account with another domestic bank. PQR found that majority of the subject clients had opened their accounts between November 2019 and March 2020. The subject clients as well as their counterparties, who enrolled in succession under sequential mobile identification numbers (MINs) and used the same background in their know-your-customer videos, thereby giving rise to the hypothesis that they opened their accounts from only one location.

- **Successive Deposits and Withdrawals –** see case study #63 in section 2 of this report**.**

- **Cash smuggling –** see case study #67 and 69 in section 2 of this report**.**

Section 3 of this report analyses STR filings related to money mules and found an increasing trend leading to the year 2022. An influx of STRs was observed in 2021, possibly due to the accelerated adoption of digital banking and electronic wallets in the midst and in the wake of the COVID-19 pandemic.

A significant share of the sample STRs were filed on the basis of two suspicious circumstances, namely 'no underlying legal or trade obligation, purpose, or economic justification' and 'the amount involved is not commensurate with the business or financial capacity of the client'. In terms of the value of transactions involved, the suspicious circumstance most reported was – 'the client is not properly identified'. The top predicate crime in terms of both volume and value appeared to be swindling.

It was noted that the suspected money mules in the Philippines utilize three modes of withdrawing funds: electronic cash cards, automated teller machines, and over the counter. Further, the majority of the suspected money mules were found to be residing in Metro Manila, Rizal, Nueva Ecija, Cavite, Bulacan, and Laguna.

Aggregated data from FX declaration forms reveal three Filipinos as among the top carriers of foreign currencies to and from the Philippines over the period 2015 Q1 to 2021 Q3. Based on open-source information, said carriers, all surnamed PQR, are part of a suspected syndicate for allegedly sneaking foreign currencies into the jurisdiction from September 2019 to March 2020. The "PQR group" was the subject of a legislative committee hearing in 2020, where it was disclosed that the undeclared cash that had entered the jurisdiction through said group from September to March 2020 alone reached USD633 million or PHP32 billion.

Case study # 112 – Money mules

cash; terrorism financing

The AMLC database captured 168 inbound and 4 outbound transactions associated with members of the PQR group. These inbound and outbound transactions amounted to USD124.3 million and USD1.1 million, respectively. Based on the available dataset, it was noted that the members of the PQR group frequently travelled from either jurisdiction A or B to the Philippines between September 2019 and March 2020. Confidential information links some members of the PQR group to Person A, a national of jurisdiction C and owner of EFX. EFX is a foreign exchange dealer based in Makati City and allegedly involved in funding the Islamic State-linked Maute Group, who was behind the Marawi City siege in 2017.

Given this context, it is possible that the money brought into the Philippines by the PQR group will be channelled to finance terrorism and/or other unlawful activities. Nonetheless, considering the nature of JKI's foreign exchange business, one can also surmise that the questioned transactions merely form part of the normal course of operations of EFX. This hypothesis can be substantiated by intelligence information gathered on the business model of EFX, which suggests that EFX sources its inventory of foreign exchange directly from ABC (a jurisdiction A -based company) and DEF (a jurisdiction B based company) through its liaison staff. Reasons cited for opting to source US dollars from foreign entities via physical transfer of cash are preferable rates (ABC and DEF offer the lowest USD selling rates to EFX); minimal documentary requirements (purchasing from ABC and DEF requires less documentation compared to banks); and availability of funds (US dollars bought from ABC and DEF are readily available for use the following day).

Investigations conducted by the AMLC on the PQR group established that PQR-4 and PQR-2 had been transporting foreign currencies in large volumes, upon the request of person A, who happened to be the business partner of PQR-4. Observations during an interview with PQR-4 and PQR-2 lend support to the allegation that both had tried to conceal the true value of foreign currencies in their suitcase during their trip on 25 September 2019.

On 26 September 2019, PQR-6 arrived at Ninoy Aquino International Airport Terminal II in Pasay City and failed to declare USD700,000 currency notes in writing and to furnish information on the source and purpose of the transport of such currency. Information gathered on PQR-6 shows that he had been a member of an foreign multi-level marketing company, through which he was able to save up and build his business GHI in 2019, in partnership with PQR-4 and JKI. GHI is a Securities and Exchange Commission (SEC)-registered company that is engaged in the business of operating and distributing therapeutic devices for treating neurological and neuromuscular diseases. In 2021, PQR-6 ventured again into another business, JKL, an SEC-registered company that is engaged in the wholesale of protective motorcycle gears and equipment and motorcycle repair services. PQR6's largest transactions in the AMLC database were three check deposits on 12 July 2021 with a combined amount of PHP4.4 million.

Source – Philippines

Philippines - Animal smuggling

Philippines

Case study # 113 Animal smuggling

environmental crime

Bank MNO client B, is a student with a declared income of PHP1,000, and is the grandchild of Person A. Client B was born in 2006. Person A is the business owner of ABC Pet Supply with a monthly income of PHP50,000 (USD 880). Open-source information reveals that Person A has been repeatedly arrested and charged with violations of RA 9147 or the Wildlife Resources Conservation and Protection Act, by the Department of Environment and Natural Resources and agents from the National Bureau of Investigation and the Philippine National Police.

Client B was suspected of being a money mule due to large turnover of funds seen in their account. According to Bank MNO, Client B opened a savings account on 12 December 2017 with a starting balance of PHP1,983,088.89 (USD35,000). From this amount, a total of PHP1,508,088.88 was transferred to a time deposit account, which recorded no prior movements. Client B also had an active joint account with Person A.

It was noted that the flow of funds to and from Client B's savings account was not commensurate with their profile. Credit transactions ranged from PHP10,000 to PHP620,000, while her debit transactions ranged from PHP10,000 to PHP1,070,000. Given that client B was only 13 years old at the time of the STRs, the covered person inferred that the bulk of the incoming and outgoing transactions in Client B's accounts possibly represented the payment/proceeds from the illegal activities of her grandfather.

Source – Philippines

Philippines - Accounts used in the Dark Web

Based on the sample dataset, a total of 24 distinct bank accounts belonging to 19 individuals were reportedly sold on the "dark web" as drop accounts.

According to the bank's report, the subject accounts were likely utilized by fraudsters as drop accounts to receive payments for stolen credentials and other sold items. There is also a possibility that mules use said bank accounts to receive from proceeds of account hackers' fraudulent transfers that are subsequently cashed out through either ATM withdrawals or remittance agents.

There were no notable similarities observed among the accountholders, in terms of age, sex, source of funds, or declared monthly income. In terms of location, many of them declared one of two locations as their mailing addresses. Meanwhile, 47.36% of them are employed with monthly incomes ranging from PHP10,000 to PHP50,000 (USD176 to 881); 21.05% are self-employed with monthly incomes ranging from PHP10,000 to PHP250,000 (USD176 to 4,406); and 26.32% are unemployed with declared allowances as source of funds, ranging from PHP999 to PHP30,000.

One of the reporting covered persons narrated that one bank account recorded total inflows amounting to PHP1.07 million, which consisted of online payments, inward remittances, and cash deposits. These funds, however, were also immediately withdrawn via ATM. It is worth noting that these transactions were not aligned with the accountholder's declared purpose for opening their account, i.e., for personal savings.

- ***Modus Operandi of Jurisdiction X Citizen Fraudsters.***
- ***Romance Scam***.
- ***Flipping of funds***.

See case studies in section 2 of this report.

Philippines - Environmental Scanning: Cybercrime Threats and Perpetrators

http://www.amlc.gov.ph/images/PDFs/2022%20SEP%20CYBERCRIME%20THREATS%20&%20PERPETRATORS.pdf

This study was based on 30,967 STRs with transaction value of PHP3,261.1 million filed by various covered persons (CPs) in relation to Citizen-related crimes from one jurisdiction in the African continent, between 1 January 2009 and 31 December 2021. According to this report, the alleged perpetrators engaged in the following activities:

- Possible pass-through accounts
- Alleged association with bank hacking incident
- Recruitment of money mules
- Package scam

See case studies in section 2 of this report.

Environmental scanning using past studies as well as more recent reports revealed that cybercrime by citizens of one jurisdiction in the African continent are of increasing prevalence. This was evidenced by the volume and value of suspicious transaction reports (STRs) from year 2009. The year 2020 saw a considerable increase of around 668.2% to 17,178 STRs from the previous year's 2,236. In terms of gross amount, the pandemic period revealed a 261.1% increase to PHP998.6 million of the total transactions from 2019's PHP276.6 million. Conversely, there was a tapering on both counts in year 2021.

Submitted STRs were grouped based on the CP's reason for filing the report – either through suspicious circumstances (SC) or predicate crimes (PC). Notably, in line with the increasing link to digitalization and cybercrimes, violations of the *Electronic Commerce Act of 2000* dominated both volume and value at 7,573 (24.5%) and PHP623.4 million (19.1%).

Further, this study identified typologies based on the significance of the amounts involved and/or frequency of reports on the suspicious activity/scheme as well as the significance of the crime involved. These included inconsistent transactional activities with the subject's business profile; package, romance, and lottery scams with pass-through accounts; deposits from unverified sources; involvement in illegal drugs as well as African drug syndicates; association with bank hacking incidents; and recruitment of money mules.

Philippines - Phishing/Hacking Typologies Brief

http://www.amlc.gov.ph/images/PDFs/2022%20OCT%20TYPOLOGIES%20BRIEF%20PHISHING%20HACKING.pdf

This study covers 50,521 suspicious transaction reports (STRs) filed by covered persons (CPs) from the year 2011 to February 2022. The following are the activities that entail phishing/hacking:

- Account holders receiving calls from people pretending to be employees of banks to gather information (examples of vishing)
- Disclosing information to a third party via call (another example of vishing)
- International inward remittances received on behalf of a person by a group of people possibly related to each other
- Client's withdrawal in cash, leaving no audit trail
- Suspicious Indicators: Not commensurate with the financial capacity of the client
- Suspicious Indicator: No underlying legal or trade obligation, purpose, or economic justification
- Account takeover, involving electronic money issuer (EMI) wallets
- Business e-mail compromise
- Internet e-mail hacking (another case of business e-mail compromise)
- Hacking of user account in social media platform

See case studies in section 2 of this report.

The STRs involving phishing/hacking showed a generally increasing trend, except for the year 2020 when a slight drop in STRs was noted. The majority of the STRs filed are for the following reasons: swindling (65%) and violations of the *Electronic Commerce Act of 2000* (23%). Other suspicious indicators, such as the amount involved is not commensurate with the business or financial capacity of the client, are also among the reasons used by CPs. Of the common transactions observed, the majority are inter-account transfers, electronic cash card loading, credit card purchases, and electronic cash card withdrawal.

It should also be noted that majority of the STRs or 99.73% are domestic transactions, while only 0.27% are international remittance transactions. The majority or 50.45% of the total domestic transactions are reported from the National Capital Region, CALABARZON, Central Luzon, Central Visayas, Ilocos Region, Davao Region, and Western Visayas, while 44.62% of the transactions' locations are unknown or cannot be determined based on available data. For international remittances, 27.21% of the transactions were from or sent to one large jurisdiction with historical connections to the Philippines.

Philippines - A Detailed Analysis of Suspicious Transaction Reports Captured in the AMLC's Year 2020 Internet-Based Casino Sector Risk Assessment[21]

This report supplements the AMLC's Internet-Based Casino Sector (IBCS) Risk Assessment (RA) released in 2020 that highlighted the ML typologies and suspicious indicators derived primarily from STRs involving the sector. The IBCS-related STR dataset comprises 1,031 STRs estimated at PHP14.01 billion (USD246 million) filed by various reporting entities between 14 June 2013 and 28 October 2019. The following typologies were gathered from the STRs filed by various CPs and requests for information included in the published IBCS-RA:

- Violations of The Electronic Commerce Act of 2000 by a Money Service Business
- No underlying legal or trade obligation, purpose, or economic justification
- Deviation from the client's profile/past transactions
- Amount involved is not commensurate with the business or financial capacity of the client
- Client is not properly identified

[21] http://www.amlc.gov.ph/images/PDFs/PR2022/ANALYSIS%20OF%20STRS%20CAPTURED%20IN%202020%20INTERNET-BASED%20CASINO%20SECTOR%20RISK%20ASSESSMENT.pdf

- Fraud (swindling)

See case studies in section 2 of this report.

Year-on-year assessment of IBCS-related STRs from 2013 to 2019 showed a sporadic trend, which peaked in 2016, with 332 STRs involving transactions amounting to PHP8.8 billion. The upward trend was observed between 2013 and 2016 followed by a relative decline beginning 2017 until 2019. The majority of the STRs filed in terms of volume are based on the suspicious circumstance of 'no underlying legal or trade obligation, purpose, or economic justification', accounting for 565 or 55% of the total STR dataset. In terms of PHP value, violations of the *Electronic Commerce Act of 2000* dominated at PHP4.94 billion, which accounts for 35% of the total PHP value of the STRs used in the study.

The assessment likewise showed that nearly all IBCS categories (i.e., IGL, IGSSP, POGO, and SP) have exposure to possible suspicious activities with the majority involving the SP category. The majority of the observed transactions are domestic in nature, largely involving cash deposits/withdrawals, cheque deposits, and incoming/outgoing remittances. This raises a significant concern, as the statistics on cash deposits and withdrawals are consistent with the inherent risk of cash transactions for ML purposes as transacting in cash tends to obscure the audit trail. In addition, considering the nature of business of the IBCS, that is, the use of online technology for its platform, the substantial flow of cash is a likely deviation from its business model.

The geographical location of the identified entities is concentrated in the cities of Manila and Makati, and the province of Cagayan, collectively with 903 STRs with transactions valued at PHP12.0 billion, or equivalent to 87.58% and 86.0% of the total volume and peso value, respectively, of the STRs used in the study. In addition, STRs were also filed on IBCS entities located entirely offshore, and foreign entities having both international and domestic addresses.

Philippines - An Analysis of the Usefulness of Foreign Currency Declaration in Detecting Possible Cross-Border Transportation of Illicit Funds[22]

This study presents the results of the first and second components of the AMLC's three-part study on foreign exchange declarations received by the AMLC for the period between the first quarters of 2015 and 2021. The AMLC received a total of 7,619 written foreign exchange declarations, which comprised 5,059 submissions from individual passengers and 2,560 from corporate passengers. According to this report, identified suspicious activities which may possibly be related to ML/TF are as follows:

Philippines - Casino-Related Transactions

Data collected on individual carriers shows that a substantial amount of foreign currencies physically transported to and from the Philippines is going to or coming from the casino sector. This is based on the transactions of the top four carriers, ranked according to the USD-equivalent values of foreign currencies declared in the foreign exchange declaration forms gathered during the observation period.

The top four individual carriers came from foreign jurisdictions. Discrepancies in the amount of foreign currencies bought by the foreign carriers onshore and the total value of foreign

[22]http://www.amlc.gov.ph/images/PDFs/USEFULNESS%20OF%20FX%20DECLARATIONS%20IN%20DETECTING%20POSSIBLE%20CROS S-BORDER%20TRANSPORT%20OF%20ILLICIT%20FUNDS.pdf

currencies they carried outbound raises the possibility of bulk-cash smuggling, especially since the amounts involved are not trivial.

Philippines - Unusually Frequent Trips

Five individuals were identified through their cross border declarations on a total of 38 inbound trips from December 2019 to March 2020 and their disclosures stated that the funds were for casino gambling. In a span of about four months, approximately USD60.9 million was brought into the Philippines by these five carriers – see case study #78 in section 2 of this report.

Philippines - Inconsistent Disclosures

The dataset revealed significant inconsistencies in information submitted by one of the top Filipino carriers of foreign currencies for the period 2015 to 2021. The most obvious inconsistency was in the spelling of the carrier's name but also his date of birth, address and passport numbers.

Another suspicious pattern of transactions was identified from the transactions of individual travellers bound for the Jurisdiction A for religious pilgrimages. This pertains to two groups of 10 residents who travelled to Jurisdiction A on two separate dates in 2015. Based on data submitted by them, the travellers carried a total of SAR3.9 million and KWD500,000 in both trips. Financial investigation showed that some of the persons had received successive deposits to an account at Bank ABC which they withdrew the same day. Some of the FX declarations stated larger sums than were withdrawn by the persons.

3.1.7 **Thailand**

AMLO published its NRA on August 2022 on its official website. The NRA can be found at: https://www.amlo.go.th/amlo-intranet/media/k2/attachments/NRAYThailandYforYPublicationYEnglish_6112.pdf

AMLO conducted and distributed reports and typologies on ML/TF methods and trends to public and private sectors as follows;

- Case Study: Money Laundering in Baan Eua Arthorn (public housing) Project Fraud Case.
- Typology Report: Laundering of Transnational Wildlife Trafficking Proceeds.
- Case Study: Money Laundering in Railway Club Savings Cooperatives Fraud Case.
- Case Study: Money Laundering in Mae Manee Ponzi Scheme (public fraud) Case.
- Typology Report: Laundering of Public Fraud Proceeds through Tour Guide Businesses.
- Case Study: Dietary Supplement Products and Package Tour Scam

3.2 Observations on emerging trends; declining trends; continuing trends

3.2.1 **China**

China has reported that cyber-enabled crimes including telecommunication fraud has become increasingly and the ML methods used in connection with these crimes feature transnational and organized crime transactions.

Online gambling has become the main form of organized gambling crimes, with a whole chain of advertising, organizing, gaming and settlement.

Underground banks (Hawala) continue to facilitate the laundering proceeds of various other crimes such as telecommunication fraud, online gambling, and corruption.

3.2.2 **Cook Islands**

The Cook Islands reported the following emerging trends: Cyber enabled financial crime; Online gambling; Fraud (Unauthorized access to accounts); Official Corruption and Facebook Scams. Continuing trends include Scam emails and Investment scams.

3.2.3 **Hong Kong, China**

Hong Kong, China reported the following emerging trends:
Predicate offences involving the use of the internet, email, and social media are increasingly common due to the advancement of technology, the prevalence of electronic financial services, and social distancing measures arising from the COVID-19 pandemic.

It is observed that the misuse of stored value facilities ("SVFs") is an increasing trend:

- Criminals used misappropriated identity cards to set up SVF accounts for transferring proceeds.
- SVFs are sometimes exploited by bookmaking syndicates for receiving betting money from gamblers.

The first virtual bank in Hong Kong, China was launched in March 2020. To date, there are eight licensed virtual banks in Hong Kong, China, providing retail banking services through the internet or other forms of electronic channels. The bloom of the remote onboarding processes has led to an increase in involvement of virtual bank accounts in criminal activities:

- Criminals recruited money mules to set up virtual bank accounts.
- In some cases, ML syndicates/money mules used fake identity documents for authentication.

Hong Kong, China reported the following continuing trends:
Fraud-related crime continued to be most common type of offending, followed by drug-related offences. Other predicate offences in Hong Kong, China, including foreign tax and foreign corruption, has remained stable.

The Banking sector continues to be the most popular conduit of money laundering activities.

The use of third parties to launder proceeds continued to be prevalent:

- ML syndicates recruited non-residents, students and low-paid stooges to open bank accounts for a small monetary reward.
- In some cases, the recruitment of stooges was found to be an employment fraud.
- In recent cases, domestic helpers were recruited as stooges.

Declining Trends:

The significant reduction in cross-boundary travelers during the COVID-19 pandemic led to a drop in cross-boundary cash transportation.

3.2.4 **Indonesia**

Risk Assessment on Cyber Fraud

Indonesia published a Sectoral Risk Assessment of Money Laundering on Cyber Fraud Crime on June 2022. The risk assessment identified the cyber fraud types/characteristics involved business email compromise and investment fraud carried out by individuals and companies in the private sector. Social engineers were identified as high-risk perpetrators.

Typologies associated with cyber fraud included:

- The use of forged identity documents.
- The creation of new accounts to receive proceeds of crime.
- The use of nominee accounts: belonging to other persons (both known/unknown/fictional).
- Transactional patterns using cash.
- The use of Company or individual names to receive remittances with the appearance of business transactions

Risk Assessment of Terrorism Financing by Indonesian Foreign Terrorist Fighters (FTF)

Indonesia published a Risk Assessment in relation to FTF in 2021. Based on the results of the analysis it was concluded that:

- Fundraising Modes include collecting funds from other people, self-funding from asset sales e.g. houses, cars and funding through social media.
- Fund Transfer Modes include cash-carrying, use of non-bank licensed fund transfer provider (PTD) services, domestic cash withdrawals and use of banking services.
- Fund Use Modes demonstrate that funds are used by third parties or individuals/members of family to facilitate travel.

Updated Risk Assessment on Corruption

Indonesia updated its Sectoral Risk Assessment (SRA) on Corruption in 2022. The previous SRA on Corruption was undertaken in 2017. Based on the analysis of the threat, vulnerability, and consequence factors for each point of concern, the following results were obtained:

- State Finances are vulnerable to a high-risk of Corruption.
- Profiles of individual perpetrators with a high risk of committing money laundering offences through corruption are civil servants (including retirees), private employees, entrepreneurs/businessmen, and Officials of the Legislative and Government Institutions.
- Profiles of business entities with a high risk of committing money laundering offenses from corruption crime, were companies in the form of limited liability companies (PT).
- Banks were identified as being at high risk of exploitation by the perpetrators for money laundering proceeds from Corruption crime.
- The infrastructure sector has a high risk of money laundering offenses on corruption crime.
- The transaction pattern of the perpetrators, namely book-entry, purchase/investment products and transfers via mobile banking, constitute high risk category as a means of laundering money from Corruption crime;
- Corporate utilization (legal person); use of nominees (borrowed names), trusts, family members or third parties; property/real estate including the role of a property agent; and mingling (incorporating illicit money in legal business) are categories of laundering typology being used by Corruption perpetrators.

Updated Risk Assessment on Taxation

Indonesia updated its SRA on Taxation in 2022 (previous SRA dated 2017). Common ML typologies identified through the Tax system include: Self-laundering conventionally with domestic sources; placing assets in banking; purchasing property; purchasing vehicles via leasing arrangements; placing business capital.

The continuing risks of Money Laundering via Tax Crimes are:
- misuse of TBTS / Tax invoices.
- False Annual Tax Returns.
- Non-deposit collection.

Risk Assessment on Cross Border Cash Carrying

Indonesia published a Risk Assessment of Money Laundering and Terrorism Financing through Cross Border Cash Carrying in July 2022. The risk assessment is carried out based on an analysis of the currency point of concern, means of transportation, countries of origin and destination for carrying cash, profiles of cash carriers, and the office supervising cross-border cash carrying.

Based on the analysis of the threat, vulnerability, and consequence factors for each Point of Concern, the results of the study were:
- The Singaporean dollar and the United States dollar are currencies with a high risk of cross-border cash carrying, while the United Arab Emirates dirham is a medium risk.
- Air transportation has a high risk of cash carrying across borders.
- The risk assessment identified jurisdictions that were high or medium risk as origin or destination for cross-border cash carrying.
- Money Changer corporations and employees are common profiles of high-risk cross-border cash carriers, while employees of private traders, entrepreneurs/entrepreneurs, and bank corporations are profiles of medium-risk cross-border cash carriers.
- Soekarno-Hatta International Airport, the ferry port in Batam and I Gusti Ngurah Rai International Airport are areas of high risk of cross-border cash carrying.

Updating the Risk Assessment of NPOs being misused as a means of Financing Terrorism

Indonesia updated its risk assessment of Non-Profit Organization in July 2022. The previous risk assessment was undertaken in 2019. There are several dynamics and challenges in the prevention and eradication of TF through NPOs in Indonesia, including:
- An increasing number of NPOs have legal entities attached to them.
- The misuse of NPOs has increased both internally and externally.
- The rise of fundraising activities by NPOs on social media and the difficulty of ascertaining the existence of these NPOs based on the area where they are operating.
- The low accountability of financial management of the NPO, including public funds managed by NPO.

3.2.5 **Japan**

Japan has identified many cases where those who plan to conduct money laundering have the victims make payment to bank accounts in the name of fictitious or other parties through domestic exchange transactions which enables prompt and secure funds transfers.

Major Transactions, etc. Misused for Money Laundering

Year \ Misused transactions	Domestic exchange transactions	Cash transactions	Deposit transactions	Credit card	Electronic money	Legal persons	Crypto-assets	International transactions (such as foreign exchanges)	Funds transfer services	Precious metals and stones	Postal receiving service	Legal/accounting professionals	Foreign Currency Exchanges	Financial Instruments	Total (Number of cases)
2019	160	61	31	15	12	14	2	14	6	3	3	1	0	0	322
2020	110	120	96	20	12	14	32	16	1	2	0	1	1	0	425
2021	208	72	40	40	23	16	9	9	9	2	0	1	1	2	432
Total (Number of cases)	478	253	167	75	47	44	43	39	16	7	3	3	2	2	1,179

Cleared cases of Money Laundering under the Anti-Drug Special Provisions Law

The total number of cleared cases of money laundering under the *Anti-Drug Special Provisions Law* in 2021 was 9. In some cases, funds acquired through drug offences, such as the smuggling of stimulants, are laundered. In these cases, offenders make customers deposit the payments for illegal drugs into a bank account in the name of another party.

3.2.6 **Lao People's Democratic Republic**

In 2022, the Lao People's Democratic Republic noted the following continuing trends received from reporting entities as STRs as follows:

- Use of personal account to conduct business.
- Conduct of high value transactions without sufficient reason.
- No provision or avoiding provision of sufficient information**.**

3.2.7 **Macao, China**

Money laundering and terrorism financing trends observed from law enforcement agencies:

Money Laundering Trend

- In 2022 a decrease in gaming-related crimes was observed, mainly due to the decrease in tourists and gaming activities.
- The Judiciary Police (PJ) are paying close attention to the reappearance of the "practice voucher" scam.
- In response to the full implementation of quarantine-free customs clearance and the orderly resumption of international flights, PJ are focussed upon the possible reappearance of drug trafficking methods by hiding in the human body and in luggage.
- Since the launch of thematic cyber-crime investigations by PJ in 2018, a decline was reported in 2022 for the first time. The decline is believed to be related to the comprehensive effect of a series of preventive measures and the increasing public awareness of crime prevention. Among them, the number of computer fraud cases such as stealing credit card information for online consumption decreased significantly.
- However, internet fraud is still on the rise. Frauds involving online shopping and pornographic service traps have increased relatively significantly, causing losses to residents and merchants. In addition, the number of sextortion scams and phone scams increase year-

on-year which may be related to the increase use of social networking during the Covid pandemic.

- PJ took a multi-pronged approach in 2022 to improve the fraud prevention and anti-fraud mechanisms, hoping to provide stronger protection for the public. PJ continues to work with the local banking industry to take preventive measures and dissuade suspicious remittances before they happen, and cooperates with overseas police to stop payments for cross-border fraudulent funds.

Terrorism Financing Trend

In recent years, it has been observed that NPOs within South East Asia have been abused for TF which has raised concerns. PJ have stayed vigilant to the situation and have continuously implemented threat analysis. Apart from the risk-based approach for CFT and the continuous observation on suspicious fund flows implemented by financial institutions, PJ launched the specialized CT investigation division in October 2020, actively analysing and investigating funds that had been remitted out to high risk jurisdictions. None of the investigations have been found to be related to TF so far, and the overall trend remains stable.

3.2.8 **Malaysia**

Malaysia remains exposed to fraud activities, especially telecommunication fraud. In response to the continuous trend on telecommunication fraud and the rise in scams generally, Malaysia established the National Scam Response Centre (NSRC) on 12 October 2022, which aims to combat online financial scams through a dedicated platform which is able to trace and block funds more rapidly as well as enable easier reporting for financial scam incidents by victims.

The NSRC is an elevation from the Anti-Scam Centre set up at the Commercial Crime Investigation Department of Royal Malaysia Police (RMP) in 2021. The NSRC was established in collaboration with the RMP, Bank Negara Malaysia (the FIU), the Malaysian Communications and Multimedia Commission, the National Anti-Financial Crime Center (NFCC), financial institutions and telecommunication companies and serves as a national public-facing multi-agency communication and scam response coordination platform.

The NSRC had enabled prompt action to be taken on online fraud/scam cases, through the launch of a hotline service and close collaboration between the collaborative partners. Between 12 October 2022 and 31 January 2023, a total of 16,752 complaints were received which led to the opening of 751 investigation papers on cheating offences and 24 investigation papers on money laundering offences.

Further information about the NSRC can be found at the website: https://nfcc.jpm.gov.my/index.php/en/soalan/about-nsrc

3.2.9 **Solomon Islands**

Based on reported STRs for 2022, one of the emerging trends identified in the Solomon Islands is the rise of identity theft cases. It appears that, most of the identity theft or impersonation cases are linked with online scams and money mule activities carried out through the use of the internet.

The FIU continues to see reported cases of tax evasion and online scams in 2022. With tax cases, use of personal bank accounts to facilitate commercial transactions remains the common method used by perpetrators to evade tax. On the other hand, with online scams, the most reported cases usually involved victims befriending unknown individuals on social media and eventually losing large amount of monies through the various tricks or schemes employed by the scammers.

3.2.10 **The Philippines**

Recent research and studies on ML/TF methods and trends conducted by the Philippines contain observations on emerging trends; declining trends; continuing trends. For brevity, these have been summarized in section 3.1.6 above.

3.2.11 **Chinese Taipei**

Human Trafficking Syndicates

Recently, police agencies of Chinese Taipei have received numerous reports alleging that domestic criminals have collaborated with human trafficking syndicates in Jurisdiction A to recruit people to work in Jurisdiction A through Facebook and other online social media channels. Under the pretense of offering excellent job conditions, such as gaming customer service, loan services, and male porn actors, the victims are lured into signing work contracts and sent to Jurisdiction A, where they have their freedom restricted and are forced to engage in online scam and phone fraud. Investigations by law enforcement in Chinese Taipei discovered that the criminal group was operating and was arranging for the victims to stay in hotels to complete relevant documents before being escorted to the airport to travel to Jurisdiction A. The police rescued 3 victims heading to the airport on May 5, 2022. Three suspects were apprehended and the request for the accused to be detained was granted.

The police conducted in-depth investigations for over a month, and then carried out simultaneous arrests and searches on ten premises on July 5, 2022, and uncovered the criminal syndicate led by Person A. Six suspects were apprehended on site. Eight computers, 1 laptop, 1 mock gun, 100 blanks, 1 cash counting machine, employment contracts (Jurisdiction A), bank books, promissory notes, and IOUs were seized as evidence. After investigation, the suspects were referred to the prosecutor's office on charges of violating Article 297 of the *Criminal Code* (A person who for purpose of gain fraudulently causes another to leave the territory...) and violation of the *Organized Crime Prevention Act*. The detention of the six suspects was approved.

LINE Group Investment Fraud

The CIB analyzed information reported by the public and determined that the fraud ring used social media such as Instagram, Facebook and YouTube to place advertisements with investment platform links and customer service IDs to attract people to click and watch, luring victims with claims such as "investment planning," "passive income," "part-time income," "guaranteed profit without losses," "easy to operate, low limits to join " and " easy paid, just have fun" so that victims can click on links, inquire and add as friend on messaging apps. After the victims added the group on LINE, the fraudsters would ask them by unsolicited private message, "Do you need money? I can help you make money", "I can teach you how to invest and make money", "profitmaking projects without charges", and "help you invest on foreign currency without charges", etc. After inducing victims to sign up for the fake investment platforms and asking members to join the LINE groups, the fraud ring's members acted as "investors" to lead the way and plant the illusion that as long as they listened to the suggestions of "instructors" or "chief instructors" to invest in cryptocurrencies, foreign exchange and futures, they would be able to profit. By doing so, victims were persuaded to remit money for investment and then were defrauded. When the victims found out they had been scammed, those fraudsters "unfriended" the victims, removed them from the LINE group or did not reply their messages. This criminal group had run for 4 months between October, 2021 and January, 2022. There were approximately 20 to 30 victims reported to the police, and the initial estimated defrauded amount was over NTD 10 million, the highest loss for one of the victims was up to NTD 2.6 million.

After investigating and gathering evidence for several months, on January 19, 2022, a simultaneous search was conducted on the fraudulent bases (two operating rooms). Thirteen members of the scam ring, including fake investors and fake instructors, were arrested on the spot for committing fraud. The court granted the request for the detention of the main leader Person A after an interrogation led by the prosecutor. After nearly 3 months of tracking, analyzing hundreds of CCTV footages, searching suspicious premises across the nation, as well as ambushes and nighttime stakeouts, Person B (another ringleader) and other suspects were discovered to be hiding out in a rural farmstead in early April. After obtaining a search warrant on April 8, the police apprehended the suspects. Person B and another suspect were interrogated by the prosecutor and were detained by the court immediately.

3.2.12 **Thailand**

In relation to Money Laundering, Thailand has observed Virtual Assets Fraud and ML using VA as an emerging trend.

Continuing trends Include:
- ML through mule accounts.
- Ponzi schemes through social media.
- ML by using nominees or third parties to purchase real estate and luxury products.
- ML through stock markets or mutual funds.
- ML through unregulated VA exchangers.
- ML through cash couriers.
- ML through underground banking.
- ML through trade activities.
- ML through e-money and e-payment services.
- ML through shell companies and cooperatives.

Thailand noted use of online banking for own accounts as a declining trend.

In relation to terrorism financing, Thailand has observed self-funding from legitimate sources and the use of the internet; banking as emerging trends:

Continuing trends include:
- Raising funds through social media.
- Raising funds through crime commission.
- Raising funds through business in foreign jurisdiction.
- Raising funds through NPOs.
- Moving funds through third parties' accounts or use of third parties.
- Moving funds through cash couriers.

Thailand noted the use of shell companies as declining trend.

3.2.13 **Vietnam**

Vietnam has observed during 2022 an increase in predicate offending in the cyber-space. These crimes include the crime of property appropriation and the crime of organizing gambling.

The Ministry of Public Security of Vietnam has discovered many criminal lines in cyberspace and money laundering, and has investigated and prosecuted a case of "Using computer networks, telecommunications, or electronic means to appropriate property; money laundering" relating to a foreign person in August 2022. Hanoi City Police investigated and prosecuted a case of fraud to

appropriate property, launder money through the form of invitations on the internet to enter data to earn money on the Web.

With the development of 4G technology, the trend of cybercrime in general and money laundering and terrorism financing in particular is expected to increase and be more complex.

3.3 Effects of AML/CFT legislative, regulatory or law enforcement counter-measures

3.3.1 Hong Kong, China

The use of offshore companies to facilitate ML activities has become less popular as financial institutions continued to enhance their customer due diligence requirements to gather information on the beneficial owners of all types of companies.

3.3.2 Japan

Deposit-taking institutions and credit card operators submitted STRs as below, concerning accounts of Japanese people and companies or contracts (including those that were declined):

- A large amount of international transfers to accounts where customer information is outdated and not updated.
- A large amount of unexpected transfers and a large amount of remittance from abroad.
- Remittances from a foreign jurisdiction where the explanation was that it was a legitimate transaction but there was no confirmation material.
- Requests from foreign banks for return funds due to fraud.
- Accounts suspected of being used in fraud cases in a foreign jurisdiction.
- Accounts being listed as frozen.
-

With this information, it was discovered that some accounts were used for an international fraud case. Several related parties, including the account holders, were arrested in violation of the *Act on Punishment of Organized Crimes (concealment of criminal procedures).*

Number of STRs Used for Investigative Purposes.

	2019	***2020***	***2021***
Number of STRs used in investigation	***307，786***	***325，643***	***353，832***

4 PROLIFERATION FINANCING METHODS & TRENDS

This section of the Typologies Report provides a brief overview of the United Nations Panel of Experts reports September 2022, March 2023, September 2023 and information from members about PF risk assessments undertaken and publications and guidance issued to mitigate risk. Four case studies have been provided by Members.

4.1 Recent risk assessments, research or studies on proliferation financing methods and trends

United Nations Panel of Experts mid-term report, dated 7 September 2022 (S/2022/668)

On 7 September 2022, the United Nations Security Council released the Panel of Experts (**PoE**) midterm report.

The PoE identified continued acceleration of the DPRK's missile programmes and claimed development of "tactical nuclear weapons". The PoE observed the DPRK's use of continuing and new methodologies for illicit oil imports and coal exports. The PoE examined evidence of cargo ships being re-configured to carry refined petroleum and of ships undertaking direct delivery and ship-to-ship transfers of illicit cargo in the DPRK's territorial waters.

Another significant source of revenue for the DPRK is generated from illicit cyber-activity. Two major cyber hacks in 2022, one attributed to the DPRK, resulted in the theft of hundreds of millions of United States dollars. Other cyber-activity was directed to stealing information to support its prohibited programmes including WMD.

The PoE made seven recommendations directed to education, communication, increased regulatory controls and implementation by Member States of the FATF guidance on virtual assets, to prevent PF, ML and TF.

United Nations Panel of Experts final report, dated 7 March 2023 (S/2023/171)

On 7 March 2023, the United Nations Security Council released the Panel of Experts (**PoE**) final report for 2022.

In 2022, the DPRK continued to develop its prohibited ballistic missile and nuclear weapons programmes, launching at least 73 ballistic missiles and missiles combining ballistic and guidance and announcing a new first-use doctrine and the "irreversible nature" of the jurisdiction's nuclear status.

The PoE reported a significant acceleration in the DPRK's acquisition of cargo ships and other vessels and use of these to import refined petroleum, directly and via ship-to-ship transfers, and export coal, in breach of UN sanctions.

The DPRK raised more illicit revenue through cyber-activity, than in any previous year. DPRK state-sponsored cyber-threat actors used ransomware and malware hacks to steal virtual assets valued at USD1 billion in 2022. Another growing revenue source for the DPRK is the virtual theft of non-fungible tokens.

In addition to reiterating previous recommendations to increase "cyber-hygiene", the PoE has recommended the designation of an individual who supports the DPRK's prohibited weapons programme as the director of a UN-designated organisation engaged in cyber-enabled illicit revenue generation and acquisition of sensitive information.

United Nations Panel of Experts mid-term report, dated 13 September 2023 (S/2023/656)

On 27 October, the United Nations Security Council released the Panel of Experts (PoE) midterm report, dated 13 September 2023.

The report includes a range of case studies and findings related to Democratic People's Republic of Korea continued violations and evasion of UN sanctions against the Democratic People's Republic of Korea, including the financial aspects of these sanctions.

The report highlights ongoing Democratic People's Republic of Korea access to the international financial system and engagement in a variety of illicit financial operations in violation of the UNSC resolutions. The Panel investigated financial institutions and representatives of the country, including banking representatives, operating abroad that support such activity. The report notes that border reopening may increase cases of Democratic People's Republic of Korea nationals couriering cash and high-value items. The Panel investigated reports of nationals working overseas earning income in violation of sanctions, including in the information technology, restaurant, medical and construction sectors. The Panel continued investigations into joint ventures, cooperative entities and illicit business activities and alleged exports of Democratic People's Republic of Korea military communications equipment, arms and ammunition, and commodities. Finally, the report emphasizes the ongoing and increasingly sophisticated illicit generation of revenue through cyber-activities by Democratic People's Republic of Korea state-sponsored actors, reportedly responsible for nearly USD1.7 billion worth of cryptocurrency theft in 2022.

Hong Kong, China

The second *Hong Kong Money Laundering and Terrorist Financing Risk Assessment* was conducted and its report published on 8 July 2022. This is the second assessment of ML/TF risks and first assessment of PF risks in Hong Kong, China.

The report assessed Hong Kong, China as a medium-low PF risk for both threat and vulnerability based on the following key findings:

- Designations by the UNSC and its relevant committees at the end of 2021, did not include any residents or operating companies incorporated in Hong Kong, China. Robust investigations by LEAs also found no evidence of PF activity in Hong Kong, China.
- Nevertheless, as an international financial, trade and transportation hub and its geographical proximity to both the DPRK and Iran, Hong Kong, China acknowledges its potential exposure to external PF threats.
- Hong Kong, China reduces any vulnerabilities through a robust counter-proliferation regime involving comprehensive legislation and an institutional framework involving government agencies, regulators/supervisors and the private sector.

The Risk Assessment can be found at: https://www.fstb.gov.hk/fsb/aml/en/risk-assessment.htm

In addition to conducting its risk assessment, Hong Kong, China's Joint Financial Intelligence Unit issues STR quarterly analysis and alert messages to STR reporting entities. These topical strategic analysis reports promote intelligence exchange on PF, triggering law enforcement action and providing insights into formulation of PF policy and regulations.

Indonesia

Indonesia undertook its PF Risk assessment in 2020 and identified a medium level of risk given existing diplomatic and economic relationships with both the DPRK and Iran. These relationships exist at a diplomatic level, through political interactions, business relationships and person to person relationships.

Indonesia introduced a number of mitigating measures to counter this risk including the ability to freeze assets of designated persons and entities and considers its overall risk and vulnerability to currently be low.

During the COVID pandemic, Indonesia recognised risk associated with the volume of cross-border transactions involving medical, chemical and biological materials.

Indonesia has not identified any cases directly linked to designated persons or entities, however between 2018 and 2022, the Directorate General of Customs and Excise (DGCE) has taken enforcement measures to counter PF in relation to Iranian and DPRK imports and exports on 113 occasions, seizing assets valued at IDR2.68 billion.

Macao, China

Macao, China undertook a risk assessment on PF in 2022 by reference to the RUSI Proliferation Financing Rapid Risk Assessment Tool.

Risks were assessed considering:

- The UNSC Panel of Experts reports on the DPRK and Iran.
- PF risk assessments from other jurisdictions.
- Analysis of demographic statistics and geographical proximity.
- Analysis of STRs and criminal cases related to PF.
- Statistics on seized chemicals, weapons and ammunition.
- Analysis of Import and Export data including dual-use goods.
- The existing legal framework and control measures.

No freezing actions related to PF have been implemented in Macao, China, nor have any cases related to PF been prosecuted since the introduction of the Asset Freezing Regime (Law no. 6/2016) which came into effect in 2016.

The Asset Freezing Regime requires FIs and DNFBPs to apply control measures to freeze the assets of individuals and legal persons included in the PF sanction lists. Supervisors have established effective communication mechanisms with the financial and gaming sectors in relation to asset freezing.

No breaches, non-implementation or evasion of the obligations in relation to targeted financial sanctions, as referred to in FATF Recommendation 7, have been detected in Macao, China.

Macao, China's risk assessment of PF is low overall, noting low inherent exposure to risk and sufficient mitigating control measures in place.

Philippines

The Philippines has identified some gaps in relation to the implementation of targeted financial sanctions on proliferation financing, such as lack of process on due diligence analysis, collecting and processing intelligence, and investigation methods specifically on PF. The Philippines has

also identified that it needs to conduct more outreach and awareness activities for targeted sectors including DNFBPs, exporters, and brokers. These measures are essential to effectively implement TFS on PF upon proposed legislation being enacted.

The Strategic Trade Management Office (STMO), in cooperation with the AMLCS, has proposed specific implementing mechanisms to respond to FATF Recommendation 7. In particular, counter PF legislation has been proposed and regulatory and operational mechanisms are needed for monitoring compliance and applying sanctions for breaches.

Singapore

Singapore considered PF risks in its 2013 ML/TF risk assessment and consistently reviews its risks via the interagency Risks and Typologies Inter-Agency Working Group (RTIG). The RTIG was set up in 2017 to identify and review Singapore's ML/TF/PF risks. Relevant authorities communicate key PF risks through industry engagement and guidance produced by the authorities.

In response to the revisions to the FATF Standards, Singapore is currently 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 it under the interagency RTIG framework which involves relevant law enforcement agencies, financial intelligence units and supervisory agencies and factors in industry feedback and exchanges of information between the public and private sectors. In addition, Singapore has set up a Work Group under the auspices of Singapore's AML/CFT Industry Partnership to seek industry feedback specifically from FIs (e.g. banks and insurers) and DNFBPs (e.g. company service providers).

Chinese Taipei

From January 2017 to October 2022, Chinese Taipei prosecutors investigated 11 cases involving violations of sanctions by DPRK. Five cases resulted in convictions, three were found not guilty, and three did not proceed to prosecution. The most common typology involving PF is the transfer of oil to DPRK ships on the high seas from third-jurisdiction ships controlled by Chinese Taipei oil companies, or transfer of oil to ships owned by third party jurisdictions who resell it to DPRK ships. There is also a case of Chinese Taipei nationals buying anthracite (coal) from DPRK in breach of UN sanctions and reselling it to other countries.

Petroleum products are still the most common commodity traded by Chinese Taipei nationals in breach of UN sanctions. Under Chinese Taipei law it is legal to transact oil trade on the high seas. Representatives or beneficial owners of shipping companies, including foreign nationals, intermediaries and involving complex business structures broker ostensibly legal trades to disguise illicit transfer of oil via ship-to-ship transfers at sea. False export information is also utilised and offshore companies and accounts used to frustrate funds tracing.

The subjective element of Article 9, Paragraph 1, Subparagraph 1 of the Counter-Terrorism Financing Act requires a suspect to "knowingly" trade with the sanctioned target, and the intervention of intermediaries has made this element difficult to prove.

Whilst violations of Chinese Taipei's Foreign Trade Act in relation to Iran have been identified, these relate to Chinese Taipei manufacturers exporting unlicensed strategic high-tech commodities and no cases have been found to involve PF.

Thailand

Thailand's NRA published in 2022 assesses the risk of PF. The NRA identified the risk of proliferation financing in Thailand as low, with the key potential methods for PF being sanction evasion and business related to dual-use items. Thailand has an existing legislative framework for countering PF.

4.2 Guidance materials provided to FIs and DNFBPs, VASPs or other sectors

Japan

The Japanese Ministry of Finance published the "Foreign Exchange Inspection Guideline" on measures 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.

Link:https://www.mof.go.jp/policy/international_policy/gaitame_kawase/inspection/e_g_zenbun.pdf

Philippines

The Philippines STMO has published guidance for the financial and associated sectors:

- The National Strategic Goods List (NSGL). Under annexure 3 prohibited imports and exports with DPRK and Iran are listed as Nationally Controlled Goods. Link: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Policies/Annex%20III.pdf
- DTI memorandum circular 20 13 which adopts the UNSC's consolidated list of individuals and entities as the STMO's List of Prohibited Users. Link: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/e-library/Laws+and+Policies/140420_MC20_13.pdf
- Issuance of DTI Memorandum Circular 21-06 to provide guidelines in the implementation of brokering and financing to satisfy requirements of UNSCR 1718 (2006), 2231 (2015) and their subsequent resolutions.
  Link: https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/Laws+and+Policies/Memorandum+Circular+No.+21-06+Implementation+of+FInancing+and+Brokering+Under+Republic+Act+No.+10697.pdf
- STMO assistance in granting authorization to access frozen assets for purposes of making payments due under prior contracts under AMLC Regulatory Issuance No. 1. This is possible when the STMO has determined that the contract is not related to any of the prohibited items, financial assistance, brokering or services and the payment is not directly or indirectly received by a person or entity subject to the measures, both referred to in UNSCR 2231 (2015) and its subsequent resolutions.
  Link:
  http://www.amlc.gov.ph/images/PDFs/Guidance%20for%20Delisting%20and%20Unfreezing%20-%20PF%20TFS%20v2.pdf

The Philippines STMO has conducted awareness activities and enhanced due diligence:

- outreach activities to covered stakeholders of possible repercussions when transacting business with sanctioned individuals and entities. These awareness activities can be in the form of one-on-one session with STMO, targeted outreach with specific sectors, and town hall sessions attended by both government and industry stakeholder.
- In addition, the STMO provides end-user business advice to ensure compliance with applicable requirements of sanctioning states. To date, the STMO has accommodated more than 10 transactions relevant to business advice on future business activities/contracts with new foreign business partners.

Links:
https://dtiwebfiles.s3-ap-southeast-.amazonaws.com/STMO/Announcements/STMO+Advisory_Sanctioned+Individual+and+Entities.pdf

https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/red+flags.pdf

https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/restricted-party-screening-2.pdf

Singapore

The Monetary Authority of Singapore (MAS) has issued guidance to FIs to assist them in countering of PF risks:

- Following a series of supervisory visits to banks on countering PF risks, MAS published a guidance paper, which covered key findings noted during the visits and sound practices observed, which FIs could use as benchmarks to enhance their existing controls.
- MAS provided guidance on countering PF, which included potential indicators of PF, in its AML/CFT Guidelines for FIs.

In addition, MAS, working in conjunction with the Association of Banks in Singapore (ABS), has made counter-PF a standing agenda item at the ABS' annual Financial Crime Seminar (FCS). The ABS FCS is one of Singapore's key AML/CFT industry outreach events and is regularly attended by over 500 practitioners from Singapore and in the region. Both experts from Singapore and overseas have spoken at the ABS FCS over the years to raise the industry's awareness of PF risks and PF risk mitigation.

Chinese Taipei

The Insurance Sectors' AML/CFT Joint Task Force of Chinese Taipei has issued guidance for the insurance sector in relation to marine insurance in relation to AML/CFT/PF risks:

- The "Best Practice Guideline for Insurance Sector to Implement Anti-Money Laundering and Combating the Financing of Terrorism (AML/CFT) - Subject: Practical Procedure to Prevent Money Laundering, Terrorist Financing and Proliferation Financing with Respect to Cargo Insurance and Relevant Lines of Insurance". The guideline provides P&C insurers with practical recommendations to ensure AML/CFT considerations during soliciting, underwriting and claims handling of cargo insurance and marine hull insurances, as well as operational practices of underwriting fishing vessel insurance involving flags of convenience (FOC) in high-risk territories.

Thailand

Thailand's AMLO provides regular information and guidance to FIs and DNFBPs about PF. Several seminars were conducted to disseminate information on identifying, assessing, and mitigating PF risks to relevant agencies including the Ministry of Commerce and PF-vulnerable businesses as well as guidelines for identifying, assessing, and mitigating PF risks in businesses related to dual-use items.

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

Case study # 114 - Ship-to-ship transfer, use of third party jurisdictions

proliferation financing; abuse of legal persons and arrangements

An international company (the 'Company') was established and registered with a Cook Islands trust office, as the 'ship owner' for a vessel that had been registered in Jurisdiction B. The Company operated its business in Jurisdiction C. The registered office and resident secretary in Jurisdiction A were not involved in any of the Company's operations, business or financial transactions, nor did they have any correspondence with the Company's sole owner and director.

A SAR was filed which uncovered that the ship had been suspended and subsequently de-registered in Jurisdiction B, due to its participation in an illicit ship-to-ship transfer with another vessel flagged under the Democratic People's Republic of Korea.

This activity represented a breach of the United Nations Targeted Financial Sanctions and led to the Company being placed on the sanctions list and de-registered in Jurisdiction A.

Source – Cook Islands

Case study # 115 - Central Bank rejection of Company application for partner operating in sanctioned jurisdiction

proliferation financing; abuse of legal persons and arrangements

The Central Bank, as supervisor, assessed an application by Company A for cooperation in relation to a potential partner. The Central Bank conducted coordination and review and identified that the potential partner was an entity operating in a sanctioned jurisdiction, identified by the FATF as High Risk. The Central Bank sought additional information and an explanation from Company A regarding the potential partner. Company A was not able to fulfil the request from the Central Bank and the supervisor decided to reject the application for cooperation from Company A.

Source – Indonesia

Case study # 116 - The Wise Honest - Ship-to-ship transfer, use of third party jurisdictions

proliferation financing

The 'Wise Honest', a bulk cargo carrier ship, was used in a scheme to transfer imports and exports between the Democratic People's Republic of Korea (DPRK) and other jurisdictions from at least November 2016 through April 2018, in breach of United Nations Targeted Financial Sanctions. Participants in the scheme attempted to conceal the Wise Honest's affiliation with the DPRK by falsely listing in shipping documentation, different countries for the ship's nationality, and the origin of coal being transported.

In 2018, Indonesia received an MLA request from Jurisdiction A in relation to a potential ship-to-ship transfer between the Wise Honest and a vessel from Jurisdiction B. Investigation by Indonesia's State Intelligence Agency (SIA) revealed a network of Indonesian and DPRK nationals involved in the scheme. The SIA passed its intelligence to the PPATK (Indonesia's FIU) to conduct a parallel financial investigation. These investigations collectively led to the successful repatriation of the Wise Honest to Jurisdiction A and Indonesia imposed an IDR400,000,000 (approx. USD26,000) fine on the captain of the Wise Honest.

Source – Indonesia

Case study # 117 - Lazarus Group

proliferation financing

Attacks similar to the methods of a cyberattack group called Lazarus, which is allegedly sponsored by North Korea, have been made against virtual currency exchange service providers in Japan. Given the above, it is strongly inferred that related businesses in Japan have been the target of this group for several years now.

Source – Japan

5 ASSET RECOVERY METHODS & TRENDS

This section of the Typologies Report focusses upon data provided by Members in relation to asset recovery efforts and relevant case studies.

5.1 Australia

Case study # 118 - Purchase of luxury goods and precious metals with drug proceeds

drug-related crime; purchase of real estate; purchase of valuable goods; financial institutions; abuse of legal persons and arrangements; wire transfer

In 2020, the Australian Border Force (ABF) detected illicit narcotics hidden in machinery. The matter was referred to the AFP for criminal investigation and asset confiscation. The dual investigations revealed that Person A is a person with dual nationality and was connected to international bank transfers, suspicious cash deposits, use of real estate agents and lawyers' trust accounts to receive bank transfers, use of domestic companies to purchase assets and the acquisition of unencumbered real properties, precious metals and classic cars.

Person A was arrested following a controlled operation and convicted in April 2022. Person A was sentenced to 11 years' imprisonment with a non-parole period of six years. Restraint action has resulted in the seizure of 44 motor vehicles, cash, gold, platinum and silver with an estimated combined value of AUD5 million (approx. USD3.2 million) which were subsequently confiscated by automatic operation of the *Proceeds of Crime Act 2002* (Cth) in October 2022.

Source – Australia

5.2 China

During 2017-2022, the competent authorities in China have recovered assets valued at approximately RMB 32.786 billion (approx. USD4.5 billion) in the special operation 'Skynet'. This operation has targeted the proceeds of crime received by fugitive corrupt officials.

5.3 Hong Kong, China

The Anti-Deception Coordination Centre ("ADCC") and the Joint Financial Intelligence Unit ("JFIU") under the Hong Kong Police Force ("HKPF") strengthened cooperation with financial institutions to mitigate victims' losses by establishing a round-the-clock contact channel with fourteen local banks. Upon receipt of reports of fraud/deception or related money laundering activities which meet relevant criteria, the ADCC liaises with the bank which will decide whether to stop the payment.

Similarly, ADCC, together with the Financial Crimes Unit of the INTERPOL jointly established the International Stop-Payment Mechanism in October 2019. Upon receipt of reports of fraud involving beneficiary accounts in financial institutions overseas, the ADCC contacts the INTERPOL to initiate the Stop-Payment Mechanism for cases that meet relevant criteria. Reciprocally, the INTERPOL also refers cases involving beneficiary accounts in Hong Kong to the ADCC for intercepting criminal proceeds.

In March 2021, the HKPF established a Cryptocurrency Stop Payment Mechanism in response to the increasing popularity of cryptocurrency trading and the potential risk that cryptocurrency might be exploited by criminals as a means to launder criminal proceeds. The platform facilitates

coordination and cooperation with cryptocurrency related stakeholders including payment platforms and crypto-ATM service providers. HKPF has put in place a mechanism to help track the relevant funds, make stop-payment requests and intercept payments to fraudsters systematically upon receiving suspected fraud complaints, thus minimising victims' losses.

The most common restrained and confiscated assets in Hong Kong, China were cash in bank accounts, real estate and securities held with licensed corporations or banks. Other assets included precious metals, stones, jewellery or wristwatches and physical cash. Around 60% of the assets were held in the name of other persons or co-owned by a company.

Case study # 119 - Successful Stop Payment in a Romance Scam

fraud; financial institutions; foreign predicate offence

A female from Jurisdiction X was lured by a romance scam to remit a total of USD3.77 million (approximately HKD296 million) to a bank account in Hong Kong, China on four occasions in mid-2022. The scam was reported by the female to the Hong Kong Police who swiftly liaised with the Bank to intercept the transfers. The remittances were successfully intercepted and the entire defrauded amount was returned to the victim.

Source – Hong Kong, China

Case study # 120 - Successful Stop Payment in a Business Email Compromise

fraud; financial institutions

In mid-2022, a manager of a local stock investment company remitted HKD9.86 million (approx. USD1.3 million) from the company's bank account to a local bank account upon the receipt of an 'instruction' in an email sent from a scammer spoofing the email address of the company's director. The scam was soon unveiled as the real director received a text message notification from the bank. The case was reported to the Hong Kong Police and the full sum in the fraudster's account was suspended. Restitution of the defrauded money is ongoing.

Source – Hong Kong, China

Case study # 121 - Money Laundering Related to Proceeds of Drug Trafficking

drug-related crime; cash; financial institutions; suspicious transaction reporting

Person A was convicted of drug trafficking offences in Jurisdiction A and sentenced to life imprisonment. Financial intelligence suggested that there were 69 cash deposits totalling HKD29 million (approx. USD3.7 million) made into Person A's bank account in Hong Kong, China. Shortly after the apprehension of Person A, funds totalling HKD12 million (approx. USD1.5 million) in his Hong Kong bank account were transferred to his wife's bank accounts. The wife resided in Jurisdiction Y and the transactions were made by phone-banking. In late 2021, a confiscation Order to forfeit the assets of Person A and his wife amounting to HKD8.8 million (approx. USD1.126million) was granted by the Court.

Source – Hong Kong, China

Case study # 122 - Confiscation of Cryptocurrency

fraud; foreign predicate offence; suspicious transaction reporting; use of virtual assets

Upon the implosion of a cryptocurrency company based in Jurisdiction Y, in mid-2022, an STR pertaining to the cryptocurrency X's founder Person A, was filed to the Joint Financial Intelligence Unit of Hong Kong, China. Person A was suspected of defrauding around HKD500

million (approx. USD64 million) from his investors. Cryptocurrencies worth over HKD157 million (approx. USD20million) were prevented from being dissipated from digital assets accounts held by Person A and his two associates. The LEA in Jurisdiction Y is cooperating with requests to initiate asset recovery procedures.

Source – Hong Kong, China

5.4 Indonesia

Case study # 123 - Complex Asset Management on Huge Corruption

bribery and corruption; international cooperation

Person A and Person B used Company A, a State-owned enterprise located in Jakarta, to embezzle funds through corruption, and subsequently laundered a total of IDR16.8 trillion through the enterprise and other companies and accounts, as well as through the purchase of vehicles in the names of the offenders, third parties and other companies. Money was spent on gambling as well as on assets abroad, which was uncovered through formal and informal international cooperation.

The Attorney General's Office (AGO) set up an asset tracing team that was independent from the investigating team in 2020. The team obtained financial information from various Indonesian authorities (e.g., Directorate General of Tax, land and motor vehicle registry, and the Commission of Eradication of Corruption/CEC) as well as using their investigative powers to obtain financial transaction information from banks to profile the suspects and to find links between the illicit proceeds and assets. As company structures were used to layer and disguise the illicit funds, the AGO also coordinated with the Financial Service Authority for information about shares and the Ministry of Law and Human Rights (MLHR) for company information.

In October 2020, assets were seized including assets of three companies, 21 cars, one motorcycle, luxury items, insurance policies, reals estate and IDR11 billion in cash. In order to preserve the value of the assets, the ARC appraised the assets and auctioned off land, stocks and shares, as well as luxury vehicles. An uncompleted luxury boat was auctioned off for IDR5.5 billion. Assets that could not be sold were kept by the Asset Recovery Center (ARC). The auction of stocks and shares as well as the re-structuring of Company A had to be carefully managed with the Ministry of Finance so as not to cause a fall in values. In order to make restitution for the losses caused to the State from the embezzlement, the ARC is considering the possibility of pursuing share assets of the offenders as well as licenses for mining operations as assets of equivalent value.

Through international cooperation mechanisms, Indonesia is also pursuing assets purchased in regional countries in the names of third parties with the proceeds of crime. For the purpose of the investigation, AGO obtained data/information from Jurisdiction B on banking transactions and share ownership through MLA requests. This information was used to prosecute the suspects. Formal MLA requests to freeze assets and informal assistance requested to file a court application for the confiscation and seizure of assets owned by the suspects are currently ongoing.

Source – Indonesia

5.5 Japan

Police have seized assets based on the Rules of the National Public Safety Commission and the guideline for the storage and management of material evidence issued by the National Police Agency. Also, the Public Prosecutors Office manages evidence based on the "Administrative Rules of Evidence" which stipulates administrative rules from receipt to disposition of evidence (articles seized and the proceeds realized by liquidation thereof).

Case study # 124 - Temporary Restraining Order for confiscation of drug-related criminal proceeds before institution of prosecution on cannabis trafficking

drug-related crime

Person A cultivated cannabis in his home and forest area and trafficked the cannabis using door-to-door delivery services to individuals. This case proceeded as a violation of the *Anti-Drug Special Provisions Law*. In this case, a Temporary Restraining Order was issued against JPY5.7 million (USD38,000) in cash that he had obtained from trafficking cannabis.

Source – Japan

Case study # 125 - Temporary Restraining Order for confiscation of drug-related criminal proceeds before institution of prosecution on drug trafficking using social media

drug-related crime; financial institutions

Suspects looked for drug customers using social media, then delivered stimulants and cannabis, nationwide by letter pack services. They transferred drug-related criminal proceeds into bank accounts in the name of another party, controlled by them. This case was cleared as a violation of the *Anti-Drug Special Provisions Law* by police officers. In this case, a Temporary Restraining Order was issued against JPY1.29 million in cash (approx. USD8600) and JPY180,000 in bank deposits obtained from trafficking the drugs.

Source – Japan

5.6 Mongolia

Case study # 126 - Abuse of authority, Money laundering

politically exposed person; purchase of real estate; abuse of legal persons and arrangements

A former high-level politically exposed person of Mongolia, Person Y gave preference to Company A in signing an investment contract, by abusing his position. Then, Person Z, an executive director of Company A, transferred a large sum of funds from Company A to an offshore Company X established by him in an offshore jurisdiction. Real estate was bought in the offshore jurisdiction by Company X in the name of a relative of Person Y.

During the investigation of this case, an FIU and a law enforcement agency extensively cooperated and collaborated with domestic competent authorities and reporting entities, as well as foreign counterparts and FIUs. A number of requests for information were sent to relevant counterpart FIUs via the Egmont network to collect additional information, and one request for mutual legal assistance was submitted to competent authorities of the offshore jurisdiction to gather evidence.

Persons Y and Z were subsequently prosecuted and convicted. They were found guilty on charges of "Abuse of authority or official position" and "Money laundering" in 2020. Criminal proceeds worth around USD6 million in total were paid as restitution by the Court's orders in 2021.

Source – Mongolia

Case study # 127 – Embezzlement of public funds

politically exposed person; purchase of real estate; abuse of legal persons and arrangements

An investigation was initiated after news was published by the International Consortium of Investigative Journalists (ICIJ) regarding politically exposed person (s) in Mongolia who had founded companies in offshore jurisdictions. When investigating the activities of these offshore companies, it was revealed that a Mongolian state-owned enterprise concluded procurement contracts with offshore companies at higher prices than market value and that public officials and PEPs abused their authority to sign those contracts. After contract payments were transferred to offshore companies, some amounts of funds were transferred back to the public officials and PEPs through their associates' bank accounts. The funds were then used to buy land and real estate concealing the origins of the proceeds of the crime.

As part of the investigation, the FIU and a law enforcement agency extensively cooperated and collaborated with domestic competent authorities and reporting entities, as well as foreign counterparts. One request for information was sent to a foreign FIU to collect additional information and one mutual legal assistance request was submitted to a foreign jurisdiction to gather evidence.

The case was resolved through a simplified procedure in 2021, in accordance with the Criminal Code, and land and real estate worth USD740,112 was confiscated.

Source – Mongolia

5.7 Singapore

Case study # 128 – Confiscation of illegal gambling proceeds

gambling activities; organised crime; racketeering

On 27 July 2022, the Singapore High Court issued a confiscation order for approximately SGD1.25 million (approx. USD922,000) against Person A who was sentenced to four years and 12 months' jail and fined SGD500,000 (approx. USD368,000) for running an illegal gambling operation. Person A was sentenced for providing a Singapore-based remote gambling service, receiving illegal lottery bets, transferring criminal benefits and being a member of an organized crime group, as well as offences related to an organized crime group. Further investigation into Person A's financial affairs found that the amount of his accumulated unexplained wealth over the years was disproportionate to his known sources of income.

Source – Singapore

Case study # 129 – Confiscation of proceeds spent on luxury goods and properties

bribery and corruption; use of real estate; purchase of valuable or cultural assets

On 31 March 2022, one of the three members of a conspiracy to misappropriate gas/oil from a petroleum facility was sentenced to 29 years' jail. Person A was also charged with two money laundering offences. The financial investigation revealed that Person A had obtained at least SGD5.6 million in criminal proceeds, which he spent on designer watches, cars and local/foreign properties. A disposal order was obtained against Person A to return SGD3,31million (approx. USD2.5 million) in cash and SGD299,922 for assets (based on purchase price) to the petroleum facility. The other two members of the conspiracy are still in courts proceedings.

Source – Singapore

Case study # 130 – Expeditious asset recovery of USD 70 million involving multiple countries

fraud; third party ML; foreign predicate offence; wire transfer

In a love scam, Victim C was deceived into transferring funds from her company to multiple entities and individuals in various countries, including bank accounts in Singapore which received over USD135 million. Upon receiving the information, the Commercial Affairs Department (CAD) swiftly seized and recovered almost USD70 million from multiple bank accounts. Assistance was sought via INTERPOL, the FIU and through direct police to police channels to trace the funds and the recovered funds were returned to the victim company within a year of seizure.

Source – Singapore

Case study # 131 – Use of Concealed Income Analysis that resulted in confiscation

smuggling; standalone ML; cash; financial institutions

In July 2019, person A was arrested by Singapore Customs for dealing in the proceeds of unpaid duties on cigarettes. During the operation, more than 300 cartons of cigarettes worth more than SGD87,000 were seized. The total duty and Goods and Services Tax (GST) evaded exceeded SGD90,000. Investigations by Singapore Customs revealed that Person A had unexplained wealth which he could not satisfactorily account for and the matter was referred to the CAD for investigation.

CAD commenced extensive financial investigation into Person A. Following screenings with the commercial banks in Singapore, approximately SGD112,000 in two bank accounts belonging to Person A was seized. To establish his financial profile, Person A was interviewed at length and asked to declare his assets, liabilities, expenses, legitimate income and other sources of income. CAD's concealed income analysis revealed that between October 2018 and July 2019, Person A had accumulated wealth amounting to SGD92,750.83 which he could not satisfactorily account for.

In May 2021, Person A was convicted for his offences under sections 128I(1)(a)(ii) and 128I(1)(b) of the Customs Act and sentenced to 3 months' imprisonment and fined SGD100,000, in default 3 months' imprisonment. In January 2022, investigators forfeited a total of SGD92,750.83 (USD67,561) representing concealed income under section 5(1) of the CDSA.

Source – Singapore

Case study # 132 – Confiscation of proceeds relating to drug trafficking

drug-related crime

Person A was arrested in 2010 for trafficking in a controlled drug under the *Misuse of Drugs Act, 1973*. On 4 February 2015, he was sentenced to suffer the death penalty for the drug trafficking offence. During his arrest, cash amounting to SGD70,295 was seized. During the concurrent financial investigations, four bank accounts with a total balance of SGD211,260 were also restrained. Financial investigations revealed that the monies seized from him were from proceeds from drug trafficking and an illegal money lending business.

To ascertain the magnitude of the benefits Person A had received from his drug trafficking activities, a concealed income analysis was computed. It showed that the accused had a concealed income of SGD167,429. This is the amount which the accused could not satisfactorily account for as part of his accumulated wealth, and was disproportionate to his known sources of income. On 17 February 2020, a Confiscation Order for SGD167,429 (approx. USD124,000), being the value of the benefits derived from drug trafficking, in accordance with Sec 4 of the CDSA, was granted.

Source – Singapore

5.8 Chinese Taipei

The confiscation provisions of Chinese Taipei's Criminal Code came into effect on July 1, 2016. As of April 2022, the total confiscation amount ordered by the Courts has reached more than NTD 27.1 billion (approx. USD920.4 million).

Case study # 133 - The Lafayette Frigates scandal

bribery and corruption

Chinese Taipei's most famous confiscation case involves the proceeds of bribery and corruption in relation to the procurement of six naval frigates by Chinese Taipei from foreign jurisdiction Y. The orders for confiscation of criminal proceeds amount to USD920.397 million (NTD27,160,910,000).

Jurisdiction Y paid bribes to secure a deal to sell frigates to Chinese Taipei through former, partially state-owned company, A. The frigates were sold via company B in Jurisdiction Y, to the Chinese Taipei Navy in a deal signed in 1991 at a cost of approximately USD2.8 billion, a price alleged to include kickbacks and bribes that facilitated the purchase. Those illicit kickbacks were received by Person A, a Chinese Taipei arms broker, and his family. The illicit assets were later traced to several European countries.

Chinese Taipei started to seek judicial assistance in 2001, and Jurisdiction Z responded positively in September 2006 to the request to freeze illicit funds. Person A and his family members were charged with corruption in the same year, however, they have absconded and remain wanted for the trial. Person A died in 2015 but the case continued against his estate and family.

Following rulings by Chinese Taipei's Supreme Court in 2019 and 2021 that permitted the confiscation of the proceeds (about USD487 million) from the heirs of Person A, MoJ and prosecutors in Chinese Taipei have been in close contact with Jurisdiction Z to have the frozen assets in that jurisdiction returned to Chinese Taipei.

Courts considered the matter and in 2022 made a ruling to the effect that confiscation of proceeds of crime is an equitable measure akin to quasi unjust enrichment rather than a penalty.

In 2022, Jurisdiction Z agreed to return the illicit assets to Chinese Taipei, and in order to express the appreciation for the long-term support and assistance provided by Jurisdiction Z, authorities in Chinese Taipei agreed to share the assets after bilateral negotiation. The illicit funds that entered Jurisdiction Z amounted to about NTD20 million, and after the deduction of the litigation costs and sharing with Jurisdiction Z, Chinese Taipei successfully recovered more than USD10 million. This is the first asset sharing case between Chinese Taipei and the another jurisdiction.

Source – Chinese Taipei

Case study # 134 – International cooperation in relation to repatriation of Proceeds

smuggling; money laundering; international cooperation

In September 2014, Chinese Taipei received a mutual legal assistance request from Jurisdiction X seeking assistance in restraining or seizing criminal proceeds, in a domestic bank account, derived from suspected criminal offenses of money laundering and smuggling by Person A. Chinese Taipei assisted in seizing Person A's bank account with a balance of approximately USD15 million.

During the proceedings, Person A pled guilty and entered into a plea agreement with Jurisdiction X. Person A agreed to voluntarily return the money seized by Chinese Taipei authorities to Jurisdiction X. Accordingly, in May 2020, Jurisdiction X submitted a supplemental

request, asking Chinese Taipei to lift the restraint/seizure to enable the criminal proceeds in the bank account to be transferred to Jurisdiction X.

In March 2022, during the COVID-19 Pandemic, and after continuous negotiations and coordination between Jurisdiction X, Chinese Taipei's MoJ, the domestic bank, Person A and the Assisting Body, Chinese Taipei successfully assisted in wiring approximately USD15 million proceeds of crime to the bank account designated by Jurisdiction X. Negotiations in relation to asset sharing and relevant domestic proceedings are still underway between Chinese Taipei and Jurisdiction X.

Source – Chinese Taipei

5.9 Thailand

Case study # 135 – International cooperation to recover proceeds of crime

fraud; international cooperation

The US FBI requested financial information from AMLO in relation to a fraud case where US persons were the victims and their funds were transferred to Thailand. AMLO investigated and found that all the receiving bank accounts were owned or controlled by Person A. The accounts received a total of 2,662,035.70 baht from the US (USD73,000). Thailand's Civil Court's final verdict was to confiscate and return the funds to the US to compensate the victims.

Source – Thailand

Case study # 136 – Recovery of Proceeds of bribery and corruption from foreign jurisdiction

bribery and corruption; politically exposed person

Person A, a Thai government official and her associates received bribes and kickbacks from a foreign businessman totalling THB60 million (approx. USD1.5 million) in exchange for government contracts. The funds were received in the form of cashier's checks and international funds transfers to Person A's daughter, and other nominees' accounts in a range of foreign jurisdictions.

The National Anti-Corruption Commission (NACC) charged Person A and her associates with corruption and unexplained wealth offences. The Supreme Court sentenced Person A and her daughter to imprisonment and ordered that their assets be confiscated including funds in foreign jurisdictions. Thailand requested enforcement of the Thai Court order through the Mutual Legal Assistance process to recover assets located in five different foreign jurisdictions.

Upon discovery of additional assets in one jurisdiction, the NACC requested AMLO's assistance to seek a Civil Court order to forfeit the funds and request enforcement of the Thai Court's order through the Mutual Legal Assistance process to repatriate USD500,000 to Thailand. The repatriation process is currently underway and Person A and her associates have also been charged with ML offences to be tried in a separate case.

Source – Thailand

6 FATF, FSRBS AND OBSERVERS' RESEARCH PROJECTS & PUBLICATIONS

This section of the report provides a brief overview of typology reports published by the FATF, FATF-style regional bodies (FSRBs) and Observers 2022 - 2023.

6.1 FATF typology reports relevant to ML, TF and PF Risks 2022-2023

6.1.1 *Virtual assets/ Ransomware financing*

The report can be found at:
https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2023.html

A brief summary of the topic

In June 2022, the FATF produced a targeted update on implementation of the Standards on virtual assets (VAs) and virtual asset service providers (VASPs), with a focus on FATF's Travel Rule. This report comes three years after FATF extended its anti-money laundering and counter-terrorism financing (AML/CFT) measures to VAs and VASPs to prevent criminal and terrorist misuse of the sector. The report builds on previous reviews by providing a short update on jurisdictions' compliance with FATF Recommendation 15, as well as exploring emerging risks and market developments.

List of research / project partners
This work was led by the Virtual Assets Contact Group (VACG), co-chaired by Japan and the US. The report also drew on input from the private sector, via ongoing discussions through the VACG.

Key findings, recommendations

The report highlights the need for countries to rapidly implement FATF's Recommendation 15, including the Travel Rule. FATF's Travel Rule requires VASPs and other financial institutions to share relevant originator and beneficiary information alongside VA transactions. The report finds that jurisdictions have made limited progress in implementing this requirement. FATF's report highlights that there are now technological solutions available to facilitate Travel Rule compliance, but notes that the private sector needs to increase interoperability between solutions and across jurisdictions.

On market developments and emerging ML/TF threats, the report highlights the continued need for jurisdictions and the FATF to monitor the growth of and the risks associated with decentralised finance (DeFi), non-fungible tokens (NFTs) markets and unhosted wallets.

6.1.2 *Countering Ransomware Financing 14 Mar 2023*

The report can be found at:
https://www.fatf-gafi.org/en/publications/Methodsandtrends/countering-ransomware-financing.html

Brief summary of the topic
Ransomware has grown in scale globally in recent years. The close link between ransomware and virtual assets is clear: ransomware payments are almost exclusively demanded in virtual assets.

This reinforces the importance of the FATF/VACG's[23] work to strengthen and accelerate the global implementation of the relevant FATF Recommendations for virtual assets and VASPs. With the involvement of virtual assets, competent authorities also need to ensure that they are equipped with the specialised skills and capabilities required to effectively investigate and prevent associated money laundering.

Ransomware attacks are generally underreported, which may have contributed to a lack of experience investigating related ML flows. The decentralised and transnational nature of virtual assets further complicates law enforcement efforts for cross-border funds tracing and asset recovery.

Ransomware is a form of extortion and should therefore be captured as a predicate offence to ML under FATF Recommendation 3. In practice, many jurisdictions pursue ransomware as a form of computer crime, which is not included in the FATF's designated categories of offences. This does not appear to have hampered ransomware-related ML investigations or prosecutions.

List of research/project partners

Experts from Israel and the United States co-led this project.

In addition, the following jurisdictions and entities contributed to the work as part of the project team: Australia, Canada, the European Commission, France, Germany, Japan, Luxembourg, Mexico, Philippines, Singapore, South Africa, Spain, Switzerland, Türkiye, the United Kingdom, the Asia Pacific Group on ML, and the Egmont Group of Financial Intelligence Units.

In total, the project team received inputs from over 40 delegations.

Key findings, recommendations

The global scale of financial flows related to ransomware attacks has grown dramatically in recent years, with industry estimates reporting up to a fourfold increase in ransomware payments in 2020 and 2021, compared to 2019. New techniques have increased the profitability of attacks and the likelihood of success. These include the targeting of large, high-value entities as well as ransomware as a service, where ransomware criminals sell user-friendly software kits to affiliates. The consequences from ransomware attacks can be dire and pose national security threats, including damaging and disrupting critical infrastructure and services.

Through this study, the FATF aims to improve global understanding of the financial flows linked to ransomware and highlight good practices to address this threat. The report also provides a list of potential risk indicators that will help authorities and the private sector detect such financial flows. The findings of this report draw upon experience and expertise from across the public and private sectors, including inputs and case studies from more than 40 delegations across the FATF Global Network.

A ransomware attack is a form of extortion and the FATF Standards require that it is criminalised as a predicate offence for money laundering. This report finds that payments and subsequent laundering of ransomware proceeds are almost exclusively conducted through virtual assets. Ransomware criminals exploit the international nature of virtual assets to facilitate large-scale, nearly instantaneous cross-border transactions, sometimes without the involvement of traditional financial institutions that have anti-money laundering and counter terrorism financing (AML/CFT) programs. Criminals further complicate their transactions by using

[23] FATF Virtual Assets Contact Group

anonymity-enhancing technologies, techniques, and tokens in the laundering process, such as anonymity enhanced cryptocurrencies and mixers.

The near-exclusive use of virtual assets in ransomware-related laundering further reinforces the importance of accelerating the implementation of FATF Recommendation 15, which requires jurisdictions to put in place measures to mitigate risks linked to virtual assets and to regulate the virtual asset service provider (VASP) sector. These efforts are critical to prevent criminals from easily accessing VASPs located in jurisdictions with weak or non-existent AML/CFT controls to launder the profit from their crimes.

This report also finds that ransomware attacks are generally underreported, whether due to challenges in detection by the private sector, negative impacts to the victim's business or a fear of retaliation from criminals if a victim reports an attack. This partly explains the lack of experience in investigating money laundering related to ransomware. Jurisdictions need to carry out further work to increase and enhance sources of detection and reporting. Authorities need to move quickly to collect key information and should have the necessary tools and skills to effectively trace and recover virtual assets.

Ransomware cuts across a wide range of areas and may involve actors outside the traditional AML/CFT authorities, including cybersecurity and data protection agencies. As such, a multi-disciplinary approach is required to effectively tackle ransomware and associated money laundering. Due to the inherently decentralised and transnational nature of virtual assets, building and leveraging existing international co-operation mechanisms is imperative to successfully tackling ransomware-related laundering.

To strengthen the global response against ransomware and related laundering, the FATF proposes that jurisdictions take the following actions:

- Implement relevant FATF Standards, including on VASPs, and enhance detection,
- Promote financial investigations and asset recovery efforts,
- Adopt a multi-disciplinary approach to tackle ransomware,
- Support partnerships with the private sector,
- Improve international co-operation.

6.1.3 *Money Laundering and Terrorist Financing in the Art and Antiquities Market*

The Art and Antiquities market has been exploited by ML and TF groups. The FATF published a report into this typology in February 2023 which can be found at:

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html

Brief summary of the topic

The global trade in art, antiquities, and other cultural objects (hereinafter referred to collectively as cultural objects) is a multi-billion-dollar industry. The estimated value of global sales of art and antiquities in 2021 reached USD 65.1 billion, increasing by 29% from the previous year[24]. The industry is diverse in size, business model and geographic reach.

Although ML/TF activities linked to cultural objects have generated some international attention, the anti-money laundering and combatting the financing of terrorism (AML/CFT) community

[24] Clare McAndrew (2022), The Art Market 2022, Art Basel and UBS, https://d2u3kfwd92fzu7.cloudfront.net/Art%20Market%202022.pdf

traditionally has not focused on assessing the ML/TF threats and vulnerabilities specifically associated with the market.

Criminals, organized crime groups and terrorists are known to have abused markets for art, antiquities and other cultural objects to launder money and fund their activities. The buying and selling of high value works of art, antiquities and other cultural objects can provide an attractive environment for criminals to exploit. The use of cash, potential for anonymity through third party intermediaries and the use of shell companies and other complex corporate structures to complete transactions also represent relevant illicit finance vulnerabilities.

While certain jurisdictions and market participants proactively implement measures to mitigate these risks, many do not take effective action. This FATF report - the first to focus on money laundering and terrorism financing linked to art, antiquities and other cultural objects - highlights how many jurisdictions need to improve their awareness and understanding of the risks associated with these markets and provides advice on how to mitigate the vulnerabilities identified.

List of research/project partners

Experts from the United States and the European Commission co-led this project.
The project team consisted of experts from the following 27 jurisdictions and international organizations: Argentina, Belgium, Brazil, China, Colombia, European Commission, France, Germany, Greece, Guatemala, Iceland, India, Italy, Mexico, Norway, Peru, Russian Federation, Singapore, Switzerland, the United Kingdom, the United States, Europol, the International Monetary Fund (IMF), the International Criminal Police Organization (INTERPOL), UNODC, the United Nations Counter-Terrorism Committee Executive Directorate (UNCTED), and the WCO.

The project relied on information, case studies, and examples provided by 25 jurisdictions of the FATF Global Network and two international organizations, as well as discussions held in a special session of the FATF Joint Experts' Meeting (JEM) on 13 December 2021. The project also solicited and considered the insights of various market participants, the academic community, associations of art and antiquities dealers, and non-profit organizations (NPOs) that responded to a questionnaire and provided comments to the draft reports between August and December 2022.

Key findings, recommendations

Art, antiquities and other cultural objects markets are diverse in size, business models and geographic reach. Most are relatively small, and the vast majority of participants have no connection to illicit activity. Nonetheless, cases over the past decade have demonstrated that this market can be exploited by criminal actors, including money launderers. Items can attract high prices, retain their value, be purchased in cash on behalf of someone else, and be discreetly transferred between people and businesses before being sold for 'clean money'. The relative ease with which small objects of high value, such as antique coins, can be transported across borders also makes them attractive to launderers.

Illicit funds laundered through these markets are generated from crimes that cause significant harm to society, including corruption, drug trafficking and financial crimes. This report outlines typical money laundering methods in the sector, which include hiding or transferring illicit proceeds by concealing the identity of the true buyer, under or overpricing items, and the use of fake sales or false auctions. It also identifies a number of proceeds-generating crimes that occur within these markets, including art forgery, fraud, theft, and illegal trafficking.

Terrorism financing is another risk for those working predominantly in the markets for cultural objects. ISIL notoriously pillaged important archaeological sites in Syria and Iraq, using sales

proceeds and taxes levied on diggers to generate funds. Although ISIL has now lost territory it previously controlled, the group and its affiliates still control territory in other parts of the world. This means they may still have access to cultural heritage sites or possess artefacts that could generate funds. Other terrorist groups, including Al-Qaeda and its affiliates, have also used similar schemes in the Middle East, North Africa and certain parts of Asia. In some cases, transnational organized crime groups have cooperated with terrorist groups to acquire such items and smuggle them out of conflict areas. These criminal groups often use common money laundering techniques, including the use of shell companies and cash transactions, to conceal or disguise the origin of the goods.

There are many challenges to addressing money laundering and terrorism financing in the art, antiquities and other cultural objects markets. The challenges can be broadly split into two distinct categories. The first concerns vulnerabilities related to the type of objects and the nature of the markets. The second category concerns investigative challenges.

To address these challenges, some countries have taken regulatory action to mitigate the money laundering and terrorism financing risks identified. Some have established specialized units and investigative training programs focused on the art, antiquities or cultural objects markets. Some countries have also developed relevant databases and promoted cooperation with experts and archaeologists to help trace, identify, investigate and repatriate cultural objects.

It is vital for jurisdictions and businesses to correctly identify and understand the specific risks associated with different cultural objects and market participants. For example, cultural objects originating from areas where terrorist groups are active can be specifically vulnerable to terrorism financing, as can those from bordering jurisdictions. Businesses working in these markets, such as art dealers and advisors, auction houses and storage facilities, face a variety of risks. Markets for digital art, non-fungible tokens (NFTs), and art finance service providers all have intrinsic characteristics that expose them to different money laundering and terrorist financing vulnerabilities.

The report highlights the importance of rapidly identifying and tracing cultural objects involved in money laundering and terrorism financing, to aid the seizure and confiscation of items, as well as any associated illicit proceeds. The report also encourages cooperation with market participants, including by providing training, guidance and ethical codes. Public-private information sharing can help overcome investigative challenges. Other good practices include the creation of cross-disciplinary networks of experts, enhanced domestic and international information sharing, and working with museums to manage seized artworks and antiquities.

Finally, the report includes a list of risk indicators that can help public and private sector entities identify suspicious activities with links to cultural objects.

6.1.4 *Money Laundering from Fentanyl and Synthetic Opioids 29 Nov 2022*

Each year, opioid trafficking is generating tens of billions of dollars for organised crime groups and contributing to the premature deaths of tens of thousands of people. In November 2022, the FATF published a report into the laundering of profits generated from manufacturing and trafficking synthetic opioids.

***Money Laundering from Fentanyl and Synthetic Opioids 29 Nov 2022* can be found at:**

https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Money-laundering-fentanyl-synthetic-opioids.html

Brief summary of the topic

The organised criminal production and trafficking of synthetic opioids generates revenues worth tens of billions of dollars annually[25], while overdoses kill tens of thousands each year[26]. Taking the profits out of synthetic opioid trafficking is one of the most effective ways to address a growing transnational crime and a public health emergency in several countries.

Organized crime groups are fueling a synthetic opioid crisis that has contributed to hundreds of thousands of drug overdose deaths in the past decade.

In North America, the non-medical use of fentanyl is the main driver behind a record number of overdoses and opioid-related deaths. In parts of Africa, a tramadol epidemic is having a significant impact on public health. While across Asia, many countries report a growing number of cases.

This report aims to (1) assist law enforcement and other operational authorities in carrying out effective financial investigations and prosecutions related to the proceeds from the trafficking of illicit synthetic opioids and to (2) raise awareness and contribute to the existing literature regarding the devastating impact of synthetic opioids trafficking. Based on lessons learned, this report will assist law enforcement authorities and relevant stakeholders by providing risk indicators and recommendations to detect and tackle the financial flows from synthetic opioid trafficking. The report provides operational and policy options and tools to detect, investigate and disrupt the finance that supports organised criminal groups and related professional money launderers. The findings for this report are based on case studies and good practices from 40 countries, alongside information and analysis gathered from the project team's consultations with law enforcement and civil society.

This report looks at the way proceeds are laundered from synthetic opioids trafficking. Organized crime groups use a range of methods including bulk cash smuggling, cash couriers, trade-based money laundering and virtual assets (crypto), as well as shell companies and the services of professional money launderers.

List of research/project partners

Experts from Canada and the United States co-led this project.

A project team was formed composed of 10 countries and two observer organisations (Australia, Canada, India, Mexico, Russia, Singapore, South Africa, Turkey, United States, Ukraine; observers include Interpol and UNODC).

The project team received inputs from questionnaires from 25 FATF and FSRB delegations in May 2022 (Australia, Germany, Canada, Mexico, Nigeria, Belgium, Estonia, Greece Seychelles, Luxembourg, Norway, the Netherlands, Sweden, Japan, Senegal, Russia, Serbia, Singapore, Slovak Republic, Slovenia, South Africa, Spain, Sweden, Switzerland, and Turkey). In May-July 2022, the co-leads co-ordinated a series of bilateral discussions with relevant experts from countries and observers that the project team co-leads have identified as high-risk or high-relevance to the project (India, Netherlands, Finland, Interpol, Europol, UNODC).

[25] Eurojust (2021), "Eurojust Reporting on Drug Trafficking".
[26] US Center for Disease Control and Prevention (2022) "Understanding the Drug Overdose Epidemic"; Canada (2022) "Opioid- and Stimulant-related Harms in Canada" and EMCDDA (2022) "Drug Overdose Deaths in Europe".

Key findings, recommendations

Synthetic opioids supply chains are diverse, and so are the methods used to launder the proceeds. There does not appear to be a single, global "business model". Rather, the methods vary on a jurisdiction-by- jurisdiction and drug-by-drug basis.

Organised crime groups who traffic in synthetic opioids use a range of methods to move the illicit proceeds across borders. These include bulk cash smuggling; cash couriers; trade-based money laundering; un-authorised money or value transfer services or the banking system; and money brokers. Criminal groups also use dark web vendor sites to market their products and, in some cases, take payment through virtual assets, some of which are anonymity-enhancing. These virtual assets are often quickly converted into fiat currency. Traffickers use shell and front companies to launder proceeds, but also procure drugs, precursor chemicals and production equipment with the proceeds.

Whereas fentanyl was procured in the past directly from chemical producers, the class-wide scheduling of most fentanyl-related substances means that today, criminals use precursor chemicals to manufacture drugs such as fentanyl. This relatively recent trend can make it difficult to detect suspicious financial activity.

Like other forms of drug trafficking, professional money-laundering networks provide their services to drug traffickers and organised crime groups. For example, there is evidence that Asian money laundering organisations co-ordinate transfers of value, by using methods that do not require money to move directly across international borders (e.g., mirror and hawala-style transfers, and other money value transfer services).

Many authorities do not fully understand the global money flows from opioids, or do not know how to identify potential procurement of chemicals, or laboratory and other specialised production equipment. In some jurisdictions, relevant authorities and reporting entities such as banks and money value transfer services look at opioids trafficking through a domestic lens, whereas this illicit trade involves major transnational organised crime groups and professional money launderers.

Even though a majority of countries identify drug trafficking as a major predicate offence for money laundering, the number of investigations and prosecutions concerning the laundering of proceeds from synthetic opioids trafficking remains low. This report aims to raise awareness about the opioid trade, including the use of precursor chemicals, and the related global financial flows. It also makes recommendations on the best approaches to detect and disrupt the criminal networks involved. These include:

- Improving risk understanding in this area, including regarding supply chains and the role of the pharmaceutical industry, to develop more robust legal and regulatory frameworks to combat the trade in illicit opioids.
- Training prosecutors and relevant authorities to carry out financial investigations, including in the precursor supply chain.
- Identifying and leveraging existing mechanisms to expand international cooperation between source, transit and destination countries to identify and disrupt synthetic opioid supply chains.
- Using public-private partnerships to raise risk awareness, of dark web marketplaces and virtual assets (crypto), share red flag information and help the private sector better identify and report suspicious activity.

The report includes relevant risk indicators that will help identify potential trafficking of illicit

synthetic opioids.

6.1.5 *ISIL, Al-Qaeda and Affiliates Financing*

Brief summary of the topic

The FATF has been regularly collecting and analysing information with the assistance of FSRBs members 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 contact their FATF representatives should they want a copy of the FATF's latest report (adopted in February 2023).
FACT links:

June 2022 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2022)10/REV2/en
October 2022 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2022)20/REV1/en
February 2023 - https://fact.fatf-gafi.org/official-document/FATF/RTMG(2023)9/REV2/en

6.2 FSRBs' and Observers' Projects 2022-2023

6.2.1 *Caribbean Financial Action Task Force*

The Caribbean Financial Action Task Force (CFATF) publishes regular education pieces providing a snapshot of crime types and associated ML typologies. During 2022-2023, papers were published in relation to modern slavery/human trafficking, environmental crimes and financial investigation of the illegal wildlife trade, the role of shell companies and beneficial ownership structures to facilitate ML, amongst other topics.

Further information can be located at the CFATF's Research Corner: https://www.cfatf-gafic.org/home/cfatf-research-corner

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

In May 2023, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL) adopted a report prepared by a project team of experts, led by the Isle of Man, into the ML and TF risks associated with Virtual Assets and their service providers.

Money Laundering and Terrorist Financing Risks in the World of Virtual Assets can be found at: https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4

The report reviews MONEYVAL members' compliance with Recommendation 15 of the FATF standards in relation to virtual assets and assesses the regulatory frameworks for supervision of VASPs and the intersection between Law enforcement and VASPs.
The report identifies risk features associated with virtual assets and highlights good practices in a risk based approach to dealing with a challenging sector.

6.2.3 *Eurasian Group*

1) **ML/TF risk assesment in the Eurasian region (link to the EAG website) – the project has been undertaken by the project team consisting of EAG mebers and the Secretariat. Adopted in June 2022.**

According to the Methodology for the purposes of this round of the project (assessment of observable ML/TF schemes (methods)), the ML/TF risks with common features and characteristic for two or more Eurasian Group (EAG) Member States, as well as those of cross-border nature, were considered as regional risks. However, ML/TF risks are not identical across the entire territory of the Eurasian region. Therefore, the specificities typical for individual sub-regions of the Eurasian region (East European, EAEU, Central Asian) were taken into account, in particular when determining the nature of existing threats, vulnerabilities and risks. The data obtained was subsequently compared with other information received from EAG member states and observers, available credible information from other sources, as well as information received from private sector actors, including during information gathering meetings, and data provided by other jurisdictions involved in cross-border money laundering and terrorism financing schemes. While the regional risk assessment covers the period since 2017 through 2020, presented in the report are also certain ML/TF trends observed by the countries later, e.g. as a result of deterioration of the situation in Afghanistan in 2021.

Money laundering threats

As per the Methodology, the ML threat refers to the criminal activities of individuals that generate criminal proceeds that are involved in money laundering processes. An increased level of threat is posed by such criminal activities carried out by organized criminal groups and criminal organizations.

The following most relevant threats have been identified at the level of the Eurasian region:

#	Type of threats
1	Tax and other mandatory payment evasion and other tax crimes (including VAT manipulation (fraud))
2	Bribery and other corruption-related offences (including misuse of the state budget funds)
3	Fraud (including misuse of the state budget funds)
4	Illicit trafficking in narcotic drugs, psychotropic substances and their precursors
5	Evasion of customs duties and fees and other customs offences
6	Pyramid scheme activities
7	Illegal business activity
8	Organization of illegal migrant smuggling

Collation of threats, vulnerabilities and institutional factors affecting them resulted in the identification of the flowing regional ML risks or their key elements in complex schemes of ML:

Regional risks requiring significant attention and enhanced risk mitigation measures	
1.1	Using nominee/controlled companies or individual entrepreneurs
1.2	Investment of proceeds of crime in the economic activity of legal entities, including those located in third countries
1.3	Using schemes (including fictitious ones) for the acquisition/sale of the real estate and other property in/out of the jurisdiction
1.4	Conducting "transit" operations involving bank accounts
1.5	Conducting cash-out operations

1.6	Withdrawal of criminal proceeds outside the region with subsequent return to the region in the form of investments in legitimate business activities
1.7	Using offshore companies
Regional risks requiring on-going monitoring and enhanced risk mitigation measures	
2.1	Through misuse of the securities market, including through transactions involving the purchase and sale of securities
2.2	Using electronic payment instruments and of virtual assets
2.3	Using money transfer systems without opening an account
Regional risks requiring standard risk mitigation measures	
3.1	Withdrawal of funds abroad using enforcement instruments

Regional terrorism financing risks

The project team's analysis identified the following terrorism financing risks specific to the region:

- online fundraising in the Internet;
- fund raising and movement of funds by relatives of terrorists to meet their basic needs;
- movement of funds using bank accounts and cards;
- physical movement of cash;
- movement of funds by way of transferring money without opening bank accounts (money transfer systems and electronic means of payment);
- use of funds to finance members of terrorist organizations by providing material assets, goods, uniform and services to them.

2) Laundering of the proceeds from tax and economic crimes – (link to the EAG website) Led by the Kyrgyz Republic, adopted in November 2022.

The project provides an overview of the current status of the national AML/CFT systems to combat tax and business crimes, including the review of the legislation, available sanctions, roles of the competent authorities, features of the detection and investigation of such crimes. Furthermore the leader of the project has analyzed the involvement of FIUs in combating ML from these crimes, along with red flag indicators, STRs, various tools and sources of information. Lastly the report contains a few cases and examples of ML methods/tools used.

3) Legalization (laundering) of the proceeds of cybercrime, as well as financing of terrorism from the said offence, including through the use of electronic money or virtual assets and the infrastructure of their providers – (link to the EAG website) led by the Russian Federation, adopted in November 2022.

The report focuses on legislative developments in the recent years on VA and VASPs, as well as provides an overview on the role of the private sector and how VASPs are being categorized in the EAG members. Furthermore, the project provides an overall information on various ML typologies, detection and investigation techniques, as well as a few examples of TF methods involving VAs.

6.2.4 *Eastern and Southern Anti-Money Laundering Group*[27]

Illicit dealings in Gold, Diamond, Rubies and associated money laundering/Terrorist Financing in the ESAAMLG Region:
https://www.esaamlg.org/reports/ILLICIT_DEALING_SEPT_2022.pdf

Eastern and Southern Anti-Money Laundering Group (ESAAMLG) published this report into ML and TF trends in the precious stones and metals (PMS) markets, in September 2022. The report is the culmination of a research study led by Eswatini and Zambia as co-chairs and supported by six Member States and the UNODC.

The report identifies that PMS provide a mechanism to convert illicit cash into a stable, anonymous and easily exchangeable asset. PMS have also been used as an alternative currency to purchase weapons or drugs. The use of PMS to fund terror groups was identified as a potential risk.

The report includes a number of cases studies and concludes with key findings and recommendations including the need to build capacity of regional FIUs and improve information exchange between jurisdictions.[28]

6.2.5 *Inter-Governmental Action Group against Money Laundering in West Africa*[29]

Inter-Governmental Action Group against Money Laundering in West Africa (GIABA) Assessment Report (2022), Beneficial Ownership Information and Asset Recovery Framework in West Africa, GIABA, Dakar, Senegal:
https://www.giaba.org/media/f/1296_Beneficial%20Ownership%20Information%20and%20Asset%20Recovery%20Framework.pdf

This report examines the legal, regulatory and compliance framework for beneficial ownership information in selected Member States and the associated ML/TF risks. The report also reviews asset recovery and asset management in the selected Member States.
GIABA's project team undertook research with key private and public stakeholders and collaboration with its development partners including the FATF, US Treasury and World Bank.

The report concludes that West African countries are vulnerable to ML and TF through the inability to identify beneficial owners of companies, trusts and other legal persons. The lack of adequate information about beneficial ownership results in poor investigation, and rare prosecutions and convictions. In addition, the asset recovery framework is little understood and rarely used heightening the region's vulnerability to ML and TF risks.

Recommendations in the report include:

- Undertaking risk assessments.
- Developing legislation for beneficial ownership disclosure and a national register for recording same.
- Creating specialised asset management agencies with dedicated databases listing assets and properties and centralised management of recovered assets.
- Engagement with training and technical assistance.

GIABA Typologies Report (2022) Money Laundering and Terrorist Financing through Corruption in West Africa, GIABA, Dakar, Senegal:

[27] This summary has been prepared by the APG Secretariat from publicly available information.
[28] This summary has been prepared by the APG Secretariat from publicly available information.
[29] These summaries have been prepared by the APG Secretariat from publicly available information.

This report can be found at:
https://www.giaba.org/media/f/1300_Money%20Laundering%20and%20Terrorist%20Financing%20through%20Corruption.pdf

This report identifies corruption as a continuing major obstacle to the emergence of West African economies. Corruption, especially involving public authorities is a major source of enrichment and money laundering.

Relevant data was collected from Member States and extensive engagement with public and private sector stakeholders was undertaken to identify eight ML typologies, supported by case studies. The typologies identified are categorised as follows:

- Use of corruption as an obstacle to AML/CFT.
- Money laundering by Politically Exposed Persons (**PEPs**).
- Laundering of proceeds of corruption by Public Officials.
- Laundering of proceeds derived from abuse of position, illicit enrichment, misappropriation of public funds.
- Laundering of proceeds derived from user fees for public services.
- Laundering of proceeds of corruption through legal persons and arrangements.
- Laundering the proceeds of corruption through "Door Openers or "Gatekeepers".
- Laundering the proceeds of corruption through Charitable organisations.

15 strategic recommendations and 14 operational recommendations are made highlighting the need to enact legislative reforms and strengthen the capacity of, and information sharing between, AML/CFT entities, FIUs and government regulators.

GIABA (2021) Research and Documentation Report, An Assessment of the Challenges Associated with the Investigation, Prosecution and Adjudication of Money Laundering and Terrorist Financing in West Africa, Assessment Report, GIABA, Dakar.

This report can be found at:
https://www.giaba.org/media/f/1302_An%20Assessment%20of%20Challenges.pdf

The report provides an overview of the AML/CFT situation in West Africa and the practical challenges on the policy front and at the operational level in AML/CFT enforcement. The FATF provided technical assistance to the project group.

The study was initiated in the context of an unsatisfactory level of criminal justice response to an increasingly complex criminal environment experienced by the Member States.

At a general level, the report found:

- West African countries are making significant efforts to prevent their territories from becoming safe havens for criminals however the fight against ML and TF is challenging in the context of porous borders, cash economies and a low level of digitalization of administrative services.
- In spite of many actions taken to enact legislative reforms, create new institutions and undertake capacity building, enforcement measures especially in the investigation and prosecution of ML and TF offences are not having a deterrent effect.

On the policy front, the report found:

- AML/CFT frameworks do not take into account individual risk profiles of jurisdictions.
- Political intrusion into law enforcement impacts integrity and independence, especially when PEPs involved.
- Inadequate understanding of AML/CFT by the criminal justice system.

- Ineffective inter-agency collaboration.
- Autonomy of FIUs is insufficient or not guaranteed.
- Ineffective international cooperation and mutual legal assistance and that confiscation of proceeds is not a priority area.

At the operational level, the report found:

- Judicial statistics for trial of ML/TF are very low and not indicative of the statistics for relevant predicate offending. Also where confiscation orders are made the lack of enforcement documents is an impediment to asset recovery.
- Judicial practitioners and experts are unfamiliar with the international cooperation mechanisms available and resort to inefficient channels for assistance.
- The lack of technology and systems for recording civil status (such as land title documents) is an impediment to compiling admissible evidence for the Judicial phase.
- Judges and prosecutors have little experience of AML/CFT legal framework and continue to require proof of predicate offending.
- A low level of financial intelligence in the Judiciary, prosecutors and other legal personnel.
- Criminal justice actors are not well informed about ML typologies and investigators do not often run parallel financial investigations which would support ML prosecutions.

Eight recommendations, together with implementation strategies, have resulted:

1. Provide resources and capacity to entities involved in the investigation, prosecution, and adjudication of AML/CFT cases, particularly the Financial Information Units, criminal investigation officers, judges and magistrates, bailiffs, anti-corruption agencies, agencies in charge of asset recovery and State judicial agencies
2. Strengthen the capacity of all entities involved in the investigation, prosecution and adjudication of money laundering and terrorist financing cases
3. Improve the understanding of the public in general and particularly judges and magistrates of national AML/CFT laws, particularly with respect to the judicial handling of evidence in ML or TF cases.
4. Promote systematically and as a matter of urgency inter-agency cooperation in the fight against money laundering and terrorist financing.
5. Strengthen the political commitment to fight against corruption in the criminal sector, money laundering and terrorist financing.
6. Prioritize the understanding by the actors of the criminal chain of ML/TF methods and techniques in the sub region.
7. Strengthen the mechanism for regional cooperation in the investigation, prosecution and adjudication of money laundering and terrorist financing cases.
8. Enhance the specialised judicial handling of ML/TF offences.

6.2.6 *Middle East and North Africa Financial Action Taskforce*[30]

(1) Middle East and North Africa Financial Action Taskforce (MENAFATF) Biennial Typologies Report 2022 – fifth edition

This report analyses the most prominent patterns of ML and TF in the region based upon 44 case studies submitted by member countries and can be found at:
https://www.menafatf.org/information-center/menafatf-publications/menafatf-biennial-typologies-report-2022

The first category of cases involve more than one instance. The typologies for these cases are:

1. Corruption/Laundering the proceeds of corruption (8).

[30] These summaries have been approved by MENAFATF.

2. Laundering of proceeds from tax offenses (4).
3. ML resulting from Trafficking in Drugs (4).
4. Trafficking in Human Beings and Smuggling of Migrants (3).
5. Use of virtual currencies/assets (2).
6. Use of new payment methods (such as T Pay) (3).
7. Trade Based ML (2).
8. Use of fake (shell) companies (2).
9. Parallel Banking Services / Alternative Transfer Services / Hawala (2).
10. Smuggling of Currency (2).

The second category of typologies involved only one case each:

1. Gambling Activities.
2. Trade in Precious Stones (jewellery).
3. Distorting competition and spoiling the investment climate (pyramid scheme).
4. Use of social media channels in TF (raising donations via social media – payments made in small amounts to a post office account).
5. Use of Offshore Non-Resident Banks, IBCs, and Trusts.
6. Investing in the capital markets and the use of intermediaries (minor children of suspect).
7. Smuggling of Gold (using camels).

The report includes data about the entities exploited and the number of cases under investigation, referred for prosecution or before the Courts.

A list of 30 important indicators of suspicious activity are extracted from the case analysis.

(2) Typologies Project Report on the abuse of NPOs in TF Activities – November 2022

This report is the result of a project to understand and examine the level of risk of abuse of NPOs in Member Countries by TF operations and to identify best practices to address such abuse without interfering with NPOs' legitimate activities.

The report can be found here: https://www.menafatf.org/information-center/menafatf-publications/typologies-project-report-abuse-npos-tf-activities

MENAFATF secretariat issued two questionnaires to collect information from the public sector (FIUs, LEAs, regulators of NPOs) and from the private sector and the NPOs themselves. Case studies were also sought from member countries and research undertaken from open source data and publications including the FATF and APG reports into this particular typology.

The ML/TF risks to the NPO sector are two-fold. Firstly through the exploitation of legitimate NPOs and secondly, through the creation of fictitious NPOs.

Case studies detailed within the report included the placement of a member of a TF organisation on a NPO board of trustees. Others involved the attempted creation of bank accounts for fake NPOs.

One study involved a charitable organisation for the welfare of children where it was found that funds were being diverted to the association's president and the children were being ill-treated and subjected to economic exploitation (agricultural and construction work) while also being indoctrinated with extremist ideas.

6.2.7 *Egmont Group*[31]

FIU – FinTech Cooperation and Associated Cybercrime Typologies and Risks

The Egmont Group published a report in July 2022 exploring the world of financial technology (FinTech) and the threats and vulnerabilities associated with new payment services and products.

The report can be found at:
https://egmontgroup.org/wp-content/uploads/2022/11/2022-Report-on-FIE-FinTech-Cooperation-and-Assoc.-Crimes.pdf

FinTech is a loosely defined term but includes computer programs and other technology to support or enable banking and financial services.

Common examples of FinTech identified in the report include internet and mobile banking, digital or electronic currencies, money transfer platforms, non face-to-face investments (robo-technologies), crowdfunding platforms and VASPs.

FinTech is the future face of financial services but the report finds that the mechanics behind FinTech products and services is little understood by FIUs and ML/TF threats and vulnerabilities associated with their exploitation is not fully appreciated. Whilst Recommendation 15 requires jurisdictions to address risks arising from new and emerging technologies, not all FinTech entities are reporting entities for the purposes of regulation.

This Egmont Group project aimed to:
- Provide an understanding of how FinTech entities cooperate with FIUs in Egmont Group member jurisdictions;
- Explore the regulatory environment in which they operate; and,
- Define potential best practices to engage with the FinTech sector.

The project group received input from 41 members across the globe. Sixteen case studies highlight the variable ways in which the FinTech sector can be exploited and the challenges for FIUs to understand data provided to them and to trace or obtain information where FinTechs are incorporated in foreign jurisdictions.

The most reported typologies involved fraud and the use of virtual assets and bank accounts held by shell companies.

In conclusion, the report noted that regulation of VASPs and blockchain technology is not yet in place in many jurisdictions and where it is, the classification of services and products varies, resulting in differing responses to risk and complicating the ability to trace international financial flows.

The report recommends that financial analysts maintain a baseline understanding of the mechanics behind FinTech products and services and how to interpret the data they provide in financial intelligence reports.

The report also recommends spontaneous streamlined dissemination of information between FIUs to enhance law enforcement internationally. To ensure appropriate mitigation of risk in this

[31] These summaries have been prepared by the APG Secretariat from publicly available information.

sector, FIUs need to agree on a standard reporting format in partnership with FinTech entities and each other.

Use of Open-Source in FIU Operational and Strategic Analysis can be found at: https://egmontgroup.org/wp-content/uploads/2023/07/202302-IEWG-Report-Use-of-OSINT-in-FIU-Operational-and-Strategic-Analysis-Sanitized-Version_FINAL3.pdf

The Egmont Group's Information Exchange Working Group has published a report in relation to the use of open source intelligence (**OSINT**) by FIUs for their operational and strategic analysis. The report applies thematic and descriptive statistical analyses to qualitative and quantitative data collected from sixty-one FIUs. The findings in the report cover:

- The number of FIUs that use OSINT.
- How OSINT is utilized.
- How OSINT and financial intelligence are compiled.
- Types of OSINT used.
- Methods used to determine OSINT reliability.
- Availability of dedicated OSINT teams and the development of OSINT tool.

The report concludes that OSINT is a valuable resource for development of typologies, identifying ML/TF trends at a macro level and identifying linkages between individuals and legal persons and other activities or persons, which are not otherwise available from suspicious transaction reports.

7 Abbreviations, Acronyms, and currency exchange rates

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
ASIC	Australian Securities and Investments Commission
ATM	Automatic Teller Machine
ATO	Australian Taxation Office
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
MLO	Money laundering organisation
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
PoE	Panel of Experts
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	Terrorism 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

Exchange rate table

Throughout this report, domestic currency values of the submitting jurisdiction have been used, except if the jurisdiction has chosen to convert the value to an approximate United States Dollar (USD) amount. The below currency conversion chart provides single point in time exchange rate on 8 November 2023, as provided by XE. The 'Conversion to USD' column represents how much USD could be exchanged for one unit of corresponding currency.

Jurisdiction	Currency (1 unit)	Abbreviation	Conversion to USD
Australia	Australian Dollar	AUD	0.643
Bangladesh	Bangladeski Taka	BDT	0.009
China	Chinese Yuan Renminbi	CNY	0.137
Cook Islands	New Zealand Dollar	NZD	0.593
European Union	Euro	EURO	1.069
Hong Kong, China	Hong Kong Dollar	HKD	0.127
Indonesia	Indonesian Rupiah	IDR	0.000063
Japan	Japanese Yen	JPY	0.006650
Korea, Republic of	South Korean Won	KRW	0.000766
Macao, China	Macau Pataca	MOP	0.124
Malaysia	Malaysian Ringgit	MYR	0.214
Mongolia	Mongolian Tughrik	MNT	0.000289
Pakistan	Pakistani Rupee	PKR	0.003
Philippines	Philippine Peso	PHP	0.017
Singapore	Singapore Dollar	SGD	0.738
Solomon Islands	Solomon Islander Dollar	SBD	0.118
Chinese Taipei	Taiwan New Dollar	TWD	0.031
Thailand	Thai Baht	THB	0.028

8 Index

References to numbers against indexed terms relate to page numbers across this Report.