APG Yearly Typologies Report 2025

Methods and Trends of Money Laundering, Terrorism Financing and Proliferation Financing.

November 2025

Asia/Pacific Group on Money Laundering

Table of contents

FOREWORD 4

METHODOLOGY 5

APG YEARLY TYPOLOGIES REPORT 2025 - AT A GLANCE 0

1 - CYBER SCAM HUBS AND HUMAN TRAFFICKING 7

1.1 Overview 7

1.2 Initial Findings 7

Sources of funds 7

Victim profiles 8

Money laundering typologies 10

Enabling conditions 12

Challenges for law enforcement responses 13

Emerging Threats 14

1.3 Conclusion and Recommendations 14

2 - MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING METHODS 15

Money laundering 15

2.1 Bangladesh 15

2.2 China 17

2.3 Hong Kong, China 17

2.4 Indonesia 22

2.5 Japan 25

2.6 Korea 27

2.7 Macao, China 28

2.8 Malaysia 30

2.9 Mongolia 31

2.10 Myanmar 33

2.11 New Zealand 34

2.12 Pakistan 35

2.13 Philippines 37

2.14 Samoa 43

2.15 Singapore 45

2.16 Chinese Taipei 49
2.17 Vietnam 52
Terrorism financing 54
2.18 Indonesia 54
2.19 Philippines 54
Proliferation financing 55
2.20 Singapore 55
2.21 Chinese Taipei 55

3 - MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING TRENDS 57

3.1 Recent research or studies on ML/TF methods and trends 57
3.1.1 Hong Kong, China 57
3.1.2 Indonesia 57
3.1.3 Japan 58
3.1.4 Macao, China 59
3.1.5 Malaysia 59
3.1.6 New Zealand 60
3.1.7 Philippines 60
3.1.8 Singapore 60
3.1.9 Chinese Taipei 61
3.1.10 United Arab Emirates 61
3.2 Observations on emerging trends; declining trends; continuing trends 62
3.2.1 Hong Kong, China 62
3.2.2 Indonesia 62
3.2.3 Japan 63
3.2.4 Macao, China 64
3.2.5 Malaysia 65
3.2.6 New Zealand 65
3.2.7 Chinese Taipei 65
3.2.8 United Arab Emirates 67
3.2.9 Vietnam 68
3.3 Effects of AML/CFT legislative, regulatory or law enforcement countermeasures 69
3.3.1 Hong Kong, China 69
3.3.2 Indonesia 70
3.3.3 Japan 70
3.3.4 Macao, China 71
3.3.5 Malaysia 72
3.3.6 Singapore 73

3.3.7 Chinese Taipei 76

4 - ASSET RECOVERY METHODS AND TRENDS 78

4.1 Asset tracing and investigation, provisional measures and confiscation. 78

4.1.1 Hong Kong, China 78

4.1.2 Indonesia 79

4.1.3 Macao, China 80

4.1.4 Philippines 80

4.1.5 Singapore 81

4.1.6 Chinese Taipei 83

4.1.7 United Arab Emirates 84

4.2 Managing frozen/seized assets: information on asset management cases and procedures or manuals available to agencies involved in asset management. 85

4.2.1 Macao, China 85

4.3 Asset confiscation: experience with the application of criminal, civil or administrative processes to recover proceeds of crime – successes and challenges. 86

4.3.1 Macao, China 86

4.4 Use and sharing of confiscated proceeds: including cases of repatriation of confiscated assets to/from other jurisdictions. 86

4.4.1 Macao, China 86

4.4.2 Chinese Taipei 86

5 - FATF, FSRBS AND OBSERVER ORGANISATIONS' PROJECTS 87

5.1 Financial Action Task Force 87

FATF-style regional bodies 88

5.2 Eurasian Group on Combating Money Laundering and Financing of Terrorism 88

5.3 The Middle East and North Africa Financial Action Task Force 90

Observer organisations 92

5.4 Asian Development Bank 92

5.5 International Monetary Fund 93

5.6 United Nations Office on Drugs and Crime 95

6 - ABBREVIATIONS, ACRONYMS AND CURRENCY EXCHANGE RATES 98

7 - INDEX 100

FOREWORD

Welcome to the 2025 APG Yearly Typologies Report.

The Asia/Pacific Group on Money Laundering (APG) has an incredibly diverse remit across 41 active members, eight observer jurisdictions and 36 observer organisations and we are the largest FATF-style regional body. Within our membership alone, we have a diverse range of unique perspectives in areas such as economies - from some of the largest economies in the world, through to micro economies - and vast diversity of cultures and history. However, despite this diversity, we share similar challenges related to implementing AML/CTF/CPF systems within jurisdictions, and law enforcement more broadly. Given the transnational nature of criminality, history has repeatedly demonstrated the ongoing challenge that jurisdictions/regions have with the displacement of this criminality. As jurisdictions/regions more effectively address certain crime types, we have seen them move to other jurisdictions/regions where there are greater challenges with the implantation of AML/CTF/CPF systems.

This ongoing challenge underscores the importance of the APG's typologies program of work, of which the Yearly Typologies Report is a key component.

The Yearly Typologies Report gives our members a great opportunity to highlight some of their successes in addressing this criminality, and improvements in implementing AML/CTF/CPF systems within their jurisdictions. However, more importantly the Yearly Typologies Report gives our members a timely, relevant and detailed mechanism for *learning from each other*. It provides our members the opportunity to share with fellow members the crime types they are encountering, an overview of how the addressed them, and what challenges they faced in addressing them.

This report, complemented by the annual APG Typologies Workshop and our 2025 Typologies Project, highlights the commitment of our members to identifying and tackling evolving typologies, most particularly through our typologies project examining cyber scam hubs and human trafficking. This exemplifies the spirit of collaboration and trust that has been vital to the APG's success in addressing regional challenges and informing global responses.

I would like to sincerely thank APG's members, observer members, observer organisations and our colleague FATF-style regional bodies for their valuable contributions to this report. I would also like to thank dedicated staff of the APG Secretariat for their great work in compiling this report.

The APG Secretariat is exceptionally proud to support such a diverse, professional and engaged body of members and observers, and our collective output as demonstrated in this report is world class.

Dr Chris Black
Executive Secretary
Asia/Pacific Group on Money Laundering Secretariat

Images: 2024 APG Typologies Workshop, held in Kuala Lumpur, Malaysia.

METHODOLOGY

The Asia/Pacific Group on Money Laundering (APG) is the FATF[1]-style regional body (FSRB) for the Asia/Pacific region. One of the mandates of the APG is to publish regional money laundering (ML), terrorism financing (TF) and proliferation financing (PF) typologies reports to assist governments and other stakeholders to better understand the nature of existing and emerging ML/TF/PF threats and pursue effective strategies to address those threats. When a series of ML/TF/PF 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/TF/PF, as well as design and implement effective preventive measures.

Each year APG members and observer organisations 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/TF/PF. Many cases or findings of assessments cannot be shared publicly due to their sensitive nature or due to ongoing investigative/judicial processes.

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.

[1] Financial Action Task Force: https://www.fatf-gafi.org/en/home.html

APG YEARLY TYPOLOGIES REPORT 2025 - AT A GLANCE

Overview

17 member jurisdictions and **one** observer jurisdiction shared their case studies.

Over **40% of the active members** contributed case studies to the report including:

- **15 members from Asia, one member from CANZUS and one member from the Pacific.**

114 case studies in total are presented in this report.

Focus Area – Asset Recovery

Members shared case studies that illustrated successful actions by competent authorities related to:

- Asset restraint including 'stop payments' related to frauds.
- Seizures of monies, securities and real estate properties (including the seizure and management of a four-star hotel).
- Asset recovery and restitution including monies and virtual assets.

Key themes - ML/TF/PF Case Studies

The key themes emerging from the case studies, across the following categories are:

Predicate offences:

- Various types of fraud: 67 case studies (59%).
- Organised criminal syndicates: 16 case studies (14%).
- Foreign predicate offences:15 case studies (13%).

Types of money laundering:

- Third-party laundering: 40 case studies (35%).
- Self-laundering: 10 case studies (9%).

Channels used:

- Financial institutions: 63 case studies (55%).
- Virtual asset service providers: 13 case studies (11%).
- Money value transfer services: 11 case studies (10%).

Payment methods:

- Cash: 37 case studies (32%).
- Credit cards/cheques: 13 case studies (11%).
- Virtual assets: 13 case studies (11%).

Context:

- Use of legal persons and arrangements: 22 case studies (19%).
- International cooperation: 17 case studies (15%).
- Transnational crime: 15 case studies (13%).

Summary of ML/TF/PF Trends

Members noted the following ML/TF/PF trends in 2024:

Predicate offences - members identified fraud, corruption, illicit drug trafficking, organised crime, and smuggling, illegal gambling/illegal betting and unlicensed moneylending and the fraudulent use of credit cards. One member noted an increase in foreign predicate offences.

A number of members noted fraud including cyber enabled fraud and scams becoming more prevalent (with one member noting it accounted for the largest share of overall crime (46.95%), representing a rise of 11.7% compared with 2023. The rise in fraud also led to the sharp rise in money laundering cases.

Money laundering - members identified the use of cash including face-to-face handovers, mule bank accounts, peer to peer virtual asset transactions, third-party payment platforms, prepaid payment instruments, and purchase of luxury goods, real estate property and vehicles in ML cases.

A number of members noted the banking sector continues to be the most predominant vehicle exploited for ML activities, while also noting the emergence of virtual asset exchanges and third-party payment platforms for money laundering, including exploiting crypto ATMs to launder proceeds of crime.

Terrorism financing - members noted cross-border online payments and fast payment systems, as well as crowdfunding as new and emerging risk areas. The vulnerability of non-profit organisations for TF remained.

Proliferation financing - members noted the geographical proximity to DPRK, globally significant international financial centres, the misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods, misuse of virtual assets and fundraising activities through dark web.

Competent authorities - members noted the need for enhanced financial risk controls, strengthened supervision of virtual asset service providers including implementation of the travel rule, strengthened intelligence sharing, and the ongoing cross-border financial flows highlight the need to strengthen international cooperation.

1 - CYBER SCAM HUBS AND HUMAN TRAFFICKING

1.1 Overview

In recent years, cyber-enabled fraud operations have escalated to industrial-scale enterprises, often orchestrated by transnational organised criminal syndicates. These criminal syndicates frequently conceal their operations within industrial or science and technology parks, establishing what are commonly referred to as 'cyber scam hubs'. These hubs have emerged as a significant challenge to APG member jurisdictions.

Southeast Asia has become a hub for online fraud operations. These areas host thousands of individuals trafficked into cyber scam hubs, predominantly located along border zones and within designated special economic zones.

The economic impact of cyber scam hubs is substantial. It is estimated that the amount of money the cyber scam industry in Southeast Asia generates is USD tens of billions annually.[2] Beyond their sheer financial scale, the inflow of proceeds of crime into local economies undermines the rule of law and governance structures. The scale and complexity of these operations suggest that many criminal syndicates benefit from protection through corruption, complicating law enforcement and regulatory responses.

In early 2025, a project team of 24 individuals from 10 member jurisdictions, one observer jurisdiction and one observer organisation was formed to undertake this work on cyber scam hubs and human trafficking. The project is co-led by Indonesia and the United Nations Office on Drugs and Crime (UNODC). The project drew on multiple information sources to prepare the report. These included a literature review, over 160 questionnaire responses from APG members' public and private sector entities, interviews with blockchain analytics companies, a roundtable discussion at the 2025 APG Annual Meeting and further discussions at the 2025 APG Typologies Workshop.

1.2 Initial Findings

Sources of funds

Cyber scam hubs are characterised by a highly profitable, multi-layered revenue model, which draws illicit proceeds from four main sources:

1. **Debt bondage from human trafficking victims:** perpetrators impose debt obligations on trafficked individuals, covering costs such as transportation, accommodation and subsistence, which victims are coerced to repay over time.
2. **Ransom payments for release:** in many cases, victims or their families are required to pay significant sums – ranging from an estimated USD 3,000 to USD 20,000 – to secure release, further increasing the criminal syndicates' profits. Alternatively, some victims are forced to secure their release by luring in more victims to work in the compounds in lieu of cash payments.
3. **Revenue generation through fraudulent activities:** victims are compelled to participate in scams, defrauding unsuspecting individuals worldwide, thereby generating direct income for the perpetrators.
4. **Recovery agents re-victimising scam victims**: in a version of an advanced fee scam, members of the cyber scam hub pose as recovery agents and contact the scam victim claiming to have recovered their stolen funds which can be returned upon receipt of a fee.

[2] Global Initiative against Transnational Organized Crime. 2025. *Compound Crime: Cyber Scam Operations in Southeast Asia.* *https://globalinitiative.net/wp-content/uploads/2025/05/GI-TOC-Compound-crime-Cyber-scam-operations-in-Southeast-Asia-May-2025.pdf*.

Case Study # 1: Suspected to be a Philippine Offshore Gaming Operator (POGO) and scam hub

Fraud including cyber scam hubs; Illicit gambling/gaming; human trafficking; cash

In late 2024, authorities raided the compound of Company A suspected to be a Philippine Offshore Gaming Operator (POGO) and scam hub. Company A is also allegedly involved in human trafficking, illegal online gambling, swindling and money laundering.

The operation was conducted in the company's compound, which consisted of several buildings inside a 2.6-hectare area in Location X where around 900 workers were rescued. Subsequently, authorities implemented a court order to open numerous safes where bundles of cash totalling PHP 112.5 million (~ USD 1.935 million) were found.

In addition, a cyber warrant in relation to crypto scamming and online sports betting scams was filed by authorities as Company A was found to facilitate money transfers for online betting applications and provide crypto services, without a necessary permit from the Philippine Amusements and Gaming Corporation.

Source - Philippines

Victim profiles

The human trafficking victims in the cyber scam hubs are typically recruited overseas through fraudulent job advertisements offering high salaries, flights, and 'dream jobs.' Upon arrival, they are trafficked to compounds – often in other jurisdictions – and forced to commit fraud against individuals worldwide. Criminal syndicates often target young adults, including multilingual university graduates with IT skills, social media literacy, and knowledge of cryptocurrency. These capabilities are essential to perform complex cybercrime activities, including online scams, money laundering, and illegal gambling.

However, the victim profile is evolving as these operations seek to diversify their scams to generate further revenue. With artificial intelligence (AI) and real-time translation tools, the requirement for diverse language skills is diminishing, while IT and social media expertise are becoming more critical. Victims who refuse participation may face coercion, including physical violence, food deprivation, electric shocks or forced drug use to maintain compliance.

Case Study # 2: Human trafficking under the guise of overseas employment for cryptocurrency-related work

Fraud including cyber scam hubs; human trafficking; financial institutions

Person A is a self-employed individual based in Batam, Indonesia. She established contact with a manager of a company identified as 'Group X', located in Jurisdiction Y, via video call using her husband's phone. During the call, the company stated it required 15–20 workers to engage in cryptocurrency-related activities, with working hours of 13 hours per day. The job requirements included possession of a valid passport, fluency in Mandarin and basic English, computer literacy, aged between 18 and 35 years, and willingness to comply with company regulations. All interviews were conducted online.

Following this, Person A enlisted the assistance of Person B to identify potential candidates. Person B recommended two individuals, Person C and Person D. Person A received IDR 95,000,000 (~ USD 5,700) in total from the company in Jurisdiction Y - transferred to a bank account after conversion from USD to Indonesian Rupiah. She accompanied Person C and Person D to the airport, from where they flew to Jakarta and continued to Jurisdiction Y. Person A received a commission of IDR 7,500,000 (~ USD 450) per person. Over the course of 2022, a total of 19 individuals were sent abroad under this arrangement.

Person A collaborated with Person E to facilitate the processing of passports, visas, ferry transportation, and flight tickets. Prospective workers from outside Batam, Indonesia were required to arrange their own lodging prior to departure. Person A informed candidates that they would be employed in Jurisdiction Y as Bitcoin telemarketers, working from apartment-based offices. The company would arrange work permits, with employment contracts valid for one year. The offered salary varied according to language proficiency: USD 1,000 (~ IDR 14,000,000) for those with foreign language skills, and USD 700 (~ IDR 10,000,000) for others. Accommodation and travel expenses were to be covered by the company, but if an employee resigned or was terminated before the end of the contract, the company would demand reimbursement of incurred costs.

In total, Person A received USD 53,200 (~ IDR 770,000,000) for sending 19 workers, averaging IDR 40,000,000 (~ USD 2,400) per individual.

Investigations revealed that Person A did not possess the required license from the Ministry of Manpower of the Republic of Indonesia to recruit and send Indonesian workers abroad. Person A was found legally and convincingly guilty of committing the criminal offense of human trafficking.

Source - Indonesia

Case Study # 3: Online scam hubs with human trafficking

Fraud including cyber scam hubs; human trafficking

At approximately 21:30 hours on 25th October 2024, seven persons including Person P, arrived at Yangon International Airport from Jurisdiction A. They reported that they had been trafficked to Jurisdiction A, where they were forced to work under coercive and exploitative conditions in an online scam operation, commonly referred to as a "Kyar Phant" scheme.

The investigation, led by Police Captain N from the No. (6) Branch of Anti-Trafficking in Person Police Force (Yangon), revealed that in June 2024, Person P and the six persons - all residents of Patheingyi Township, Mandalay Region - had sought opportunities to work abroad. During their search, they came into contact with Person C, a resident of North Okkalapa Township, Yangon Region, via the Telegram platform. Person C informed them that customer service jobs were available in Jurisdiction A, offering a monthly salary of USD 800 with free meals, and persuaded them to accept the offer.

Person H and Person S subsequently arranged the necessary travel documents and facilitated their departure from Yangon International Airport to Jurisdiction A, via Jurisdiction B. Upon arrival in the capital of Jurisdiction A, the victims were transported to a regional city, where they were forced to work for an online scam operation.

Using Instagram, WhatsApp, and Line accounts, they were made to lure potential victims online. Upon successfully engaging a customer, they were instructed to transfer the contact to a foreign national via WhatsApp or Line. They were compelled to work in these conditions for approximately three months without receiving any salary.

The investigation confirmed that Person P and the six persons were subjected to forced labour under coercion, with the traffickers profiting unlawfully from their labour. As a result, legal action was initiated against Person C (arrest), Person H (arrest), and Person S (under investigation) under applicable laws.

Police Officer N from the No. (6) Branch of Anti-Trafficking Task Force (Yangon) filed a formal complaint. On 27th October 2024, at 20:40 hours, an official case was opened at the Waibargi Ward Police Station in North Okkalapa Township under Case No. (Pa) 118/2024, in accordance with Sections 35, 36, and 44 of the ***Anti-Trafficking in Persons Law***.

Source - Myanmar

Case Study #4: Suspected illegal Philippine Offshore Gaming Operator (POGO) allegedly involved in human trafficking and scamming activities

Fraud including cyber scam hubs and romance scams; human trafficking

In mid-2024, authorities received information that the businesses in a compound in Location L were allegedly involved in human trafficking and scamming activities. Around 2,724 individuals were rescued, purportedly to be victims of human trafficking. The rescued victims were composed of 1,534 Filipinos with the rest from the Asia region, and jurisdictions as far away as Africa.

The rescued individuals were recruited through Facebook. Filipinos and other foreign nationals received between PHP 24,000 (~ USD 410) and PHP 40,000 (~ USD 690) in compensation each month, and they were not allowed to leave their workplace and were required to work for 12 hours per day.

Company X was the subject of several adverse news articles, where its operation was suspected to be illegal POGO.

According to reports, Company X is believed to have fostered foreign fugitives and harboured trafficking victims, as demonstrated by a raid that targeted seven POGO operations in the compound.

Information and pieces of evidence gathered by the authorities linked Company X to possible involvement in human trafficking, cryptocurrency, and love scams among other illegal activities.

Source - Philippines

These operations target scam victims in jurisdictions with higher disposable income, broad financial access, and strong cryptocurrency adoption both within the Asia/Pacific region and beyond. Criminal syndicates often exploit the linguistic and cultural familiarity of trafficked victims to target additional regions across the globe. Targeting strategies adapt continuously as new victims bring different skills and cultural awareness, enabling criminal syndicates to expand both their operational scope and sophistication.

Case Study # 5: Pig butchering scam

Fraud including cyber scam hubs and romance scams; human trafficking; cash

The police received intelligence that gang members Person A and his wife Person B, were suspected of organising a cyber scam syndicate in Jurisdiction X and cooperating with wanted criminal Person C (Chinese Taipei national stranded in Jurisdiction X), to lure Chinese Taipei nationals to go to Jurisdiction X to engage in cyber scams. The police then formed a special task force and reported to the prosecutor's office for command of the investigation.

The investigation found that Person A and Person B have been organising a cyber scam syndicate since March 2022, recruiting young adults from disadvantaged families in Chinese Taipei to join. At the same time, they set up a cyber scam hub with Person C and a cyber scam syndicate leader Person D (Jurisdiction Y national).

Using "well-paid job opportunities abroad" and "monthly salary of TWD 100,000" (~ USD 3,270) as attraction, they lured 11 people from Chinese Taipei to go abroad to engage in cyber scam and used the method of "pig butchering" to defraud people from other jurisdictions. If the members' performance is not good, they will be beaten and abused with electric batons, and detained.

After the task force obtained key evidence, it was discovered that members of the syndicate frequently entered and exited Jurisdiction X from 2022 to 2024 and continued to operate an overseas cyber scam syndicate. During the period when the syndicate members returned to Chinese Taipei for the Chinese New Year, a total of 15 people were arrested, two people were notified for interview, and 11 criminal bases were raided. Among them, Person A and his wife Person B were both detained incommunicado.

In addition, mobile phones used in the crime, TWD 420,000 (~ USD 13,700) in cash, passbooks, ATM cards, vests, hats, baseball bats and other evidence were seized. The case was referred to the prosecutor's office for violating the *Organized Crime Prevention Act*, the *Human Trafficking Prevention Act*, and aggravated fraud and extortion in the ***Criminal Code***.

Source – Chinese Taipei

Money laundering typologies

Organised criminal syndicates primarily exploit three financial channels to move proceeds of crime linked to these cyber scam hubs and associated human trafficking:

- **Use of mule accounts**: 76% of members noted the use of mule accounts and mule networks to launder proceeds from cyber scam hubs. Mules are attractive to criminal syndicates as they represent a quick and easy way to move and layer funds through the banking system. Weaknesses in CDD and KYC procedures can be readily exploited and different mule accounts can be used when existing accounts have been identified by authorities. Private sector respondents also noted the prevalence of mule accounts in relation to laundering proceeds from cyber scam hubs, with 45% of respondents including this as a primary typology.

- **Unlicensed or unregulated remittance**: Criminal syndicates exploit unlicensed or unregulated remittance services due to regulatory inconsistencies and limited oversight across jurisdictions. These channels are challenging to investigate, however, evidence indicates their prominent use in funding cyber scam hubs and human trafficking operations. 59% of members noted the use of illegal/unlicensed remittance systems to launder proceeds from cyber scam hubs. This includes the misuse of informal money transfer systems (hawala/hundi). 30% of private sector respondents also noted the use of unlicensed and illegal remittance systems were used to launder proceeds.

- **Cryptocurrency and cryptocurrency platforms**: Cryptocurrency is favoured for its perceived anonymity and ease of use. Criminal syndicates exploit unlicensed exchanges, over-the-counter brokers, and informal peer-to-peer platforms as on and off ramps, often with minimal customer due diligence. These platforms facilitate conversion of cryptocurrency into fiat currency or other assets. Further,

these platforms are frequently used as intermediaries between scam victims' funds — often converted into stablecoins — and cash-out points in other jurisdictions. 71% of members identified the exploitation of VASPs and cryptocurrencies as key methods to launder the proceeds of scams and cyber scam hubs. The perceived anonymity or pseudonymity of cryptocurrencies, as well as the quick and relatively inexpensive means to transfer funds across borders appeal to these criminal syndicates. 25% of private sector respondents also noted the exploitation of VASPs.

Members have identified a number of financial indicators which may assist in the detection of transactions linked to cyber scam hubs and associated human trafficking. These indicators will be included in the final APG report.

Case Study # 6: Typology of human trafficking-related financial transactions linked to online scams in Southeast Asia

Fraud including cyber scam hubs; human trafficking; use of virtual assets; virtual asset service providers; transnational crime; financial institutions

During 2024, based on reports from the Indonesian financial intelligence unit (FIU/PPATK), analysts identified instances of human trafficking, allegedly perpetrated by individuals suspected to be part of a transnational human trafficking syndicate associated with online scams operating in Jurisdiction A and Jurisdiction B. These suspicions were based on transaction descriptions or remarks indicating activities such as the recruitment, harbouring, and transportation of human trafficking victims. The transactions involved were valued at approximately IDR 141 billion (~ USD 5 million).

Analysts identified funds suspected to be proceeds of human trafficking in Jurisdiction A which had been received through Jurisdiction A bank accounts. These funds were subsequently used to purchase the cryptocurrency asset USDT (Tether), amounting to USD 295,373 (~ IDR 4,578,281,500), through foreign virtual asset service providers.

On the same day, the criminal syndicate liquidated a portion of the USDT, and the proceeds amounting to IDR 2,592,678,322 (~ USD 156,300) were transferred into Indonesian bank accounts belonging to the criminal syndicate. The criminal syndicate conducted the transfers using a peer-to-peer method through foreign virtual asset service providers.

Source - Indonesia

Case Study # 7: Money laundering through Philippine Offshore Gaming Operations (POGOs)

Fraud including cyber scam hubs; transnational crime; human trafficking; purchase of real estate; Illicit gambling/gaming; financial institutions; currency exchange; use of cheques; cash

In 2024, hundreds of Filipinos and foreign nationals were rescued after the police raided a Philippine Offshore Gaming Operator (POGO). The joint raid was conducted based on search warrants issued following the testimony of a foreign national who escaped from the POGO compound, showing signs of physical abuse. The raid was also prompted by a letter from Jurisdiction A's Embassy, which sought help in rescuing several of their citizens victimized by a job scam syndicate.

The investigation revealed that POGO X was operating under the guise of a legitimate offshore gaming corporation while actually engaging in cryptocurrency investment scams and romance scams, commonly known as "pig butchering." According to the trafficked workers, they posed as attractive males or females seeking romantic interests on social media.

The raid was instigated? by the Philippines financial intelligence unit (FIU), the Anti-Money Laundering Council's (AMLC) intelligence gathering and financial analysis against the POGO and persons of interest (POIs). Simultaneously, the Philippine Senate held public hearings for fact-findings and inquiry in aid of legislation relative to said case.

During the financial analysis, it was seen that the amounts involved in the accounts of various persons of interest (POIs) in this case reached billions of pesos. The following are the initial findings:

- There was a significant increase in both the transaction volume and the amounts involved in a POI's accounts upon the inception of the POGOs.
- A substantial number of foreign exchanges were funded by cash or cheque deposits made on or near the date of the exchange.
- There were cheque payments representing the acquisition of real estate properties totalling PHP 409.7 million (~ USD 7.1 million).

- There was layering of funds from one account to another, multiple deposits in one day, large withdrawals after deposits, creation of transit bank accounts, and misrepresentation of figures on their Audited Financial Statements.
- Establishment of potential shell companies related to real estate development and business involved in the retail of high-end second-hand cars.
- Incorporation documents of POGOs disclosed information such as same email addresses and contact persons connected to one of the POIs.
- There were inconsistencies in one of the POI's profile and identity based on his/her declared personal and financial information on customer due diligence documents.

AMLC also coordinated with various government agencies to identify the networks, businesses, affiliations, assets, and derogatory records of POIs.

It was also discovered that two of the POIs were recently convicted for the biggest money laundering case in Jurisdiction B. Aside from enhancing cooperation with local counterparts, AMLC made requests for information/intelligence to other FIUs through the Egmont Secure Web (ESW).

AMLC conducted coordination meetings and information exchanges with Jurisdiction B's FIU, to ensure that intricate details regarding the foreign fugitives involved in Jurisdiction B's biggest money laundering case, as well as POIs' possible relationship or link to them, were collected and integrated with other findings from the investigation.

As the hearings and investigations persisted, one of the POIs along with her cohorts and siblings, were reportedly able to leave the country despite being subject to an Immigration Lookout Bulletin Order. Purportedly, they had been to three jurisdictions in Asia. Hence, AMLC reached out through ESW to the corresponding FIUs to seek assistance in providing information regarding their financial transactions, travel history records, any properties under the name of these POIs, or any other information which may assist in the investigation.

Source - Philippines

Enabling conditions

Existing research, and the experience of APG members, demonstrate cyber scam hub operations exploiting a number of vulnerabilities to establish, expand and diversify their operations. Enabling conditions for this illicit activity include:

- **Exploitation of special economic zones**: Special economic zones (SEZs) in Southeast Asia, initially established to attract foreign investments and stimulate economic growth, are increasingly exploited by criminal syndicates as operational hubs for cyber scams. While members generally noted cyber scam hubs were typically located in urban centres (71% of member responses) or border areas (53% of member responses), these often coincide with the location of special economic zones. These special economic zones are also often subject to lower regulatory oversight, limited law enforcement presence and also provide the necessary internet access, availability of space to accommodate the operations, and other facilities to support the number of people involved in these hubs. The proximity to international borders facilitates cross-border trafficking, logistical coordination, and the movement of both personnel and funds.

- **Complex corporate structures (including using gatekeepers/DNFBPs) to obfuscate beneficial ownership**: Criminal syndicates frequently exploit corporate vehicles – including shell companies, trusts, and other complex legal entities – to provide a façade of legitimacy for cyber scam hubs, thereby facilitating the concealment of illicit activities and proceeds of crime. Professional intermediaries, such as lawyers, accountants, trust and company service providers (TCSPs), and corporate formation agents may either knowingly or inadvertently facilitate the establishment and administration of these structures. These complex corporate structures are established as the cyber scam hubs are being developed and operate in a similar way to large scale businesses. 65% of members noted the use of complex corporate structures, including shell or front companies, as a primary means of laundering proceeds from cyber scam hubs. Some gatekeepers have also been involved in facilitating the scam activities themselves.

Case Study # 8: Investment fraud

Investment fraud; use of legal persons; transnational crime

An investigation into a fraudulent investment scam led to raids on multiple locations, including raids on call centres, companies, and residential houses.

A criminal syndicate based in Malaysia was in operation only for a few years yet had allegedly amassed close to RM 200 million (~ USD 47.2 million) of proceeds of crime. Despite the operation being based in Malaysia, the syndicate members were from various foreign jurisdictions using Malaysians as facilitators.

The syndicate's ***modus operandi*** was to offer fake investment portfolios through advertisements on social media. The scam made use of professional enablers, particularly company secretaries, to set up companies to defraud victims into believing that they were investing in a legitimate investment scheme or purchasing shares of a real company.

The operation resulted in four foreign individuals being charged, convicted and fined for predicate offences under the penal code. Asset forfeiture actions in relation to the money laundering offences are ongoing.

Source - Malaysia

- **Corruption**: Public officials may directly facilitate or shield these activities in exchange for financial or economic incentives, or they may fail to intervene due to limited capacity, reluctance, or conflicts of interest. Such a compromised governance and regulatory environment significantly undermines oversight mechanisms, allowing cyber scam hubs to operate with minimal scrutiny, reduced risk of detection, and limited exposure to legal accountability. 41% of members noted corrupt or complicit local authorities enabling the establishment and continued operation of cyber scam hubs.

Challenges for law enforcement responses

Whilst over the past year there have been successful investigations against those operating cyber scam hubs, there remain a number of challenges for law enforcement responses. These include:

- **Challenges with international cooperation**: while most members identifyed the cross-border nature of cyber scam hubs and human trafficking as a key challenge (76% of respondents) for investigations, international cooperation is considered a vital aspect of addressing these crimes. Members noted several challenges with securing international cooperation, both with investigations of cyber scam hubs, as well as assisting and repatriating trafficked individuals. Challenges were often associated with a lack of communication or a delayed response from jurisdictions where these hubs were housed, legal or policy barriers to information sharing and challenges with mutual legal assistance requests.

- **Asset recovery**: The majority of respondents were unable to provide an estimate of the total value of assets linked to cyber scam hubs and human trafficking laundered in their jurisdictions. Only two jurisdictions (12% of respondents) considered themselves successful in tracing and seizing proceeds laundered from cyber scam hubs in their jurisdiction or from foreign jurisdictions. The use of virtual assets hampered a jurisdiction's ability to confiscate assets along with challenges associated with international cooperation. Further challenges identified included the use of foreign nominees and front companies which contributed to a lack of successful confiscation of laundered proceeds.

- **Limited expertise in cryptocurrency investigations/tracing**: 71% of members surveyed noted tracing illicit funds through virtual asset service providers and cryptocurrencies was a primary challenge in investigating and prosecuting ML cases linked to cyber scam hubs. A lack of specialised investigative? expertise in relation to cyber-enabled fraud and scam was also noted as a key challenges by 65% of member respondents.

Emerging Threats

Cyber scam hubs are increasingly adopting decentralisation strategies to mitigate detection and disruption by law enforcement and regulatory authorities. In practice, this approach involves fragmenting large-scale operations into smaller, mobile units and relocating them across different areas within cities or regions. By dispersing their activities, criminal syndicates are able to obscure operational footprints, complicate investigative efforts, and minimise the risk of large-scale enforcement actions. More than one third of APG member jurisdictions surveyed reported encountering or being aware of instances of decentralisation, highlighting its growing prevalence as a strategic adaptation of cyber scam hubs.

Artificial Intelligence (AI) is emerging as a transformative tool in cyber scam operations, enhancing both the sophistication and efficiency of illicit activities while enabling unprecedented scalability. Criminal syndicates are increasingly leveraging AI to automate processes, expand reach and optimise the targeting of victims. Members noted the use of AI through chatbots, deepfakes, voice-cloning and the generation of scam content in expanding the operation of these cyber scam hubs.

1.3 Conclusion and Recommendations

Initial findings from this project highlight the complexity, adaptability, and transnational nature of cyber scam hubs and human trafficking in the Asia-Pacific region. These criminal syndicates exploit sophisticated financial channels, opaque legal structures, emerging technologies, regulatory gaps, and corruption to maintain and expand operations. The emerging use of decentralisation and AI demonstrates an increasing operational sophistication that enables these criminal syndicates to scale activities while minimising the risk of detection and legal accountability.

Effective mitigation of this evolving crime type requires continued monitoring, enhanced regional and global cooperation, targeted intelligence sharing, and the strengthening of AML/CFT frameworks across member jurisdictions. These measures are critical to disrupt cyber scam hubs, protect victims, and safeguard the integrity of financial systems against highly organised criminal syndicates engaged in technology-enable crimes.

Note: the complete findings, indicators and recommendations of the project will be published in the forthcoming *Cyber Scam Hubs and Human Trafficking Report* (2026).

2 - MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING METHODS

The following case studies 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 have been included and further referenced in the index in Section 7 of this report.

Money laundering

2.1 Bangladesh

Case Study # 9: Abuse of mobile financial services platform for online gambling and facilitating hundi/hawala activities

Fraud; online gambling; smuggling of currency; suspicious transaction reporting; money value transfer services; financial institutions

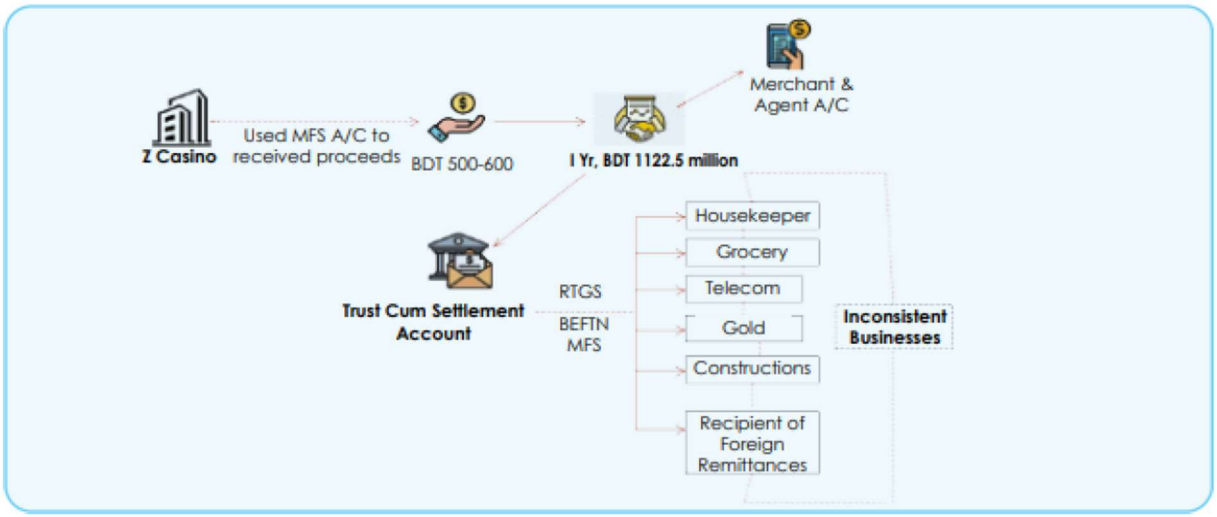
A suspicious transaction report from a mobile financial services (MFS) provider revealed that financial transactions occurred through the online gambling app 'Z Casino', using MFS accounts. Analysis revealed that a total of 51 MFS accounts (46 merchant accounts, four personal accounts, and one agent account) registered to 50 businesses were linked to Z Casino for collecting gambling proceeds. Through these accounts, BDT 1,122.5 million (~ USD 9.2 million) was collected within a year where most of the transactions were in small denomination and repetitive in nature (e.g. BDT 100 (~ USD 82 cents), BDT 200 (~ USD 1.64), BDT 500 (~ USD 4.10), BDT 600) (~ USD 4.92).

The businesses associated with these MFS accounts seemed as legitimate entities, such as e-commerce platforms, telemedicine providers, construction suppliers, restaurants, and advertising agencies. However, they were found to be operating online gambling under the guise of these businesses and huge amount of funds have been collected through MFS accounts.

Funds deposited in these MFS accounts were transferred to 10 Trust Cum Settlement (TCS) bank accounts, which collectively received BDT 532.6 million (~ USD 4.376 million) within two years. Further analysis showed these TCS accounts credited funds from various other MFS accounts linked to Z Casino.

The money from TCS accounts was transferred to individuals and businesses whose activities were inconsistent with the nature of the MFS-linked businesses. These included remittance beneficiaries, housewives, travel agencies, cattle farms, and gold businesses, among others. It is suspected that the funds were smuggled abroad via Hundi/Hawala networks, transferring proceeds to the accounts of Hundi/Hawala dealers.

An intelligence report on 50 individuals and entities involved in this operation has been disseminated to the relevant LEAs for necessary action under the *Money Laundering Prevention Act 2012*.



Source – Bangladesh

Case Study # 10: Crypto currency and illegal online foreign exchange transactions via MFS accounts

Cryptocurrency trading: smuggling of currency; suspicious transaction reporting; currency exchange; financial institutions

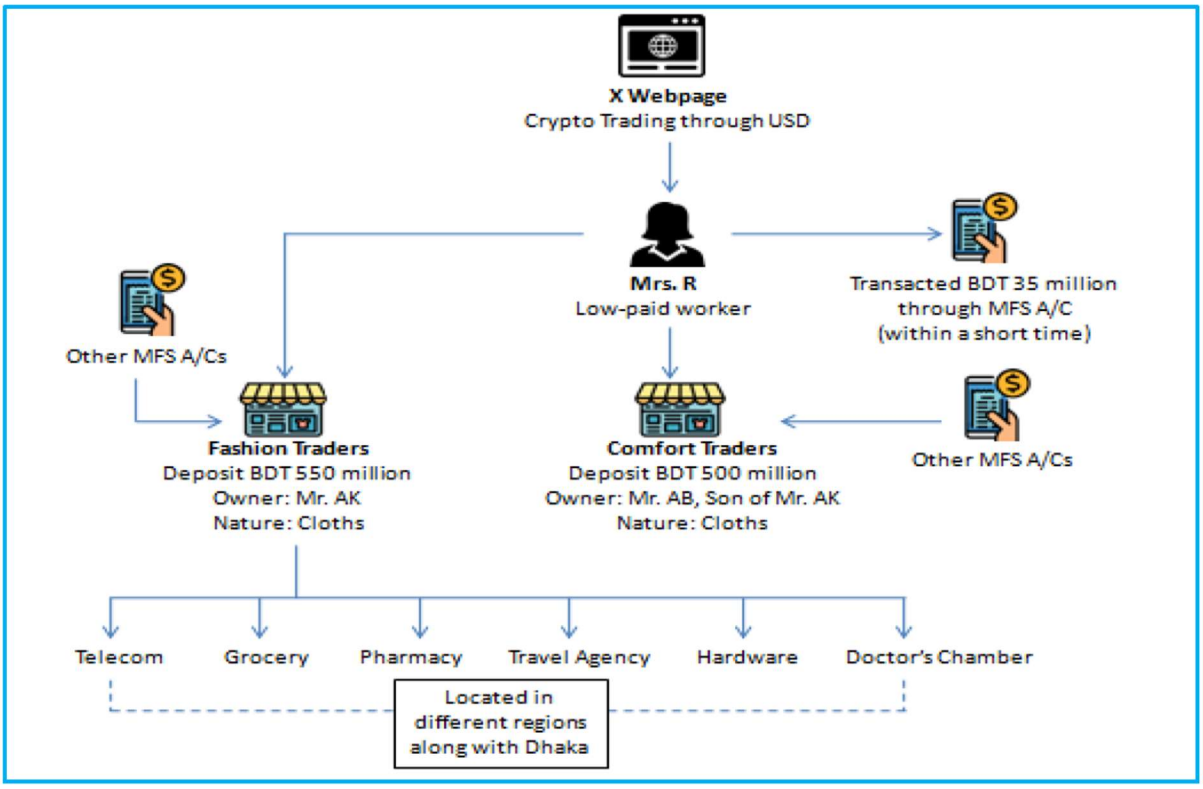
A reporting entity submitted a suspicious transaction report to the Bangladesh Financial Intelligence Unit indicating the misuse of mobile financial services (MFS) platform for illegal trading of foreign currencies and cryptocurrencies. It was found that Mrs. R's personal MFS account was linked to these transactions, through which BDT 35.0 million (~ USD 287,300) was transacted within a short period. Mrs. R, a day labourer by profession with average monthly earnings of around BDT 10,000 (~ USD 82); and resides in a remote area of the southern part of the jurisdiction.

Her profession, monthly earnings and location of residence do not commensurate with the pattern and nature of the above-mentioned transactions.

Analysis revealed that funds from Mrs. R's MFS account were transferred to the bank accounts of two clothing stores located in the said remote area of the jurisdiction named 'Fashion Traders' and 'Comfort Traders', owned by Mr. AK and his son, Mr. AB, respectively. These accounts showed deposits and withdrawals totalling BDT 1,050.0 million (~ USD 8.619 million), inconsistent with their business nature.

The funds were further distributed to individuals and unrelated businesses across Bangladesh, including drug stores, travel agencies, and grocery stores, raising suspicion of illegal foreign exchange trading.

Analysis indicated Mr. AK and Mr. AB as the actual users and beneficiaries of Mrs. R's MFS account. An intelligence report was disseminated to law enforcement agencies for taking further necessary action under the *Money Laundering Prevention Act 2012*.



Source – Bangladesh

2.2 China

Case Study # 11: Combating telecom fraud "black/grey industries" and money laundering criminals

Third-party laundering; fraud; foreign predicate offence; cash; financial institutions

Telecom fraud has given rise to a range of criminal 'black and grey industries'. Criminals sell illegally obtained personal information, such as ID numbers and phone numbers though they're fully aware that the buyers are committing telecom fraud. This trade in sensitive data effectively supplies 'fraudulent leads' that enable downstream crimes. Furthermore, criminals also traffic in stolen social media account credentials, which serve as direct 'tools for fraud' for criminal networks.

A case from China demonstrates successful action against these illegal industries and their associated money launderers.

Person A illegally obtained large quantities of citizens' personal data and sold it to domestic and foreign telecom fraud syndicates. The information provided by Person A was used in over 400 fraud cases, with total proceeds of crime exceeding RMB 10 million (~ USD 1.4 Million). Person B, acting under Person A's direction, withdrew cash from third-party bank accounts to launder Person A's proceeds of crime.

Based on Person A's circumstances of crime, the court ruled that Person A was an accomplice to telecom fraud. Person B was convicted of concealing and disguising proceeds of crime for he has assisted in laundering the illicit money.

Source - China

2.3 Hong Kong, China

Case Study # 12: Ransom payment in form of cryptocurrency

Fraud including cyber scam hubs; kidnapping; ransom; forced labour, human trafficking and migrant smuggling; virtual assets; virtual asset service providers

In December 2024, a Hong Kong, China citizen, Person A fell prey to a job scam and told her family members that she would be leaving Hong Kong, China (HKC) for a few days for a quick cash job in Jurisdiction X. Later, the victim realised the job was actually related to a cyber scam hub in Jurisdiction Y, which is adjacent to Jurisdiction X.

She sent screenshots of her GPS location near the border of Jurisdiction X to her family members and told them that she was requested to pay HKD 350,000 (~ USD 45,000) in the form of USDT (Tether) to several designated cryptocurrency wallets to be released back to HKC.

Her family eventually agreed to pay the money in exchange for victim's return. The victim's family paid a total of HKD 210,000 (~ USD 27,000) in form of USDT (Tether) to the designated cryptocurrency wallets on two occasions. Two days later, the victim was released and safely returned to HKC.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 13: Laundering of the proceeds of crime via cryptocurrency

Third-party laundering; fraud; cash; use of virtual assets; virtual asset service providers; financial institutions

In 2023, intelligence suggested a local criminal syndicate controlling a group of suspicious bank accounts in Hong Kong, China had made substantial cash withdrawals after receiving proceeds of crime originating from local deception cases. Subsequent investigation unveiled the criminal syndicate had utilised numerous local bank accounts to dissipate the proceeds of crime totalling HKD 200 million (~ USD 25.64 million) between March 2023 and May 2024.

Once the proceeds of crime were remitted into the accounts, the criminal syndicate immediately tasked their members to make cash withdrawals and used the cash to purchase cryptocurrency via over-the-counter cryptocurrency exchange shops in order to conceal the origin of the funds and break the fund flow trail.

In August 2024, the police arrested 12 syndicate members.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 14: Online casino and money laundering syndicate

Third-party laundering; illicit gambling/gaming

In late 2024, intelligence suggested that an overseas-based illegal gambling website had actively promoted online gambling in Hong Kong, China. Further investigation identified a local bookmaking and money laundering syndicate which was in control of the online platforms through local operating centres and utilised mule (or 'stooge') accounts for top-up and cash-out of illegal gambling credits.

These stooge accounts laundered more than HKD 110 million (~ USD 14.10 million) gambling proceeds between May and October 2024. In early 2025, the police raided three operating centres and arrested 12 culprits.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 15: Money laundering through the purchase of gold bars

Cross-border third-party money laundering; cash; use of precious metals and stones

In August 2020, intelligence suggested that a local couple acted as couriers on four occasions to purchase 600 gold bars with about HKD 58 million (~ USD 7.44 million) in cash that originated from another jurisdiction, on behalf of a money laundering syndicate. The police conducted an extensive investigation leading to the arrest of the couple and the masterminds of the criminal syndicate who were the ultimate recipient of the gold bars.

The police conducted a house raid which seized gold bars, cash and valuables amounting to HKD 124 million (~ USD 15.90 million). Their accounts and properties amounting to HKD 468 million (~ USD 60 million) were subsequently frozen under Restraint Order. The offenders were eventually convicted after trial.

The confiscation proceedings are ongoing.

Source - Hong Kong, China

Case Study # 16: Laundering of the proceeds of crime via digital bank accounts

Cross-border third-party laundering; financial institutions

In mid-2024, intelligence indicated that numerous digital bank accounts with suspicious account activities were accessed by two common IP addresses which were subscribed as public Wi-Fi, at a shared office in an industrial building. Further investigation suggested that a money laundering operation centre was located at the building. The mastermind of the money laundering syndicate activated the bank cards collected from mules and carried out 'test payment' thereafter.

Subsequent investigation revealed that these stooge accounts were used to receive proceeds of crime from over 30 deception cases reported in Hong Kong, China between March and June 2024. Some transactions were also found conducted in neighbouring Jurisdiction X after activation. During the offence period, the criminal syndicate had laundered over HKD 12 million (~ USD 1.54 million). A total of nine local syndicate members including the mastermind were arrested by the police.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 17: Money laundering through automatic teller machine and virtual asset over-the-counter exchange shop

Illicit gambling/gaming; third-party laundering; cash; use of virtual assets; virtual asset service providers; financial institutions

Intelligence unveiled an online gambling-related money laundering syndicate exploiting seven bank accounts to dissipate over HKD 13 million (~ USD 1.67 million) of suspected proceeds of crime between May and July 2024 in Hong Kong, China. Approximately HKD 12.9 million (~ USD 1.65 million) was

withdrawn in cash by local money mules via automatic teller machines and the cash was further dissipated by purchasing cryptocurrency through over-the-counter exchanges shops.

In August 2024, the police mounted an arrest operation with a total of 11 syndicate members arrested, including a core member who instructed the money mules to withdraw money from ATMs. Around HKD 0.5 million (~ USD 64,102) cash and over 100 bank cards belonging to others were seized during the operation.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 18: Cross-border money laundering through mules and cryptocurrency

Organised criminal syndicate; third-party laundering; use of virtual assets; virtual asset service providers; cash; financial institutions

Intelligence unveiled a cross-border money laundering syndicate exploiting 76 local bank accounts opened by non-locals to launder around HKD 580 million (~ USD 74.36 million) between October 2023 and March 2024, including around HKD 25.9 million (~ USD 3.32 million) originated from 36 local scam cases.

The syndicate arranged transport and accommodations for overseas money mules to travel to Hong Kong, China, and instructed them to open bank accounts and make large cash withdrawals at bank counters/ATMs. The accumulated cash was then dissipated by purchasing cryptocurrency through over-the-counter exchanges with a view to concealing the origin of the funds.

In March 2024, the police mounted an arrest operation with nine persons, including the mastermind and money mules, arrested and about HKD 1.6 million (~ USD 0.21 million) cash was seized at the scene.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 19: Cross-border money laundering syndicate

Organised criminal syndicate; third-party laundering; fraud; foreign predicate offence; international cooperation; money value transfer services; cash

Since early 2024, police of Southeast Asia Jurisdiction A identified that its nationals, having fell prey in tech-support scams, were instructed to remit monies into money mules' ('stooge') accounts in Hong Kong, China. Through proactive intelligence exchange between the police, Jurisdiction A's police and INTERPOL, controllers of these stooge accounts were identified. The accounts had at least laundered HKD 102 million (~ USD 13.08 million) of deceived monies originated from local and overseas victims.

The arrest operation turned overt in August 2024 and resulted in the arrest of seven persons in HKC and one person in Jurisdiction A. During the operation, cash HKD 661,000 (~ USD 84,743.59) of suspected proceeds of crime was seized from the arrested persons and their hideouts and over HKD 1.9 million (~ USD 0.24 million) of residual balance in arrestees' accounts was prevented from further dissipation.

The arrested persons were charged and remanded in jail pending subsequent court proceedings.

Source - Hong Kong, China

Case Study # 20: Cross-boundary e-shopping fraud with malware

Fraud; cross-border organised criminal syndicate; international cooperation

In mid-June 2024, a joint operation with Jurisdiction A and Jurisdiction B was conducted to dismantle a cross-border scam syndicate. The criminal syndicate lured victims into installing malicious mobile applications (apps) with malware. These apps allowed the criminal syndicate to gain control of victims' mobile devices, access victim's e-banking accounts, and steal funds through unauthorised transactions.

Between September 2023 and April 2024, over 1,900 cases in Jurisdiction A and Hong Kong, China (HKC) were reported, incurring a total loss of HKD 210 million (~ USD 26.92 million). The criminal syndicate masterminds in Jurisdiction B and stooge account holders in HKC were identified through regional intelligence exchanges. During the operation, Jurisdiction B arrested two masterminds, who were subsequently extradited to Jurisdiction A while 26 stooge account holders were arrested in HKC. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 21: Stored value facility fraud through bounding with stolen credit card credentials

Fraud; third-party laundering; use of credit cards

Between December 2023 and January 2024, 39 victims reported that they were deceived by phishing SMS purportedly sent by mobile network operators, and surrendered their credit card credentials and one-time passwords on bogus websites.

Soon after falling prey, victims found unauthorised transactions were made with their credit cards, including:

- Cash advancement transferred to unknown stored value facility (SVF) accounts.
- Physical/online purchases via unknown SVF accounts, which incurred HKD 227,000 (~ USD 29,102.56) of loss in total.

In April 2024, the police operation turned overt and resulted in the arrest of one local mastermind and five local syndicate members for 'Conspiracy to Defraud' and 'Money Laundering'.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 22: e-Banking fraud through misusing national identity cards and stolen property of victims

Fraud; third-party laundering; financial institutions; use of credit cards

Between June 2023 and February 2024, the national identity cards of five victims were stolen by a criminal syndicate. The criminal syndicate altered the portraits of the stolen national identity cards and used them for account opening/loan applications at various financial institutions, totalling HKD 50,000 (~ USD 6,410.26).

Using the stolen national identity cards, the criminal syndicate also changed the mobile service on behalf of a victim to intercept SMS containing one-time passwords sent by banks and fraudulently stole the funds totalling HKD 304,000 (~ USD 38,974.36) in another account belonging to the victim. The stolen funds were transferred to the personal bank accounts of two of the members of the criminal syndicate.

Apart from misusing the victims' personal data, the criminal syndicate also used a stolen credit card of a victim for making fraudulent purchases totalling HKD 32,000 (~ USD 4,102.56).

A total loss of HKD 386,000 (~ USD 49,487.18) was incurred from various fraudulent activities.

In May 2024, the operation turned overt and resulted in the apprehension of nine members of the criminal syndicate for 'Conspiracy to Defraud' and 'Money Laundering'.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 23: Trade-based money laundering with record-breaking laundered amount

Trade-based money laundering; dealers in precious metals and stones; foreign predicate offence; international cooperation; transnational crime; organised criminal syndicate; trade in precious metals and stones; suspicious transaction reporting; financial institutions

In January 2024, Hong Kong, China's customs service uncovered its largest-ever money laundering case, dismantling a transnational criminal syndicate for laundering approximately HKD 14 billion (~ USD 1.8 billion) through dubious trade activities.

The investigation stemmed from a suspicious transaction report alleging that a few trading companies were stooge companies. Upon analysis of the fund flows, the investigation scope was enlarged to encompass other companies which were also established by the criminal syndicate. Substantial amounts of funds were injected from overseas entities through purportedly exporting of diamond, precious stones, and electronic products to different jurisdictions, including Jurisdiction A.

In-depth data analysis revealed that the companies' transactions in financial institutions, declared turnover of trade volume, the business modes of the companies and relevant official records were alarmingly incommensurate and thus raising doubts on exploitation of transnational trade to move illicit funds.

Upon intelligence exchange with Jurisdiction A, part of the 'legitimate payment' for goods amounting to HKD 2.9 billion (~ USD 373 million) were identified as proceeds from mobile application scams in Jurisdiction A.

The total funds laundered amounted to HKD 14 billion (~ USD 1.8 billion).

Between January and May 2024, customs arrested eight persons for money laundering in Hong Kong, China and froze HKD 168 million (~ USD 21.6 million) worth of assets.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 24: Financial investigation against the smuggler of endangered species

Smuggling; environmental crime; financial institutions

In January 2024, Hong Kong, China's customs service conducted follow-up investigation against the offender of a sea smuggling case involving seizure of 230 kg of endangered corals. Suspicious transaction records amounting to HKD 6.7 million (~ USD 861,000) between 2021 and 2023 were uncovered in the offender's bank accounts without legitimate source of funds.

In June 2024 the offender was formally charged for money laundering in connection with the suspected proceeds of crime. In September 2025, the offender was convicted of two counts of money laundering charges and sentenced to 40 months' imprisonment, with the successful application of enhanced sentencing under the *Organized and Serious Crimes Ordinance* (OSCO), Chapter 455, Laws of Hong Kong, China.

This was the first time customs had arrested and convicted an individual on money laundering charges related to endangered species smuggling since the inclusion of certain wildlife trafficking offences to the OSCO in August 2021 which, demonstrated customs' enforcement capability to tackle illicit wildlife trade.

Source - Hong Kong, China

Case Study # 25: Money laundering through gold smuggling

Smuggling; self-laundering; trade in precious metals and stones

In March 2024, Hong Kong, China's customs service detected a smuggling case involving 146 kilograms of gold amounting to HKD 84 million (~ USD 10.8 million) and arrested the director of a consignor company for smuggling. The gold was moulded and disguised as part of air compressor machines which were about to be exported to Jurisdiction A.

Subsequent financial investigation revealed that the director received suspicious funds of about HKD 7.4 million (~ USD 951,000) from various suspicious counterparties. The gold concealed in the machine was also suspected to be the proceeds of crime.

In December 2024, customs arrested the director for money laundering.

The investigation is ongoing.

Source - Hong Kong, China

Case Study # 26: Money laundering with drug related crime

Drug related crime; suspicious transaction reporting; financial institutions

In June 2024, Hong Kong, China's customs service detected a dangerous drug case involving approximately HKD 28 million (~ USD 3.59 million) worth of drugs and arrested three local persons. Subsequent financial investigation and fund flow analysis revealed that there were numerous suspicious transactions in the personal bank accounts of the trio between January 2021 and June 2024.

Additionally, the investigation uncovered that another local person received suspected proceeds of crime from the drug syndicate and handled large sums of money from unknown sources during the same period. The total value of suspicious transactions linked to the four persons amounted to about HKD 53 million (~ USD 6.8 million).

In November 2024, customs arrested the four persons for money laundering. The investigation is ongoing.

Source - Hong Kong, China

2.4 Indonesia

Case Study # 27: Fake gold investment scheme on social media uncovered

Fraud; self- laundering; trade in precious metals and stones; cash; financial institutions

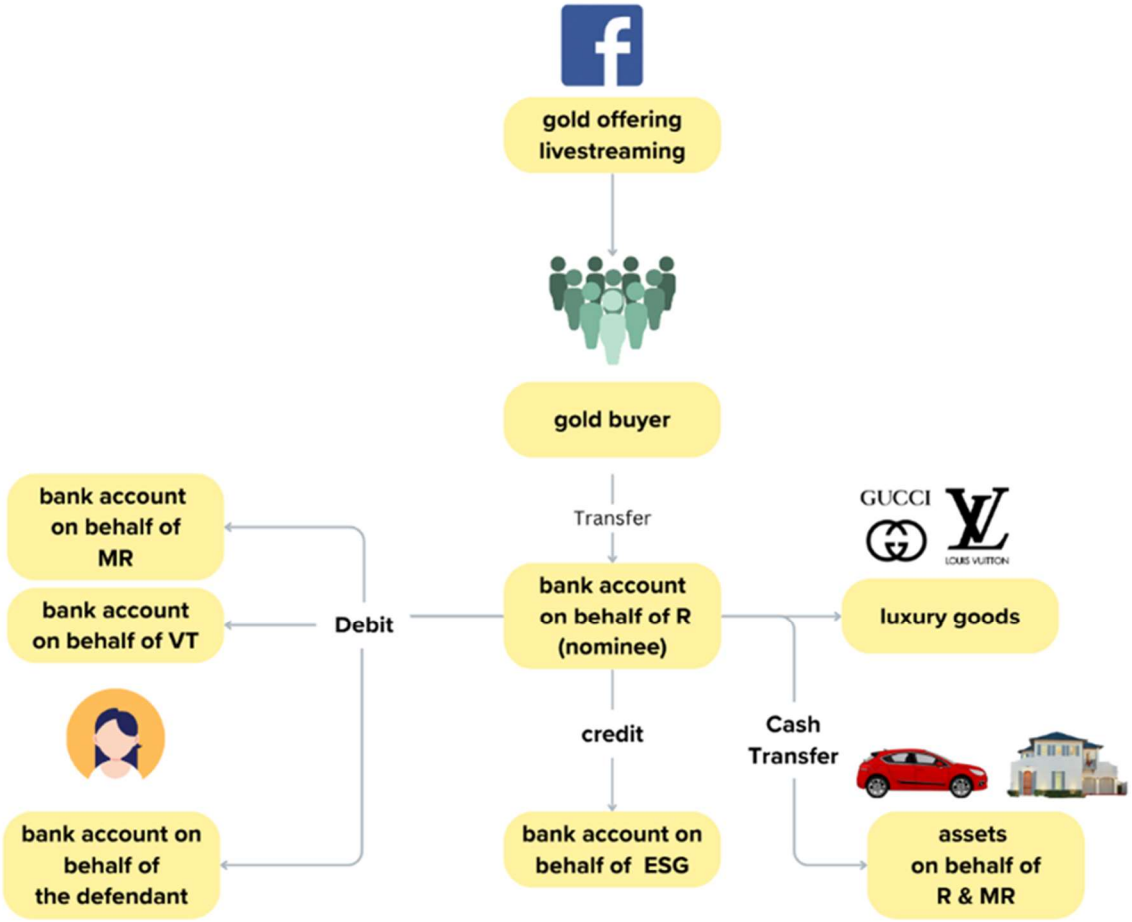
The defendant - Person X, utilised her Facebook account to promote the sale of gold bullion at relatively low prices. She conducted the promotions through livestream session, during which Person X displayed updated gold price list and showcased the bullion allegedly for sale. Person X claimed that the gold originated from a reputable bullion company however, investigations revealed that she actually purchased the gold from local gold shops in a shopping mall and a traditional market in Jakarta, Indonesia raising doubts about its authenticity. Furthermore, Person X was not licensed to engage in gold trading.

To facilitate payment, Person X provided a bank account number belonging to an associate, Person R. Initially, transactions appeared legitimate, and buyers received the goods. However, in subsequent transactions involving larger sums, the promised gold was never delivered.

Funds deposited into Person R's account for the gold purchases were subsequently transferred to the Person X's personal account. Person X used the proceeds of crime for various expenditures and financial transactions, including:

- Purchasing luxury goods (brands such as Louis Vuitton, Gucci, Christian Dior, and Off-White).
- Transferring funds to the accounts of individuals identified as Person Y and Person Z.
- Receiving funds from an individual identified as Person A.
- Purchasing land, buildings, and vehicles, both in cash and on credit.

The court found Person X legally and convincingly guilty of committing fraud and money laundering. The court sentenced Person X to four years of imprisonment and fined her IDR 500,000,000 (~ USD 30,000).



Source - Indonesia

Case Study # 28: Fraud and money laundering scheme involving fictitious medical device sales

Fraud; self-laundering; financial institutions

Person. A (currently on a wanted list) contacted Person B to obtain a bank account under false identity (nominee) to facilitate payments related to fictitious online sales of medical devices advertised on his website, www.bastmed.com. In return, Person A promised Person B 20% of the funds received through the account. Person A subsequently approached Person C to assist in acquiring such accounts, offering the same commission. Person C succeeded in obtaining a fraudulent bank account by purchasing it from Person D for approximately IDR 3,000,000 (~ USD 180). The package included the account under the name of Person M, along with the associated savings book and ATM card. This information was relayed to Person B, who then passed it to Person A.

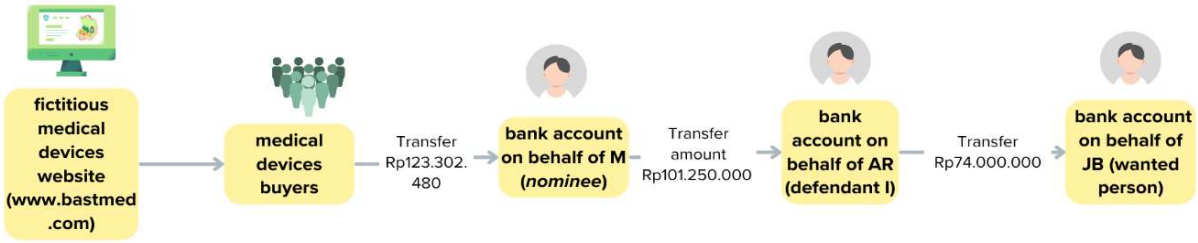
Person A informed Person B that a potential buyer, Person E, would be contacting them. Person B was instructed to respond to Person E via the email address sales@bastmed.com regarding the purchase of two VERSA-TRAC Lumbar Retractor Master Set medical devices, priced at USD 8,400. Following a price agreement, Person B altered the company profile and invoice to reflect Person M's account details in order to convince the victim of the legitimacy of the transaction.

Subsequently, Person C informed Person B that a payment of USD 8,400 (~ IDR 123,302,480) had been received from the victim, Person E into the fraudulent account. From these funds, Person C received a commission of IDR 24,000,000 (~ USD 1,440), while the remaining amount was transferred to Person B via several transactions:

- IDR 45,000,000 (~ USD 2,700) via teller deposit at Bank C, Branch A;
- IDR 47,250,000 (~ USD 2,800) via teller deposit at Bank C, Branch B;
- IDR 9,000,000 (~ USD 540) via mobile banking at Bank M.

Person B subsequently transferred the remaining funds to Person A (via Bank C) after deducting IDR 16,000,000 (~ USD 965) as personal compensation. The final amount transferred to Person A was IDR 74,000,000 (~ USD 4,460).

Both Person B (defendant I) and Person C (Defendant II) were found legally and convincingly guilty of fraud and conspiracy to launder money by transferring assets known to be proceeds of crime with the intent to conceal their origin. Each defendant was sentenced to one year and eight months of imprisonment and fined IDR 50,000,000 (~ USD 3,000).



Source - Indonesia

Case Study # 29: Thousands defrauded in a fake robot trading scheme disguised as a legitimate investment platform

Fraud; use of capital markets

Person A, in collaboration with Person B, established a robot trading business under the guise of a legitimate investment scheme. Person A acted as the founder and director of FSP AP Company, while Person B was the founder of LGB Company. FSP AP Company operated as the distributor of the Fahrenheit robot trading application, whereas LGB Company served as the broker for robot trading activities. They conducted their business operations in violation of the scope of the business licenses held.

They conducted marketing and promotional activities extensively through social media platforms, including YouTube, TikTok, Instagram, Twitter, and Facebook. Additionally, they disseminated digital flyers via WhatsApp Stories, created and distributed by an individual identified as Person C. They employed a multi-level marketing (MLM) strategy, wherein members who successfully recruited new members (downlines) were offered various incentives such as precious metals, vehicles (cars and motorcycles), laptops, mobile phones, and commission-based rewards. These incentives, however, were not funded by legitimate trading profits but were instead financed using funds deposited by other members, thereby constituting a ponzi-type scheme. The Fahrenheit robot trading scheme promised returns of 1% per day, or

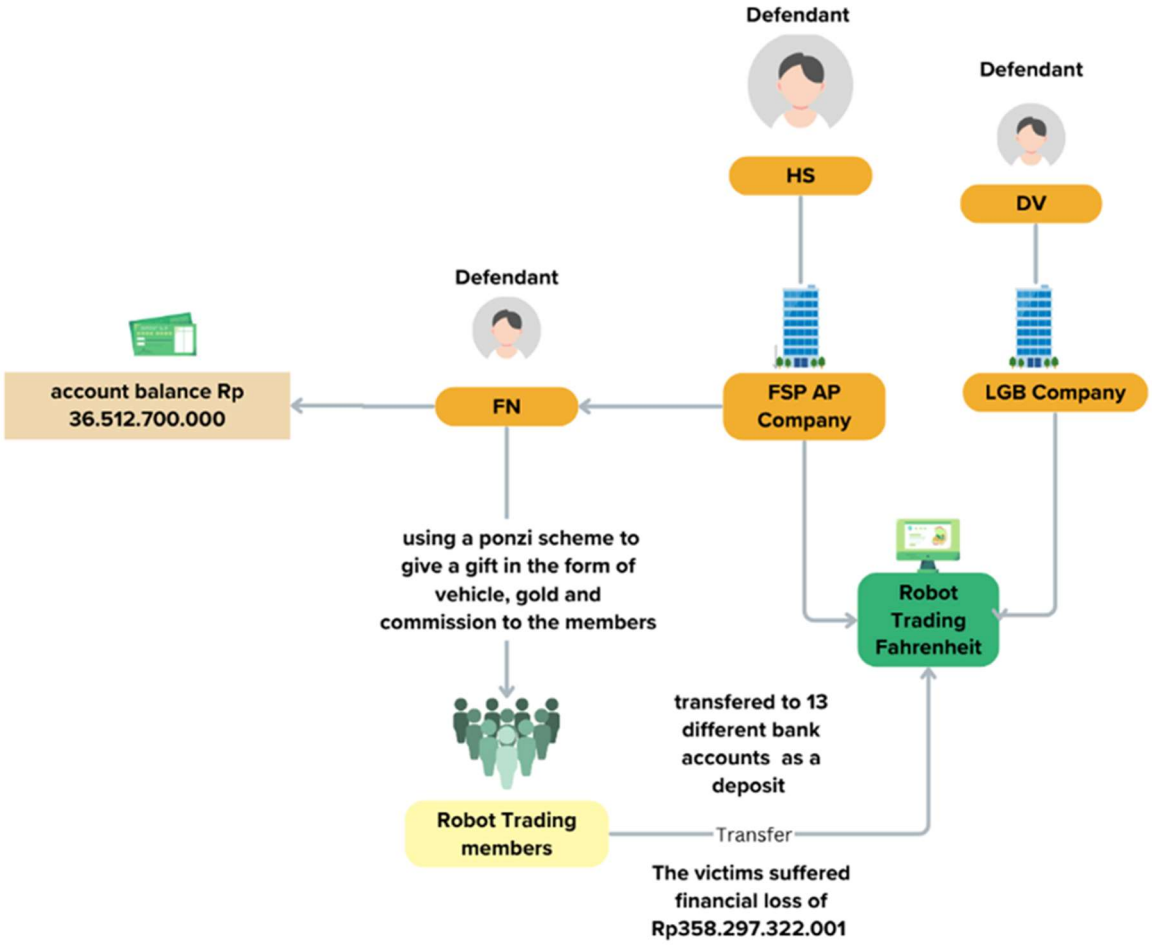
20%–25% per month. They permitted members to open two or more accounts using the same identity or email address.

Between 25 February 2022 and 7 March 2022, members of the Fahrenheit platform suffered significant investment losses, resulting in the total depletion of their capital. They presented this loss to members as a result of a market margin call, although in reality it was part of a fictitious transaction fabricated by Persons A and B as an exit strategy. An audit revealed that out of an estimated 20,000 members, 1,449 members formally reported losses totalling approximately IDR 358,297,322,001 (~ USD 21.6 million).

The court found Persons A and B legally and convincingly guilty of:

- Spreading false and misleading information detrimental to consumers in electronic transactions; and
- Money laundering, by concealing and disguising the origin of proceeds from criminal activity.

Each person was sentenced to 10 ten years of imprisonment and fined IDR 3,000,000,000 (~ USD 180,000). In the event the fine is not paid, it will be substituted with an additional six months of imprisonment.



Source - Indonesia

Case Study # 30: Green financial crime – public/private partnership with non-government organisation

Third-party laundering; fraud; use of legal persons and arrangements; trust and company service providers; foreign predicate offence; transnational crime; smuggling; financial institutions

The initial detection of this case originated from intelligence provided by an undercover agent affiliated with a civil society organisation active in the environmental sector. The information was subsequently reported to the financial intelligence unit (PPATK). The informant disclosed the nominal identity of the suspected perpetrator and detailed that the wildlife smuggling operation was carried out via sea routes using unauthorised and illegal shipping channels. This intelligence triggered further analysis of financial transactions, which ultimately led to the uncovering of a broader illegal wildlife trafficking network.

Person X is reasonably suspected of committing money laundering involving proceeds derived from the transnational trafficking and/or trade of protected wildlife species. Based on the analysis of financial

transactions conducted between 2021 and August 2023, the total turnover across all of Person X's bank accounts amounted to IDR 264.27 billion (~ USD 17.27 million). Of this amount, approximately IDR 34.41 billion (~ USD 2.25 million) is suspected to have originated from predicate offenses, with IDR 24.80 billion (~ USD 1.62 million) identified as laundered funds.

Person X is believed to have been involved in the transportation and/or trade of protected wildlife from Aceh Tamiang, Medan, and Jakarta (Indonesia) to Jurisdiction A, utilising illicit maritime routes. The proceeds of these activities were allegedly concealed and/or disguised through accounts held in the name of Person. X's child before being transferred back into Person X's personal accounts.

The illicit funds were subsequently used to acquire assets such as motor vehicles and to finance business ventures, including palm oil plantations, vehicle trading, and a café business.

Source - Indonesia

Case Study # 31: Systemic bank hacking and laundering of illicit funds via crypto assets and money laundering syndicates

Third-party laundering; fraud; use of legal persons and arrangements; trust and company service providers; foreign predicate offence; transnational crime; structuring; financial institutions

Between June 2024 and April 2025, multiple incidents of banking system intrusions were reported, affecting several financial institutions and resulting in total losses of approximately IDR 641 billion (~ USD 90 Billion). The cases originated from complaints submitted by the affected banks, which reported suspicious transactions involving the unauthorised transfer of funds from customer accounts to accounts held at other banks. Notably, the withdrawn funds were not customers' deposits but the banks' own liquidity. Subsequent analysis revealed several distinct methods and typologies employed by the perpetrators:

- Timing exploitation: The attacks were executed during public holidays and weekends to take advantage of reduced monitoring and slower response times.
- Use of nominee accounts: The proceeds of crime were funnelled through nominee accounts registered under individual names and sole proprietorships, as well as cryptocurrency wallets obtained from account trading (bank and cryptocurrency).
- Exploitation of banking features: The perpetrators leveraged specific banking features — such as scheduled transfers — available exclusively to corporate or sole proprietorship accounts.
- Transaction structuring: The proceeds were fragmented into smaller transactions, each nearing the maximum limit allowed per transfer, and were rapidly distributed within a short time window, demonstrating high-speed layering tactics.
- Conversion to crypto assets: A portion of the illicit funds was converted into crypto assets, particularly USDT (Tether), through licensed crypto asset traders and peer-to-peer trading platforms.
- Use of professional laundering syndicates: The perpetrators engaged professional money laundering networks, some of which were previously linked to proceeds from narcotics trafficking, fraud, and human trafficking.
- Fake identities and cross-border activity: The crypto accounts used were registered with fraudulent identities, and the associated IP addresses traced back to jurisdictions including Thailand, the Philippines, Vietnam, Cambodia, Malaysia, and Lao PDR - jurisdictions also known for involvement in transnational crime.
- Use of un-hosted cryptocurrency wallets: Once converted, the crypto assets were entirely transferred to un-hosted cryptocurrency wallets associated with online gambling platforms, scam operations, and other criminal enterprises.

In response to the incidents, PPATK coordinated with relevant financial service providers and implemented mitigation measures, including the temporary suspension of suspect transactions.

Source - Indonesia

2.5 Japan

Case Study # 32: International joint operation with a foreign law enforcement agency

Fraud including romance scams; use of virtual assets; virtual asset service providers; transnational crime

The Japanese police participated in an INTERPOL-led operation named 'Operation Jackal', which aimed to take down organised financial crime rings in West Africa region. The National Cyber Department within the

National Police Agency of Japan analysed information regarding social media-based investment and romance scam cases happened in Japan and traced flows of involved virtual assets.

As a result, it was revealed that defrauded funds related to multiple cases had been transferred to virtual asset accounts owned by Jurisdiction A nationals. Therefore, the Japanese police provided related information with Jurisdiction A's police, and suspects in Jurisdiction A were apprehended. In addition, intermediaries in Japan were arrested by the Japanese police as well.

Source - Japan

Case Study # 33: The case of unauthorised acquisition and misuse of credit card information

Fraud including phone/SMS/email fraud/social media; transnational crime; use of credit cards

The Japanese police and Jurisdiction B's police identified Person A - the suspect of phishing cases based in Jurisdiction B. Person A used a phishing tool to obtain Japanese victim's credit card information and made unauthorised orders with their credit card information on some electronic commerce sites.

Jurisdiction B's police arrested Person A, and it was the first case for the Japanese police to clear a phishing case involving a suspect in a foreign jurisdiction by collaborating with a foreign law enforcement agency.

Source - Japan

Case Study # 34: Money laundering case using virtual assets regarding the case of an underground bank

Underground banking/alternative remittance services/hawala; use of virtual assets; virtual asset service providers; financial institutions

The suspect, who was **operating an underground bank** had received money at a domestic bank account from his client. Subsequently, he transferred it to an account of virtual asset service provider and purchased virtual assets using accounts under the name of fictitious or another person which had been obtained illegally.

In addition, he transferred the virtual asset to a virtual asset wallet in a foreign jurisdiction and sold it through a peer-to-peer transaction to obtain foreign currency and transferred it to a foreign bank account designated by the client.

Police arrested the suspect for violating the *Banking Act* and the *Organized Crime Punishment Act* (concealment of criminal proceeds).

Source - Japan

Case Study # 35: Money laundering case regarding the case of international fraud

Fraud; financial institutions

The Person A (not a Japanese citizen) was victim of a fraud case occurred abroad was being defrauded of money by repeatedly transferring money from an account in the name of Person A's employer to numerous foreign bank accounts.

Person B - the suspect who managed the deposit account in Japan received the money into a legal person account managed by Person B, disguising it as an export advance payment for a legitimate trade transaction (export of computer equipment).

Police arrested the suspect for violating the *Organized Crime Punishment Act* (concealment of criminal proceeds).

Source - Japan

Case Study # 36: Money laundering case misusing a shell company 1

Fraud; Use of legal persons and arrangements

Members of a criminal syndicate purchased a shell company, Company A and had the fraudulent funds transferred to an account in the name of that company. Subsequently, they transferred the funds to an account in the name of another company, Company B then used the account in the name of another company to purchase crypto assets to exchange them into a fiat currency.

Police arrested the offenders for violating the *Organized Crime Punishment Act* (concealment of criminal proceeds).

Source - Japan

Case Study # 37: Money laundering case misusing a shell company 2

Fraud including social media; use of legal persons and arrangements; Illicit gambling/gaming

A member of a criminal syndicate was arrested for recruiting people to become representatives of shell companies for rewards through social media. The syndicate member instructed them on how to set up legal persons and open legal person accounts and launder the proceeds of crime using those accounts.

It has become clear that this criminal syndicate, claiming to operate as a receiving agent, managed many shell companies and thousands of company accounts in an organised manner, and undertook money laundering of proceeds of crime from online and telephone fraud, social media-based investment fraud, online casinos, etc., committed by other criminal groups.

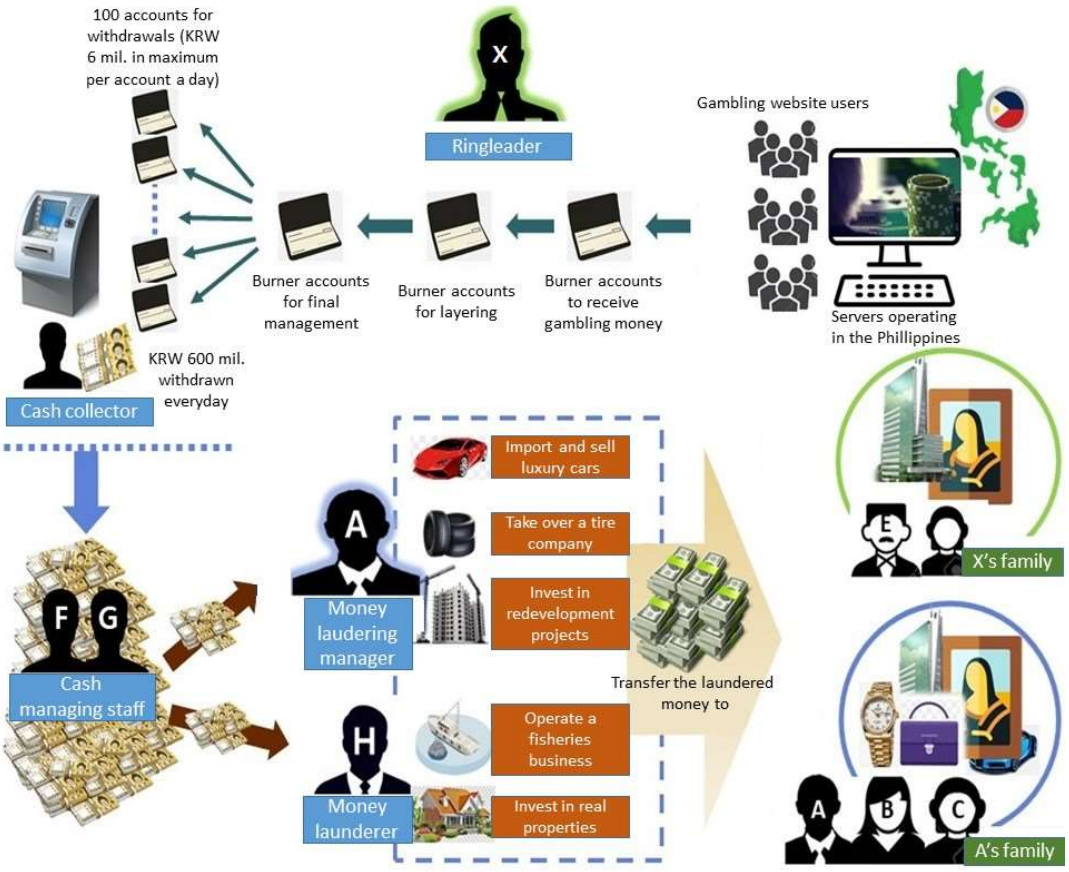
Police arrested the offenders for violating the *Organized Crime Punishment Act* (concealment of criminal proceeds).

Source - Japan

2.6 Korea

Case Study # 38: Laundering proceeds of crime from illegal gambling, etc. by means of cryptocurrency exchanges

Illicit gambling/gaming; trust and company service provider; purchase real property; purchase high value products/art pieces; financial institutions



The competent authority of Korea investigated a crime organisation which laundered proceeds of crime of about KRW 55 billion (~ USD 39 million), generated from illegal gambling websites with their servers in the Philippines from about July 2018 to about August 2022. Through the investigation, the competent

authority identified nine members of the organisation who committed money laundering by selling luxury cars, taking over a tire company, investing in redevelopment projects, operating a fisheries business (purchasing a vessel, etc.), purchasing a luxury apartment, using family's bank accounts, etc.

The competent authority prosecuted them in January 2024 and further secured assets worth about KRW 53.5 billion (~ USD 37.8 million) liable to forfeiture.

In December 2024, Person X, the ringleader who generally managed operations of the gambling websites, was arrested in Jurisdiction Z.

Extradition procedures on Person X are currently underway.

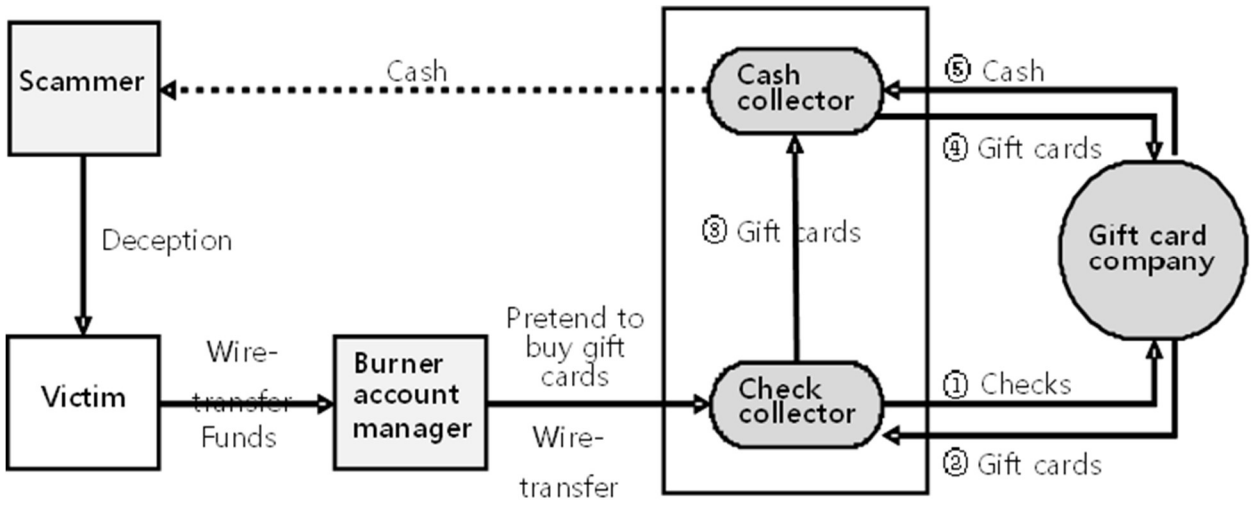
Source - Korea

Case Study # 39: Laundering proceeds of crime from voice phishing scheme by means of gift cards

Fraud (voice phishing); exchange/conversion to cash; abuse of legal person and legal system

While investigating a check collector involved in a voice phishing scheme in Korea, the competent authority detected a money laundering organisation which concealed proceeds of crime of about 20 billion (~ USD 14.1 million) from voice phishing. From about July to October 2023, the organisation, disguising itself as a gift card company, laundered proceeds of crime for the voice phishing organisation by converting gift cards of the voice phishing organisation into cash, pretending to carry out normal gift card transactions.

In November 2024, the Korean authority charged five criminals (including the CEO of the gift card company and check collectors) with fraud and violation of the *Act on Regulation and Punishment of Criminal Proceeds Concealment*. In addition, the authority seized proceeds of crime of about 2.8 billion through search and seizure, and asset recovery procedures against them, such as restraint for confiscation, are currently underway.



Source - Korea

2.7 Macao, China

Case Study # 40: Crackdown on criminal syndicate and money laundering case

Fraud; third-party laundering; use of credit/debit cards, cheques, promissory notes etc.; international cooperation; suspicious transaction reporting; use of legal persons; financial institutions; cash

The Judiciary Police (PJ) of Macao, China received reports from the police of Jurisdiction Z, the financial intelligence office of Macao, China and a local bank of Macao, China, alleging that five Macao, China-based companies were suspected of using corporate accounts to receive and process illicit funds obtained through telecommunications fraud in Jurisdiction Z. An investigation was subsequently launched.

Following an in-depth probe by PJ, the case was found to involve a criminal organisation composed of the residents of both Macao, China and Jurisdiction Z. Members of the group registered five companies –

purportedly engaged in frozen meat business, alcohol wholesale, electronics sales, and other businesses – as fronts. These companies utilised local POS payment platforms, personal accounts, and corporate accounts at the financial institutions in Macao, China to receive and process at least 438 transactions confirmed by the police of Jurisdiction Z as proceeds of fraud, involving approximately MOP36 million (~ USD 4.5 million).

During the investigation, PJ successfully intercepted the transfer of part of the illicit funds and seized over MOP 7 million (~ USD 870,000) in illegal proceeds.

On 22nd May 2024, PJ arrested two local male suspects. The PJ seized bank cards used to receive, transfers, and withdraw illegal funds, along with USD 34,000 in cash suspected to be proceeds of crime from their residences.

Based on evidence gathered, the two suspects were charged with criminal syndicate offences and money laundering and have been referred to the Public Prosecutions Office (MP) of Macao, China for further legal proceedings.

Source - Macao, China

Case Study # 41: Fraud syndicate laundered funds using third parties' bank accounts

Organised criminal syndicate; fraud; third-party laundering; professional money laundering; cash; wire transfer; financial institutions

From at least July 2023, three local suspects agreed with several other individuals to work together, each in a specialized role, to participate in a criminal association for the purpose of committing fraud and money laundering.

In order to conceal the illegal source of the proceeds of crime and the identity of the criminals, the three suspects allowed the syndicate members to use their personal bank accounts, assisting them to receive the defrauded money. They made their bank accounts available to persons higher-up in the syndicate to transfer the funds to other local bank accounts or made the transfer according to the instructions of persons higher-up in the syndicate or withdrew these funds in cash to designated persons.

This assisted the persons higher-up in the syndicate in collecting and transferring the funds obtained by committing fraud crimes to achieve the purpose of money laundering. The amount received and processed through their bank accounts exceeded MOP 2 million (~ USD 250,000).

In 2024, the Public Prosecutions Office prosecuted the three suspects for criminal association and money laundering.

Source - Macao, China

Case Study # 42: Crackdown on credit card fraud syndicate

Fraud; third-party laundering; use of credit/debit cards, cheques, promissory notes etc.; suspicious transaction reporting; cash; financial institutions

In December 2023, six local merchants in Macao, China were reported to be involved in conducting false transactions by using stolen credit cards. Most of the funds were withdrawn by cash after transferring to the shareholder Person X and his spouse Person Y's bank accounts.

The FIU of Macao, China (GIF) received STRs from several local banks indicating that an overseas card-issuing organisation had detected more than 100 unusual credit card transactions by dozens of overseas customers at local card dealers, beauty salons and engineering companies in December 2023, with a reported loss of around USD 1 million, and that it was suspected that the transactions were related to fraud. GIF then reported the suspicious transaction reports to the Public Prosecutions Office for further investigations by law enforcement agencies.

In March 2024, Judiciary Police (PJ) closed down a bank card fraud syndicate and arrested three local men and women involved in the case, who operated local car dealership, beauty salons and engineering businesses. Evidence showed that the illegal gains involved at least MOP4.4 million (~ USD 550,000).

After in-depth investigation, PJ found that a large number of credit cards were frequently and intensively used within a short period of time in a number of stores in Macao, China, including car dealerships, beauty salons and engineering companies, involving a total of 110 transactions, all of which were bundled with cell phones in the form of online payment transactions. PJ analysed and found that the flow of funds was related to the persons in charge of the above stores, including Person X, Person Y and Person Z. The investigation revealed that these fraudulent credit card transactions began at the end of November 2023.

The case involved the credit card information of 71 overseas customers, none of whom were local residents.

Source - Macao, China

Case Study # 43: Suspected money laundering syndicate

Fraud; illegal extortion; child abuse; third-party laundering; account transfer; cash; international cooperation; suspicious transaction reporting; financial institutions

The FIU of Macao, China (GIF) received suspicious transaction reports indicating that between January and October 2022, a local resident Person L of Macao, China used his bank account to receive cash and fund transfers from third parties. The funds were then withdrawn in cash by ATM. However, one of the transfer counterparty Person H was involved in a fraud case in April 2022, and Person L was also being investigated. It was suspected that Person L was using his bank account to handle illegal proceeds related to fraudulent activities which was subject to investigation.

In addition, the source of funds from another transaction counterparty Person D, who was a resident of Jurisdiction B, also came from cash deposits and third-party transfers during January 2022 to August 2023. She then withdrew all the funds in cash and transferred them to other third parties who were also residents of Jurisdiction B. GIF proactively sent request to the FIU of Jurisdiction B and asked for intelligence, if any.

Later on, intelligence provided by the FIU of Jurisdiction B indicated that Person D and several other individuals were suspected to be involved in criminal activities such as fraud, illegal extortion, and child abuse in Jurisdiction B. In light of this, the case was passed to the Public Prosecutions Office for further investigation in 2024.

Source - Macao, China

2.8 Malaysia

Case Study # 44: Money laundering through company formation

Fraud; counterfeit products; financial institutions

In May 2023, the Malaysian FIU made a financial intelligence disclosure to a lead ministry in Malaysia. Following the receipt of the information, an enquiry paper was initiated to obtain more information for the purpose of investigation and identification of potential predicate offences.

In December 2023, a joint operation was initiated involving multiple law enforcement agencies, where actions had been taken under the *Trademarks Act 2019* and the *Anti-Money Laundering, Anti-Terrorism Financing and Proceeds of Unlawful Activities Act 2001* (AMLA), targeting the distribution of suspected counterfeit and unregistered cough medicines by a syndicate.

The company/syndicate was suspected of processing and storing various raw materials and packaging bottles to produce counterfeit cough medicine, using well-known brands as a cover. The counterfeit cough medicine was then distributed to local pharmacies and other places for purposes other than medicine.

During the joint operation, 10,000 bottles of suspected counterfeit cough medicine and approximately 900 litres of liquid in a mixing machine were seized. Additionally, a vehicle and other equipment used for processing the suspected fake cough medicine were found.

Authorities have taken significant actions against companies and individuals involved in illicit activities. A total of 56 bank accounts, amounting to RM10.5 million (~ USD 2.5 million), have been frozen, and two premises used as processing sites, valued at RM2.6 million (~ USD 614,000), have been seized. Further investigations led to the seizure of 18 more accounts totalling RM7.9 million (~ USD 1.86 million) under section 50(1) of AMLA. Additionally, two immovable properties worth RM2,607,181.02 (~ USD 614,000) were seized under section 51(1) of AMLA, along with movable properties found within these buildings under section 45(2) of AMLA 2001.

In May 2024, two companies and two company directors were charged at the Sessions Court under Section 100 of Trademarks Act 2019, related to a predicate case. The investigation into money laundering activities is still on-going.

Source - Malaysia

Case Study # 45: Money laundering through company formation

Use of legal persons and arrangements; financial institutions

The case involved a pyramid scheme offered by a multinational corporation. Under this scheme, each member was required to invest a certain amount of money and recruit in two downlines (each downline providing a similar amount of investment value as the upline) to enable the member to obtain returns.

The directors of the corporation were alleged to have used the bank accounts belonging to the corporation as instruments to launder proceeds of unlawful activities. The proceeds of crime were allegedly deposited in three different banks in various locations between 2016 and 2020. 16 premises belonging to the corporation were raided during a joint enforcement, following a month-long investigation by the authorities from various agencies.

In September 2020, the corporation was sentenced to a fine of RM 9 million (~ USD 2.1 million) by the Sessions Court on three charges of money laundering offences. The directors were also charged with three counts of using the corporation's bank accounts as instruments for money laundering. The trial is currently ongoing.

Source - Malaysia

Case Study # 46: Methamphetamine and cocaine drug trafficking syndicate

Foreign predicate offence; drug related crime

In early June 2024, the Narcotics Crime Investigation Department of the Royal Malaysian Police (RMP) received a drug syndicate intelligence from a foreign jurisdiction involving methamphetamine and cocaine being smuggled to foreign jurisdictions.

RMP investigated based on the information given and found a few drug syndicate members in Malaysia. After a close follow-up and surveillance on this drug syndicate, an operation was launched in July 2024.

During this operation, RMP successfully arrested three Malaysians and seized a total of 44.9 kg of cocaine, 60,000 ml of illicit liquid chemical and 1kg of powder chemical. The total drug seized is worth of RM 8.9 million (~ USD 2.1 million) and property seized worth RM 1.49 million (~ USD 352,000).

The Malaysian FIU assisted the RMP to obtain financial intelligence on the three main suspects. Case is on-going, and all the arrestees are being investigated under Sec. 39B of *Dangerous Drugs Act 1952* (DDFOPA). (When prosecuting ML related to drug trafficking, Malaysian authorities also use the DDFOPA).

Source - Malaysia

2.9 Mongolia

Case Study # 47: Corruption, money laundering

Corruption and bribery; politically exposed persons; international cooperation; cash; financial institutions

In 2023, based on information submitted by the relevant Mongolian ministry, the law enforcement authority opened a case under Article 22.1-2 of the Special Part of the *Criminal Code of Mongolia*.

In 2015, the Government of Mongolia signed a Financing Agreement with the donor agency for USD 12.7 million to implement the 'E-Health' project in Mongolia's healthcare sector. As part of this project, an international open tender was conducted in two phases to develop and implement a Health App - a digital platform for the exchange medical information.

On 16 April 2020, the Evaluation Committee reviewed the bids and approved the signing of a contract with a consortium of Company B and Company T (located in Jurisdiction V) for USD 6,038,000. The Evaluation Committee issued a notification on 10 June 2020, and the contract was officially signed a partnership agreement with Company B and Company T on 19 August 2020. According to the tender documents, Mongolian Company A was designated to work as a subcontractor under the partnership of the project's general contractors, Company B and Company T.

During the investigation, it was revealed that the donor agency's project team leader had issued a letter suspending funding due to the consortium's unsatisfactory performance. Despite this, a politically exposed person, Person S abused his position to favour Company A, resulting in the transfer of USD

1,161,360 from Company T to a bank account at Bank H in Jurisdiction V on 7 July 2022. The law enforcement agency also cooperated with the FIU-Mongolia in exchanging information during the investigation.

Upon tracing the second funding instalment of USD 1,161,360, the following transactions were identified in Company A's account:

1. USD 260,416.96 received from Company T (Jurisdiction V) on 22 July 2022
2. USD 99,585.04 received from Company B (Jurisdiction V) on 21 July 2022
3. USD 597,495.24 received from Company B (Jurisdiction V) on 2 August 2022

Total: USD 957,497.24

On 30 March 2022, Company A signed a fraudulent contract worth USD 910,800 with Company K for the supply of computers, servers, and equipment. On 8 August 2022, Company A transferred USD 660,000 and USD 250,800 - totalling USD 910,800 - to Company K's USD account at a bank in Mongolia.

Subsequently, CEO of Company K, Person Y, withdrew the funds in cash and used them to purchase a 1,200 sqm commercial property in Ulaanbaatar, from Person T. The property was later transferred to another company jointly owned by fugitive suspect Person E (50%) and Person M (50%), who were determined to have shared interests.

On 4 March 2024, the District Criminal Court of First Instance issued a 48-hour arrest warrant for the fugitive Person E, effective from his date of entry into Mongolia. He is also internationally wanted under INTERPOL's Blue Notice. In addition, the relevant Mongolian authorities have submitted a mutual legal assistance request to the competent authorities of the jurisdiction where Person E is currently residing - seeking his extradition as the perpetrator of the crime, and are jointly conducting the related proceedings.

Following multiple formal and informal meetings between law enforcement agencies and representatives of the donor agency to recover stolen funds from Mongolia, a decision was made on 3 April 2024, to debar Company T from participating in tenders announced by the donor agency for a period of 30 months and to impose related sanctions.

On 19 June 2024, Company T refunded USD 1,718,360 to Mongolia's Ministry of Finance, so it could fully compensating the donor agency for its losses.

Source - Mongolia

Case Study # 48: Illicit gambling/gaming, money laundering

Illicit gambling/gaming; purchase of real estate; self-laundering

Citizens of Mongolia, Person A and Person B, operated an illegal gambling business called 'Poker Paradise' from October 2021 to February 2024, in an apartment located in Khan-Uul District, Mongolia. They used information technology to conduct games of chance with unpredictable outcomes, intending to generate profits via public social media platforms. The perpetrators, fully aware of the illegal nature of the gambling operation, concealed the proceeds of crime by purchasing vehicles and real estate in the names of others during this period with the intention of laundering money.

As it was confirmed during the investigation, Person B was involved in withdrawing the illicit funds obtained from this criminal activity through commercial bank ATMs and POS devices. Person A and Person B were found to have laundered proceeds of crime obtained from criminal activity totalling USD 162,000.

They purchased real estate worth USD 81,510, including two land plots and one immovable property, under the names of family members, and transferred USD 37,600 to their associates to conceal the origin of the funds and commit the crime of money laundering.

During the investigation, through the timely information exchange and acquisition of financial information of Person A and Person B, and their related parties via FIU-Mongolia, the investigation was promptly organised, enabling the examination of the use of illicit income and the restriction of asset transfers.

The District Criminal Court of First Instance sentenced defendants Person A and Person B to a fine on 31 December 2024. Additionally, illegal assets obtained from the afore-mentioned crimes, including two land plots, one real estate property, and funds in the accounts of their associates, were confiscated and transferred to state revenue by the court order.

Ultimately, a total of USD 119,100 was recovered as state revenue.

Source - Mongolia

2.10 Myanmar

Case Study # 49: Human trafficking via online

Fraud; human trafficking

At approximately 09:00 hours on 9 June 2023, Police Officer Z, while serving as the duty officer at the No. (1) branch of Anti-Trafficking in Person Police Force (Tachileik), received a report from a woman Person Y, residing in Yan Aung Village, Tarlay Town, Tachileik Township. She reported that her elder sister, Person L, had been trafficked as a bride in exchange for approximately USD 4,200 and requested assistance in rescuing her.

Upon investigation, it was found that in or around June 2023, Person L became acquainted with a woman identified as Person E via Facebook. Person E had posted an advertisement stating that females who interested in exclusive job opportunities could contact her. Person L reached out and Person E persuaded her that if she married a foreign national in Jurisdiction A, she would receive a large sum of money and could return home after one year of cohabitation.

Subsequently, on 24 May 2023, Person. E transported Person L by motorcycle to an individual Person N in Kyaing Tong. On next day, another individual Person S transported Person L by motorcycle in stages from Kyaing Tong to Mong Yawng, and then to Mong Pauk. From Mong Pauk, Person L was trafficked across the border to Jurisdiction A, where Person L was sold to a foreign national for approximately USD 4,200.

On 18 January 2024, Person L managed to return to Myanmar. Based on the findings, legal action was initiated against Person E (arrested), Person N (arrested), and Person S (absconding), by Police officer Z of the No. (1) Branch of Anti-Trafficking in Person Police Force (Tachileik), who filed a formal complaint requesting prosecution in accordance with the law.

As a result, on 10 June 2023 at 23:55 hours, a case was officially opened at Tarlay Police Station under Case No. (Pa) 4/2023, pursuant to Sections 35/44 of the ***Anti-Trafficking in Persons Law***.

Source - Myanmar

Case Study # 50: Human trafficking via trust

Fraud; human trafficking

At approximately 09:00 hours on 27 September 2024, while Police Officer K was on duty with the No. (11) Branch of Anti-Trafficking in Person Police Force (Mandalay) a report was received stating that a woman Person M had fled near Tekkone Village, Patheingyi Township, fearing that she was about to be trafficked and sold as a bride. Acting on this information, an investigation and inquiry were promptly conducted.

Findings revealed that on 30 August 2024, Person M had been seeking to apply for a passport with the intention of going to work in Jurisdiction Y. During her search online, she came across a TikTok account belonging to an individual identified as Person D, which advertised that passport applications could be arranged and that inquiries could be made via Telegram. Upon contacting Person D, Person M was informed that a passport could indeed be arranged. She was subsequently brought to stay at Person D's residence in Tekkone Village, Mandalay, under the pretence of processing her passport.

On 2 September 2024, Person M was taken to the Department of Immigration offices in Myawaddy, via Mandalay and Kawthoung, to apply for a passport. After completing the application process, she returned to Person D's residence in Mandalay.

On 21 September 2024, Person D proposed that if Person M was willing to become a bride, she would receive approximately USD 5,600 as a dowry, a set of gold jewellery, and a monthly support payment of MMK 2,000,000 (~ USD 950) for her parents. Person D further contacted a foreign national through the WeChat platform and showed him full-body photographs of Person M. Additionally, Person D's husband, Person C, attempted to further persuade Person M to agree to the arrangement. It was also discovered that Person D had deleted the Telegram and Viber accounts from Person M's phone, removed both SIM cards, and confiscated them. Person M was not permitted to leave the premises freely.

On 25 September 2024, which was Person M's birthday, Person D arranged for a foreign national in Jurisdiction Z, who was intended to marry her, to transfer approximately USD 420 as a form of gift. While Person D was briefly out of the house, Person M, unwilling to go through with the arranged marriage, took her hidden national registration card and smart card from beneath a mattress and fled.

Following the investigation, it was determined that legal action should be taken against Person D (arrested) and Person C in accordance with the law. Therefore, Police Officer K of the No. (11) Branch of Anti-Trafficking in Person Police Force (Mandalay) filed a formal complaint requesting prosecution.

Subsequently, on 2 October 2024, at 18:10 hours, a case was officially opened at Patheingyi Township Police Station under Case No. (Pa) 310/2024, pursuant to Section 35 of the Anti-Trafficking in Persons Law.

Source - Myanmar

2.11 New Zealand

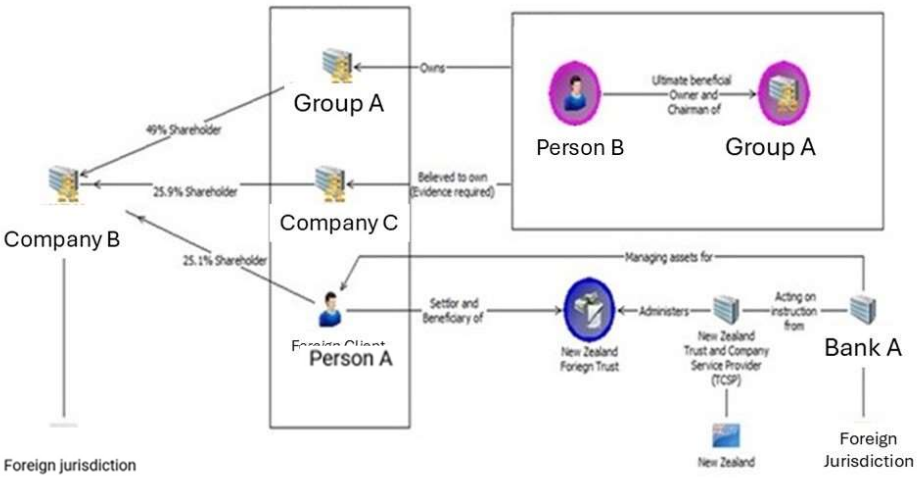
Case Study # 51: Misuse and abuse of trust and company service providers by sanctioned entities

Third-party laundering; third-party laundering; use of legal persons and arrangements; trust and company service providers; foreign predicate offence; sanctions evasions

The Department of Internal Affairs (DIA) became aware that a foreign national (Person A) who was a client of a New Zealand trust and company service provider (TCSP) may be subject to the New Zealand's domestic sanctions legislation. An investigation by New Zealand Police was therefore instigated to determine if the Person A's close association to a sanctioned foreign person (Person B), deemed him sanctioned also. If the Person A is found to be sanctioned by association, the TCSP has breached the legislation by not taking action to cease providing financial services to Person A and dealing with his assets held in his New Zealand foreign trust.

Cessation is a requirement under New Zealand's domestic sanctions legislation. The TCSP would also be in breach of another key requirement which requires a suspicious transaction report to be submitted to the financial intelligence unit about their dealings with a sanctioned person. The TCSP is providing the financial services on instruction from Bank A in a foreign jurisdiction; who is an asset management firm who manages assets for Person A.

Person A is a business associate of a prominent foreign oligarch (Person B) who was listed as a sanctioned person on New Zealand's domestic sanctions legislation Register on 20 April 2022. Person B has ties to a prominent politically exposed person (Person C) and owns 'Group A'; a group of global companies involved in the aluminium, oil, energy, real estate, telecoms and other sectors. The client is a real estate subsidiary of Group A. Such a position held in a company that is 50% or more owned by the Person B, deems Person A an 'associate' as defined under New Zealand's domestic sanctions legislation. It also states that 'associates' are a class of person that are deemed sanctioned persons.



The difficulty is Group A restructured the ownership of their group of companies prior to New Zealand, and other jurisdictions, enforcing sanctions against Person B. It is believed this was done deliberately to evade sanctions. As a result of the restructure, Group A only owns 49% of Company B; this is below the '50% or more' threshold of ownership required by the Regulations to deem a subsidiary and its director an 'associate'.

However, the investigation has found it is likely Person Bis the true owner of the company - Company C, which owns 25.9% of Company B. If evidence can be obtained proving this, the '50% or more' threshold will be met as Person B effectively owns 74.9% of Company B:

This case reinforces how trusts can be exploited/misused by sanctioned entities to obfuscate beneficial ownership information. The risk of TSCPs mainly lies with their willingness and thoroughness in checking the legitimacy of people (including trustees, directors, and shareholders etc) involved in the proposed New Zealand company - known as know your customer (KYC) in the industry. The standards for KYC are set out in the *Anti-Money Laundering and Countering Financing of Terrorism (AML/CFT) Act 2009*. A TCSP can be actively deceptive, as in the example of the now infamous shell company creation giant Mossack Fonseca, which was exposed by the Panama Papers.

However, TCSPs can also be negligent in their dealings with sanctioned entities or providing services to a sanctioned entity. While this is not active deception, the failure to properly assess the risks posed by their clients and apply the relevant standards outlined in the AML/CFT Act poses just as much of a threat to both the TCSP themselves and New Zealand.

Source – New Zealand

2.12 Pakistan

Case Study # 52: Money laundering through IMVTS

Tax evasion; offshore beneficial ownership; use of legal persons; hawala/hundi; international cooperation; corruption and bribery; cash

A pharmaceutical company in Pakistan, has its directors (Person A and Person B) serving as nominee directors of an offshore company registered in an offshore financial centre. Within less than a year, the pharmaceutical company transferred hundreds of millions of rupees to a partnership firm - M/s T Services - through high-value transactions. Enhanced due diligence conducted by the bank to determine the purpose and nature of these transactions revealed that, through its arrangement with M/s T Services, the pharmaceutical company concealed excessive marketing expenses, generated fake invoices for luxury goods, and used the supply contract to funnel bribes in the form of supplies.

Further, currency transaction reports worth billions of rupees were reported against the pharmaceutical company within a period of around two years. A number of these transactions were conducted with unrelated parties. Financial intelligence on six of these unrelated counterparties from a high-risk region, who deposited cash into accounts of the company, had previously been shared with the law enforcement agencies **on suspicion of hawala/hundi operations** and tax evasion.

This case is under investigation with the relevant law enforcement agency. As part of the investigation, the law enforcement agency has also raised a request for informal international cooperation on one of the directors serving as its nominee in the offshore company.

Source - Pakistan

Case Study # 53: Human trafficking concealed under the guise of human resource services and travel agencies

Misuse of debit card; organised criminal syndicate; human trafficking; money value transfer services

Pakistan-based human resource services provider (Company B) supplied construction workers and engineers to an energy sector company to a North African jurisdiction. An individual - Person A, residing in a gulf jurisdiction, made remittances equivalent to millions of rupees on behalf of Company B from a gulf jurisdiction into the accounts of different individuals in Pakistan. Person X, another individual residing in Pakistan and working as an employee of a travel agency (Company J) owned by her close relatives, also remitted millions of rupees into the accounts of individuals who received remittances from Person A.

All beneficiaries of the remittances/transfers from Person A and Person X held their accounts in different branches of the same bank. During customer due diligence inquiries, one of the remittance recipients disclosed that his brother is currently in a refugee camp in a European jurisdiction. Another branch disclosed that the son of other remittance beneficiary is imprisoned in a North African jurisdiction.

Further analysis revealed suspicious use of a debit card issued to Person IA (a beneficiary of remittances from Person A) in some European jurisdictions for a small-value POS and cash transactions. These locations are commonly associated with the 'Dunki' Route, a term used for illegal migration or human

trafficking. While Person A's debit card was used abroad, travel records confirmed that Person A never officially travelled abroad.

This case is under investigation with the law enforcement agencies.

Source - Pakistan

Case Study # 54: Human trafficking through travel consultant

Cash deposits; human trafficking; use of cheques; suspicious transaction reporting

Person B was placed on *Red Book of Human Smugglers and Traffickers* during 2023 due to multiple cases registered against her by a concerned law enforcement agency. Accordingly, various banks raised suspicious transaction reports against her. In terms of the information shared, she was running a travel consultancy business under two different names. Person B maintained multiple personal and business accounts and routed millions of rupees to unrelated counterparties through mobile-banking and cheque deposits.

Analysis of multiple suspicious transaction reports filed by banks highlighted frequent cash deposits and transfers in Person B's accounts from different geographies mismatching with her profile as a travel consultant. Further, she made frequent visits to one of the gulf jurisdictions.

The intelligence was shared with law enforcement agencies for facilitation in further investigation.

Source - Pakistan

Case Study # 55: Money laundering through cash-intensive business

Cash deposits/withdrawals; hawala/hundi; IMVTS; smuggling; tax evasion

An individual Person C, running a supermarket in a border region of Pakistan, was flagged by several banks for suspicious financial activity. Despite declaring himself as a small-scale businessman, he opened numerous personal and business accounts with different banks, including some accounts in the names of minors. He conducted high value financial transactions with parties located in different geographical locations and was found involved in businesses unrelated to his declared line of business. Turnover in Person C's accounts exceeded over a billion PKR (~ USD 3.5 million) in the last few years, which was primarily routed through high-value cash transactions.

As per travel records, Person C had undertaken visits to high-risk jurisdictions, while tax records fail to support the financial activities in his accounts and those of his main counterparties. Also, financial intelligence on Person C's counterparties was previously disseminated to concerned LEAs **on account of hawala** and smuggling, and the parties are under inquiry.

Considering Person C's transactional activity and the above findings, the case of Person C was disseminated to LEAs to investigate possible involvement in smuggling, tax evasion and hawala.

Source - Pakistan

Case Study # 56: Money laundering through benami accounts

Cash deposits; benami (nominee) account; financial institutions

In 2024, a young adult - Person D was reported due to discrepancies in his know your customer information provided to the banks. The individual opened multiple personal and business accounts at various banks during the last three years, each with a different signature, while declaring himself as a construction-related contractor. The differences raised suspicion regarding the true beneficiary of the funds. These accounts received substantial cash deposits, which were withdrawn shortly afterwards and deposited to the Person D's other bank accounts.

The total transactional activity across Person D's accounts amounted to billions of rupees, which corresponded neither to his reported profile and business financial activity nor reflected in his tax record. Analysis indicated potential money laundering activity involving the placement and movement of funds through these apparently benami accounts.

The financial intelligence was shared with the relevant law enforcement agencies which are currently investigating the case.

Source - Pakistan

Case Study # 57: Affiliation with human trafficker

Cash deposits; human trafficking; suspicious transaction reporting; financial institutions

A suspicious transaction report was reported on Person E on account of a mismatch with his declared profile and the transactional activity in the bank account. He declared that he would receive funds from his brother for financial support into his bank account. Later, the account activity showed high turnover with credits exceeding 100 million PKR within a year's time. The account received funds either through cash deposits or online funds transfers.

Counterparty analysis revealed that Person E had transferred millions of rupees to Person Z, who is already under investigation with the relevant law enforcement agency regarding human trafficking case related to a boat capsizing incident (February 2025), which led to death of a number of Pakistani nationals. Person Z's identification documents indicated that his place of birth was a North African jurisdiction. He maintained multiple bank accounts, where turnover exceeded half a billion rupees. Travel records further showed recent visits of Person Z to the North African jurisdiction.

The financial intelligence was disseminated to law enforcement agencies to further investigate the matter for possible involvement in human smuggling activities.

Source - Pakistan

2.13 Philippines

Case Study # 58: The PHP 200,000 job that never was

Fraud; third-party laundering; financial institutions

The use of social media by scammers to entice people to pay placement fees for a job abroad.

In December 2020, Person B was using his personal social media account to search for a job. He met Person E and Person D who introduced themselves as representatives of Agency H, a legitimate online recruiter.

Person B inquired about the legitimacy of Agency H through the social media platforms messaging service. Person B's discussion with Agency H was transferred later to a social messaging platform. Transactions were made through the said social messaging platform.

In January 2021, Person B was instructed several times to transfer amounts to Person D's different bank accounts for payment of Person B's placement fee. Person B transferred a total of PHP 200,000 (~ USD 34,460) to Person D's bank accounts. In June 2021, Person B was once again instructed to pay another placement fee. It was at this moment that Person B realised that he was scammed.

Person B made several follow-ups regarding the job but to no avail. Person B filed a complaint before the Philippine National Police. Complaints were filed against Person D (and other conspirators) before the Department of Justice (DOJ). After evaluation, the DOJ charged Person D et. al. for violating Article 315 of the *Revised Penal Code* (Swindling/Estafa) and the *Migrant Worker and Overseas Filipino Act*.

Source - Philippines

Case Study # 59: No OTP, no mercy

Fraud; third-party laundering; use of cheques; financial institutions

Swindling and Estafa involving hacking through phishing.

In May 2023, customers of an electronic money issuer (EMI) took to social media the alleged unauthorised transfers from their wallets to a bank account without the need for any one-time password (OTP) confirmation.

Later, the bank wherein funds were transferred sent a confidential email to the Bangko Sentral ng Pilipinas (BSP), confirming that the beneficiary account of the unauthorised EMI transfers is under the name of Company A. The bank further reported that one of the beneficial owners and authorised signatories of Company A, went to one of the bank's branches, together with a representative, to inquire about the balance of the subject account. When the bank questioned the number of online transfers, they explained that these were payments from online customers from Lazada, Shopee, and TikTok, for which they undertook to provide the invoices for the transactions. Later, the representative returned to cash a cheque from Company A, signed by its authorised signatory, worth PHP 3 million (~ USD 51,700). When the bank

verified the issuance and encashment to Company A, the same was confirmed by the authorised signatory.

The bank noted that there were 1,122 EMI transfers from 988 various individuals totalling PHP 28,300,872 (~ USD 487,600) to Company A's account starting at around 9:00am in the morning until around 3:00pm in the afternoon, just before the cheque encashment by Company A's representative.

Since the volume and velocity of transactions deviated from Company A's profile, the bank decided to hold the remaining funds in accordance with the provisions of BSP Circular No. 1160 series of 2022, implementing Republic Act (RA) No. 11765 otherwise known as the 'Financial Products and Services Consumer Protection Act', which states that in case of unauthorised transactions, the receiving financial institution, pending investigation, should hold the disputed funds, if still intact, or perform such other necessary actions to protect the Financial Consumer's interest and/or assets, such as but not limited to, account blocking or freezing of funds.

According to the bank, Company A attempted to negotiate four more cheques payable to 'cash' by depositing the same to another bank account in the name of Company E or Company S. Total amount of four cheques is PHP 25 million (~ USD 430,750). The bank decided not to clear the remaining four cheques issued by Company A dated xx May 2023, hence, the said cheques were returned on 9 May 2023.

In June 2023, the Bank received a letter from the EMI requesting the bank to continue the freezing of Company A's bank account pending its investigation. The EMI attached in their letter a Sworn Statement stating that their initial probe revealed that an organised phishing attack happened, resulting in the successful change of devices linked to the victims' EMI accounts. Consequently, a total of PHP 28,300,872.16 (~ USD 487,600) was siphoned to Company A's bank account. The EMI likewise attached an Indemnity Letter declaring that the bank and/or any of its officers, employees, agents, and representatives are absolutely, completely, and forever released, cleared, and discharged from any action, damages, demands, and any further liability whatsoever emanating from the continuous freezing of Company A's bank account pending the EMI's investigation.

In July 2023, the bank requested the assistance of AMLC to obtain a freeze order which will facilitate the preservation of the funds, in view of the inadequacy of detailed guidelines of RA No. 11765 as regards the duration of freezing the funds, the conditions for the release, and what to do in case of conflicting claims, among others. Thereafter, an EMI representative executed a Complaint-Affidavit narrating in detail how the phishing scheme was implemented by the cybercriminals through Company P, an unlicensed online casino which ostensibly operates Company H, Company K, and Company D.

The EMI further averred that after gathering and analysing information and documents, it was discovered that aside from the 1,122 unauthorised transfers to Company A's bank account, worth over PHP 28.3 million (~ USD 487,600), there were additional 485 transfers totalling PHP 8,918,707.85 (~ USD 153,687) on the same day to another bank account. In sum, EMI customers were robbed an aggregate amount of PHP 37,219,580.01 (~ USD 641,200) through 1,607 fund transfers to Bank A and Bank Z.

Source - Philippines

Case Study # 60: Romanced and robbed

Fraud; romance scam; third-party laundering

Person M narrated that she was messaged by a social media account named Person O. Person M and Person O made a deeper conversation and connection with each other for more than a month which resulted in a "romantic relationship". Person M and Person O continued their conversation in a social messaging application, because Person O's social media account was allegedly hacked in November 2021.

Person O mentioned that he sent a package for his commitment and love to Person M and told that someone will call to pay any charges/fees. Thereafter, Person M deposited PHP 216,300 (~ USD 37,270) a Bank B account under the name of Person D for payment of "demurrage" (the costs of holding the package).

Later, a certain Person S, represented that she is a representative from 'U Logistics'. Person S instructed Person M to pay PHP 250,000 (~ USD 4,300) for the release of the said package. Person O and Person M argued about the amount. Person O promised Person M that she can recover the amount from the package. Thus, Person M deposited PHP 250,000 (~ USD 4,300) to Bank C under the name of Person D for payment of 'Tax Certificate'. Thereafter, Person M deposited PHP 150,000 (~ USD 2,600) to Bank B under the name of Person G for payment of 'demurrage'.

After all the payments, Person M tried to contact Person S and Person D for the confirmation of payment and the delivery date of the package. However, their numbers are already inactive after the transaction. Person M reported the incident to the Philippine National Police.

Source - Philippines

Case Study # 61: From sweet talks to wire transfers

Fraud; romance scam; third-party laundering; wire transfers; money value transfer services; financial institutions

Romance scam with international inward remittance.

The Philippine National Police sent a several letters to the AMLC regarding the scamming activities of Group A. In one of the letters, it was alleged that Person Z was a victim of a romance scam. According to the said letter Person Z was invited through social media by one of the members of the Group A. Person Z's exchange with one of the members of the Group A led to an 'intimate relationship'.

Person Z was thereafter led to deposit money to the bank accounts provided by the members of the Group A.

Financial investigation revealed that the bank accounts wherein Person Z deposited money belonged to Person M. Further investigation led to the discovery of several reports filed by a money service business (MSB) against Person M for possible romance scam involvement. The subject transactions reported were in the form of international inward remittances from different foreign jurisdictions which includes the United States of America, Sweden, and South Korea.

Source - Philippines

Case Study # 62: From crypto craze to criminal case

Fraud; third-party laundering; financial institutions

Solicitation through social media by an unlicensed entity engaged in cryptocurrency trading.

The AMLC's investigation was triggered by letters from the Securities and Exchange Commission (SEC) following a public advisory against dealing with Company A, an unregistered and unlicensed entity engaged in investment solicitation through social media.

Company A was a trading company that used to perform cryptocurrency trading. It had invited the public to invest in it by guaranteeing a 3% return on investment every working day or a profit of 150% of the amount invested in 50 working days. On top thereof, Company A assures the public of an additional 5% that would be given for Direct Referrals under the investor's name or .5% for Indirect Referrals. Company A started soliciting investments sometime in August 2020, which abruptly ended on 14 April 2021.

After further investigation, the SEC filed a complaint before the Department of Justice for violation of the SRC against Person G and Person R, the top head of Company A, among others, in connection with Company A's investment scheme

Financial investigation revealed that Company A is not registered with the SEC either as a corporation or as a partnership. It is neither authorised to solicit investments/placements from the public nor issue investment contracts and other forms of securities. It has not secured prior registration and/or license from the SEC as prescribed under Sections 8.1 and 28.1 of the SRC. Furthermore, a Criminal Complaint for Estafa/Swindling was filed against members and soliciting agents of Company A, in connection with the latter's investment scheme.

Further financial investigation revealed that Person G is the main orchestrator of Company A. Person G's Bank Account had been used as the repository of the collected investments to Company A. The said account had been the recipient of money transferred by persons related to the investment scheme, such as Person R, who was known as the top head of the investment scheme, and Person, a known member and soliciting agent of Company A.

Source - Philippines

Case Study # 63: Foreign currency and false promises

Fraud; third-party laundering

Online solicitation for investment scam.

The Securities and Exchange Commission (SEC) requested the AMLC to investigate relative to the unauthorised investment solicitation activities of Person S, Person A, Person P, Person V, Person L, Company X, Company Y, and all persons connected therewith.

The Philippine National Police (PNP) requested the AMLC for information on SSS, for the crime of Swindling/Estafa, in relation to *Cybercrime Prevention Act* of 2012.

Based on the reports gathered by the SEC, from 2017 to 2020, Person S and Person A of Company X (doing business under the name Company Z) invited the public to invest in foreign currency trading under a fund management service called Investment P.

The Investment P Services Agreement contains the terms and agreements executed by the investor and fund managers. Person S and Person A were the designated fund managers and the traders. The said agreement stated that the money will be invested for three months. After a trading cycle, the profits will be distributed by 60:40, i.e. 60% for the investors and 40% as management fees. Additionally, the investors can opt to re-invest the principal and accumulated earnings and have them rolled over for another three months. Further, to compute the investor's net profit and balance, Person S and Person A provided them with a step-by-step guide and a Monthly Investment Report to keep track of their investment.

From 2018 to 2020, Person S and Person A represented Company X in their dealings with the public. The victims made investments after hearing that the forex trading business earned a good return despite the jurisdiction still being under a pandemic. Most of their investors were their friends, former colleagues in auditing firms, other professionals, and some Overseas Filipino Workers (OFWs) they recruited online.

Company X was registered as a corporation in July 2018 with SEC Registration. Its primary purpose was to engage in the business of a consultancy firm, providing management objective advice and assistance relating to the strategy, structure, management, and operation of an organisation or individual in the pursuit of its long-term purposes and objectives. However, the corporation was neither authorised to solicit, accept or take investments/placements from the public nor issue investment contracts.

In order to attract new and existing investors to deposit more funds, in March, June, and November 2019, Person S and Person A offered a promotion wherein the deposits received within the said months are only subject to a 30% management fee instead of 40%. Many availed of the promotion and made additional deposits. Some placed amounts that are even higher than their initial investments. Since the investments earned a good return, based on monthly reports, many opted to roll over their monies for a substantial gain.

Sometime in February 2020, Person S and Person A suddenly informed their investors that Company X would undergo corporate restructuring. They would only accommodate large accounts, discontinue trading under Company X, and terminate the Investment P contracts. All the funds, including the gains as of the cut-off date would be released on a scheduled basis. However, Person S and Person A added that in order not to lose the opportunity to earn during the pandemic, they offered their investors a 're-investment option', but this time, it would be under a new fund management service under Company Y.

In August 2021, the SEC issued an advisory due to the numerous complaints received from victims of Company X, particularly against Person S and Person A. The SEC warned the public not to invest or stop investing in any investment scheme being offered by any individual or group of persons allegedly for or on behalf of Company X.

Subsequently, in December 2021, the SEC issued a Cease and Desist Order on Company X, Person P, Person C, Person S, Person A and Person L including Company Y. Further, the Enforcement and Investor Protection Department of the SEC also secured certification that Company Z is not a registered corporation.

Based on the complaints attached to the SEC referral, the total investment of the eight complainants is PHP 4,750,025.60 (~ USD 81,850). According to complainants, aside from them, there are more victims who invested an aggregate amount of PHP 80 million (~ USD 1.4 million) due to the enticement of Person S and Person A, et al.

Source - Philippines

Case Study # 64: Remittances of abuse

Sexual exploitation, including sexual exploitation of children; wire transfer; use of the internet; money value transfer services

Online sexual abuse and exploitation of children.

One of the most notable money laundering cases predicated on OSAEC was triggered by the referral of the National Crime Agency of the United Kingdom to the AMLC, through the Philippine Internet Crimes Against Children Center (PICACC), regarding remittances made to the Philippines by a certain British citizen - Person P in favour of a Filipino - Person C. Person P was a subject of investigation in the UK for his involvement in child exploitation through the use of the internet. From 2018 to 2019, Person P revealed, through online chat platform, his predilection for girls aged 12 to 14 years old.

Person P had sent payments to Person C via a remittance facility in a Philippine banking institution, as payment for live streaming of children being sexually abused. The entrapment operation resulted in the rescue of eight victims, whose ages ranged from 12 to 17 years old. Among those rescued were two children of Person C. Other rescued victims were neighbours, while some were recruited or lured by Person C to do 'show' in front of the clients.

The AMLC database revealed 646 suspicious transactions in the name of Person C. These transactions were made through money service business (MSBs) and mobile money services, 444 of which came from foreign individuals who, based on their names, were mostly males with no confirmed familial relationship with Person C.

There are two venues of ML cases against Person C as the latter made transactions from two different branches of a money service business (MSB). The prosecution presented witnesses from the AMLC, the Philippines National Police (PNP) and the MSB. The financial investigator from the AMLC testified on the results of the search on AMLC's transaction reports database, and the coordination made with the PNP and the MSB, through which the transactions were made.

Source - Philippines

Case Study # 65: Storefront or smokescreen? How drug traffickers laundered millions through a general store

Drug related crime; financial institutions

Use of Filipinos and businesses as dummies by foreign nationals

The bank account of General Merchandise Store X (Store X), which is located in a shopping mall in Metro Manila, is used by illegal drug traffickers as a remittance account for illegal drug proceeds. Department of Trade and Industry (DTI) records show that Person J is the registered owner of Store X. A certain Person Z, who is a resident of Jurisdiction C, however, has full control of the said account. Person Z also opened other bank accounts, using fictitious identification documents. In one account, Person Z even declared sales from Store X as a source of income. These accounts are used by various illegal drug traffickers in depositing illegal drug proceeds.

Store X was established in 2017, and within one year, deposits in Store X's bank account totalled approximately PHP 109 million (~ USD 1.9 million). This averages gross sales of PHP 9.12 million (~ USD 157,100) per month, equivalent to PHP 350,780 (~ USD 6,000) worth of sales per day, which is highly unlikely for a newly established store.

As per DTI records, although Store X is owned by Person J, it is managed by Person Z. As observed in similar illegal drug-based money laundering cases, the modus operandi often involves foreigners, mostly from Jurisdiction C, directing Filipino nationals to open retail/wholesale businesses (sole proprietary type) under their names. These businesses are used to open bank accounts, which will be fully controlled by foreigners, using a Special Power of Attorney (SPA).

Another modus operandi is the use of a bank account with an automatic transfer facility. Person J, the owner of Store X, executed an SPA in favour of Person Z to manage and control the said bank account, thus, making Person Z the authorised signatory of the account. Also, Person Z declared that the source of income of the account is from Store X, raising the suspicion that Person Z is the beneficial owner.

Person Z's deep connection with illegal drug trafficking was further established when Person Z's name and bank account were associated with a drug suspect, who was caught in Region IV-A. In 2018, the said bank account had one transaction worth PHP 120,000 (~ USD 2,000) linked to the said drug suspect. The said bank account was also referred by another informant as the recipient account of illegal drug proceeds in the Visayas region. Further, Person Z and the said bank account appeared in the mobile phone recovered from another drug suspect arrested in the Autonomous Region of Muslim Mindanao (ARMM).

For a period of three months in 2017, Person Z's account had deposits/credits, totalling PHP 114.6 million (~ USD 1.975 million) and averaging PHP 548,000 (~ USD 9, 400) per transaction. These significant deposits appeared to have no legal trade or underlying economic justification. In 2018, the same account received PHP 4.12 million (~ USD 71,000) worth of funds from Person S, who was involved in one of the biggest illegal drug cases (W Enterprise Case) under investigation by the AMLC.

In summary, this scheme involves two separate bank accounts from two universal banks: Store X's bank account, which is managed and controlled by Person Z; and Person Z's bank account. Both are recipient accounts of illegal drug proceeds. The account of Person Z with an estimated value of PHP 2.61 million (~ USD 45,000) was frozen in 2018.

Source - Philippines

Case Study # 66: Nailed it: the billion-peso drug laundering behind hardware companies

Drug related crime; use of cheques; cash; financial institutions

Use of Filipinos and businesses as dummies by foreign nationals.

Person W and Person X, both residents of Jurisdiction C, opened bank accounts in the Philippines and transacted hundreds of millions of pesos. They declared a hardware company – Company J as their source of income. Department of Trade and Industry (DTI) records showed that Company J was registered under the name of Person Y, a Filipino national.

In one of its investigations, a local drug law enforcement agency noted that Person A, who was in prison for illegal drug trade, was still involved in illegal drug activities and still received proceeds of illegal drug trafficking through associates, using several bank accounts maintained at different universal banks. It was further discovered that Person A received messages from cohorts and associates, regarding cash deposits from illegal drug proceeds and the laundering of these proceeds.

One of the bank accounts used by Person A was the joint bank account of Person W and Person Y. The said account received an approximate amount of PHP 6 million (~ USD 103,250) in less than two months. Person W and Person Y declared that their source of funds is Company J, which is located in Metro Manila.

The local drug enforcement agency also established a connection between Person W and Agency H (case study 58) due to recovered deposit slips from arrested drug suspects. It was noted that Person W's bank account in Universal Bank B received a PHP 295,000 (~ USD 5,000) cash deposit from arrested drug suspects and the Agency H's bank account in Universal Bank C also received approximately PHP 2.7 million (~ USD 46,400) from the arrested drug suspects. In a separate buy-bust operation in 2018, a deposit slip, bearing the joint account number of Person W and Person Y was recovered, raising suspicion that the joint bank account of Person W and Person Y was used in laundering the proceeds of illegal drugs.

DTI and The Securities and Exchange Commission (SEC) both certified that there were no businesses registered under the name of Person W and Person X. Also, per the investigation of Universal Bank C and Thrift Bank A, the submitted registration documents of Person W were all fictitious. Moreover, DTI certified that a certain Company J, located in an address different from what was stated in the bank account opening form, is owned by Person Y. There were also no records in the SEC of any business associated with Person Y.

The declaration of Company J as business by the accountholders (Person W, Person Y, and Person X) indicated deceit to hide activities and the source of substantial transactions with several banks. The joint bank account of Person W and Person Y made millions' worth of transactions, despite the lack of legitimate sources or business operations.

Person X, on the other hand, transacted about PHP 1.5 billion (~ USD 25.8 million) in a span of one year. Two universal banks noted that there were substantial debit and credit transactions that were not commensurate with the client's declared source of funds. Person X had six accounts from six universal banks.

Filipino national Person B, the wife of Person W, was also involved in illegal drug-based money laundering. Her modus is to register another Hardware company – Company K with the DTI under her name and provide the accounts of Company K to different drug personalities to be used to facilitate illegal drug proceeds. Company K has no business operations and, thus, classifies as a shell company similar to Company J.

Person B's bank accounts had numerous cash deposits, totalling approximately PHP 800 million (~ USD 13.7 million) in a span of one year. The total cash inflow amounted to PHP184 million (~ USD 3.17 million), while cash outflow totalled PHP 50 million (~ USD 860,400) in a span of seven (7) months. Furthermore, the said bank accounts had 503 cash and cheque deposit transactions, totalling PHP 133 million (~ USD 2.3 million); and 89 cheque issuances, encashment, and withdrawals, totalling PHP 128 million (~ USD 2.2 million) in a span of two months. Also, Universal Bank A noted that the account of Person B with them is a pass-thru account.

Company K has been registered with the DTI since 2019, and within one year of operation, its cash deposits reached an approximate amount of PHP 1.04 billion (~ USD 17.9 million). Company K, which is registered under the name of Person B, has seven bank accounts from universal and commercial banks. All of which are linked to the illegal drug trade.

Source - Philippines

Case Study # 67: Shells, shabu, and suspicious transfers

Drug related crime; money value transfer services; financial institutions

Use of Filipinos and businesses as dummies by foreign nationals.

In a similar scheme, Person L used a Filipino national to justify transactions worth hundreds of millions. Person L's bank account with Commercial Bank B was one of the 12 identified accounts as disclosed by an arrested drug suspect, Person D. Per Person D, after distributing a number of grams of methamphetamine or 'shabu' to his trusted pushers, these pushers would, in turn, remit funds, ranging from PhP200,000 to PhP600,000 (~ USD 3,440 to USD 10,325) to him, representing the proceeds of illegal drug sales. Person D would then remit said proceeds to the 12 bank accounts provided to him by another drug suspect.

Person L is a foreigner from Jurisdiction C. Similar with other modus operandi, Person C presented business documents of a certain Enterprise G under the name of a Filipino national, Person E. Person L was unable to provide supporting documents for deposit transactions worth PHP 473 million (~ USD 8.14 million) and withdrawal transactions, estimating PHP 28.7 million (~ USD 493,890) In a span of 15 years. Person L also sent PHP 5 million (~ USD 86,045) worth of funds to Person E, whose accounts have been frozen and who is facing a money laundering complaint for engaging and transacting proceeds of illegal drug trafficking.

Person L also sent funds to Person F via an inter-account transfer, amounting to PHP 1.2 million (~ USD 20,650). Person F is the subject of a separate investigation for being a recipient of illegal drug proceeds.

Source - Philippines

2.14 Samoa

Case Study # 68: Wheels that never turned – laundering methamphetamine profits through phantom imports

Drug related crime; trade-based money laundering; third-party laundering; self-laundering; financial institutions; wire transfers; cash; suspicious transaction reporting; transnational crime; organised criminal syndicate; international cooperation; structuring; fraud

The following case study illustrates how a complex network of financial flows, trade fraud, and drug trafficking was uncovered through routine reporting mechanisms. This spontaneous case developed rapidly following a container seizure, eventually revealing a sophisticated laundering scheme with international linkages.

Summary:

Who:

- Person A.
- Company E.
- Associates: Person B, Person C, Person D.

Agencies involved:

- Jurisdiction X financial intelligence unit
- Customs Authority (MCR).
- Police (Drugs and Organized Crime Division).
- Transnational Crimes Unit.
- Bank 1.
- Bank 2.

Foreign counterparts:

- Preliminary information exchange initiated with Jurisdiction Y.
- Outreach to U.S. partners in progress (e.g. Company F linkages under informal review).

When:

- Period: 2020–2025.
- Major enforcement and investigative actions occurred in 2024–2025.
- STR filed by Bank 1 in early 2025.

Where:

- Primary jurisdiction: Jurisdiction X.
- Foreign jurisdictions involved: Jurisdiction Y and Jurisdiction Z (via Company F and travel records).

Detection:

- STR filed by Bank 1 related to unverified cash deposits.
- Seizure of methamphetamine shipment by Customs Authority.
- Financial analysis and red flag identification by FIU.
- Police investigation into business and banking records.

International Cooperation:

- Early-stage cooperation initiated with Jurisdiction Y.
- Information sharing planned with relevant Jurisdiction Z authorities.
- Cross-border wire transactions under further review.

Predicate offences:

- Importation of methamphetamine approximately WST 9.5 million (~ USD 3.4 million).
- Fraudulent trade-based transactions using vehicle imports.
- Structuring to avoid threshold reporting.
- Possible concealment of proceeds of crime through loan repayments and rental income.

Legislation involved:

- Section 152A, Jurisdiction X ***Crimes Act 2013*** (money laundering offence).
- Section 26 Jurisdiction X ***Money Laundering Prevention Act 2007***.

Typologies Identified:

- Trade-based money laundering.
- Use of third-party payments (e.g., Company F).
- Integration of funds through loan repayments and property-related activities.

Outcome of investigation:

- Case remains under active investigation by law enforcement and the FIU.
- Methamphetamine valued at WST 9.5 million (~ USD 3.4 million) seized.
- Multiple STRs filed.
- Over WST 1.5 million (~ USD 534,400) in unexplained cash deposits.

In early 2025, the national customs authority seized a container arriving from Jurisdiction Z linked to a domestic trading company, revealing WST 9.5 million (~ USD 3.4 million) worth of methamphetamine. The seizure triggered a broader investigation by the national Financial Intelligence Unit (FIU) and law enforcement, uncovering a web of suspicious financial activities involving the business operator and related entities.

Subsequent analysis identified multiple telegraphic transfers (TTs) totalling more than WST 743,000 (~ USD 264,700) to an overseas car dealership in a neighbouring jurisdiction, purportedly for vehicle imports. However, the national customs authority confirmed that no such vehicles were imported, suggesting a trade-based money laundering (TBML) scheme.

Further red flags emerged from WST 1.5 million (~ USD 534,400) in 2024 for cash deposits, with many just under the reporting threshold. These funds lacked corresponding business records or justification.

The case also involved frequent international travel patterns by family members of the business operator, some on the same day, and inconsistencies in immigration records. Payments to unrelated third parties without clear commercial purpose raised further suspicion of third-party laundering.

As of May 2025, the case remains under active investigation, with preliminary cooperation initiated with authorities in the neighbouring jurisdiction and outreach to international agencies for further intelligence. The typologies identified — drug trafficking, TBML and cash deposits — underscore the sophistication and cross-border nature of the laundering network.

Source - Samoa

2.15 Singapore

Case Study # 69: Creation of money laundering network of shell companies by foreign professional money launderer

Professional money laundering; shell company network; foreign predicate offence: suspicious transaction reporting; structuring; fraud; money value transfer services; financial institutions

At various points between 2019 and 2020, the Commercial Affairs Department of Singapore Police Force received multiple reports that funds exceeding USD $8 million allegedly derived from foreign investment scams had been transferred into the Singapore bank accounts of four different shell companies in Singapore.

Investigators were able to draw links across the different reports as the bank accounts of each company similarly exhibited pass through transactions, the companies were found to have transacted with one another and had some common counterparties. Screening further disclosed that they were incorporated by the same corporate service provider (CSP) in Singapore, Company O. Company O had been approached by one Person N to incorporate the companies. Person N appointed various foreign nationals as directors of the companies and engaged Company O for provision of local resident directors. Investigators worked in tandem to submit a global recommendation in respect of the companies linked to Person N.

At the commencement of investigations in 2020, Person N and foreign directors were not in Singapore. A stop list was placed against them for investigators to be notified if they re-entered Singapore. Investigators continued to analyse the bank accounts of the companies and the STRs filed against them. Requests for information to relevant foreign jurisdictions helped to identify two additional foreign victims who had remitted funds as a result of investment fraud.

In November 2022, Person N and one of the foreign directors, Person T, were intercepted when they were transiting Singapore. Both were arrested by CAD to assist in the earlier investigations. Person N's laptop was also seized during investigations. Digital forensics revealed evidence that Person N was the mastermind of a professional service-based money laundering scheme whose clients operated call centre investment scams overseas. Multiple spreadsheets were found in Person N's laptop containing:

(i) the login credentials and passwords of the companies and their bank accounts;
(ii) records of fund transactions, including references to the victims in the case;
(iii) commission-sharing arrangements between multiple parties;
(iv) records of the transactions that were subject to fund recall and fraud investigations; and
(v) records of numerous false invoices supposedly issued by the companies for software or IT services which they did not provide.

Person N claimed that he was providing an 'escrow' service for his clients, but there were no documents to prove that such a service existed. Instead, evidence pointed that they were used simply as mule accounts to receive and transfer monies in exchange for exorbitant commissions of up to 15%. Further, steps were taken to hide the true nature of the transaction through false invoices and structuring the transactions in such a way as to avoid suspicion from the banks.

In September 2024, Person N was charged for four counts of being in possession of proceeds which he had reasonable grounds to believe were benefits from criminal conduct and four counts of failing to satisfactorily account for proceeds in his possession reasonably suspected to be benefits from criminal conduct. Prosecution is ongoing.

The case against Person T and one of the local directors Person G is currently under legal assessment. No further action was taken against the remaining local directors and CSP as no offences were made out. Specific to the CSP, it had taken steps to brief the local directors of their duties and performed additional reviews of the companies leading to the filing of STRs. It also took steps to ensure the companies were struck off in response to CAD's investigations.

Source - Singapore

Case Study # 70: Crackdown of SGD $1.27 million drug money laundering network linked to overseas drug syndicate

Drug related crime; organised criminal syndicate; third-party laundering; public/private partnership; use of financial intelligence; suspicious transaction reporting; financial institutions

This is Singapore's largest prosecution for laundering the benefits from drug dealing. The case first began in September 2020 where the Central Narcotics Bureau (CNB) of Singapore identified and arrested two major drug traffickers in Singapore – Persons A and B, from which drugs were also seized.

Investigations by the CNB into Persons A, B and their associates revealed that their drugs supplier was Person C, who was linked to an overseas drug syndicate. Multiple operations were carried out to establish the supply routes and identities of the local major drug traffickers linked to Person C. CNB worked closely with its counterparts in Jurisdiction Z, where Person C was based, to share information on the syndicate. The close collaboration culminated in Person C's arrest in March 2023 in Jurisdiction Z. He was eventually deported back to Singapore on 16 April 2023.

Concurrently, CNB carried out parallel financial investigation into Person C. It collaborated closely with the private sector, both through:

(i) direct bilateral engagement with Bank D with which Person C maintained accounts in Singapore as well as;
(ii) the AML/CFT Industry Partnership (ACIP) Case Specific Information (CSI) mechanism involving the nine ACIP banks. The ACIP CSI project on the case commenced in July 2023, during which CNB provided identifiers of 74 entities (including drug traffickers and money couriers) linked to Person C to establish the extent of Person C's financial network.

The collaboration with the banks resulted in targeted and high quality STRs filed, which allowed CNB to swiftly identify many suspicious inflows and outflows. This included transfers of large amounts by Person C to the same few counterparties and funds transfers made by Person C to bank accounts in Country Y and Country Z. CNB continued to enhance the financial intelligence received through further investigations and sending requests for assistance to Country Y and Country Z through the Egmont channel. Armed with the intelligence, CNB was able to elicit the truth from Person C who admitted to the ML offences.

With this, CNB was able to develop a fuller picture of Person C's modus operandi in laundering the proceeds from drug dealing. Person C was not just a drug mule but a central member in the syndicate. His role involved coordinating both the supply of drugs into Singapore as well as payment for the drugs. Person C was found to have received not only his drug trafficking proceeds in his bank account but also that of a fellow syndicate member, Person D. Where Person D's proceeds were transferred to Person C's bank accounts, Person C would retain a portion as remuneration. Person C also transferred his own proceeds from his accounts in Singapore to various accounts in Jurisdiction Z and his girlfriend's bank account in Jurisdiction Y. The total amount laundered by Person C amounted to SGD 1.27 million (~ USD 982,072) and comprised his own proceeds of about SGD 203,000 (~ USD 157,000) and Person D's proceeds of about SGD 1.07 million (~ USD 827,400). Person C was also found to have reaped a six-figure sum from coordinating the syndicate's operations.

On 30 December 2024, Person C pleaded guilty to one count of drug trafficking and four counts of money laundering derived from drugs-related offences. Another 18 charges for drug-related offences and money laundering money laundering were taken into consideration. He was sentenced globally to 28 years and nine months' jail*. For the money laundering charges alone, he received 38 months' imprisonment, the highest tariff for drug-related ML offence till date.

Investigations into Person C also implicated Persons A and B for drug-related money laundering offences. Person A was charged with one count of assisting Person C to retain benefits of drug dealing and one count of possession of over SGD 2,833 (~ USD 2,190) of benefits of drug dealing under the Corruption, Drug Trafficking and Other Serious Crimes

(*Confiscation of Benefits*) *Act 1992* (CDSA).

Person B faces one count of possession of over SGD 12,150 (~ USD 9,395) in benefits of drug dealing under the CDSA.

On 24 February 2025, Person B pleaded guilty to one count of drug trafficking, three counts of other drug-related offences and one count of money laundering derived from drug-related offences. Another nine drug-related charges were taken into consideration. He was sentenced globally to 27 years four months' imprisonment and 15 strokes of the cane. For the money laundering charge alone, he was sentenced to six months' imprisonment and SGD 12,150 (~ USD 9,395) was to be forfeited to the State.

On 17 March 2025, Person A* pleaded guilty to one count of drug trafficking, three counts of other drug-related offences and one count of money laundering of assisting Person C to retain benefits of drug dealing. Another 13 charges for drug-related offences and money laundering were taken into consideration. He was sentenced globally to 27 years seven months' imprisonment and 15 strokes of the cane. For the ML charge alone, he was sentenced to 18 months imprisonment, and SGD 2,833 (~ USD 2,190) was to be forfeited to the State.

*Persons A and C are appealing against their sentence.

Source - Singapore

Case Study # 71: Prosecution of money laundering syndicate seeking to launder proceeds of cyber-enabled fraud-linked to transnational syndicate through cryptocurrency trading scheme

Use of intelligence; money laundering syndicate; use of cryptocurrency, transnational crime; use of the internet; fraud; financial institutions

This was an intelligence-led investigation into a transnational cyber-enabled fraud syndicate which sought to launder its proceeds of crime via a money laundering syndicate in Singapore through bank accounts and cryptocurrency.

The money laundering syndicate was led by Person G, who was introduced to the criminal enterprise by an unidentified Person H he met at a gambling den in Singapore. Person G orchestrated the money laundering activities by buying ATM cards from other people to receive funds from Person H. Person G also illegally solicited and procured bank accounts through Telegram channels and job postings on free online classified advertisement portals. These accounts mainly came from foreigners. In a period of four months, Person G received more than SGD 800,000 (~ USD 618,628) from Person H through more than 50 bank accounts, to exchange for USDT (Tether).

Person G subsequently recruited cryptocurrency traders to sell and buy USDT (Tether) as individuals and ATM runners to withdraw monies deposited by the USDT (Tether) buyers using the ATM cards he provided to them. More than SGD 640,000 (~ USD 494,900) was withdrawn in this manner. In addition, on Person H's instructions, Person G provided Person H with internet banking access to a bank account in Singapore, which was then used to receive and dissipate another sum of more than SGD 570,000 (~ USD 440770).

In February 2024, Person G was convicted of money laundering offences and offences under the *Computer Misuse Act 1993* (CMA). He was sentenced to four-and-a-half years jail.

Between 2023 and 2024, one of the cryptocurrency traders was convicted and sentenced to 13 months imprisonment for money laundering offences, while the other was convicted and sentenced to 20 months imprisonment for money laundering and offences under the CMA.

Despite the large number of bank accounts misused, only three bank account holders were found to remain in Singapore and are currently under investigation. Upstream probes on the fund flows are still ongoing to establish further syndicated links to criminal or scam organisations.

Source - Singapore

Case Study # 72: Trade-based money laundering scheme to launder proceeds of conspiracy to cheat employer and the successful recovery of proceeds of crime

Cheating; forgery; self-laundering; asset recovery; trade-based money laundering

In 2018, acting on leads received, investigations were initiated by Singapore's Corrupt Practices Investigation Bureau (CPIB) against a group of employees alleged to have siphoned monies from a local construction firm by submitting false claims totalling to about SGD 9.7 million (~ USD 7.5 million).

Investigations revealed an elaborate scheme where the group of employees first used three corporate entities to submit the false claims to the construction firm and receive the payments. Thereafter, to layer the proceeds of crime, the group approached several sub-contractors to issue invoices to these three corporate entities so that the siphoned monies could be transferred to these sub-contractors despite not having any works carried out. After the illicit funds were received by the sub-contractors, the monies were withdrawn in cash and subsequently passed to the group. In return, these sub-contractors had received commissions for their assistance in the scheme.

In September 2021, the group of employees as well as the sub-contractors who assisted with the scheme were charged in Court for Penal Code and/or Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) offences. To date, at least seven of the accused persons have been taken to task for their respective offences, including two individuals who were convicted and sentenced in 2024 for offences under the CDSA. Valuables such as luxury watches and cash were also seized during investigations, and applications will be made to the Court for the confiscation of these ill-gotten gains.

Court proceedings against the other accused persons are ongoing.

Source - Singapore

Case Study # 73: Prosecution of money laundering for converting drug proceeds to luxury sedan

Drug related crime; self-laundering

On 27 September 2023, Person A was arrested for trafficking in a controlled drug under the *Misuse of Drugs Act 1973* (MDA). During his arrest, a luxury sedan was seized. Investigations revealed that the said luxury sedan was partially funded by proceeds from his drug trafficking activities.

Person A was charged for drug trafficking and drug possession under the MDA, and conversion of benefits of drug dealing under the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA). He was also charged for several traffic offences.

On 8 August 2024, Person A was found guilty and sentenced to a minimum of 12 months detention in a reformative training centre and disqualified from holding or obtaining all classes of driving licences for a period of two years. Additional nine charges were taken into consideration for sentencing. Following his sentencing for the predicate offences, CNB applied for the forfeiture of the luxury sedan.

Source - Singapore

Case Study # 74: Prosecution of professional intermediaries linked to large-scale anti-money laundering bust in Singapore involving 10 foreign nationals

Organised criminal syndicate; professional intermediaries; third-party laundering; suspicious transaction reporting; Illicit gambling/gaming; cash; financial institutions

The Singapore Police Force (SPF) launched a comprehensive, coordinated intelligence probe after receiving information on suspicious activities. This included suspicious transaction reports on the use of suspected forged documents to substantiate sources of funds in bank accounts in Singapore and their alleged involvement in remote gambling activities in other jurisdictions. This led to one of Singapore's largest AML law enforcement operations to-date. In August 2023, nine men and one woman (persons of interest, i.e. POIs) were arrested following a massive island-wide operation by the SPF.

Investigations revealed that the laundering in Singapore was in the integration stage. These 10 persons were subsequently charged and convicted for various offences, including forgery and ML linked to foreign remote gambling offences. They received global sentences ranging from 13 months to 17 months and assets worth a total of $944 million (~ USD 730 million) was ordered to be forfeited to the State.

Working closely with the respective DNFBP regulators, SPF further investigated two bankers Person A and Person B, who were former relationship managers at separate banks, and whose clients included some of the POIs. Person A and Person B were found to have abetted two of the POIs in creating forged documents which were submitted to the banks to substantiate the source of wealth or the receipt of large transactions in their bank accounts. In addition, one of them was in possession of approximately SGD 480,000 (~ USD 371,175) in cash which allegedly belonged to a POI, for which he was not able to satisfactorily account for.

In August 2024, both Person A and Person B were prosecuted for forgery-related offences under the Penal Code. In addition, Person A was handed a money laundering charge under Section 55 of the CDSA involving the sum of approximately SGD 480,000 (~ USD 371,175) which is reasonably suspected to indirectly constitute one of the POI's proceeds of crime.

Prosecution is in progress.

Source - Singapore

Case Study # 75: Prosecution of directors of a Singapore-incorporated company for tax and related money laundering offences

Tax evasion; self-laundering; financial institutions

This was a joint investigation between the Commercial Affairs Department (CAD) and the Inland Revenue Authority of Singapore (IRAS). Investigations disclosed that a Singapore-incorporated company, Company A, had issued cash sales invoices for a portion of its business without charging GST over a period of six years.

The cash sales were neither deposited into Company A's bank accounts nor reported to the company's accountant and tax agent. Instead, its directors, Person A and Person B, arranged for the cash receipts to be deposited into a personal joint bank account before being distributed amongst themselves over the course of the years, resulting in approximately SGD 2.8 million (~ USD 2.165 million) in taxable income being under-declared in the company's income tax returns. This resulted in income tax being

undercharged by more than SGD 450,000 (~ USD 348,000) and GST being undercharged by more than SGD 200,000 (~ USD 164,660).

Court proceedings are ongoing against Person A and Person B for income tax and GST evasion offences, and money laundering offences.

Source - Singapore

2.16 Chinese Taipei

Case Study # 76: Money laundering using USDT (Tether)

Fraud; use of virtual assets; virtual asset service providers; financial institutions

In July 2023, Person A met Person B through the LINE app while shopping online. Later in August 2023, through Person B's indirect introduction, Person A had come to know Person C and Person D and provided online bank account and password for them to use. Person C and Person D used fake investment platform and misled victim to transfer a total of TWD 400,000 (~ USD 13,000) to Person A's bank account. Person D then instructed Person A to use all the funds to buy USDT (Tether) and sent the USDT (Tether) to their cryptocurrency wallet, in order to conceal the proceeds of crime. The case was indicted in December 2024, for offence of aggravated fraud committed jointly by three or more co-offenders and money laundering.

Source - Chinese Taipei

Case Study # 77: Investment fraud committed by fraud syndicate

Fraud; forgery; cash

In June 2023, Person A responded to a recruitment advertisement on Facebook, joining a fraud syndicate, in order to earn a reward of TWD 10,000 (~ USD 330) for each successful cash transportation. Person A then joined a Telegram group to await instructions from superiors of the fraud syndicate.

The syndicate members used fraudulent investment group to lure victims into investing in Company B. In August 2023, a superior of the fraud syndicate met with Person A and handed over a forged employee ID card and receipt of Company B. Person A then went to one of the victim's residence and used the falsified ID and receipt to collect a total of TWD 797,904 (~ USD 26,500) investment fund from the victim. After obtaining the money, Person A kept TWD 10,000 (~ USD 330) as his reward and went to a supermarket, where he placed the rest of the money in the men's restroom. The money was then retrieved by other members of the fraud syndicate.

The case was prosecuted in September 2024. Person A was charged with aggravated fraud, money laundering, and using forged private documents.

Source - Chinese Taipei

Case Study # 78: Disclosure of official secrets by a government official

Cash; corruption and bribery; financial institutions

Person A is a squad leader of a police department and is a government official who, in accordance with the law, has statutory authority to investigate criminal cases. Person A, being entrusted by his friends Person B and Person C, without a formal case filing, used his account and password to login to the police department online system, searched for case information of many victims, and gave the information to Person B and Person C.

Analysis of the bank statements of Person A revealed that in the period of three years, Person A deposited in multiple transactions a total of TWD 8,432,495 (~ USD 275,000) in cash into their three bank accounts, the source of which was neither salary nor any other reasonable income. During this period, Person A repeatedly and intensively deposited the unexplained cash in amounts slightly below the TWD 500,000 (~ USD 16,300) reporting threshold stipulated by the *Money Laundering Control Act*, by splitting the cash into multiple smaller transactions on the same day and deposited into different or the same accounts, with the intent of evading the aforementioned reporting requirements. These actions showed a clear mismatch between his asset growth and his declared income.

After being ordered by the prosecutor to explain the source of the suspicious assets, Person A was still unable to provide a lawful explanation for TWD 1,395,680 (~ USD 45,495) of the remaining funds.

In March 2025, Person A was referred to the prosecutor's office for violation of the *Criminal Code, Anti-Corruption Act, Money Laundering Control Act,* and *Personal Data Protection Act*.

Source - Chinese Taipei

Case Study # 79: City councillor corruption case

Structuring; use of cheques; corruption and bribery; fraud; cash; financial institutions

Person A is a city councillor. Person B, Person C, and Person D each provided bank accounts for Person A's use. Person A then falsely reported them to the city council as publicly funded assistants. As a result, the city council was misled into believing that Person B, Person C, and Person D were legitimately serving as the councillor's assistants and disbursed funds such as assistant subsidies, Lunar New Year bonuses, and year-end bonuses. The assistant subsidy payments were transferred monthly into the bank accounts provided by Person B, Person C, and Person D. Through this fraudulent method, Person A unlawfully obtained a total of TWD 3,848,568 (~ USD 128,000).

Person A instructed and authorised Person E to withdraw part of the fraudulently obtained funds in cash, which were then used to cover monthly rent, utilities, wedding and funeral contributions, raffle prizes for community events, office printing and administrative expenses, bottled water for various sponsored activities, and other constituent service-related expenses.

The remaining amount was deposited — after being withdrawn in cash by Person E — into a bank account belonging to Person A's friend - Person F. Person F then issued a cheque to Person E, which Person E deposited into their bank account and subsequently transferred to another bank account for personal use, including stock trading. They conducted placement, structuring, and integration through these accounts to conceal the origin of the proceeds of crime and to evade detection and investigation by law enforcement authorities.

Person A was referred to the prosecutor's office for violation of the *Anti-Corruption Act, Money Laundering Control Act,* and the *Criminal Code*.

Source - Chinese Taipei

Case Study # 80: Third-party payment company assisting online gambling money laundering

Illicit gambling; third-party laundering; new payment method; use of legal persons and arrangements; fraud; cash

In order to combat fraud and money laundering crimes, the Police had been in close contact with various banks recently and thus has learned that transactions in several company accounts were abnormal. After analysis, it was determined that the company accounts might be involved in gambling and fraud, so a special task force was formed and reported to the prosecutor's office, to direct the investigation.

The investigation revealed that the syndicate established 14 shell companies through Person A and others and used the shell companies to sign collection contracts with third-party payment companies to provide gamblers with deposit services. When the gamblers filed fraud complaints for failing to receive winnings from the online gambling website, the bank account of the third-party payment company would be notified and warned by the banks.

The third-party payment company would then assist the syndicate in contacting the gamblers to sign a settlement and provide false documents such as service contracts with the shell companies, purchase orders and customer information to the police, pretending that the transactions were legal in order to lift the account alert, thereby helping to conceal or hide the flow of money from the gambling website.

After a long period of evidence collection, a crackdown operation was carried out on October 8, 2024. Troops were divided into multiple groups and simultaneously carried out raids (13 suspects were successfully arrested). Cash of TWD 15 million (~ USD 500 thousand), computers, mobile phones, bank receipts, money counting machines, contracts and other evidence related to suspected gambling and money laundering transfers were seized on the scene. The court adjudicated to seize illegal funds in the account (TWD 160 million, ~ USD 5.3 million), one house and one land holding (market value exceeding TWD 22 million (~ USD 700 thousand).

The case was referred to the prosecutor's office for suspicion of gambling and violating the *Money Laundering Control Act*.

Source - Chinese Taipei

Case Study # 81: Fraud and money laundering case of a cryptocurrency exchange

Organised criminal syndicate; self-laundering; structuring; lawyer: use of virtual assets; virtual asset service providers purchase of real estate; fraud; cash

Since 2019, the criminal syndicate led by Person B, Person C, and Person D, has been engaged in fraud and money laundering through virtual asset service provider – Company A, which is established by the syndicate. The syndicate allegedly used fabricated white papers, manipulated virtual asset prices, promoted worthless cryptocurrencies to defraud investors, and defrauded victims of substantial protection fees by impersonating military officials. The total amount of illicit gains exceeded TWD 2.2 billion (~ USD 72 million).

On April 26, 2024, the prosecutor's office concluded its investigation and filed formal charges against 32 suspects, including Person B, Person C, Person D, Person E (the president of Company A), and Person F (a lawyer who assisted in the unlawful disclosure of confidential information related to the investigation).

The syndicate transferred proceeds of crime in the form of cash and cryptocurrencies, including BNB (Binance), BTC (Bitcoin), ETH (Ethereum), and USDT (Tether). To obscure the money trail, they employed multiple accounts and cryptocurrency exchanges to create breakpoints in the transaction flow. A significant amount of cash was concealed in the northern areas of Chinese Taipei. The group further laundered the proceeds by using illicit funds for capital increase of Company A and investing in real properties. In addition, a portion of the funds was transferred to Jurisdiction X.

This case reveals the high-risk characteristics of fraudulent and money laundering activities within the virtual asset domain. The criminal syndicate carried out large-scale scams by operating a self-established exchange and disseminating false information, exploiting the anonymity and cross-border features of virtual assets to conduct fraud and launder illicit funds. The case also involves unauthorised disclosures by a licensed attorney and the harbouring of a fugitive, indicating that virtual asset crimes may intersect with traditional organised crime, further complicating efforts in investigation and prevention.

Findings from the investigation suggest that if Chinese Taipei's current regulatory framework focused solely on anti-money laundering measures, would be insufficient to effectively prevent and address illegal activities in virtual asset trading. It is therefore essential to promote the enactment of a dedicated law on virtual assets and enhance regulatory oversight. This includes establishing comprehensive regulatory mechanisms for various types of virtual asset service providers, implementing robust listing standards for new tokens, and clearly defining penalties for violations and exit mechanisms. These measures aim to better protect investors and safeguard overall financial stability.

Furthermore, AML obligations and supervision for DNFBPs—such as attorneys—must also be strengthened. This will ensure that the Anti-Money Laundering system remains responsive to emerging financial technologies and criminal tactics, thereby enhancing national capabilities to combat money laundering and fraud.

Source - Chinese Taipei

Case Study # 82: Judge A of a certain District Court violated the *Money Laundering Control Act*

Organised criminal syndicate; professional facilitators including lawyers, notaries and accountants; cash; purchase of real estate; fraud

In 2023, Judge A, who was serving at a district court, was fully aware that the TWD 100,000 (~ USD 3,300) in cash handed over to him by Lawyer B constituted proceeds of crime derived from Lawyer B's participation in a fraud syndicate. Nevertheless, in order to conceal the origin and flow of these illicit funds, Judge A accepted the money and passed it on to Lawyer C.

In addition, to conceal the proceeds of crime obtained from participation in the fraud syndicate, Lawyer B transferred cash to Judge A, with the total sum of TWD 800,000 (~ USD 26,400) in 2023, and TWD 2.5 million (~ USD 82,500) in 2024. Furthermore, Lawyer B and Judge A conspired to use the illicit funds to purchase a newly built property which was to be registered under Judge A's name. Prior to the payment, the proceeds of crime were hidden in Judge A's office.

Subsequently, Lawyer B was caught by the district prosecutor's office and detained for involvement in fraudulent activities. Fearing that his role in concealing Lawyer B's illicit gains might be exposed, Judge A contacted Person D, Lawyer B's sister, and falsely claimed that he intended to return Lawyer B's investment in the joint real estate purchase. Judge A then visited Lawyer B's residence and handed over the aforementioned proceeds of crime totalling TWD 3.3 million (~ USD 108,900) to Person D. In an attempt to evade criminal liability for money laundering, Judge A further instructed Person D — based on his verbal directions — to complete and alter the *Money Laundering Prevention Declaration for Real Estate*

Sales Transactions to disguise the origin and flow of proceeds of crime derived from Lawyer B's participation in the fraudulent scheme.

in August 2024, Judge A was prosecuted for violating the *Money Laundering Control Act*.

Source - Chinese Taipei

2.17 Vietnam

Case Study # 83: Transnational money laundering case

Fraud including forgery; use of legal persons and arrangements; third-party laundering; transnational crime; financial institutions

According to the investigation results, from 2022 to 2024, Person T, a permanent resident of City D, forged national ID cards to establish multiple businesses. Person T also forged various seals of banks, government agencies, and notary organisations to authenticate the fake ID cards and business registration licenses of these companies.

Person T personally registered several bank accounts under the names of these businesses (each business registered two–three accounts) and then sold them to other individuals for the purpose of legitimizing the flow of money originating from criminal activities (such as fraud and gambling) from abroad into the jurisdiction, in an attempt to evade detection by the authorities.

The Criminal Investigation Agency determined that the total amount of transactions conducted through the afore-mentioned bank accounts was nearly 30 trillion VND (~ USD 1,136,692,786). Of that, foreign currency transactions were estimated at over 300 billion VND (~ USD 11,636,927.9).

Person T's criminal network is connected to Person A, Person B, Person C, and Person D, among whom Person C is a bank employee who colluded with Person T to open multiple bank accounts and sell them to other individuals for money transfer transactions. Person C also provided account information to Person T to withdraw funds originating from criminal activities from the registered business accounts.

The police have initiated a criminal case, prosecuted the accused, and temporarily detained five individuals - Person T, Person A, Person B, Person C, and Person D - for investigation on charges of 'Money Laundering', 'Illegal Trading of Bank Account Information' and 'Forgery and Use of Seals and Documents of Agencies and Organisations'.

The case is currently under further investigation.

Source - Vietnam

Case Study # 84: Cyber-enabled fraud and money laundering case

Fraud including phone/social media; robbery, theft; financial institutions; use of credit/debit cards

A woman - Person X sent a message via the Telegram app to another woman - Person Y, asking Person Y to receive a sum of 5 billion VND (~ USD 193,948,798) transferred from Person X's bank account at Bank A, and then to transfer this amount from her own account (opened at Bank B) to Person Z, an acquaintance of Person X.

Person Z then transferred the money back to Person X through her account at Bank A. During the exchange on Telegram. Both Person X's and Person Y's Telegram accounts were hacked and taken over, as a result, the bank account information of Person Z that Person X had sent to Person Y was deleted and replaced with the account information of an individual Person N who had an account at Bank B.

During the inspection process and verification of the fund transfers between accounts opened at various banks, the police department of City N determined that the bank account of Person N, opened at Bank B, had received the 5 billion VND (~ USD 193,948,798). This amount was subsequently transferred by Person N to Person Q's account at Bank C, and then to Person P's account at Bank D. The funds continued to circulate through multiple transfers, from Person P to Person S (with an account at Bank E), and from Person Q to Person S (with an account at Bank F).

Since 2022, Person T has frequently travelled abroad (to Jurisdiction P) for gambling and job-seeking purposes.

Person V is an individual in need of renting bank accounts for use.

Person T opened 10 bank accounts at various banks and rented them out to Person V (who lives in Jurisdiction P). Under Person V's guidance, Person T went to Jurisdiction P to work at Company H, a business based in Jurisdiction P owned by a foreign national from Jurisdiction Q named Person Z. At

Company H, Person T rented accounts to the company for receiving and transferring money from online fraud, using methods such as hacking accounts and taking control of victims' Facebook and Telegram accounts to steal money.

The group of individuals who are the owners of the bank cards, including Person T Person N, Person Q Person S, and Person R, opened bank accounts for Company H to use for the purpose of receiving and transferring money obtained through fraud. These individuals were responsible for biometric scanning or facial recognition to authorise transfers when Company H successfully defrauded victims.

The funds were broken into smaller amounts and transferred through multiple accounts to conceal the criminal activity. Ultimately, the money was transferred to Person S and Person R, who were responsible for laundering the money.

In addition, another group of individuals was involved in the criminal network, specialising in tracking the flow of money in and out of accounts and creating transfer orders based on instructions from the ringleader.

Source - Vietnam

Case Study # 85: Fraud case involving cryptocurrency, transnational criminal activity

Fraud; use of capital markets; market manipulation; transnational crime; currency exchange

In 2025, the Criminal Investigation Agency of District N Police initiated a criminal case involving online fraud that occurred in 2023. Seven individuals were charged with the crime of fraud and two individuals were charged with money laundering.

In November 2023, an individual named Person X was invited by a criminal syndicate to invest in foreign exchange trading on an international stock exchange platform called 'Fnory', with the website address: fnory.com. The criminal syndicate sent Person X a link to create an account on the website fnory.com and instructed Person X to download an application called MetaTrader 5 and create a trading account using this app. Person X followed the instructions and deposited money in VND into the MetaTrader 5 account.

Orders were placed directly through the MetaTrader 5 app. The order process involved selecting a currency pair to trade, choosing the trade volume, adding the required options, and clicking on 'Sell by Market' if predicting a price drop in the future, or 'Buy by Market' if predicting a price rise. The profit or loss was directly calculated based on the account balance. To withdraw funds, Person X logged into the website fnory.com, accessed the account, selected the withdrawal option, and chose either a bank transfer or another method.

Person X deposited a total of 2,070,000,000 VND (~ USD 80,294.800) into the trading account and was able to withdraw approximately 730,000,000 VND (~ USD 28,316.524). The remaining funds were used to place trading orders according to the instructions of the criminal syndicate, resulting in losses.

When the criminal syndicate saw that Person X stopped depositing money to continue trading, they repeatedly pressured and encouraged Person X to deposit more money to keep trading, promising that Person X would lock in profits and recover the invested funds. However, Person X did not continue to deposit money, and about two weeks later, Person X was removed from the group.

Person X's trading account on the website fnory.com was also no longer accessible.

Source - Vietnam

Case Study # 86: Fraud case via TikTok

Fraud including social media; market manipulation; purchase of real estate; cash

Fraud and Money Laundering Case Involving TikTok user - Person P, who has millions of views and followers.

The Criminal Investigation Agency of City H Police, in coordination with specialised units, has dismantled a cyber-fraud ring that operated in City H and several provinces and cities across the Jurisdiction.

Person P frequently live streamed analyses, forecasts, and commentary on gold prices, cryptocurrency, and more. Person P built multiple chat groups on Telegram and lured members to participate through a copy trade model (an investment method where users replicate trading positions that are opened and managed by Person P himself).

Initial findings indicate that since 2019, Person P and Person N conspired to set up a fraudulent operation to misappropriate assets, using a structure similar to that of securities brokerage companies. The perpetrators operated under the guise of legitimate companies and websites engaged in telemarketing,

tele sales, financial investment consulting, and stock brokerage. They used high-profile stock symbols such as Facebook, Apple, Pepsi, Microsoft, and Adidas to attract and deceive potential investors.

The accused created a website called 'artexvina.co' to recruit staff and craft the image of a well-organised, professional company specialising in international stock investment consultancy. A team of employees was used to approach and persuade individuals to invest. At the same time, the group established branches nationwide and even abroad, executing the scam under the guise of brokerage firm operations, thereby defrauding numerous victims.

The City H Police conducted an urgent search inside the accused' residences and workplaces, seizing and freezing assets worth of over VND 5.000 billion (~ USD 193,948,798). The asset included: VND 127 billion (~ USD 4,926,299) in cash, approximately VND 306 billion (~ USD 11,869,666) worth of savings books, 216kg of gold, 128 real estate properties, 30 cars of various types, freezing VND 9 billion (~ USD 349,107) of bonds and many other valuable assets.

Authorities are continuing with investigation, searching for victims to reach a final conclusion.

Source - Vietnam

Terrorism financing

2.18 Indonesia

Case Study # 87: Terrorist financing through sham non-profit organisations and cryptocurrency channels

Third-party laundering; fraud; use of legal persons and arrangements; trust and company service providers; foreign predicate offence; terrorism financing; use of virtual assets; virtual asset service providers

Non-profit organisation (NPO) X and NPO Y are two Indonesia-based sham NPOs established by an Indonesian foreign terrorist fighter Person A. In 2014, the Person A departed for Syria to join a terrorist group affiliated with the Al-Nusrah Front for the People of the Levant (a.k.a. Hay'at Tahrir al-Sham or HTS), which has been listed under the UN Sanctions List since 5 June 2018.

Masquerading as humanitarian organisations, these NPOs actively raised public donations via social media by leveraging narratives focused on aiding orphans, the underprivileged, and conflict victims. From January 2020 to February 2024, they successfully collected more than IDR 40 billion (~ USD 2.4 million).

Between August 2018 and October 2020, funds collected through NPO X's accounts were funnelled to Person B – Person A's brother-in-law. Acting under Person A's instructions, Person B transferred approximately IDR 15.97 billion (~ USD 1 million) to an individual in Turkey – Person C via conventional bank transfers.

In anticipation of law enforcement actions, the group established a new NPO, NPO Y, in 2021. Mirroring NPO X's approach, NPO Y continued to solicit public donations using similar humanitarian appeals, collecting over IDR 29.5 billion (~ USD 1.8 million) from February 2021 to February 2024. The funds were then transferred to Person B and Person D, a key operational figure. Following Person A's instructions, a substantial portion of the donations was converted into over 1.8 million USDT (Tether) through the local virtual asset service provider.

Of that amount, 200,000 USDT (Tether) was transferred to a Binance hot cryptocurrency wallet controlled by Person E, a French national convicted in absentia in 2016 and sentenced to 10 years for terrorist conspiracy. Person E has been identified as a member or affiliate of ISIS/ISIL. An additional 172,000 USDT (Tether) was transferred to an un-hosted cryptocurrency wallet associated with HTS fundraising campaigns, along with four cryptocurrency wallet addresses linked to two cryptocurrency exchanges in Idlib, Syria – Bitcoin Transfer and Bitcoin Xchange - both suspected to be under jihadist control.

In early 2023, the Indonesian government designated NPO X under the Indonesia's domestic terrorist sanctions list, resulting in the freezing of nine of NPO X's bank accounts.

Source - Indonesia

2.19 Philippines

Case Study # 88: Extortion Funds of Group Z

Terrorist financing; cash

On 11 August 2023, during implementation of a search warrant, joint operatives from the military and police arrested Person A, the finance officer of Group Z - a terrorist group for illegal possession of firearms. During his arrest and upon search of his person, he was found to be in possession of the amount of approximately PHP 400,000 (~ USD 6,900) composed of various currencies in cash. Intelligence reports also revealed that Person A oversees the extortion operations of Group Z at the national level.

Evidence revealed that Person A would personally select the businesses to be targeted by Group Z, authored the extortion letters to several companies, met with the latter's representatives to negotiate amount, and collect the extorted cash for Group Z. He, along with his team, would also bring the extorted funds they collected to the finance head of Group Z.

This case proceeded to prosecution.

Source - Philippines

Proliferation financing

2.20 Singapore

Case Study # 90: Prosecution of company for money laundering arising from proliferation financing-related offences

Use of legal persons; proliferation financing; financial institutions

In December 2023, three companies, Company A, Company B and Company C, and their respective directors, Person D and Person E, were charged in Singapore's Court for offences relating to the illegal export of gasoil to the Democratic People's Republic of Korea (DPRK) and money laundering. Specifically, Company B was charged with money laundering offences, while Company A and Company C were charged with offences under the United Nations (Sanctions – DPRK) Regulations 2010.

Person D, the director of Company A and Company B, had allegedly conspired with five other individuals based overseas to supply gasoil to the DPRK from September to November 2019 via ship-to-ship transfers, and used Company A's bank account to facilitate payment transactions for the purchase and supply of gasoil to the DPRK. Company B's bank account was also used by Person D to receive payment for the prohibited supply of gasoil to the DPRK. Person E, the director of Company C, allegedly used Company C's bank account for the purchase of gasoil, which facilitated the prohibited supply of the said gasoil to the DPRK.

On 3 February 2025, Person E and Company C were convicted for proliferation financing offences. Court proceedings against Person D, Company A and Company B are currently ongoing. Person D and Company A face money laundering charges.

Source - Singapore

2.21 Chinese Taipei

Case Study # 91: DPRK proliferation case

Underground banking; new payment method; Proliferation financing; financial institutions

In August 2017, a Jurisdiction X national - Person A established an art gallery in Chinese Taipei under the name of their mother (a Chinese Taipei national), selling artworks with the official certificates from DPRK 'Mansudae Overseas Project Group of Companies' (UNSCR 1718 Sanctions List) through Facebook, LINE chat groups, and exhibitions.

Some of the artworks were purchased in DPRK, while the rest of the artworks were purchased through a wholesaler in Jurisdiction X. Person A used the bank accounts of their mother to receive payments from the clients. After transferring the funds to their bank account in Jurisdiction X **through underground banking,** Person A paid the wholesaler via mobile payment service.

The case was referred to the prosecutor's office in August 2024, and Person A was prosecuted for violation of the *Counter-Terrorism Financing Act* in March 2025.

Source - Chinese Taipei

3 - MONEY LAUNDERING, TERRORISM FINANCING AND PROLIFERATION FINANCING TRENDS

This section of the typologies report includes information from members and observers about research and studies being undertaken (part 3.1), reports about ML/TF trends observed over the 2024-2025 period (part 3.2) and observations about the effectiveness of AML/CFT measures (part 3.3).

Jurisdictions with weak or ineffective controls are especially attractive for money launderers and financiers of terrorism. These criminals seek to conceal their criminal activities by exploiting the complexity of the global financial system, the differences between domestic laws, and the speed at which money can cross borders.[3] This means ML/TF activity in one jurisdiction can have serious adverse effects across borders, and even globally. Combating TF continues to be a central part of many jurisdictions' counter-terrorism strategies[4].

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

3.1.1 Hong Kong, China

The police in Hong Kong, China have regularly been conducting money laundering (ML) situation analysis. Areas of focus include ML threats and predicate offences (number of cases and amount of crime proceeds involved), origin of funds and conduits of ML (sector being exploited).

Stooge accounts are heavily exploited by criminal syndicates to launder proceeds of crime. Further analysis was conducted on the stooge account holders' profiles (age, gender, occupation, residence, etc.). Case studies suggested that criminals recruited non-locals to open bank accounts in Hong Kong, China, which were then used as stooge accounts (on average two weeks after account opening). Test payments of small amounts were observed in the stooge account before being used to launder a significant amount of crime proceeds within a short period. The purpose of the account opening was often claimed to be 'for savings/ investment', yet a pattern of temporary repository of funds was observed.

Hong Kong, China is currently conducting the 3rd ML/TF Risk Assessment. Based on the latest quantitative and qualitative data, key findings include:

- Prevalence of the exploitation of money mules (or 'stooges').
- Digitisation of the modus operandi of predicate offences and the associated ML methods.
- Increasing use of virtual assets.

3.1.2 Indonesia

***Sectoral Risk Assessment of Money Laundering and Terrorist Financing from Cybercrime* (2024)**

Criminals are increasingly leveraging cyberspace and sophisticated technologies to launder proceeds derived from a wide range of predicate offences. ML convictions related to cybercrime remain significantly lower compared to the number of convictions for the predicate offences themselves. This gap highlights the need to enhance the detection and enforcement of ML cases originating from cybercrime, particularly those linked to online gambling.

- Online fraud and online gambling have been assessed as high-risk predicate offences for ML.
- From a profiling perspective, entrepreneurs and private sector employees have emerged as high-risk categories for involvement in cybercrime-related ML. Perpetrators of cybercrime often engage in

[3] International Monetary Fund - *The IMF and the fight against money laundering and terrorism financing* : https://www.imf.org/en/About/Factsheets/Sheets/2023/Fight-against-money-laundering-and-terrorism-financing
[4] Department of the Treasury - *2024 National Terrorist Financing Risk Assessment*: https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf

self-laundering, directly managing the illicit funds without the use of intermediaries.

- Geographically, the Jakarta region has been identified as having a higher concentration of ML risks
- In terms of reporting entities, the banking sector continues to report the highest volume of suspicious transactions related to cyber-enabled offences, indicating its elevated exposure to cybercrime-related ML.
- With respect to typologies, the use of virtual currencies and online gambling platforms have been identified as among the most prevalent and high-risk methods used for laundering illicit funds.
- High-risk transaction patterns include structured cash transfers, withdrawals, and deposits.

The level of TF risk associated with cybercrime could not be quantified in this study due to limited available data. However, international case studies suggest a potential link between cybercrime (particularly fraud) and TF activities.

There is increasing evidence of the misuse of financial technologies (such as crypto assets) as well as the exploitation of cyberspace for communication, propaganda, and recruitment purposes. These trends warrant greater vigilance and proactive monitoring by law enforcement and financial intelligence units.

3.1.3 Japan

Japan has published the following documents:

1. *National Risk Assessment-Follow-up Report* (2024)[5]
2. Japan published the first report of the *National Risk Assessment of Proliferation Financing* in March 2024. The Inter-Ministerial Council for AML/CFT/CPF Policy produced the report. Key findings include:
    - Potential exposure to various threats from actors that:
        - seek to steal funds via trade, service, and cyberattacks.
        - seek to steal technologies and goods through trading dual-use items, illegal ship-to-ship transfers.
        - use complex structures and opaque beneficial owners.
    - Japan's vulnerabilities lie in factors such as geographical proximity to DPRK, and its role as a globally significant international financial centre, and major industrial centre and open economy regime.
    - Japan reduces risks through various mitigating measures including relevant legislation and close coordination involving government agencies, the private sector, and foreign/international agencies.

    Japan updated this report in December 2024. In addition to updating the data and adding more case studies, the updated report highlighted further measures for countering proliferation financing in Japan. Key measures include:

    - In March 2024, Japan issued an alert to companies and other organisations regarding North Korean IT workers.
    - In April 2024, Japan made it obligatory for crypto asset exchange service providers, and bank and other entities that handle foreign currency transactions to become prepared to implement asset freezing and other measures based on the *Foreign Exchange and Foreign*

[5] Japan Financial Intelligence Centre - *National Risk Assessment-Follow-up Report (2024):* https://www.npa.go.jp/sosikihanzai/jafic/en/nenzihokoku_e/nenzihokoku_e.htm (English)

Trade Act.

- In May 2024, Japan designated eight additional jurisdictions to impose the travel rule relating to crypto asset transactions based on the *Act on Prevention of Transfer of Criminal Proceeds*. As a result, the total number of jurisdictions subject to travel rules has increased to 28.
- In September 2024, Japan put the *Partial Amendment of the Ordinance* into force in order to revise the list of items subject to export control and the specifications of the existing listed items.

3. Japan also recommends the report *North Korean Activity in the Casino and Gaming Sector: How Do Jurisdictions Respond?*[6] published by RUSI in September 2024.

3.1.4 Macao, China

Common ML methods detected from suspicious transaction reports (STR) received and identified ML and TF trends in 2024 included:

- Chips conversion without/with minimal gambling activities.
- Irregular large cash withdrawals.
- Currency exchanges/cash conversion.
- Significant cash deposit with non-verifiable source of funds.
- Use of ATM, phone banking, cash deposit machines.
- Chip conversion/marker redemption/gambling on behalf of third parties.
- Use of cheques/account transfer etc. to transfer funds.
- Use of online banking/internet.
- Suspicious wire transfers.

Throughout the period from January to December 2024, a total of 5,245 STRs were received by the Financial Intelligence Office of Macao, China (GIF), with 3,837 STRs from the gaming sector, 1,097 STRs from the financial sector (including banking, insurance and financial intermediaries) and 311 STRs from other sectors. During the same period, 142 STRs were disseminated to the Public Prosecutions Office for further investigation. These cases were mainly related to fraud.

3.1.5 Malaysia

Malaysia completed its *National Risk Assessment 2023*[7] (NRA 2023), with the objective to identify, assess, and understand the ML/TF risks within the jurisdiction. The assessment draws on a wide range of quantitative (e.g., statistics from various agencies, reporting institutions, etc.) and qualitative data (e.g., surveys and focus group discussions with law enforcement agencies, reporting institutions and other domestic and international stakeholders). Similar to NRA 2020, the NRA 2023 identified that fraud, corruption, illicit drug trafficking, organised crime, and smuggling remained as the prevailing crimes in the jurisdiction.

[6] Royal United Services Institute - *North Korean Activity in the Casino and Gaming Sector: How Do Jurisdictions Respond?:* https://www.rusi.org/explore-our-research/publications/emerging-insights/north-korean-activity-casino-and-gaming-sector-how-do-jurisdictions-respond

[7] Bank Negara Malaysia - *National Risk Assessment 2023* (Executive Summary): https://amlcft.bnm.gov.my/publications

In addition, Malaysia also completed five thematic risk assessments[8]. These risks assessments collectively provide a holistic understanding of Malaysia's ML/TF/PF risk landscape.

3.1.6 New Zealand

Cryptocurrency (crypto) ATM companies have entered the New Zealand market over the last 18 months. Their appearance has caused concern for law enforcement and regulatory agencies. Analysis of the cash pick-ups before and after their arrests suggests it is possible organised criminal syndicates have exploited crypto ATMs to launder the proceeds of their illicit activity.

Furthermore, it is possible individuals with links to organised crime are conducting account take-over activity to launder these illicit funds. Persons with links to organised crime are believed to have been conducting transactions using accounts belonging to other people. However, it is not known if the 'taken over' accounts are sold by the original customer, handed over willingly, or hacked.

Although there have been no reports of increases in suspicious persons or activity around crypto ATMs, following ram-raids seen in Australia, it is likely that NZ will also see crypto ATMs targeted in a ram-raids in the near future.

3.1.7 Philippines

Philippines' *Third National Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) Risk Assessment* (NRA).

The Anti-Money Laundering Council is slated to publicly release the Philippines' *Third National Anti-Money Laundering/Counter Terrorism Financing (AML/CTF) Risk Assessment* (NRA) by Q3 2025. The Third NRA is a whole-of-government effort involving over 70 participating agencies and stakeholders, structured across 14 technical working groups. These working groups conducted comprehensive assessments of sectoral and cross-cutting ML/TF threats and vulnerabilities through data collection, inter-agency workshops, and technical consultations.

The NRA provides an evidence-based understanding of the jurisdiction's exposure to ML/TF risks and supports the effective prioritisation of AML/CTF efforts in line with the Philippines' national strategy and FATF Recommendations.

3.1.8 Singapore

To update and deepen Singapore's proliferation financing (PF) risk understanding, Singapore carried out a PF National Risk Assessment[9] (NRA), building on their existing PF risk understanding and tapping into relevant Singapore authorities and private sector players for a comprehensive assessment.

Taking into consideration information from a range of sources including investigations, suspicious transaction reports, intelligence and international typologies (including those featured in the relevant United Nations Security Council Panel of Experts' reports), Singapore has assessed that it faces the key PF threats of misuse of legal persons, ship-to-ship transfers, movement of dual-use goods, export of luxury goods and misuse of virtual assets. More details can be found in Singapore's PF NRA report, which was published on 30 October 2024.

[8] These are the Proliferation Financing Risk Assessment (PFRA), the Legal Arrangements Risk Assessment (LARA), the Legal Persons Risk Assessment (LPRA), the Non-Profit Organisations Risk Assessment (NPORA) and the Virtual Assets Risk Assessment (VARA).

[9] Monetary Authority of Singapore - *Proliferation Financing (PF) National Risk Assessment and Counter-PF Strategy*: https://www.mas.gov.sg/publications/monographs-or-information-paper/2024/proliferation-financing-national-risk-assessment-and-counter-pf-strategy

Singapore also updated its terrorist financing (TF) risk understanding in a refreshed 2024 TF NRA[10], which built on the previously published 2020 TF NRA. The 2024 TF NRA considered Singapore's latest TF risk environment; captured key terrorism and TF developments at the local, regional, and global levels, including potential spillovers from the ongoing conflicts and developments in the Middle East; and identifies the key corresponding risk areas within Singapore's National Countering the Financing of Terrorism system.

While the 2024 TF NRA identified Singapore's overall TF risk as Medium-Low, Singapore has increased the Digital Payment Token Service Providers' TF risk from Medium-Low to Medium-High, and identified new emerging TF risk areas – cross-border online payments and cross-border fast payment systems (within the ambit of the banking sector – Medium-High TF risk), and online fundraising (within the NPO sector – Medium-Low TF risk). More details can be found in Singapore's TF NRA report, which was published on 1 July 2024.

3.1.9 Chinese Taipei

Money laundering trends in the past year (2024–2025)

According to the sector vulnerability assessment of the 2024 NRA, VASPs are identified as 'very high risk', third-party payment service providers are identified as 'high risk', and online games enterprises are identified as 'medium risk'.

Chinese Taipei has also identified the diversification of ML methods, including the use of mule accounts, third-party payment platforms, virtual asset exchanges, and physical storefronts for virtual assets to rapidly transfer and obscure illicit funds.

Terrorism financing and proliferation financing risks

Although Chinese Taipei currently faces a relatively low risk of terrorism financing (TF) and proliferation financing (PF), the rapid development of financial technology and emerging industries may introduce new channels that could elevate TF and PF risks, particularly through the use of virtual assets and third-party payment service providers. In response, Chinese Taipei continues to enhance its AML/CFT/CPF legal framework to effectively prevent and mitigate potential TF and PF threats.

3.1.10 United Arab Emirates

UAE FIU Strategic Analysis Report on Trade-Based Money Laundering[11]

This report maps out existing and emerging trade-based money laundering (TBML) methods, highlights high-risk items and sectors, reviews the involvement of trading parties (such as front/shell firms and intermediaries), and makes passing references to related financial crimes (e.g., Trade-Based Terrorist Financing/TBTF, sanction circumvention).

UAE FIU Organized Financial Fraud: Trends and Enablers - A Strategic Analysis Report[12]

The study observes a major increase in reports of fraud, quantifies financial losses incurred, elaborates on the most common fraud type (including phishing, BEC, impersonation, the role of different enablers such as money mules, social engineering and shell entities), and the role of Organised Crime Groups. The report also highlights fraud as a key predicate to ML.

[10] Ministry of Home Affairs - *Singapore Refreshes the Terrorism Financing National Risk Assessment and National Strategy for Countering the Financing of Terrorism*: https://www.mha.gov.sg/mediaroom/press-releases/singapore-refreshes-the-terrorism-financing-national-risk-assessment-and-national-strategy-for-countering-the-financing-of-terrorism/#

[11] United Arab Emirates Financial Intelligence Unit - *UAE FIU Strategic Analysis Report on Trade-Based Money Laundering*: https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

[12] United Arab Emirates Financial Intelligence Unit - *UAE FIU Organized Financial Fraud: Trends and Enablers - A Strategic Analysis Report*: https://www.uaefiu.gov.ae/en/more/knowledge-centre/publications/trends-typology-reports/organized-financial-fraud/

***United Arab Emirates National Money Laundering and Terrorist Financing Risk Assessment Report* (2024)[13]**

The NRA identifies ML threats including foreign proceeds, TBML, misuse of legal persons, third-party laundering, cash smuggling, real estate, DPMS, Virtual Assets and TF risks such as misuse of non-profit organisations, Hawala, funding via legitimate businesses and crowdfunding. It also evaluates risks in financial institutions, virtual asset service providers, DNFBPs, legal persons and free trade zones.

3.2 Observations on emerging trends; declining trends; continuing trends

3.2.1 Hong Kong, China

In 2024, Hong Kong, China continued to experience a rise in overall crime, totaling 94,747 cases and recorded a 4.95% increase when compared with 2023. Deception cases reached 44,480 which accounted for the largest share of overall crime (46.95%), representing a rise of 11.7% compared with 2023. The rise in deception leads to the sharp rise in ML cases. Approximately 97.50% of these ML cases were associated with fraud/deception offences, while ML associated with other predicate offences and standalone ML accounted for the remaining. In terms of case numbers, telephone deception dominated the statistics, followed by frauds related to investment, e-shopping, employment, and loans. These five categories of offences constituted 85.15% of all fraud/deception cases reported in 2024, generating an aggregate loss of HKD 9,727.88 million. In terms of amount laundered in fraud/deception ML cases, investment fraud rated top, followed by telephone deception, illegal gambling, email scam, and employment fraud, which collectively accounted for 84.49% of the total laundered properties.

Cross-border elements in Hong Kong, China were also observed. When compared to 2023, the proportion of laundered proceeds generated from domestic predicate crime proceeds declined from 64.50% to 58.89% of overall proceeds laundered. Meanwhile, proportion of proceeds linked to foreign jurisdictions rose markedly from 35.50% to 41.11%, an increase of 6.54%, suggesting a shift of composition.

In 2024, a total of 10,496 persons were arrested for involvement in various types of deception and ML offences, including about 7,700 money mules for selling or allowing their accounts to be used for ML, representing an increase of 13.6% compared with 2023.

In terms of conduits for ML, the banking sector continues to be the most predominant vehicle exploited for ML activities in Hong Kong, China. In recent years, the ML methodology has evolved beyond traditional bank remittances to encompass digital banks, cross-border payment gateways and virtual assets (VA). ML using VA service providers typically involved 'stooges' withdrawing cash from their bank accounts upon receipt of crime proceeds and subsequently purchased VA (primarily USDT and Bitcoin) in exchange shops known as over-the-counter intending to conceal the traces of transaction.

3.2.2 Indonesia

In the *Sectoral Risk Assessment (SRA) of Money Laundering and Terrorist Financing from Cybercrime (2024),* Indonesia identified the following emerging trends:

- Abuse of artificial intelligence.
- Abuse of e-wallets.
- Use of crypto-coin mixer services.
- Sending links/files containing viruses or for attempts to take over user data.
- Use of private wallet addresses.

[13] United Arab Emirates National Anti Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee - *United Arab Emirates National Money Laundering and Terrorist Financing Risk Assessment Report:* https://www.namlcftc.gov.ae/media/jvejlwgq/nra-annual-report-eng-r13.pdf

- Web and crypto asset exploitation.
- The assessment noted a decline in TF from illicit sources, while the following trends continued: Use of cash.
- Use of bank accounts.
- Purchase of luxurious goods.
- Purchase of property and vehicles.
- Transaction peer to peer virtual asset service providers.

3.2.3 Japan

Japan provided the following tables and analysis.

Numbers of cleared money laundering cases under the *Act on Punishment of Organised Crimes* and the *Anti-Drug Special Provisions Act*, categorised by predicate offence

Year	Fraud	Theft	Computer fraud	Violation of the Investment Act/Money Lending Business Act	Drug-related offences	Habitual gambling/ running a gambling venue for profit	Violation of the Immigration Control and Refugee Recognition Act	Violation of the Amusement Business Act	Violation of the Trademark Act	Document forgery offences	Other	Total
2021	243	217	42	26	9	12	16	14	8	4	57	**648**
2022	254	257	105	13	21	11	7	4	10	12	59	**753**
2023	334	319	160	16	22	17	6	9	9	9	54	**955**
Total	831	793	307	55	52	40	29	27	27	25	170	**2,356**

Year / Misused transactions	Domestic exchange transactions	Cash transactions	Credit cards	Deposit transactions	Prepaid payment instruments	Crypto assets	Funds transfer services	Legal persons	International transaction	Precious metals and stones	Financial instruments	Real estate	Foreign currency exchange	Legal/accounting professionals	Money lending	Bills and checks	Postal receiving services	Total
2021	208	72	40	40	21	9	9	16	9	2	2	0	1	1	0	0	0	**430**
2022	266	105	55	24	39	16	10	6	7	1	0	0	0	1	0	0	0	**530**

2023	311	129	51	36	40	29	21	15	11	3	3	4	2	0	2	1	1	**659**
Total	785	306	146	100	100	54	40	37	27	6	5	4	3	2	2	1	1	**1,619**

Major transactions misused for money laundering

The results of the analysis of the cleared ML cases and STRs are as follows:

- There were 785 cases of domestic exchange transactions, followed by 306 cases of cash transactions and 100 cases of deposit transactions, with the majority of transactions misused for ML involving products and services offered by deposit-taking financial institutions.
- There are many cases where offenders have victims make payments to bank accounts opened in the name of fictitious or other parties through domestic exchange transactions, which enables prompt and secure fund transfers.
- Ultimately, the proceeds of crime deposited into accounts through domestic exchange transactions or deposit transactions are often cashed out, making subsequent fund tracing extremely challenging.
- The number of cases where credit cards were misused for ML was the third highest. With the significant increase in fraudulent use of credit cards, the number of misuse cases has also risen.
- There is an observable expansion in the misuse of various payment methods, including prepaid payment instruments, crypto-assets, and funds transfer services, reflecting the diversification of payment methods.

In addition, there are also many ML cases without using the products and services of specified business operators, including the following:

- Cases where proceeds of crime were mailed under someone else's name, and where mailed proceeds of crime were received under someone else's name after being left in a vacant room or a parcel box.
- Cases where proceeds of crime were sold by impersonating someone else or by asking a third party who was unaware of the situation.
- Cases where proceeds of crime were concealed in coin lockers in online and telephone fraud.

3.2.4 Macao, China

Macao, China noted the following ML, TF and PF trends observed from law enforcement agencies:

Money Laundering (ML) Trends

ML activities in Macao, China increased in 2024, accompanied in particular by an increase in fraud cases. Fraud cases have increased significantly in recent years, especially phone scams and cyber fraud, which use a variety of methods including government officials impersonation scam, investment fraud, ticket fraud and phishing text messages.

Terrorism Financing (TF) Trends

In recent years there have been instances in Southeast Asia where non-profit organisations have been exploited for TF, which has raised concerns. The Judiciary Police (PJ) has remained vigilant and continuously assessed the threat, noting that no connections have been found within Macao, China. As of

now, PJ has not identified any local terrorist organisations or foreign terrorist personnel operating in Macao, China.

Additionally, besides the risk-based approach and continuous monitoring on suspicious fund flows implemented by the financial institutions, the dedicated counter-terrorism department operated under PJ has been scrutinising suspicious funds flowing to high-risk areas and has not identified any concerning activities.

Proliferation Financing (PF) Trends

Media reports have indicated that individuals are using virtual currencies to finance or purchase components for weapons of mass destruction, as well as utilising fundraising activities through dark web. It is believed that these methods have become a trend.

Law no.12/2024 (Legal Framework for the Control of Weapon and Related Items) came into effect in 2024 in Macao, China, criminalising the sale and financing of weapons and related items (which include weapons of mass destruction) further preventing and mitigating the threat of proliferation of weapons of mass destruction. As of now, no cases involving PF have been identified, nor have any regulated entities been penalised for violating the related financial sanction guidelines.

3.2.5 Malaysia

Malaysia identified fraud as a key trend. Cheating is a major contributor to fraud risk, with money mules playing a key role in these activities. Due to the current broad digital adoption, most cases of fraud were cyber-enabled (i.e. online scams).

On the other hand, in relation to organised crime, illegal gambling/illegal betting and unlicensed moneylending have moved to the cyberspace, and it has been observed that gambling/lottery draws are offered via online platforms, while illegal gambling/illegal betting websites/loans are advertised via social media.

3.2.6 New Zealand

The NZ 2024 AMLCFT NRA identified cyber enabled fraud and scams becoming more prevalent for laundering of illegally obtained funds, which is consistent with global patterns with minor variances in fraud/scam typologies. Fraud and scams are a global security challenge and have wide ranging impacts on communities and lower confidence and trust in government and institutions. Cyber enabled frauds and scams accounted for approximately 40% of ML activity in NZ, followed by drug crimes and laundering illicit funds through remitters to offshore jurisdictions.

3.2.7 Chinese Taipei

Chinese Taipei provided an overview of trends associated with peer-to-peer (P2P) lending platforms. These are online platforms that act as an intermediary to match lenders and borrowers or facilitate the transfer of creditor rights. They enable the general public to participate in lending to unspecified individuals for profit. Compared to traditional banks (which require credit checks and detailed reviews of borrowers' repayment capacity through a lengthy application process) P2P lending platforms allow borrowers to obtain loans more quickly and easily. However, borrowers often take advantage of these characteristics to seek higher-interest investment loans, which in turn exposes P2P lending platforms to greater risks than traditional banks.

From 2019 to 2024, the FIU received a total of 156 suspicious transaction reports (STRs) related to P2P lending platforms (2019: 5 STRs, 2020: 8 STRs, 2021: 3 STRs, 2022: 10 STRs, 2023: 88 STRs, 2024: 42 STRs). Among the 300 reporting subjects, 185 were natural persons, and 115 were legal persons. The reporting entities often identify whether a client or their transaction counterpart is associated with a P2P lending platform through KYC procedures, open source intelligence, or negative media reports.

The P2P lending platform business models identified by the reporting entities includes the following:

- **Personal microloans (P2P credit):** borrowers are individuals. Some platforms target specific borrower groups, such as students or migrant workers.
- **Corporate accounts receivable (bill) transfer:** borrowers are legal persons. The model involves corporate borrowers transferring their accounts receivable (bills) to the lending platform, after which investors provide funding either individually or collectively.
- **Real estate-backed lending: loans are secured with real estate as collateral.** The platform facilitates the setting of real estate mortgages and provides services related to the transfer of creditor rights. Some platforms also offer overseas real estate debt as investment products.
- **P2P loan clubs (Hui):** this model operates similarly to traditional informal loan clubs. In each round, borrowers compete through bidding, and the winner receives the pooled funds for that period.

Common crime patterns and abuse risks associated with P2P lending platforms are mainly divided into the following categories:

- **Fraudulent fundraising under the guise of P2P lending:** as intermediaries between borrowers and investors, P2P lending platforms should primarily earn revenue through service fees paid by users. However, when a business' performance falls short of expectations, dishonest platforms may create fake borrowers or fabricate false debt instruments to deceive investors into believing there are high-interest lending opportunities. In reality, the incoming funds from new investors are used to repay earlier ones — essentially operating a Ponzi scheme. Moreover, since all borrower and investor data is controlled by the platform operator, unscrupulous platforms may also create fake investors to purchase debts, creating a false impression of active investment activity to lure real investors.
- **Breach of trust and bankruptcy risks:** The collection and disbursement of funds vary by P2P platform business models. In some cases, investors transfer funds directly to the platform, which then disburses them to borrowers. This method removes the need for direct financial interactions between lenders and borrowers, offering convenience. However, if internal misconduct occurs (such as embezzlement by platform staff or mismanagement of operations) the platform may face risks of breach of trust or bankruptcy, leading to potential losses for investors.

Case Study # 92: Use of forged proxy-written wills to apply for the registration of inherited real properties.

Fraud; real estate

A District Prosecutor's Office received a report from the land administration bureau of a city government that a criminal syndicate used forged proxy-written wills to apply for the registration of inherited real properties to the land administration agency, so the prosecutor directed the Police to form a special task force to investigate, and key evidence was found linking the main suspect, Person A, to the fabrication of proxy-written wills.

After reviewing a large number of household registration, land administration, national tax, finance and other related documents, it was found that six proxy-written wills were certified by Person A in his capacity as a lawyer. After further investigation, it was found that many employees of Company B run by Person A were involved.

The modus operandi and pattern of the syndicate is to:

- Download the list of uninherited land or buildings from the land registry.
- Obtain relevant information of the descendants.
- Exploit police and household registration officer to inquire about personal information.
- Send the sales agents of Company B go to inspect the buildings of the descendants.

If it was found that a descendant has no children or the heirs cannot be contacted, they would forge a lease contract and ask an innocent locksmith to open the door to find the descendant's handwriting and relevant household registration, land title deeds and other information in order to forge a proxy-written will.

After six months of in-depth investigation into the criminal syndicate's organisational structure, modus operandi and division of labour among its members, two waves of arrest and raid operations were carried out on July 23 and September 5, 2024, and a total of 51 suspects were arrested, including lawyers, village representatives, police officers, household registration officers, land administration agents and other professionals.

The court ordered the incommunicado detention of Person A and 5 others and approved the seizure of 7 houses and 14 land holdings (with an initial estimated market value of approximately TWD 60 million (~ USD 2 million). Further investigation revealed that the group used this method to apply for 11 real estate transfers (6 successful and 5 unsuccessful), with illegal gains of TWD 140 million (~ USD 4.6 million).

The case was referred to the district prosecutor's office for offence of fraud, forgery of documents, and violation of the *Anti-Corruption Act*.

Source – Chinese Taipei

Chinese Taipei also noted the following ML trends:

Emerging Trends

- Virtual asset exchanges and third-party payment platforms have become new and emerging channels for money laundering.

Declining Trends

- The online gaming industry, identified as high risk in the sector vulnerability assessment of 2021 NRA, was reclassified as medium risk in 2024.
- The proportion of victims remitting funds via over-the-counter bank transfers or online banking decreased significantly—from 69% (as of end of 2023) to 20% (from August 2024 to February 2025).

Continuing Trends

- Continued use of mule bank accounts, virtual asset service providers accounts, and third-party payment accounts to facilitate money laundering.
- A sharp increase in face-to-face cash handovers by victims, rising from 23% (end of 2023) to 46% (August 2024 to February 2025).
- Ongoing cross-border financial flows associated with money laundering highlight the need to strengthen international cooperation.

3.2.8 United Arab Emirates

Insights from the *UAE FIU Strategic Analysis Report on Trade-Based Money Laundering*[14]

- **Ongoing focus on established TBML techniques:** authorities are still witnessing and responding to traditional TBML techniques, such as the use of fictitious trade documents (e.g. fictitious documents or manipulated invoices) and with various shipping-related frauds (e.g. false shipments or misrepresentation of goods). More attention and action have been focused on the fraud in the name of front-end/back-end legal persons and third-party intermediaries.
- **Focused surveillance over high-risk sectors for TBML:** continuous surveillance over sectors and products with high TBML risk profiles. This encompasses a variety of items, including foodstuffs, building materials, electronic products, auto parts, dual-use material, and valuable metals and stones, especially gold. The UAE has used all its means to protect the legitimacy of trade in these various sectors.
- **Links with predicate activities (TBML):** the authorities acknowledge that TBML is connected to several predicate crimes. The emphasis is on attacking those financial flows linked to such crimes as fraud, tax evasion and drug trafficking and to the laundering of the proceeds of foreign violations.
- **Broader TBML scope**: there is a continued emphasis on addressing the broader trade-based financial crime issues. This also involves monitoring for trade-based terrorist financing (TBTF), trade sanctions evasion, passing off customs duties, misuse of unlicensed Hawala and service-based

[14] Ministry of Home Affairs - *Singapore Refreshes the Terrorism Financing National Risk Assessment and National Strategy for Countering the Financing of Terrorism*: https://www.mha.gov.sg/mediaroom/press-releases/singapore-refreshes-the-terrorism-financing-national-risk-assessment-and-national-strategy-for-countering-the-financing-of-terrorism/#

money laundering (SBML).

Insights from the *UAE FIU Organized Financial Fraud: Trends and Enablers - A Strategic Analysis Report* [15]

- **Action on emerging fraud enablers:** the use of technology to perpetrate fraud is a well-known major and evolving threat. Therefore, the UAE is focused on understanding and countering key enablers such as the misuse of money mules, social engineering tactics, the establishment of clone and shell entities, identity theft, and the exploitation of social media and digital platforms. In addition, efforts also target malicious software attacks and the use of fraudulent documents.
- **Dealing with sophisticated fraud:** they are also dealing with the sophisticated fraud techniques. Though several techniques like phishing and vishing are well known, importance is also attached to elaborate practices such as fraudulent impersonation, business email compromise, account takeover, investment frauds, advance fees scams, overtime and various online and occupational frauds. Law enforcement also seeks to combat frauds involving organised criminal syndicates.
- **Fraud being a principal predicate offense:** the reports repeatedly refer to the large role played by fraud as a predicate offense to ML and the UAE focuses on this connection through all its anti-money laundering strategies.

Insights from the *United Arab Emirates National Money Laundering and Terrorist Financing Risk Assessment Report* [16]

- **Focus on emerging ML/TF risks:** the UAE knows financial crime is an evolving and a dynamic matter and it is focused on emerging areas of risk. This also involves an emphasis on risks related to virtual assets for both ML and TF, misuse of crowdfunding and other online platforms for TF. The authorities are also aware that as technology advances, this could open new channels to carry out illegal financial activities and are responding accordingly.
- **Focus on Key ML threats and typologies:** the UAE retains a strong focus on the supervision of key ML threats. These include the movement of illicit funds abroad to ensure that they are not detected and confiscated, the risk associated with both trade-based money laundering and the misuse of legal persons and legal arrangements to hide the ultimate beneficial owner of funds. Continued focus is also given to third-party laundering, cash smuggling and potential ML risks in the real estate sector and the dealers in precious metals and stones sector.
- **Continued actions against TF risks and typologies:** The abuse of Hawala and other informal value transfer systems, and the prospect of terrorist financiers exploiting legitimate commercial activities and emerging technologies such as virtual asset to source and move funds.

3.2.9 Vietnam

In recent times, the cybersecurity landscape in Vietnam has continued to evolve in a complex and challenging manner. Alongside the positive aspects, Vietnam's deeper and broader integration into the global cyberspace has brought about significant risks and challenges. Legal violations and high-tech crimes are increasing rapidly in the online space, with online fraud standing out as the most prominent, accounting for 57% of all cybercrimes. These crimes are expanding in both scope and scale, employing increasingly sophisticated methods and thoroughly exploiting new technologies — especially artificial intelligence (AI) — causing losses amounting to thousands of billions of USD annually.

The trading and use of virtual currencies and cryptocurrencies have become increasingly complex and difficult to control, yet there are currently no sufficient legal regulations in place to govern these activities.

Cryptographic assets are being used by criminals as illegal payment channels for activities such as

[15] United Arab Emirates Financial Intelligence Unit - *UAE FIU Strategic Analysis Report on Trade-Based Money Laundering*: https://www.uaefiu.gov.ae/media/vduba40z/updated-strategic-analysis-report-on-trade-based-money-laundering-rsas-2024.pdf

[16] United Arab Emirates National Anti Money Laundering and Combatting Financing of Terrorism and Financing of Illegal Organizations Committee - *United Arab Emirates National Money Laundering and Terrorist Financing Risk Assessment Report:* https://www.namlcftc.gov.ae/media/jvejlwgq/nra-annual-report-eng-r13.pdf

smuggling, illegal money transfers, ML, tax evasion, and fraud. Particularly notable is the use of popular stablecoins with relatively stable value, such as USDT (Tether). In some localities, there have been emerging 'clubs' or 'groups' that promote and lure people into investing in 'junk crypto asset projects' (essentially worthless tokens) as a means of defrauding and appropriating assets. The typical method used by these criminal groups is to convince people to believe in the promise of high returns from such 'crypto assets' in the future and then persuade them to transfer funds for investment entrustment, 'purchasing on behalf,' or participating in virtual asset mining. Later, the group claims the investments have failed and deletes all related data.

Common methods and tactics of ML using crypto assets include through:

- Centralised cryptocurrency exchanges
- Decentralised finance (DeFi) systems.
- Cryptocurrency mixers.
- Over-the-counter (OTC) peer-to-peer trading markets.
- Anonymous cryptocurrencies
- Online gambling platforms.

3.3 Effects of AML/CFT legislative, regulatory or law enforcement countermeasures

3.3.1 Hong Kong, China

The rise in the use of virtual assets for ML activities has prompted heightened efforts to combat such crimes. Notably, a decline was observed in 2024, with VA-related crime cases dropping by 902. This positive development can be attributed to the concerted effort of the Police and other stakeholders in combatting VA-related crimes i.e. the government's proactive measures in introducing licensing requirements for Virtual Asset Trading Platforms (VATPs) in Hong Kong, China. Formulation of legislation to regulate other VA-related activities is also underway.

The Hong Kong Monetary Authority (HKMA), HKPF and the Hong Kong Association of Banks (HKAB) also implemented a series of new measures to prevent, detect and disrupt financial crime, including fraud and associated mule account networks. Currently, ten banks are already sharing information on the Financial Intelligence Evaluation Sharing Tool (FINEST) platform operated by HKPF, which allows them to share information related to corporates suspected to be involved in fraudulent or illegal activities.

To strengthen protection for customers, legislative amendment to enable sharing of information of personal accounts when banks become aware of suspicious activity that may indicate possible prohibited conduct (including money laundering and terrorist financing) is being introduced in the Legislative Council, and the result is expected to be announced at the end of 2025.

Also, HKPF and HKMA introduced a Suspicious Account Alert mechanism which is linked to 'Scameter' operated by HKPF. If the recipient's account number has previously been reported in a crime case, the system will send a high-risk alert to the customer before money remittance. The mechanism has been extended from the Faster Payment System to cover internet banking and physical branch transactions and transactions at automated teller machines. The mechanism has covered the majority of the public's day-to-day transfers.

The *Anti-Deception Alliance*, where representatives of major banks work alongside Police officers in a co-location, continues to play a pivotal role. The Police-Bank cooperation proactively conducts transaction monitoring (e.g. payments made to identified stooge accounts) and sends alerts to potential victims. A total of 3,051 ongoing deception cases had been intervened successfully by the end of 2024.

With a view to expediting the prosecution of stooge account holders, HKPF have collaborated with the Department of Justice (DoJ) to streamline the procedures for evidence gathering and prosecution of straightforward money laundering cases. Also, HKPF and DoJ have established a protocol for applying enhanced sentencing. Since the implementation of this protocol, HKPF succeeded in enhancing the sentence of a number of stooge account holders, on average by 20% of the sentencing.

3.3.2 Indonesia

Financial Services Authority Regulation No. 8 of 2023 on the Program for Implementing Anti-Money Laundering, Counter-Terrorism Financing, and Counter-Proliferation Financing of Weapons of Mass Destruction in the Financial Services Sector provides the legal basis for conducting individual risk assessments related to PF. This regulation aligns with the latest FATF Recommendation 1, emphasising the risk-based approach in the financial sector.

PPATK Regulation No. 01 of 2024 concerning the Procedures for Imposing Administrative Sanctions for Violations of Reporting Obligations establishes the legal framework for enforcing administrative sanctions against reporting entities under PPATK supervision that fail to comply with mandatory reporting requirements.

PPATK Regulation No. 1 of 2025, which revokes the previous *Regulation of the Head of PPATK* (Per-02/1.01/PPATK/02/15), enhances the application of the risk-based approach in customer due diligence. It takes into account the results of national and sectoral risk assessments on money laundering and terrorism financing and reflects international AML/CFT standards.

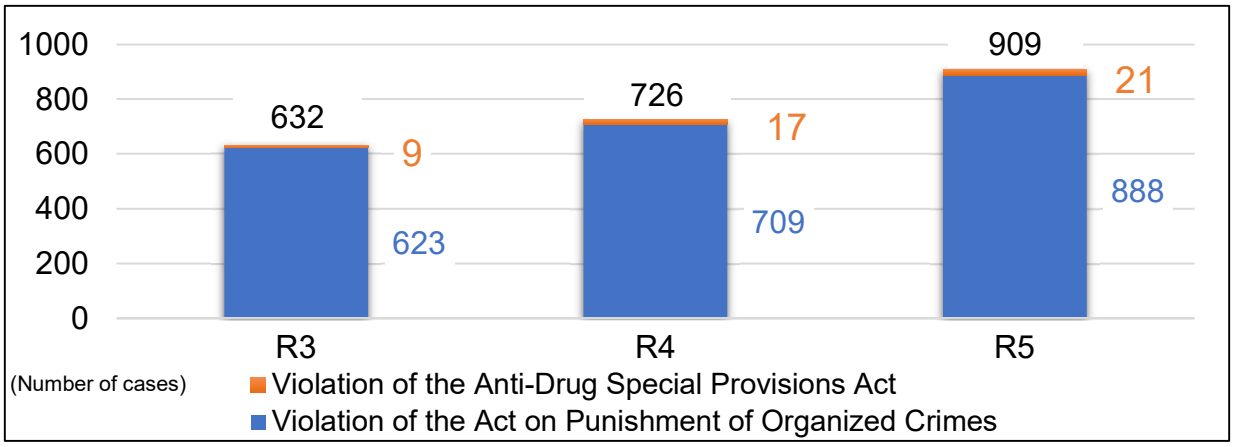
Joint Regulation No. 12 of 2023, which amends the *2017 Joint Regulation* issued by the Ministry of Foreign Affairs, the National Police, PPATK, and the Nuclear Energy Regulatory Agency, addresses deficiencies identified in the previous mutual evaluation report by improving procedures for listing individuals and entities involved in proliferation financing and terrorism activities

3.3.3 Japan

Japan's countermeasures are leading to steady increases in STR reporting and ML cases.

Japan noted that it had an increase in the number of cleared ML cases over the years 2021 - 2023.

Number of cleared money laundering cases



Japan noted that it had an increase in the number of suspicious transaction reports reported by regulated entities over the years 2021-2023.

Annual reported number of STRs by business type

	2021	2022	2023
	Number of reports	Number of reports	Number of reports
Financial institutions	495,029	542,003	661,838
Deposit-taking institutions	411,683	435,728	522,649
Banks	390,381	414,651	498,155
Shinkin banks, credit cooperative	18,461	18,520	21,636
Labour banks	318	316	397
Norinchukin banks, etc.	2,523	2,241	2,461
Insurance companies	3,458	3,939	4,575
Financial instruments business operators	19,718	19,032	20,550
Money lenders	35,442	45,684	63,954
Funds transfer service providers	10,499	20,271	29,232
Crypto-assets exchange service providers	13,540	16,550	19,344
Commodity derivatives business operators	388	318	846
Currency exchange operators	201	430	655
Electronic monetary claim recording institutions	7	0	14
Others	93	51	19
Financial leasing operators	163	71	214
Credit card operators	34,904	41,106	45,674
Real estate brokers	4	11	18
Dealers in precious metals and stones	48	124	138
Postal receiving service providers	0	1	30
Telephone receiving service providers	0	0	0
Telephone forwarding service providers	2	1	17
Total	**530,150**	**583,317**	**707,929**

3.3.4 Macao, China

Macao, China noted the following AML/CFT legislative or regulatory developments in 2024.

Insurance Intermediary Business Ordinance Law no. 15/2024 (Insurance Intermediary Business Ordinance (IIBO)) was approved by the Legislative Assembly in July 2024, which will enter into force on 1 August 2025 and will replace *Decree-Law no. 38/89/M of 5 June Legal Framework for the Carrying on of Insurance Intermediary Business.* The IIBO introduces the fit-and-proper assessment by incorporating the ML/TF conviction as a consideration factor with the aim to enhance licensing and ongoing supervision regimes of insurance intermediaries and to promote sustainable development of the insurance sector.

In the gaming sector, during the year of 2024, taking into consideration the revision of *Law no. 16/2001 (Legal framework of the exploitation of games of fortune in land based casinos)*, and respective complementary legislation, as well the outcomes of the Macao, China's *Risk Assessment on ML/TF/PF 2022*, the Legislative Assembly of Macao, China, approved and enacted two legislative acts (laws), namely *Law no.*

7/2024, regarding credit for gambling in the land based casinos, and *Law no. 20/2024*, regarding the prevention of crimes associate with illegal gambling.

Law no. 7/2024 revokes previous *Law no. 5/2004* and restricts the entities which are legally entitled to grant credit to the land-based casino patrons, the casino concessionaires. Therefore, junket operators are not authorised to grant credit directly to the patrons, unless under a contract of representation in which they act on behalf and representation of the casino concessionaires. New penalties are introduced to enforce the legal provisions as well the criminal liability of the legal persons.

Law no. 20/2024 revokes *Law no. 8/96/M (regarding illicit gambling), Law no. 9/96/M (regarding criminal illicit on pari-mutuels betting on animals racing)* paragraph i) and j), number 1, of Article 1 and Article 11 of *Law no. 6/97/M (regarding organised crime)*, *Decree no. 67/95/M (regarding the use of illicit devises and technology at pari-mutuels on animals racin*g), and finally amendment in subparagraph h), number 1, of Article 1, of *Law no.6/97/M*, and Article 1 and Article 193 of the *Criminal Procedure Code*.

Law no. 20/2024 increases the penalties on several crimes and administrative infractions associated with illicit gambling, and introduces new types of crimes, namely:

- Illicit online crime on games of fortune or on pari-mutuels.
- Crime on non-authorised foreign exchange activities for gambling.
- Establishes the criminal liability of legal persons in all of the special types of crimes covered by this law.

Moreover, it introduces the legal status of the informants on the types of crime defined in Law no. 20/2024 and establishes provisions on precautionary measures for the suspects of those crimes as mentioned above.

In response to the calls from international organisations for greater transparency of beneficial ownership, the Financial Services Bureau, supervisor of accountants, amended the *Guidelines for the Prevention and Suppression of Money Laundering and Financing of Terrorism* in October 2024, which came into force on 1 November 2024, to include a definition of beneficial owners of legal persons and legal arrangements and requirements for verifying the identity of beneficial owners.

3.3.5 Malaysia

The new *National Coordination Committee to Combat Money Laundering (NCC) Roadmap 2024-26* (new Roadmap) was endorsed and implemented, setting clear milestones and guiding parameters with measurable targets for prioritisation and effective monitoring. The new Roadmap continues Malaysia's comprehensive strategy to combat financial crimes by focusing on:

- Strengthening the deterrence and disruption of financial crimes.
- Heightening the compliance culture among reporting institutions.
- Enhancing the understanding of emerging risk areas based on global and domestic developments.
- Sustaining awareness and capacity building efforts amongst NCC members.

The new Roadmap also incorporates key recommendations from the NRA 2023 and five thematic risk assessments as mentioned above. Generally, the Roadmap ensures that AML/CFT/CPF efforts remain effective in addressing Malaysia's risk exposures amid national, regional and global developments.

The National Fraud Portal (NFP) went live in April 2024 to support the operations of Malaysia's National Scam Response Centre (NSRC). NSRC acts as a primary contact point for victims to quickly lodge reports of fraud, and NSRC officers use the NFP as a platform for tracing the flow of fraud transactions, sharing information among financial institutions and monitoring the intervention actions taken by financial institutions.

The NFP helps to share information and analyse fraudulent funds by integrating transactions and mule account data from multiple sources. This comprehensive collection of data enables the NSRC to perform enhanced analysis and detection of mule accounts, shown by a 65% increase in the number of mule accounts identified by the NSRC. This has resulted in a 75% reduction in the time taken to obtain complete information on fund flow and a 41% increase in cases being escalated to the Royal Malaysian Police for further investigation. Subsequently, this has led to a 47% increase in the average monthly earmarked sum of fraudulent cases.

NSRC's key outcomes in 2024:

- Opened 9,588 investigation papers involving cheating and freeze orders on targeted collection accounts amounting to RM8 million (~ USD 1.8 million).
- Identified and disrupted 71,037 suspected mule accounts, reducing opportunities to layer transactions to conceal the origin of stolen funds.
- Attended to 95,449 calls on online financial scams from the public, of which 40,010 calls were from scammed victims.

3.3.6 Singapore

Singapore provided the following case studies to illustrate the effectiveness of AML/CFT legislative or regulatory or law enforcement countermeasures (including cases developed from suspicious or cash/threshold transaction reports).

Case Study # 93: Case involving recruiter of money mule bank accounts

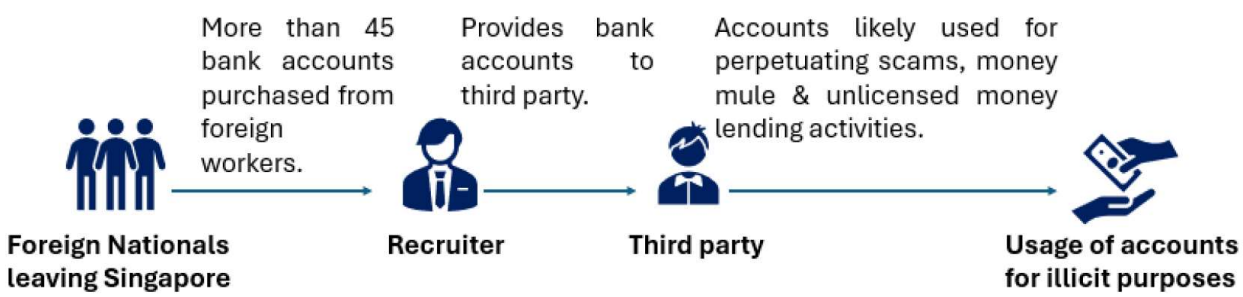
Suspicious/cash transaction reporting; organised criminal syndicate; third-party laundering; structuring; wire transfer; financial institutions

In March 2024, the Suspicious Transaction Reporting Office's (STRO) analysis into a group of suspected money mules which had been involved in a series of scams and unlicensed money lending activities, unveiled a much larger network involving significant syndication.

STRO's analysis uncovered that that two common foreign registered telephone numbers had been used by 89 unrelated bank account holders as their registered contact number with various banks. The STRO conducted an in-depth analysis which uncovered further bank accounts with other commonalities through three residential addresses in Singapore registered with the banks. Notably, these bank account holders, about 100 of them, were foreign workers and they did not reside at these residential addresses in Singapore. These accounts were mostly opened in 2022 and 2023.

Given these, the STRO suspected that a recruiter was facilitating the registration of bank accounts on behalf of a third party and subsequently taking control of them. The common addresses used for these bank accounts were likely intended for managing hard copy correspondences from the banks.

Pursuant to the STRO's analysis of the transactional patterns in these bank accounts which showed characteristics typical of money mule and unlicensed moneylending (UML) activities, The Commercial Affairs Department of the Singapore Police Force commenced investigation, and the said individual was convicted and sentenced in March 2024 to two months' imprisonment and a fine of SGD 30,000 (~ USD 23,200) for an offence under the *Moneylenders Act 2008*, with the offence under *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992* (CDSA) being taken into consideration.



Source - Singapore

Case Study # 94: Case involving fraudulent proceeds from overseas seized in Singapore

Suspicious/cash transaction reporting; fraud; third-party laundering; international cooperation; foreign predicate offence; use of legal persons; financial institutions

In October 2024, the Suspicious Transaction Reporting Office (STRO) received information that between July and August 2024, suspected fraudulent proceeds of about EUR 29 million (~ USD 34 million) had been transferred from two companies - Company X and Company Y incorporated in Jurisdiction B to Company Z's payment account maintained with a financial institution in Singapore. The owners of Company X and Company Y, Person X and Person Y, were featured in adverse media reports as the alleged masterminds of an online investment platform that reportedly defrauded victims, including those from Jurisdiction A, of approximately EUR 100 million (~ USD 117 million). The online investment platform, which was reported to have closed abruptly in September 2024, was also previously flagged by Jurisdiction A's authorities to be operated by an unauthorised company to offer collective investment schemes.

As the STRO's analysis suggested that alleged fraudulent proceeds have flowed to Singapore, the matter was expeditiously disseminated to the Commercial Affairs Department (CAD) for commencement of investigation and possible seizure of funds. The STRO also concurrently engaged its FIU counterparts in Jurisdiction A and Jurisdiction B to seek further information on the online investment platform as well as the entities involved including those reported in the adverse media reports.

Information received from the financial intelligence units (FIU) in Jurisdiction A and Jurisdiction B revealed that the two companies incorporated in Jurisdiction B, the company operating the online investment platform. Further Person X and Person Y are traced to ongoing investigations by their jurisdictions' law enforcement authorities for involvement in alleged investment fraud scheme and/or fraud-related offences.

Further financial intelligence shared by Singapore's counterpart also revealed that the bank accounts of the two companies incorporated in Jurisdiction B, which were identified as the main sources of funds in Company Z's payment account in Singapore, had received funds from possible investments related transactions. This further corroborated the STRO's findings that Person X and Person Y had possibly laundered their proceeds from the alleged investment fraud through these two companies to Company Z's payment account in Singapore. The STRO subsequently shared the additional information and findings with the CAD investigation unit, with the FIUs in Jurisdiction A and Jurisdiction B's consent.

The CAD commenced investigation and subsequently seized funds of approximately EUR 11 million (~ USD 12.9 million) in Company Z's payment account in November 2024. The remaining funds had been transferred out of Singapore prior to information being received by STRO.

Investigations are ongoing.

Source - Singapore

Case Study # 95: Spontaneous sharing with positive outcomes

Suspicious/cash transaction reporting; fraud; self-laundering; international cooperation; foreign predicate offence; financial institutions

In November 2023, the Suspicious Transaction Reporting Office (STRO) received a Request for Assistance (RFA) from a North American jurisdiction's FIU regarding Person A, who was being investigated in the North American jurisdiction for fraud. In April 2020, Person A allegedly used fraudulent documents to obtain public loans totalling to approximately USD 2.3 million and had purportedly escaped the

jurisdiction. The suspected fraudulent funds were transferred overseas and allegedly deposited in an investment account held at a financial institution in Singapore.

STRO engaged the FI to obtain the necessary information in order to identify the investment account belonging to Person A. Based on the financial intelligence gathered and further analysis conducted, STRO detected that there was a possibility that fraudulent proceeds were received in Person A's investment account in Singapore. Within three weeks of STRO's initial discovery of the information, beyond providing the requested information to the North American jurisdiction's FIU, STRO also proactively alerted the North American jurisdiction's FIU to the possibility that the proceeds of crime were in Singapore.

STRO received consent from the North American jurisdiction's FIU to disseminate its analysis to Singapore's law enforcement agencies and did so on the same day. This led to the prompt seizure of the investment account that contained approximately SGD 1 million (~ USD 773,285) and the commencement of an investigation within the week, as well as the ongoing pursuit of asset recovery efforts with the foreign LEAs. Investigations are ongoing.

The North American jurisdiction's FIU provided feedback that the information provided by STRO was useful and assisted in their investigation into the recovery of proceeds of crime.

Source - Singapore

Case Study # 96: Case involving transnational money laundering by an overseas organised criminal syndicate

Suspicious/cash transaction reporting; illicit gambling/gaming; third-party laundering; transnational crime; organised criminal syndicate; foreign predicate offence; international cooperation; money value transfer services; financial institutions

In 2021, the Suspicious Transaction Reporting Office (STRO) received STRs and information relating to two foreign-incorporated companies, reported to be assisting an organised criminal syndicate from Jurisdiction A to launder proceeds of crime. Significant funds in the Singapore bank accounts of the companies were alleged to be derived from various criminal conduct in Jurisdiction A and other jurisdictions.

STRO's analysis on the STRs revealed that the two companies-maintained bank accounts with several banks in Singapore. Extensive mapping of relationships in the analysis between these companies and their directors, beneficial owners and authorised signatories eventually revealed that the two foreign companies were linked to two individuals listed on INTERPOL's Red Notices. These two individuals had been placed on the INTERPOL's notices in January 2021 for offences of controlling and running gambling houses. Fund tracing by STRO led to the further identification of remittance agents and possible shell company accounts allegedly used in moving funds to the two foreign companies.

Using data from various sources, including information from foreign counterparts and bank records, STRO identified certain documents to be dubious, and uncovered strong links between the two foreign companies to the individuals listed on the INTERPOL Red Notice. The transaction pattern in the bank accounts also suggested that they were used for money laundering.

STRO disseminated the results of its analysis to the Commercial Affairs Department (CAD), which led to an investigation with over USD $188 million being seized from the Singapore bank accounts of the two foreign companies. Financial intelligence from STRO provided further leads to CAD, leading to investigators seeking further assistance from foreign law enforcement counterparts as well as seeking mutual legal assistance for further information on the foreign predicate offences involved.

CAD received a response in April 2023 from Jurisdiction A that Person S was sentenced to eight years' imprisonment for organised crime, particularly for operating illegal online gambling platforms with two other Jurisdiction A nationals. In addition to Jurisdiction A, CAD is exchanging information with LEA/FIU counterparts from Jurisdiction B and Jurisdiction C for the transfers received from both jurisdictions.

Money laundering investigations are ongoing.

Source - Singapore

Case Study # 97: Money laundering investigation in relation to organised crime commenced from STR referral

Suspicious/cash transaction reporting; organised criminal syndicate; third-party laundering; foreign predicate offence; international cooperation; purchase of real estate; Illicit gambling/gaming; financial institutions

In August 2023, the Suspicious Transaction Reporting Office disseminated its analysis on Person Y and his associate to Commercial Affairs Department (CAD). There was information suggesting that Person Y had absconded from Jurisdiction A and was on INTERPOL Red Notice issued by Jurisdiction A for his role as the owner and controller of an illegal online gambling syndicate.

These online gambling platforms purportedly attracted gamblers from Jurisdiction A into playing gambling games over websites and mobile applications with more than 500,000 persons having participated and illegal profits obtained by the group amounting up to SGD 900 million (~ USD 696 million). Through further identification of assets, it was determined that Person Y had substantial financial assets and real estate properties in Singapore.

In view of the nexus to Singapore and the identification of another associate of Person Y who may be involved in laundering the suspected proceeds of crime, CAD commenced money laundering investigations against Person Y and the associate. Significant financial assets worth SGD 36 million (~ USD 27.8 million) in bank accounts, real estate and a car were seized/issued with prohibition of disposal orders during the course of investigations to prevent asset dissipation.

Person Y and the associate are based overseas and have not re-entered Singapore since the commencement of investigations. CAD has reached out to foreign counterparts to obtain further information on details and fund flows relating to these third-party accounts and investigations are ongoing.

Source - Singapore

3.3.7 Chinese Taipei

Case Study # 98: Use of credit cards to launder through jewellery stores.

Fraud; organised criminal syndicate; wire transfers; cash; use of credit cards; third-party laundering; dealers in precious metals and stones; financial institutions

In 2023, multiple transactions involving credit cards used for purchases at jewellery stores in Chinese Taipei were flagged as suspicious and reported. After analysis by the FIU, the financial intelligence was forwarded to the police.

The investigation revealed that, starting in 2023, Fraud Syndicate A impersonated officials of law enforcement agencies and prosecutors of Jurisdiction X. They contacted victims in Jurisdiction X and falsely claimed that the victims were involved in fraud or money laundering cases, deceiving them into transferring funds to designated accounts in Jurisdiction X.

Members of another money laundering group, including Person B, then used credit cards to make purchases in Chinese Taipei, forging the cardholder's signature to bypass KYC procedures. They then converted the purchased high-value gold and electronics into cash.

From March 2023 to August 2024, Person B and seven others laundered a total of TWD 209,922,791 (~ USD 7 million) for Fraud Syndicate A using this method.

In February 2025, the MJIB referred Person B and the others to the prosecutor's office under charges of fraud, violations of the *Money Laundering Control Act*, and the *Organized Crime Prevention Act*.

Source – Chinese Taipei

Legislative Developments

The *Money Laundering Control Act* was comprehensively amended in 2024, which included Article 6, which extends criminal liability to virtual asset service providers and third-party payment providers that fail to complete required AML registrations, and Article 11, which regulates fiduciary relationship. Both Article 6 and Article 11 came into force on 30 November 2024, while the other articles came into force on August 2, 2024. In accordance with the amendment, relevant regulations were issued by the relevant supervisors, all of which took effect on November 30, 2024.

Public-Private Collaboration

- **Enhanced financial risk controls**: several district prosecutor's offices signed MOUs with financial institutions. After concluding fraud case investigations, de-identified case data is shared with financial institutions, which utilise AI-driven analytics to optimize fraud detection and early-warning systems.

- **Strengthened supervision of virtual asset service providers**: Article 6 of the amended *Money Laundering Control Act i*mposes criminal penalties on virtual asset service providers that operate without completing AML registration or are offshore entities without proper local company or branch registration. The prosecutor's office established data integration systems with several virtual asset exchanges, allowing access to transaction and account-opening records. In addition, the prosecutor's office developed the 'Virtual Asset Seizure and Management Platform for the Prosecuting Authority', officially launched on April 15, 2024. This system ensures secure custody of seized virtual assets belonging to defendants or suspects. Once a final judgment is reached, assets can be either confiscated or returned to victims, ensuring the deprivation of proceeds of crime from the defendants or suspects.

Interagency Collaboration and Strengthened intelligence sharing: Chinese Taipei completed the development of a 'Third-Party Payment Virtual Account Inquiry Platform' for use by prosecutors. Law enforcement agencies are also working closely together to integrate databases of high-risk accounts (e.g., belong to migrant workers) and reprimanded accounts, facilitating control of bank accounts, VASP accounts, and third-party payment accounts.

4 - ASSET RECOVERY METHODS AND TRENDS

This section of the typologies report focusses upon data provided by APG members and observers in relation to asset recovery efforts and relevant case studies.

4.1 Asset tracing and investigation, provisional measures and confiscation.

4.1.1 Hong Kong, China

Hong Kong, China provided the following case studies to illustrate its asset tracing, including restraining actions.

Case Study # 99: Successful identification of overseas victim and stop payment in a case of money laundering (pretend CEO fraud)

Fraud; financial institutions

In August 2024, the Hong Kong Police Force received information from a local bank through the established channel of 'Upstream Scam Intervention' Scheme, indicating that a stooge account had received a sum of potential fraud payment. The Police then collaborated with two involved banks to conduct extensive reverse fund tracing, which revealed that the funds were sourced from a company in Jurisdiction A.

The Police contacted the victimized company through INTERPOL and realised that the company had fallen victim to a CEO Fraud, resulting in losses exceeding HKD 507 million (~ USD 65 million). A total of HKD 148.2 million (~ USD 19 million) in 23 fraudsters' accounts was suspended from further dissipation.

The restitution of the defrauded money is ongoing.

Source - Hong Kong, China

Case Study # 100: Successful stop payment in a case of money laundering (technical support scam) involving overseas victim

Scam; money value transfer services; financial institutions

In April 2024, a victim in Jurisdiction B had fallen into a technical support scam and was conned into remitting a total of HKD 2.44 million (~ USD 313,000) into two Hong Kong bank accounts. The case was referred to the Hong Kong Police Force by the law enforcement agency in Jurisdiction B.

Upon the Police's immediate liaison with the local beneficiary banks, a total of USD 277,000 (~ HKD 2.16 million) in three fraudsters' accounts was suspended from further dissipation. Subsequently, District Court granted the repatriation of frozen funds of USD 123,000 (~ HKD 959,400) to the victim in Jurisdiction B.

Source - Hong Kong, China

Case Study # 101: Successful stop payment in a case of money laundering (pretend CEO fraud)

Pretend CEO Fraud; financial institutions

In December 2024, employees of the victimized company in Jurisdiction C received false instructions and recordings from a fraudster impersonating the CEO requesting money for the purpose of an acquisition. Believing so, nearly HKD 5.74 million (~ USD 736,000) was transferred to a bank account in Hong Kong, China (HKC). Upon receiving a notification through INTERPOL's Global Rapid Intervention of Payments mechanism, the Hong Kong Police Force immediately processed the stop payment request and followed up with local banks in HKC.

All the fraudulent funds were successfully intercepted and reverted back to the victimised company's remittance bank accounts.

Source - Hong Kong, China

Case Study # 102: Successful recovery of cryptocurrency

Theft; fraud

A group of three cryptocurrency owners (victims) was lured to carry out cryptocurrency trade with a criminal syndicate. The syndicate arranged the victims to meet physically, agreeing to buy USDT (Tether) from victims with the return of fiat money via bank transfer. During the trade, the victims were instructed to open a new cryptocurrency wallet and transfer all USDT (Tether) into this cryptocurrency wallet. While they were opening this cryptocurrency wallet, the criminal syndicate members secretly captured the password (i.e. recovery seed).

The criminal syndicate then accessed to the victims' cryptocurrency wallet using the fraudulently obtained password and transferred the USDT (Tether) out from the cryptocurrency wallet to their cryptocurrency wallets and fled. Upon the Police investigation and request, the USDT (Tether) issuing company - Tether assisted to freeze 1.3 million USDT (Tether) (~ HKD 10 million).

Victims had filed for civil claim directly against Tether and subsequently recovered the frozen USDT (Tether) from Tether itself.

Source - Hong Kong, China

Case Study # 103: Money laundering via bank and securities accounts

Drug related crime; cash

In late 2021, a local drug peddler - Person A was arrested by Hong Kong, China's customs service for drug trafficking. A substantial amount of cash banknotes amounting to HKD 454,000 (~ USD 58,200) were found from his domicile. Financial investigation revealed that between 2020 and 2021, Person A had laundered about HKD 3.13 million (~ USD 401,300) through his bank and securities accounts.

Money laundering hallmarks observed were, for instance, temporary repository, large amount of counterparties with uncertain relationship, and significant turnover which was not commensurate with his financial profile.

Person A was subsequently convicted for drug trafficking and money laundering offences with realisable properties of HKD 940,000 (~ USD 120,500) being confiscated in November 2024.

Source - Hong Kong, China

4.1.2 Indonesia

Indonesia provided the following case studies to illustrate its asset tracing investigations and provisional measures to freeze and seize assets.

Case Study # 104: Tracing illicit assets and beneficial ownership in a palm oil land grabbing case

Wire transfer; beneficial ownership; use of legal persons; corruption; money laundering

A corruption and money laundering case involving Person X resulted in estimated state losses of IDR 78 trillion (~ USD: 4.7 billion), stemming from the illegal occupation of 37,095 hectares of oil palm plantation land in District Z.

The Indonesian Financial Intelligence Unit (PPATK) conducted asset tracing and fund flow analysis involving Person X and his immediate family members, focusing on companies under their control. Person X and his family were linked to 75 companies under the 'Group A' group of companies. Of these, Person X was identified as the beneficial owner of 42 companies where he was not listed as a shareholder, suggesting deliberate efforts to conceal the ownership and origin of illicit assets.

Although Group A accounts had been blocked since 2019, 17 companies under Person X's control received inbound transfers totalling approximately IDR 613.9 billion (~ USD: 37 million) from jurisdictions including the United States, Singapore, Malaysia, China and Hong Kong, China.

During the same period (2020 to July 2022), these companies also transferred approximately IDR 1.77 trillion (~ USD: 107 million) abroad, including to Singapore, Australia, China, Saudi Arabia, Malaysia and Hong Kong, China. Notably, some of the destination entities appeared to be unrelated to Group A's legitimate business operations and were suspected to be owned by Person X or his relatives.

Between July 2022 and April 2024, seven companies continued to conduct outbound transfers totalling IDR 376.4 billion (~ USD: 22.7 million) to foreign entities, raising further suspicion of ongoing laundering activities.

In July 2024, seven companies under the Group A - primarily in the palm oil sector and one holding company - were designated as suspects in the money laundering investigation. Most transactions were conducted internally, with the holding company functioning as the primary fund consolidation hub. In December 2024, Company E and Company F, subsidiaries of Holding Company S, were also designated as suspects. Holding Company S was found to have transferred funds to Bank C and Company Z, which is directly owned by Person X.

As of 2025, joint efforts by the Attorney General's Office and PPATK have resulted in the blocking of assets valued at IDR 1.21 trillion (~ USD: 73 million) and the seizure of assets worth IDR 1.47 trillion (~ USD 89 million), all linked to Person X and Group A's network.

Source - Indonesia

Case Study # 105: Asset recovery from online gambling proceeds: The seizure and management of a four-star hotel in Indonesia

Illicit gambling/gaming; cash; wire transfers; use of legal persons

Person F, an Indonesian entrepreneur, is suspected of operating and controlling an illegal online gambling network with an estimated turnover reaching hundreds of billions of rupiah. According to investigative findings covering the period of 2020–2022, Person F's personal accounts were identified as recipients of significant fund transfers originating from nominee (mule) accounts managed by gambling agents affiliated with various online gambling platforms. These funds, transferred both electronically and in cash, amounted to approximately IDR 356 billion (~ USD: 21.5 million) to Account A and IDR 46 billion (~ USD: 2.8 million) to Account B, both registered under Person F's name.

Subsequently, a substantial portion of the proceeds was transferred to Company M, a company where Person F's son, Person R, holds the position of Director. Of these funds, approximately IDR 146 billion (~ USD: 8.8 million) was used to finance the construction of a four-star hotel. In response to these findings, the Indonesian Financial Intelligence Unit (PPATK), in coordination with the Indonesian National Police (INP), has frozen a total of IDR 72.3 billion (~ USD: 4.4 million) across multiple accounts belonging to Person F and his associates.

At the time of this report, the case is under judicial process, and the hotel project has been officially seized by law enforcement authorities.

Source - Indonesia

4.1.3 Macao, China

Regarding the ML cases shared in this report, the Judiciary Police of Macao, China have taken relevant actions to seize assets, however, as relevant procedures are still underway, no further data is able to be shared at this point. During 2024, no relevant TF/PF has been identified during investigation of criminal cases.

4.1.4 Philippines

As of 31 May 2025, a total of five cases related to human trafficking had assets seized, with the total preserved assets amounting to PHP 4,980,296,717 (~ USD 85,711). Further as of 31 May 2025, human trafficking gathered the highest amount of preserved assets due to a number of big ticket cases on human trafficking which started to build up, beginning in August 2024 up to the present.

Case Study # 106: Human trafficking case

Human trafficking;

Within these total forfeited assets, a human trafficking case accounted for PHP 187,824,360 (~ USD 3,232,200) or approximately 10.91% of the total forfeited assets.

In this case, there are two Business Process Outsourcing (BPO) entities engaged in the trafficking of persons. The trafficked persons were then forced to conduct various online scam operations. In view of this, the Philippine National Police - Anti-Cybercrime Group (PNP-ACG) applied for and was granted search

warrants in the buildings located at the LMNOP Corporation in Pampanga where human trafficking victims were being held.

During the implementation of the search warrants, the PNP-ACG discovered monies composed of various currencies in the vaults located within the premises of Company A.

The court in the issuance of the Provisional Asset Preservation Order directed the PNP-ACG, the government agency in custody of the monies, to immediately preserve the same. Hence, the PNP-ACG continues to be in custody of the subject monetary instruments which will thereafter be delivered to the AMLC upon issuance of the Order of Finality and Writ of Execution and will be subsequently turned over to the National Government.

Source - Philippines

4.1.5 Singapore

Singapore provided the following case studies to illustrate its preservation measures and confiscation actions.

Case Study # 107: Money laundering prosecution of former director for helping global CEF-syndicate launder SGD $10.2 million from massive business email compromise fraud

International cooperation; transnational crime; organised criminal syndicate; significant proceeds of crime seized; use of Cash Movement Reports in investigations; extensive funds tracing; fraud; cash; financial institutions

In March 2020, during the Covid-19 pandemic, a European health products company was defrauded by criminals pretending to be their regular supplier into transferring EUR 6,636,000 (~ USD 7,768,000) into a corporate bank account in Singapore for the purchase of 2.9 million masks and 2 million bottles of hydroalcoholic gel. The company did not receive the products and after contacting the supplier, realised that they had been defrauded.

The Singapore bank, upon receiving a recall of funds request from the originating bank regarding the EUR 6,636,000 (~ USD 7,768,000) transfer, alerted the Singapore Police Force. Through quick intervention and close collaboration with seven banks, more than SGD 6.4 million (~ USD 4,9 million) was frozen by the Anti-Scam Centre across multiple corporate and personal bank accounts within the same day.

Investigations commenced into the director of the Singapore-incorporated company which the corporate bank account was registered under. He was out of Singapore at that point but was arrested upon his return. Extensive asset tracing was conducted which revealed how the initial sum of more than SGD 10 million (~ USD 7,732,849) was dissipated from the receiving account within days.

Investigations revealed that in October 2019, the director became acquainted with a male subject in a foreign jurisdiction and agreed to receive a large sum of money in a corporate bank account in Singapore under the director's sole control.

Checks by investigators revealed that the accused had submitted two Cash Movement Reports concerning moving SGD 1 million (~ USD 773,289) out of Singapore each, both within a week of receiving the funds. By comparing the dates of the Cash Movement Reports and the cash withdrawals, together with the director's travel records, investigators formed a better picture of how the illicit funds were laundered back to the foreign fraud group.

- Day 1: SGD 10.2m (~ USD 7.9 million) deposited into corporate account 1 (by victim) and SGD 1 million (~ USD 773,289) withdrawn in cash.
- Day 2: SGD 1 million (~ USD 773,289) withdrawn from corporate account 1 and SGD 300,000 (~ USD 231,985) withdrawn from corporate account 2.
- Day 3: The director submitted a Cash Movement Report on the outward movement of SGD 1 million (~ USD 773,289) cash.
- Day 5: SGD 1 million (~ USD 773,289) withdrawn from corporate account 2.
- Day 6: SGD 200,000 (~ USD 154,657 withdrawn from corporate account 1 and SGD 200,000 (~ USD 154,657) withdrawn from corporate account 2.
- Day 8: SGD 50,000 (~ USD 61,861) withdrawn from corporate account 1 and SGD 30,000 (~ USD 23,200) withdrawn from corporate account 2. The director submitted a Cash Movement Report on the outward movement of SGD 1 million (~ USD 773,289) cash.

Interviews with the director revealed that he was instructed by the male acquaintance to hand cash over to the latter and another person in two different jurisdictions, and he had left Singapore with SGD 2,000,000 (~ USD 1,546,570) on Day 3 and SGD 1,780,000 (~ USD 1,376,450) on Day 8. Confronted with the Cash Movement Reports written and signed by the director, he admitted that the SGD 1 million (~ USD 773,289)

stated in both Cash Movement Reports were lower than the actual amounts he was moving out of Singapore.

The director was charged with various offences including multiple counts of money laundering. The authorities in the European jurisdiction provided a statement pursuant to Section 74 of the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992 (CDSA) describing the foreign predicate offence of fraud perpetrated by an organised group, which was tendered as evidence to support the domestic money laundering charges.

Following a trial in November 2024, the director was convicted of seven counts of money laundering and two counts of failure to submit a full and accurate report of cross-border cash movement and sentenced to eight years' and eight months' imprisonment in total. A court order has been issued for the return of most of the seized funds to be returned to the European health products company.

The case is pending appeal.

Source - Singapore

Case Study # 108: Successful restraint of assets funded in part by proceeds of crime

Corruption and bribery; fraud/falsification; self-laundering

In 2021, Corrupt Practices Investigation Bureau (CPIB) received information that Person A, a director of a private healthcare corporation, had given improper payments and benefits to Person B, a former insurance executive, for the purposes of advancing the business interests of the said private healthcare corporation.

Investigations revealed that between 2015 to 2019, two other management personnel linked to the private healthcare corporation and Person A had, over multiple occasions, allegedly conspired and given gratifications of SGD 668,000 (~ USD 516,500) to Person B, as inducements to advance business interests of the companies under the said private healthcare corporation with the insurance companies which Person B was employed with.

It was revealed that between 2016 to 2019, to give the gratifications to Person B, the trio had allegedly conspired and falsified entertainment claims to companies under the said private healthcare corporation into paying Person A for entertainment expenses purportedly incurred. Investigations also revealed that Person B had used part of the proceeds of crime to purchase a landed property, which he subsequently sold off to purchase his current property.

In 2023, Person B was prosecuted on a single count of corruptly obtaining gratification and CPIB had also applied for a restraint and charging order on Person B's current property. In 2024, additional charges pertaining to corruption and money laundering offences were brought against Person B, while Person A and the two other management personnel were prosecuted for offences relating to corruption and falsification of accounts.

In the same year, the High Court ordered for the sale of the said property, of which up to a maximum of SGD 685,500 (~ USD 530,100) will be held by the court pending the outcome of the case.

Court proceedings are still ongoing.

Source - Singapore

Case Study # 109: Confiscation of proceeds of crime relating to drug trafficking

Drug related crime; significant drug proceeds seized; confiscation order

On 3 May 2017, Person A was arrested for trafficking in a controlled drug under the *Misuse of Drugs Act (MDA) 1973*. He was subsequently released on Court bail. On 12 February 2018, Person A was arrested for the second time, again for a drug trafficking offence, in which his court bail was revoked.

On 25 April 2019, he was sentenced to an imprisonment term of 15 years and 10 months and 16 strokes of the cane for his drug predicate offence.

For the two arrests, Person A's assets totalling SGD 25,393 (~ USD 19,636) were seized.

To ascertain the magnitude of the benefits Person A had received from his drug trafficking activities, concealed income analysis on Person A was computed. It showed that Person A had a concealed income of SGD 35,209 (~ USD 27,227) with realisable amount of SGD 25,393 (~ USD 19,636). This was the amount which Person A could not satisfactorily account for as his accumulated wealth, which was disproportionate to his known sources of income.

On 18 March 2025, a Confiscation Order for SGD 25,393 (~ USD 19,636) being the value of the benefits derived from Person A's drug trafficking, in accordance with Section 6 of the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) 1992* was granted by the Courts.

Source - Singapore

Case Study # 110: International cooperation leading to recovery of USD 40 million linked to business email compromise scam

International cooperation; successful recovery; fraud; financial institutions

In early July 2024, an employee of a Singapore company had received an email that purported to be sent by his company's supplier of liquefied natural gas. The email contained new details of a bank account maintained in Jurisdiction A, for the payment of USD 42.3 million to be made by the company to its supplier. Unbeknownst to the employee, the email account of the supplier was likely to have been compromised, and the correspondence between his company and the supplier had been intercepted by unknown perpetrators.

As a result of this email, on 19 July 2024, the employee transferred USD 42.3 million to the bank account maintained in Jurisdiction A. The employee subsequently discovered the fraud and lodged a police report on 23 July 2024. SPF swiftly requested assistance from authorities in Jurisdiction A through multiple channels, including INTERPOL's Global Rapid Intervention of Payments mechanism, ARIN-AP, FIU-to-FIU and mutual legal assistance.

On the following day, the Anti-Scam Centre was alerted that USD 39.3 million had been successfully withheld from the fake supplier's bank account in Jurisdiction A. Further joint investigations with Jurisdiction A authorities led to the arrest of nine suspects in Jurisdiction A and the recovery of over USD 2 million within two days.

Additionally, pursuant to information that some of the funds transferred to bank accounts in Jurisdiction B were maintained by two of the arrested individuals, Singapore Police Force sought assistance from Jurisdiction B's authorities to provisionally freeze the said proceeds of crime in Jurisdiction B.

With close cooperation between the authorities (FIUs, law enforcement agencies and mutual legal assistance Central Authorities) from all three jurisdictions, USD 39.3 million had been successfully returned to the victim in Singapore.

The remaining USD 2 million is pending return from Jurisdiction A.

Source - Singapore

4.1.6 Chinese Taipei

Chinese Taipei provided the below information on its confiscation regime:

Confiscation: According to Article 38 and Article 38-1 of the *Criminal Code*, a thing used in the commission of or preparation for the commission of an offense or a thing derived from or acquired through the commission of an offense and proceeds of the crime should all be confiscated.

Extended confiscation: According to Article 25, Paragraph 2 of *Money Laundering Control Act* and Article 19, Paragraph 3 of *Narcotics Hazard Prevention Act*, when investigating the defendant, if there is sufficient evidence confirming that a property from unidentified sources at the disposal of the defendant is in fact incomes of other unlawful activity, it shall be confiscated.

Seizure and forced collection: According to Article 133, Paragraph 1 of the *Code of Criminal Procedure*, an item that is subject to confiscation, may be seized, and according to Paragraph 2, 'to ensure a forced collection, a certain portion of the property of the suspect, accused, or a third party, may be seized with discretion as required'.

For accounts, remittances, currency or other payment methods suspected of money laundering, according to Article 18 of *Money Laundering Control Act*, a prosecutor may request a court order to prohibit the withdrawal, transfer, payment, delivery and assignment, or to make other necessary disposition of such property.

4.1.7 United Arab Emirates

The United Arab Emirates provided the following case studies to illustrate its preservation measures and confiscation actions.

Case Study # 111: Trade-based money laundering and complex structures

Trade-based money laundering drug related crime; use of legal persons and arrangements; third-party laundering; international cooperation; purchase of real estate; cash; financial institutions

Nine individuals and four legal persons were prosecuted and convicted for an AED 61.8 million (~ USD 17,000,000) trade-based money laundering (TBML) scheme. This investigation revealed that millions of dirhams generated through drug trafficking committed in a foreign jurisdiction were moved to the United Arab Emirates (UAE) to four shell companies through the formal banking system under the cover of consultancy services, and eventually used to purchase luxury vehicles, then exported to a foreign jurisdiction. An incoming informal international cooperation request to UAE Customs shed light on several bank accounts in the UAE that were linked to drug trafficking investigations in a foreign jurisdiction, and that several shipments of vehicles are potentially involved.

Upon analysis of export and re-export databases, among others, the FIU harnessed financial information from all financial institutions and DNFBPs, and open sources, which led to identifying and tracing the proceeds of criminality to multiple accounts. In addition, the FIU established that international wirings were made in effect of consultancy fees and commercial letters of credit. Complex transactions were then linked to multiple outlets. Moreover, information from the National Economic Registrar database and Unified National Platform on involved legal persons established that they were in fact shell companies. Access to the Federal Authority For Identity, Citizenship, Customs and Port Security databases demonstrated that the legal persons were abused by orchestrating international trade.

In parallel to the FIUs analysis, Authorities identified the controllers and mules involved by utilising multiple investigative techniques, such as wiretapping, remote device monitoring, GPS tracking, controlled delivery, and undercover operations. The Live Facial Recognition Software through public CCTV was critical in uncovering events of cash withdrawals, purchases and export, and persons involved.

Evidence provided by UAE Customs through its exports-related databases and others, in its capacity within the taskforce, established that the purchased vehicles were immediately exported through the legal persons to several consignees in a foreign jurisdiction.

Building on the intelligence, arrest and search warrants were issued and all individuals were arrested, premises searched, and assets were seized in the form of cash, electronic devices, gold, vehicles, and real estate. The individuals were imprisoned for 3 to 8 years, a total fine of AED 62 million (~ USD 17,000,000) was imposed on all persons, confiscation of assets seized in value of AED 61.8 million (~ USD 17,000,000), deportation and license revocation.

Source - United Arab Emirates

Case Study # 112: Foreign predicate offence

Foreign predicate offence; corruption and bribery; use of legal persons and arrangements; financial institutions; international cooperation

United Arab Emirates (UAE) FIU received a spontaneous dissemination from a foreign FIU regarding several foreign suspects being under investigation for corruption and bribery, which was led by several authorities internationally. Upon receiving the information, the FIU conducted a financial analysis of the data and sent multiple requests for information domestically and to foreign FIUs.

The financial intelligence obtained from 11 financial institutions and 134 financial accounts on four natural persons and eight legal persons was analysed and a freezing order was issued. The PP issued a warrant against the foreign suspects for laundering the proceeds of a foreign predicate offence, and an extension of the freeze order was warranted. Total assets effectively traced, identified and frozen amounted to AED 44,118,901 (~ USD 12,000,000).

Source - United Arab Emirates

Case Study # 113: Drugs stashed on container ship

Drug related crime; international cooperation; transnational crime; organised criminal syndicate; smuggling; use of the internet

In July 2022, the United Arab Emirates (UAE) Police and UAE Customs collected intelligence that a cargo ship departing a port in a foreign jurisdiction had one of its containers stashed with methamphetamine; through the informal cooperation channels via RELO, the UAE authorities notified counterparts about the shipment, and they organised a special operation to seize and search the cargo ship upon arrival.

Moreover, the counterpart authorities boarded the ship and methamphetamine was seized. The resulting joint operation and informal international cooperation led to the second biggest drug bust ever made in the history of this Jurisdiction. The outgoing dissemination was based on intelligence intercepted from a regional known organised criminal syndicate specialised in the smuggling of methamphetamine in the Asian region.

Source - United Arab Emirates

Case Study # 114: P/3PML including international facilitators-virtual asset service providers

Use of virtual assets; virtual asset service providers; third-party laundering; use of legal persons and arrangements; cash

In July of 2023, 11 individuals and four legal entities were investigated for operating unlicensed virtual asset service providers. In addition, the lack of a compliance function was exploited by ill-actors to move, convert, and conceal ill-gotten proceeds of criminality. All persons were detained, investigated, all assets were seized, and are prosecuted.

Through deploying 164 officers on the ground, a large-scale sting operation, which was conducted simultaneously in nine locations, yielded the arrest of all individuals involved, seizure of AED 18,883,508 (~ USD 5 million) in cash, virtual assets - mostly USDT (Tether) valued at AED 59,217,580 (~ USD 16 million) and 11 additional unpaid 'tokens' and 'vouchers', 2 cryptocurrency ATM machines, multiple laptops, phones, luxury watches, documents, and over 278 large files of unofficial invoices and ledgers.

In August 2023, the Money Laundering Court convicted all subjects, applied fines (which ranged from AED 200,000 to AED 5 million (~ from ~ USD 55,000 to USD 1.4M million) and confiscated all seized assets.

Source - United Arab Emirates

4.2 Managing frozen/seized assets: information on asset management cases and procedures or manuals available to agencies involved in asset management.

4.2.1 Macao, China

The asset seizure mechanism and procedure of Macao, China are mainly regulated by the Criminal Procedure Code. According to the law, judicial authorities may approve or order the seizure of objects that were used for or prepared to be used for criminal actions, those that constitute the products, profit, price or rewards of a criminal offence, as well as other objects that may be regarded as evidence. The seized objects shall be attached to the case file, and when impossible, entrusted to the custody of the judicial employee responsible for that proceeding or of the depositaries. If the seized assets may be lost or damaged, or are hazardous, judicial authorities may, as circumstances require, order to have these assets sold, destroyed or used for social benefits.

To systematically and efficiently handle seized assets during the course of proceedings, the Public Prosecutions Office (MP) of Macao, China built the 'seized assets management system' with a seized assets handling guideline and user manual available. MP is gradually developing a structured format for the transmission of seized assets information with the law enforcement agencies, and it will continue to discuss and promote relevant systematic exchange of data.

4.3 Asset confiscation: experience with the application of criminal, civil or administrative processes to recover proceeds of crime – successes and challenges.

4.3.1 Macao, China

With respect to confiscating instrumentalities and proceeds of crime, the *Criminal Code of Macao, China* has set aside specific chapters with stipulations regarding the loss of objects or rights related to criminal activities. It also has provisions for the handling of objects used for or to be used for criminal actions, or those as a result of such crimes, as well as confiscating any rewards, items, rights or profits directly or indirectly obtained through criminal activities. In case certain proceeds of crime cannot be seized in a material manner, a certain amount of money will have to be paid to Macao, China as compensation.

4.4 Use and sharing of confiscated proceeds: including cases of repatriation of confiscated assets to/from other jurisdictions.

4.4.1 Macao, China

Regarding illicit assets that have been transferred to other jurisdictions, the recovery of cross-border illegal assets is carried out through mutual legal assistance and international cooperation mechanism, mainly according to the *Law on Mutual Legal Assistance in Criminal Matters of Macao, China*, and the relevant provisions of the *United Nations Convention against Corruption* and the *United Nations Convention against Transnational Organized Crime* applicable to Macao, China. No cases of asset recovery through mutual legal assistance have been carried out in 2024

4.4.2 Chinese Taipei

Previously in 2022, Chinese Taipei handled its first case of returning proceeds of crime, successfully returning illicit assets derived from drug trafficking and money laundering offenses nearly USD 16 million to the U.S. Government. The U.S. Department of Justice later expressed sincere appreciation for Chinese Taipei's assistance and actively undertook the relevant domestic procedures for international sharing.

After more than two years of processing and multiple rounds of bilateral consultations, in August 2024, following deductions for administrative fees, related costs, and victim compensation, the U.S. shared 50% of the illicit forfeited assets—approximately USD 7 million—with Chinese Taipei.

5 - FATF, FSRBS AND OBSERVER ORGANISATIONS' PROJECTS

This section of the typologies report provides a brief overview of typology reports published by the FATF, FSRBs and observer organisations in 2024/2025.

5.1 Financial Action Task Force

The FATF developed the following reports that outline some of the latest AML/CFT/CPF methods and trends.

Money Laundering National Risk Assessment Toolkit[17]

FATF launched a Money Laundering (ML) National Risk Assessment (NRA) toolkit designed to help jurisdictions develop and strengthen their risk-based approach to fighting financial crime.

These new practical resources will support countries in assessing their ML risks in line with the FATF Standards.

Money Laundering National Risk Assessment Guidance[18]

This guidance document supports jurisdictions in conducting an NRA focused on the assessment of ML risks, drawing on insights from over 90 jurisdictions across the Global Network and over 500 respondents to public consultation. Key sections include:

- NRA Preparation and Setup: This section identifies the prerequisites to a successful NRA. It covers such key foundational parts of the NRA such as political commitment, an inclusive NRA mechanism, objective setting, and the acquisition of information and data.
- Assessing and Understanding ML Risks: Offers a flexible yet structured methodology for analysing threats, vulnerabilities, and risks, allowing jurisdictions to implement a coherent methodology that is adapted to their capacity and unique risk and context.
- Post-NRA Actions: Recommends follow-up actions, including aligning mitigation measures with identified risks, communicating findings, and refining the NRA process.

This guidance serves as a practical resource for jurisdictions aiming to strengthen their AML/CFT systems and align them with proven practices across the Global Network.

The guidance was updated on 28 August 2025 to take into account changes to the FATF Standards on R.1 and the Guidance on Financial Inclusion and AML/CFT Measures.

Complex Proliferation Financing Sanctions Evasion Schemes[19]

The Complex Proliferation Financing and Sanctions Evasion Schemes report reveals that significant vulnerabilities remain across the global financial system in countering the financing of weapons of mass destruction (WMD).

The report provides a detailed analysis of the evolving methods and techniques used to evade PF-related sanctions, including those imposed under Recommendation 7 of the FATF Standards, as well as other national and supranational regimes beyond the FATF Standards. It outlines how proliferation networks are

[17] Financial Action Task Force - *FATF launches National Risk Assessment toolkit to help countries identify greatest money laundering risks*: https://www.fatf-gafi.org/en/publications/Fatfgeneral/FATF-launches-National-Risk-Assessment-toolkit-to-help-countries-identify-greatest-money-laundering-risks.html

[18] Financial Action Task Force - *Money Laundering National Risk Assessment Guidance*: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-National-Risk-Assessment-Guidance.html

[19] Financial Action Task Force - *Complex Proliferation Financing Sanctions Evasion Schemes*: https://www.google.com/search?safe=strict&sca_esv=2b402440a197c26d&q=fatf+Complex+Proliferation+Financing+Sanctions+Evasion+Schemes&spell=1&sa=X&ved=2ahUKEwiu74m5vc2QAxVV1DQHHdz1OUcQBSgAegQIERAB&biw=1272&bih=652&dpr=1.5

sourcing dual-use goods, technologies, and knowledge—often through procurement networks and front companies—and using various financial channels to access the global financial system.

The report identifies four major typologies used in sanctions evasion:

- Use of intermediaries to evade sanctions
- Obscuring beneficial ownership information (BOI) to access the financial system
- Using virtual assets and other technologies
- Exploiting the maritime and shipping sectors

To support responses to these challenges, the report outlines common enforcement obstacles and shares examples of good practices, such as public-private partnerships to improve information sharing, and the issuing of detailed alerts and practical risk indicators to help competent authorities detect and report sanctions evasion. The report also highlights the need for a more coordinated and globally consistent response—one that aligns with existing international obligations and reflects the complexity of current PF and sanctions evasion schemes.

Detecting, Disrupting, and Investigating Online Child Sexual Exploitation (OCSE): **Using Financial Intelligence to Protect Children from Harm**[20]

This report draws on experiences across the Global Network to examine two distinct forms of OCSE:

- **Live-streamed Sexual Abuse of Children (LSAC)** is the broadcasting of sexual abuse of children for financial gain. This involves consumers paying to watch real time live sexual abuse of children.
- **Financial Sexual Extortion of Children (FSEC)** involves a victim being invited to exchange sexually explicit photographs or footage, or to join a sexually explicit video call which is recorded. Once the perpetrator has the sexually explicit material, they threaten victims to pay a ransom.

The report identifies profiles of perpetrators and victims for these crimes and the use of Money or Value Transfer Services (MVTS), online peer-to-peer (P2P) payment systems such as PayPal, and direct bank transfers or transfers of virtual assets (VAs) through virtual asset service providers (VASPs) as common financial channels used.

To assist in the identification of transactions linked to LSAC and FSEC, the report provides examples of indicators which can be shared with reporting entities. These indicators include transaction types, amounts, descriptions, timing, frequency, and the pattern of transactions between the victim and perpetrator.

The report also outlines challenges in detecting and combating OCSE including the lack of understanding of the scope and scale of OCSE and its proceeds. Jurisdictions are not sufficiently considering these crime types when identifying and assessing their domestic ML risks or coordinating prevention efforts. Emerging challenges including AI and other technological developments may also expand the reach of perpetrators and increase the number of victims.

FATF-style regional bodies

5.2 Eurasian Group on Combating Money Laundering and Financing of Terrorism

The Eurasian Group on Combating Money Laundering and Financing of Terrorism (EAG) completed the following typology projects.

[20] Financial Action Task Force - *Detecting, Disrupting, and Investigating Online Child Sexual Exploitation (OCSE): Using Financial Intelligence to Protect Children from Harm:* https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Online-child-sexual-exploitation.html

Criteria for identifying suspicious money recovery lawsuits for the purpose of money laundering[21]

EAG Member States contributed and the EAG Secretariat led the project.

The EAG Regional Risk Assessment report identified a regional risk, that requires standard measures to be taken in order to mitigate it (to the lowest level of risk). This risk is using schemes to access offshore funds through enforcement means. It is often manifested in practice in the use of court judgements rendered on fictitious grounds. For example, a non-resident company files a claim with a court against a resident company seeking the recovery of funds for failure to discharge obligations on various grounds (loan, services, suretyship under other agreements, etc). The judiciary bodies render a judgement to recover the debt from the resident company in favour of the non-resident company and the funds are transferred in a compulsory manner.

Moreover, in a number of cases, it is possible to reach the objectives of the litigation mechanism even without the enforcement of the judgment. Funds are given the appearance of being received under a judicial act in order to lend a veneer of legality to such funds, and the proceeds of crime – with the source of their true origin concealed – therefore become legalised.

Monitoring the Risks of Use of Virtual Assets for Criminal Purposes[22]

EAG Member States, Republic of Azerbaijan, Republic of Armenia, Mongolia, Republic of Serbia, CIS Anti-Terrorist Center (CIS ATC) all contributed, with the EAG Russian Federation leading the project.

At the 37th EAG Plenary meeting in November 2022, a typology project on 'Monitoring the Risk of the Use of Virtual Assets for Criminal Purposes' led by the Russian Federation, was supported by all member states.

This project is part of the implementation of one of the EAG key priorities of the 2022-2023 Chairmanship: *Monitoring the risks of use of virtual currencies for criminal purposes*.

The current agenda in the expansion of global cryptocurrency markets is increasingly focused on the problem of identifying and minimizing the risks and threats of their use for criminal purposes. This is due to the involvement of an increasing number of people in the activities of criminal groups operating in the payment instrument markets. Despite significant growth in the use of virtual assets for money laundering, jurisdictions lack regulatory harmonisation of the cryptocurrency market. In addition, the level of implementation of the FATF Recommendations is still insufficient.

The widespread use of virtual assets and schemes to exploit them in illicit activities explains the need for close inter-agency coordination and international cooperation.

In implementing the project, the following objectives were achieved:

- Development of the virtual asset industry has been assessed.
- Threats, vulnerabilities and risks associated with the use of virtual assets for criminal purposes have been identified.
- Tools and best practices to minimize the risks of the use of virtual assets in unlawful activities have been analysed.
- Information sources to improve the effectiveness of financial investigations have been identified.

[21] Eurasian Group on Combating Money Laundering and Financing of Terrorism - *Criteria for identifying suspicious money recovery lawsuits for the purpose of money laundering*: *https://eurasiangroup.org/files/uploads/files/Public_typology_reports/Criteria_for_identifying_suspicious_money_recovery_lawsuits_eng.pdf*

[22] Eurasian Group on Combating Money Laundering and Financing of Terrorism - *Monitoring the Risks of Use of Virtual Assets for Criminal Purposes*: https://eurasiangroup.org/files/uploads/files/Public_typology_reports/Monitoring%20the%20Risks%20of%20Use%20of%20Virtual%20Assets_eng.pdf

- Recommendations for representatives of competent authorities and the private sector to prevent the use of virtual assets for criminal purposes have been made.

5.3 The Middle East and North Africa Financial Action Task Force

The MENAFATF published/started the following products.

Typologies Report on ML/TF through legal persons and legal arrangements in the MENA region[23].

MENAFATF developed and completed a typologies project on ML/TF risks associated with the misuse of legal persons and legal arrangements in the MENA region. This initiative was a response to ongoing regional and international concerns regarding the abuse of corporate structures for illicit financial activities.

The study aimed to support member jurisdictions in understanding the scale, nature, and typologies of ML/TF through legal entities, particularly in the context of recent changes to FATF Recommendations 24 and 25. These amendments emphasise beneficial ownership transparency and the need for robust mechanisms to prevent the misuse of legal vehicles.

The project was built upon:

- comprehensive literature review of international and regional studies.
- structured questionnaire sent to MENAFATF member jurisdictions, with assistance from external expert.
- compilation and analysis of relevant case studies and typologies.

The final report categorises regional threats into misuse of shell companies, obscured beneficial ownership, use of nominee structures, and layering through cross-border arrangements. It also explores the role of trust service providers and DNFBPs in enabling or preventing such misuse.

Key findings/recommendations include:

- Updating anti-money laundering and counter-terrorist financing policies.
- Enhancing regional and international cooperation.
- Strengthening regulatory measures on non-profit organisations.
- Enhancing financial transparency by mandating beneficial ownership registries.
- Monitoring international financial transfers linked to high-risk entities.
- Tightening oversight into free zones and tax havens.
- Combating the misuse of shell companies and complex legal structures.
- Raising compliance levels in financial institutions.
- Regulating the remittance and exchange company sector.

***Update the Study on 'R.25 and Endowments' in the MENA region*.**

This study aims to reassess and clarify the classification of Islamic endowments 'WAQF' under the FATF Recommendation 25, which deals with transparency of beneficial ownership of legal arrangements. The project was launched in response to conflicting conclusions between an earlier 2012 study—which treated WAQF as legal persons—and mutual evaluation reports that considered them legal arrangements.

[23] MENATFATF - *Typologies Report on ML/TF through legal persons and legal arrangements in the MENA region*: https://www.menafatf.org/sites/default/files/Newsletter/Typologies%20Report%20of%20MENAFATF.pdf

The update of the study investigates whether WAQF should be viewed as legal arrangements or legal persons, by analysing their structures, functions and alignment with the characteristics of express trusts as defined under FATF standards and the Hague Trust Convention. It seeks to develop a regional mechanism to uniformly classify different forms of WAQF and update guidance considering recent FATF amendments, particularly the March 2023 changes to Recommendation 25.

Although the report is not finalised and still in the analysis process, there are some recommendations based on the situation thus far:

- There is inconsistency across MENA jurisdictions in classifying WAQF, with descriptions ranging from legal arrangements to legal-Sharia arrangements or legal persons.
- Many jurisdictions consider WAQF is similar to express trusts and evaluate them under R.25.

The project recommends:

- Developing clear criteria (structural and functional) for evaluating WAQF as legal arrangements.
- Establishing a unified regional mechanism to classify WAQF.
- Creating a regional reference document identifying WAQF types/forms compliant with FATF standards.

The project is not yet finalised.

Regional Risk Assessment Methodology for Money Laundering and Terrorism Financing

The Regional Risk Assessment (RRA) Methodology project aims to establish a unified and structured approach for evaluating ML/TF risks across MENAFATF member jurisdictions. Recognizing the diversity in national risk profiles, the methodology provides a standardised framework that enables jurisdictions to consolidate and compare risk data at the regional level. The project offers a model to classify and analyse threats based on objective indicators. This framework supports the identification of risk priorities, enhances the strategic value of national findings and promotes regional consistency in AML/CFT risk analysis.

Ultimately, the methodology is designed to assist MENAFATF member jurisdictions in aligning their risk understanding with global standards, facilitating joint planning, cross-border cooperation, and more effective targeting of resources and policies.

Key findings/recommendations include:

- A formal Regional Risk Assessment Methodology was developed and proposed for adoption by the Plenary meeting.
- The model is based on reliable, neutral, and up-to-date national data ensuring regional comparability.
- The risk classification system helps identify high-risk areas and supports targeted intervention strategies.
- The methodology aligns with FATF and World Bank standards and uses Euclidean distance formulas for composite risk scores (i.e., combining frequency and severity).
- Recommendations include:
    - Adoption of the methodology.
    - Collection of standardised risk data from member states.
    - Continued regional analysis of ML/TF risks.
    - Promotion of common understanding of high-risk typologies across member states.

The methodology is adopted but not yet published.

Observer organisations

5.4 Asian Development Bank

The Asian Development Bank (ADB) published the following products.

Solving Adoption Challenges of New Technology: The Case of ISO 20022 for Cross-Border Payment Messages[24]

This brief addresses the need for standardization and coordinated implementation using the example of ISO 20022 in cross-border payments and examines five key inhibitors that prevent industry-wide adoption of technology.

Comparative Lessons from Asia's National Digitalization Strategies: Indonesia, the Republic of Korea, Singapore, and Thailand[25]

This brief shares lessons from the digitalization journeys of Asian economies, highlighting the importance of strategic leadership, inclusive design, and systemic investment.

Digitalization for Inclusive Growth[26]

This brief looks at how policymakers can reduce digital disparities and harness the adoption of digital technologies to promote inclusive growth, trade, and innovation.

The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific[27]

This book explores how the evolving digital landscape is reshaping trade dynamics and regulation in Asia and the Pacific, examines digital economy agreements, and considers how the digital economy can drive inclusive growth.

Cross-Border Bank Flows, Regional Household Credit Booms, and Bank Risk-Taking[28]

This paper provides novel microlevel evidence from Germany that cross-border bank flows are an important means for households to access credit.

Digitalization and Income Inequality: Evidence from Households[29]

This paper uses household data from the People's Republic of China to examine how digitalization affects income inequality.

Mainstreaming Forest Conservation Finance: Integrating Positive Incentives with Due Diligence in Global Supply Chains[30]

[24] Asian Development Bank - *Solving Adoption Challenges of New Technology: The Case of ISO 20022 for Cross-Border Payment Messages*: https://www.adb.org/publications/adoption-challenges-new-technology

[25] Asian Development Bank - *Comparative Lessons from Asia's National Digitalization Strategies: Indonesia, the Republic of Korea, Singapore, and Thailand*: https://www.adb.org/publications/lessons-asia-digitalization-strategies

[26] Asian Development Bank - *Digitalization for Inclusive Growth*: https://www.adb.org/publications/digitalization-inclusive-growth

[27] Asian Development Bank - *The Role and Future of Digital Economy Agreements in Developing Asia and the Pacific*: https://www.adb.org/publications/digital-economy-agreements-asia-pacific

[28] Asian Development Bank - *Cross-Border Bank Flows, Regional Household Credit Booms, and Bank Risk-Taking*: https://www.adb.org/publications/cross-border-bank-flows-household-credit-booms

[29] Asian Development Bank - *Digitalization and Income Inequality: Evidence from Households*: https://www.adb.org/publications/digitalization-income-inequality-evidence-households

[30] Asian Development Bank - *Mainstreaming Forest Conservation Finance: Integrating Positive Incentives with Due Diligence in Global Supply Chains*: https://www.adb.org/publications/mainstreaming-forest-conservation-finance

This brief underscores the economic and environmental importance of forests and looks at ways Asia and the Pacific can develop innovative payments for ecosystem services (PES) that preserve its forests and underpin sustainable development.

Digital Transformation for the Sustainable Development Goals: Framework and Road Maps to Drive Prosperity, Inclusion, Resilience, and Sustainability[31]

This publication outlines how digital solutions can fast-track progress toward meeting the Sustainable Development Goals (SDGs) by 2030 and shows how the Asian Development Bank can assist in inclusive and resilient digital transformations.

Redefining Financial Ecosystems in Asia and the Pacific: A New Era of Open Banking, Open Finance, and Inclusive Growth[32]

This publication examines the rapid evolution of innovative open finance frameworks and considers their potential to transform Asia and the Pacific's financial landscape to make it more inclusive, efficient, and equitable.

5.5 International Monetary Fund

The International Monetary Fund (IMF) published the following products[33].

Selected Issues Paper: *Remittances to Samoa: A Safe Payment Corridor*[34].

This paper provides a targeted analysis of ML/TF risks pertaining to remittances to Samoa, confirming limited risks, and discusses potential opportunities for streamlining applicable AML/CFT requirements to operationalize regional remittances risk assessments. Over the past decade, Samoa has been subject to de-risking, which has resulted in Correspondent Banking Relationship (CBR) withdrawals, CBR fragility and rising concentration risks, especially for money transfer operators (MTOs). The paper presents an analysis of authorities' and the financial sector's risk understanding and publicly available information on crime and the ML risk environment and concludes that there are limited ML/TF threats to the main remittance corridors to Samoa. Samoa's ML/TF vulnerabilities - mostly related to capacity and resource constraints - are alleviated by the low ML/TF threat environment and regional information exchange and capacity building. Based on these findings, the paper provides an overview of potential regulatory and supervisory measures to promote a risk-based approach to CBRs to streamline the AML/CFT requirements for low-risk remittances to Samoa.

Working Paper: *Targeted Transparency: Sectoral Approach to Beneficial Ownership in Procurement and Real Estate*[35].

Identifying the natural person who ultimately owns or controls an asset—known as the beneficial owner—is a key transparency measure to prevent misuse for criminal or unethical purposes. This is especially critical in high-risk sectors, where vulnerabilities are amplified during economic or existential crises, such as financial bubbles or climate change. While many countries are establishing centralized beneficial ownership registries—often linked to commercial registers for AML/CFT compliance—these may not fully meet the needs of sector-specific oversight. Agencies like procurement authorities or land registries often require more granular or tailored beneficial ownership data, such as information on foreign entities or lower

[31] Asian Development Bank - *Digital Transformation for the Sustainable Development Goals: Framework and Road Maps to Drive Prosperity, Inclusion, Resilience, and Sustainability*: https://www.adb.org/publications/digital-transformation-sustainable-development-goals

[32] Asian Development Bank - *Redefining Financial Ecosystems in Asia and the Pacific: A New Era of Open Banking, Open Finance, and Inclusive Growth*: https://www.adb.org/publications/redefining-financial-ecosystems-asia-pacific

[33] The views expressed in the referenced documents are those of the author(s) and do not necessarily represent the views of the IMF, its Executive Board, or IMF management.

[34] International Monetary Fund - *Remittances to Samoa: A Safe Payment Corridor*: https://www.imf.org/en/Publications/selected-issues-papers/Issues/2025/05/14/Remittances-to-Samoa-A-Safe-Payment-Corridor-566996

[35] International Monetary Fund - *Targeted Transparency: Sectoral Approach to Beneficial Ownership in Procurement and Real Estate*: https://www.imf.org/en/Publications/WP/Issues/2025/09/12/Targeted-Transparency-Sectoral-Approach-to-Beneficial-Ownership-in-Procurement-and-Real-570051

thresholds for politically exposed persons (PEPs). A sectoral approach to beneficial ownership transparency addresses these gaps by aligning data collection and use with the unique risks and operational realities of each sector. This allows for flexible implementation—from basic disclosures in transactions to advanced verification—while complementing national beneficial ownership frameworks. Importantly, the design should consider sectoral capacity and minimize compliance burdens. Drawing on lessons from the COVID-19 pandemic, where beneficial ownership transparency in procurement helped mitigate corruption risks, this approach is now being explored for other high-risk areas such as real estate, which is particularly vulnerable to money laundering.

Working Paper: *Decrypting Crypto: How to Estimate International Stablecoin Flows*[36].

This paper presents a novel methodology—leveraging a combination of AI and machine learning to estimate the geographic distribution of international stablecoin flows, overcoming the "anonymity" of crypto assets. Analysing 2024 stablecoin transactions totalling $2 trillion, our findings show: (i) stablecoin flows are highest in North America ($633bn) and in Asia and Pacific ($519bn). (ii) Relative to GDP, they are most significant in Latin America and the Caribbean (7.7%), and in Africa and the Middle East (6.7%). (iii) North America exhibits net outflows of stablecoins, with evidence suggesting these flows meet global dollar demand, increasing during periods of dollar appreciation against other currencies. Further, we show that the 2023 banking crisis significantly impeded stablecoin flows originating from North America; and finally, offer a comprehensive comparison of our data to the Chainalysis dataset.

Working Paper: *Digital Financial Inclusion and Income Inequality in China*[37].

This paper uses both macro and household-level data to examine the relationship between digital financial inclusion, measured by the Peking University digital financial inclusion index, and income inequality in China. We find that a higher level of digital financial inclusion is associated with significantly lower income inequality within provinces, including through having larger positive effects on lower-income households' incomes from salaries and public and private transfers. However, we do not find a significant impact of digital financial inclusion on income inequality across provinces, as households in the relatively more developed southern region benefitted more from digital financial inclusion than those in the northern region. We also find that digital financial inclusion has larger effects on the incomes of rural, female-headed, and less educated households, which have likely contributed to the narrowing of the overall income inequality, but a smaller effect on the income of elderly households—pointing to the "digital divide" problem among the elderly in China.

Working Paper: *Could Digital Currencies Lead to the Disappearance of Cash from the Market?*[38]

Private and public agents' plans and actions to introduce digital currencies and other innovative payment instruments could produce some unintended consequences, including the potential disappearance of physical cash. This study employs a two-sided market model to examine how payment systems might respond to new currencies. Numerical simulations indicate that the success of a new currency hinges on a large-scale launch. However, even unsuccessful attempts could disrupt existing systems, potentially resulting in the elimination of cash. If cash plays a critical role as a safeguard, regulatory and monetary authorities should give due consideration to ensure its continued availability when payment innovations are introduced.

Working Paper: *Prometheus Unbound: What Makes Fintech Grow?*[39]

[36] International Monetary Fund - *Decrypting Crypto: How to Estimate International Stablecoin Flows*: https://www.imf.org/en/Publications/WP/Issues/2025/07/11/Decrypting-Crypto-How-to-Estimate-International-Stablecoin-Flows-568260

[37] International Monetary Fund - *Digital Financial Inclusion and Income Inequality in China*: https://www.imf.org/en/Publications/WP/Issues/2025/04/04/Digital-Financial-Inclusion-and-Income-Inequality-in-China-565383

[38] International Monetary Fund - *Could Digital Currencies Lead to the Disappearance of Cash from the Market?*: https://www.imf.org/en/Publications/WP/Issues/2025/03/21/Could-Digital-Currencies-Lead-to-the-Disappearance-of-Cash-from-the-Market-565377

[39] International Monetary Fund - *Prometheus Unbound: What Makes Fintech Grow?*: https://www.imf.org/en/Publications/WP/Issues/2025/02/21/Prometheus-Unbound-What-Makes-Fintech-Grow-562159

The rise of financial technologies (fintech) could have transformative effects on the financial landscape, expanding the reach of services beyond the confines of geography and creating new competitive sources of finance for households and firms. But what makes fintech grow? Why do some countries have more financial innovation than others? In this paper, I use a comprehensive dataset to investigate the emergence and spread of fintech in a diverse panel of 98 countries over the period 2012–2020. This empirical analysis helps ascertain economic, demographic, technological and institutional factors that enable the development of fintech. The magnitude and statistical significance of these factors vary according to the type of fintech instrument and the level of economic development (advanced economies vs. developing countries). Finally, these findings reveal that policies and structural reforms can help promote financial innovation and cultivate fintech ventures—particularly by strengthening technological and institutional infrastructures and reducing cybersecurity threats.

Working Paper: *On Cross-Border Crypto Flows: Measurement Drivers and Policy Implications*[40]

Cross-border crypto flows (CBCFs) are not systematically measured and are poorly understood. After defining CBCFs and the channels through which they materialize, we review the various approaches to measure them through two case studies. We also quantify the dynamics and drivers of CBCFs through a push/pull factor SVAR model. We find an increasingly large volume of CBCFs, although considerable heterogeneity remains across estimates. Furthermore, CBCFs are more sensitive to push factors than regular capital flows. Our findings call for accurate and comprehensive measurement and monitoring of CBCFs and the need to rethink capital account restrictions in a more digitalized world.

5.6 United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime published the following.

***World Drug Report 2025*[41]**

A global reference on drug markets, trends and policy developments, the World Drug Report 2025 offers a wealth of data and analysis and in 2025 comprises several elements tailored to different audiences. The web-based Drug patterns and trends contains the latest analysis of global, regional and subregional estimates of, and trends in, drug demand and supply in a user-friendly, interactive format supported by graphs, infographics and maps. Key findings provides an overview of selected findings from the analysis presented in Drug market patterns and trends and the thematic chapters of Contemporary issues on drugs, while Special points of interest offers a framework for the main takeaways and policy implications that can be drawn from those findings.

***The Nexus Between Cybercrime and Corruption*[42]**

This paper provides a comprehensive analysis of the deepening nexus between corruption and cybercrime. It examines how these two phenomena are mutually reinforcing threats to governance and institutions, causing significant harm to victim governments, companies and individuals.

Emerging threats: *The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*[43]

[40] International Monetary Fund - *On Cross-Border Crypto Flows: Measurement Drivers and Policy Implications*: https://www.imf.org/en/Publications/WP/Issues/2024/12/20/On-Cross-Border-Crypto-Flows-Measurement-Drivers-and-Policy-Implications-559166

[41] United Nations Office on Drugs and Crime - *World Drug Report 2025*: https://www.unodc.org/unodc/data-and-analysis/world-drug-report-2025.html

[42] United Nations Office on Drugs and Crime - *The Nexus Between Cybercrime and Corruption*: https://www.unodc.org/roseap/uploads/documents/Publications/2025/2025.10.21_The_Nexus_Between_Cybercrime_and_Corruption.pdf

[43] United Nations Office on Drugs and Crime - *Emerging threats: The intersection of criminal and technological innovation in the use of automation and artificial intelligence in the cybercrime landscape of Southeast Asia*: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Report_Emerging_threats_-_The_intersection_of_criminal_and_technological_innovation_in_the_use_of_automation_and_AI.pdf

This brief introduces the evolving concept of crime automation, with a particular focus on the integration of AI into cybercrime methodologies. It explores how automation, both traditional and AI-powered, is being exploited to conduct, scale, and conceal criminal activity, particularly in the Southeast Asian context.

Application of counter-trafficking legislation to address trafficking in persons into criminal activities: A comparative case analysis of select ASEAN countries[44]

This case law analysis considers a selection of 15 criminal cases from the ASEAN region that have been mounted in response to this form of trafficking in persons, to better understand the challenges that criminal justice practitioners have faced in leveraging trafficking in persons legislation to address it. The analysis is offered from the perspective of international criminal law, specifically, the United Nations Convention against Transnational Organized Crime (UNTOC) and its supplementary Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children (Trafficking in Persons Protocol).

Southeast Asia and the Pacific Organized Crime Threat Alert: *Strategic infiltration of vulnerable jurisdictions through criminal foreign direct investments: the case of Timor-Leste*[45]

This brief is part of a series of reports analysing and assessing the latest developments in organized crime and their impact on Southeast Asia and the Pacific. The series is released as new information emerges or when key events in the region warrant timely assessment. This report focuses on providing insight into emerging issues rather than offering a comprehensive overview.

Minerals Crime 2025 - Crimes in the supply chains of critical energy transition minerals[46]

This report examines the criminal exploitation of the global pharmaceutical supply chain, with a particular focus on contaminated medicines and the role of pharmaceutical excipients. It highlights how weak regulatory oversight, fraudulent documentation, and complex supply chains are manipulated by criminal networks. Through country case studies, the report assesses vulnerabilities in excipient sourcing and distribution, and offers actionable recommendations to strengthen supply chain integrity, regulatory cooperation, and criminal justice responses. It underscores the urgent need for enhanced international collaboration to protect public health and uphold the integrity of global medicines.

The Global Analysis on Crimes that Affect the Environment: Part 2b – Minerals Crime: Illegal Gold Mining[47]

This study is an overview of evidence of how these criminal actors are structured and how they perpetrate these crimes. Sections of the study summarize the evidence of how illegally mined gold makes its way from extraction to refining to manufacturing to sale, including the role of fraud and corruption.

Global Analysis on Crimes against the Environment - Forest Crime[48]

This study is an overview of how criminal actors are structured, documenting involvement of organized criminal groups (traditional organized crime groups, politically motivated crime groups, criminal networks) compromised corporations (ranging from unintentional to intentional perpetration), corrupt officials, and individuals.

[44] United Nations Office on Drugs and Crime - *Application of counter-trafficking legislation to address trafficking in persons into criminal activities: A comparative case analysis of select ASEAN countries*: https://www.unodc.org/roseap/uploads/documents/Publications/2025/Application_of_counter-trafficking_legislation_TIP_FINAL.pdf

[45] United Nations Office on Drugs and Crime - *Strategic infiltration of vulnerable jurisdictions through criminal foreign direct investments: the case of Timor-Leste*: https://www.unodc.org/roseap/uploads/documents/Publications/2025/UNODC_Alert_Strategic_infiltration_of_vulnerable_jurisdictions_through_criminal_foreign_direct_investments.pdf

[46] United Nations Office on Drugs and Crime - *Minerals Crime 2025 - Crimes in the supply chains of critical energy transition minerals*: https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/Minerals_Crime/Critical_minerals_2025.pdf

[47] United Nations Office on Drugs and Crime - *The Global Analysis on Crimes that Affect the Environment: Part 2b – Minerals Crime: Illegal Gold Mining*: https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/ECR25_P2b_Minerals_Crime.pdf

[48] United Nations Office on Drugs and Crime - *Global Analysis on Crimes against the Environment - Forest Crime*: https://www.unodc.org/documents/data-and-analysis/Crimes%20on%20Environment/ECR25_P2a_Deforestation.pdf

***International Classification of Crime for Statistical Purposes (ICCS): Implementation Manual*[49]**

In 2015, the United Nations Statistical Commission (UNSC) and the United Nations Commission on Crime Prevention and Criminal Justice endorsed the International Classification of Crime for Statistical Purposes (ICCS) in line with plans approved by the UNSC in its decision 44/110 and by the Economic and Social Council in its resolution 2013/37. ICCS is the international standard for defining and classifying criminal offences to produce and disseminate statistical data on crime and criminal justice. The manual offers concrete steps to promote uptake of ICCS, determine the scope of implementation, build a correspondence table and produce data according to ICCS.

***Global Report on Trafficking in Persons 2024*[50]**

This report is a call to be alert and to act for the people being trafficked and exploited in today's volatile context. After a marked decrease in the detection of victims during the COVID-19 pandemic, the number of victims detected globally in 2022 increased sharply again and even surpassed pre-pandemic levels, rising by 25% compared to 2019. This may partly be a reflection of improved detection capacity, but it is likely also a reflection of the fragility seen in every corner of the globe.

[49] United Nations Office on Drugs and Crime - *International Classification of Crime for Statistical Purposes (ICCS): Implementation Manual*: https://unstats.un.org/unsd/classifications/Meetings/UNCEISC2024/Session4_ICCS_Manual_Draft.pdf

[50] United Nations Office on Drugs and Crime - *Global Report on Trafficking in Persons 2024*: https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

6 - ABBREVIATIONS, ACRONYMS AND CURRENCY EXCHANGE RATES

AFP	Australian Federal Police
AML	Anti-money laundering
AMLC	Anti-Money Laundering Council
APG	Asia/Pacific Group on Money Laundering
ATM	Automatic teller machine
BDT	Bangladeshi Taka
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
FATF	Financial Action Task Force
FI	Financial institution
FIU	Financial intelligence unit
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, China Dollar
IDR	Indonesian Rupiah
IFTI	International funds transaction instruction
INTERPOL	International Criminal Police Organisation
JPY	Japanese Yen
KRW	South Korean Won
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
MONEYVAL	Committee of Experts on the Evaluation of AML Measures and the Financing of Terrorism
MOP	Macao, China Pataka
MVTS	Money or value transfer services
NGO	non-government organisation
NPO	Non-profit organisation
NRA	National risk assessment
NZD	New Zealand Dollar
PEP	Politically exposed person
PF	Proliferation financing
PHP	Philippine Peso
PKR	Pakistan Rupee
PPATK	Indonesian Financial Transaction Reports and Analysis Centre
PPP	Public private partnerships
RMB	Chinese Renminbi
RM	Malaysian Ringgit
SEC	Securities and Exchange Commission (Philippines)
SGD	Singapore Dollar
STR	Suspicious transactions report
STRO	Suspicious Transaction Reporting Office, Singapore's Financial Intelligence Unit
SVF	Stored value facilities
TF	Terrorism financing
UNODC	United Nations Office on Drugs and Crime
USD	United States Dollar
VND	Vietnamese Dong
WST	Samoan Tala

Exchange rates

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 currency conversions were completed using exchange rates provided by XE at various points in time between April and October 2025. Therefore, these values are ***indicative only***.

7 - INDEX

References to numbers against indexed terms relate to **case study numbers** across this report.

Predicate offences:

Organised criminal syndicate

18, 19, 20, 23, 41, 53, 70, 74, 81, 82, 93, 95, 96, 98, 106, 112

Terrorism, including terrorist financing

87, 88

Proliferation financing

90, 91

Sexual exploitation, including sexual exploitation of children

64

Drug related crime

26, 46, 65, 66, 67, 68, 70, 73, 103, 109, 111, 113

Illicit trafficking in stolen and other goods

nil

Robbery, theft

84, 102

Corruption and bribery

47, 52, 78, 79, 104, 108, 112

Fraud including, but not limited to:

- Cyberscam hubs
- Phone/SMS/email fraud/social media
- Identity fraud or romance scams,
- Forgery, and
- Business email compromise

1, 2, 3, 4, 5, 6, 7, 8, 9, 11, 12, 13, 19, 20, 21, 22, 27, 28, 29, 30, 31, 32, 33, 35, 36, 37, 39, 40, 41, 42, 43, 44, 49, 50, 58, 59, 60, 61, 62, 63, 68, 69, 71, 72, 76, 77, 79, 80, 81, 82, 83, 84, 85, 86, 87, 92, 94, 95, 98, 99, 100, 101, 102, 107, 108, 110

Illicit gambling/gaming

1, 7, 9, 14, 17, 37, 38, 48, 74, 80, 96, 97, 105,

Counterfeiting (inc. currency) and piracy of products

44

Ransom

12

Smuggling (including currency smuggling and in relation to customs and excise duties and taxes)

9, 10, 24, 25, 30, 55, 113

Tax crimes (direct taxes and indirect taxes)

52, 55, 75,

Insider trading and market manipulation

85, 86

Foreign predicate offence

11, 19, 23, 30, 31, 46, 51, 69, 87, 94, 95, 96, 97, 112

Human trafficking

1, 2, 3, 4, 5, 6, 7, 12, 49, 50, 53, 54, 57, 106

Types of money laundering:

Self-laundering

25, 27, 28, 68, 72, 73, 75, 81, 95, 108

Third-party laundering

11, 13, 14, 15, 16, 17, 18, 19, 21, 22, 30, 31, 40, 41, 42, 43, 51, 58, 59, 60, 61, 62, 63, 68, 69, 70, 71, 74, 80, 83, 87, 93, 94, 96, 97, 98, 111, 114

Trade-based money laundering

23, 68, 72, 111

Structuring/smurfing/refining/mingling

31, 68, 69, 79, 81, 93

Channels:

Financial institutions

2, 6, 7, 9, 10, 11, 13, 16, 17, 18, 22, 23, 24, 26, 27, 28, 30, 31, 34, 35, 38, 40, 41, 42, 43, 44, 45, 47, 56, 57, 58, 59, 61, 62, 65, 66, 67, 68, 69, 70, 71, 74, 75, 76, 78, 79, 83, 84, 90, 91, 93, 94, 95, 96, 97, 98, 99, 100, 101, 107, 110, 111, 112

Casinos, gambling houses

nil

Dealers in precious metals and/or stones

23, 98

Underground banking/alternative remittance services/hawala

9, 34, 52, 55, 91

Currency exchange/cash conversion

7, 10, 39, 85

Money value transfer services

9, 19, 34, 52, 53, 61, 64, 67, 69, 96, 100

Use of capital markets

29, 85

Virtual asset service providers

6, 10, 12, 13, 17, 18, 32, 34, 71, 76, 81, 87, 114

Payment methods:

Cash

1, 5, 7, 11, 13, 17, 18, 19, 27, 40, 41, 42, 43, 47, 52, 54, 55, 56, 57, 66, 68, 72, 74, 77, 78, 79, 80, 81, 82, 86, 88, 98, 103, 105, 107, 111, 114

Wire transfer

41, 43, 61, 64, 68, 93, 98, 104, 105

Use of virtual assets (cryptocurrencies or other virtual assets

6, 10, 12, 13, 17, 18, 32, 34, 71, 76, 81, 87, 114

Use of credit/debit cards, cheques, promissory notes etc.

7, 21, 22, 33, 40, 42, 53, 54, 59, 66, 79, 84, 98

Trade in precious metals and stones

23, 27, 80

New payment method

80, 91

Context:

International cooperation

19, 20, 23, 40, 43, 47, 52, 68, 94, 95, 96, 97, 107, 110, 111, 112, 113

Transnational crime

6, 7, 8, 23, 30, 31, 32, 33, 68, 71, 83, 85, 96, 107, 113

Politically exposed persons (PEPs)

47

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

64, 71, 113

Purchase of real estate

7, 38, 48, 81, 82, 86, 92, 93, 111

Use of non-profit organisations (NPOs)

87

Use of legal persons and arrangements (including international business companies, offshore companies or trusts

8, 30, 31, 36, 37, 39, 40, 45, 51, 52, 69, 80, 83, 87, 90, 94, 104, 105, 111, 112, 114

Trust and company service providers

30, 31, 38, 51, 82, 87

Suspicious transaction reporting

9, 10, 23, 26, 40, 42, 43, 54, 57, 68, 69, 70, 74, 93, 94, 95, 96, 97

Purchase of valuable / cultural assets (art works, antiquities, racehorses, vehicles, etc.

38