Asia/Pacific Group
ON MONEY LAUNDERING

APG Yearly Typologies Report 2024

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

November 2024

Asia/Pacific Group on Money Laundering

Table of contents

FOREWORD

Welcome to the APG Yearly Typologies Report 2024.

Each year, APG members, observer organisations, and a range of non-observer bodies work with the APG Secretariat to develop accessible and comprehensive insights into current and evolving money laundering, terrorism financing and proliferation financing (ML/TF/PF) typologies in the Asia/Pacific region, and the broader international trends.

These threats, like the crime with which they are intertwined, increasingly involve complex transnational financial crime, that often take most practical shape locally. The *FATF Recommendations* are critical to mitigating these threats across the globe, and the APG plays a crucial role in supporting its members to implement them across the Asia/Pacific region.

The work of the APG Operations Committee (OC), particularly the OC Co-Chairs, is key to the APG's typologies program. Critical to its success is the excellent leadership of outgoing Co-Chair Secretary Pandey from India (replaced by incoming Co-Chair Swain), and the consistent and longstanding leadership of Governor Atalina from Samoa.

This report, complemented by the annual APG Typologies Workshop and the ongoing work of the OC, highlights the commitment of our members to identifying and tackling evolving typologies, most particularly the misuse of legal persons and the role of professional facilitators. It notes that these threats arise in the context of the success of existing AML/CTF/CPF reforms that have significantly tightened the exploitation of more anonymous bank accounts and shell banks vulnerabilities.

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. It also underscores the need for it continue and the typologies work to be closely aligned with broader APG activity.

I would like to sincerely thank the APG members and our observer organisations for their valuable contributions to this report. I would also like to thank the non-observer organisations for their contributions, and the talented and 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: 2023 APG Typologies Workshop, held in New Delhi, India.

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. A currency conversion chart has been provided at Section 7 for reference.

The APG Operations Committee has oversight of the typologies research programme and is co-chaired by Governor Maiava Atalina Ainuu-Enari of the Central Bank of Samoa and Mr Smarak Swain of the Ministry of Finance, India.

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

1 - MISUSE OF LEGAL PERSONS

1.1 Overview

People use legal persons for a range of legitimate commercial activities, and they play an essential role in a jurisdiction's economy. In most jurisdictions, people can quickly and easily form legal persons, with independent legal personality, which in turn have ready access to the global financial system through the financial products that reporting entities provide them, including company bank accounts, corporate cards, loans, etc.

Legal Persons

Legal persons refers to any entities other than natural persons that can establish a permanent customer relationship with a financial institution or otherwise own property. This can include companies, bodies corporate, foundations, anstalt, partnerships, or associations and other relevantly similar entities.

As jurisdictions implement AML/CTF/CPF reforms, anonymous personal bank accounts and shell banks (banks that do not have any physical presence in any jurisdiction) are no longer widely available. Therefore, legal persons, including shell companies have emerged as primary vehicles misused by criminals for ML/TF/PF purposes.[2]

Two key vulnerabilities associated with legal persons are the ease with which people can create them and the ability to obscure their control and ownership. Complex and/or opaque structures involving legal persons make it increasingly difficult for competent authorities to obtain accurate beneficial ownership information which frustrates the process of identifying culpability for criminal actions and tracing financial flows and assets. This is exacerbated when the beneficial owners, and/or the professional enablers, such as trust and company service providers (TCSPs), who can facilitate the misuse of legal persons, reside in another jurisdiction.[3]

Stronger standards by FATF

In March 2022, the FATF strengthened Recommendation 24 (R.24) and its Interpretive Note of the *FATF Recommendations* regarding the transparency and beneficial ownership of legal persons. The FATF has also published updated guidance on the beneficial ownership of legal persons, to assist jurisdictions implement the strengthened R.24 requirements.[4]

R.24 now requires jurisdictions to assess and address the risks posed by legal persons, not only by those created in their jurisdictions, but also those created by foreign persons which have sufficient links with their jurisdiction. Significantly, R.24 explicitly requires jurisdictions to take a multi-pronged approach, i.e. to use a combination of different mechanisms to collect beneficial ownership information and to ensure it is available to competent authorities in a timely manner.[5]

There are many reasons why criminals may misuse a legal person, or a network of legal persons, including:

- Distancing themselves from the criminal activity.
- Hiding the true ownership of assets, including those owned by politically exposed persons (PEPs).
- Providing an apparent legitimate, commercial justification for movements of large amounts of funds.
- Comingling the proceeds of crime with legitimately sourced funds.
- Spending or investing the proceeds of crime.
- Enabling corruption, fraud, and tax evasion.
- Transferring bribe payments or embezzled public funds.

[2] World Bank Group - *National Money Laundering and Terrorist Financing Risk Assessment Toolkit:* https://star.worldbank.org/sites/default/files/2023-03/Legal%20Persons%20and%20Arragements%20ML%20Risk%20Assessment%20Tool.pdf
[3] The Association of Banks in Singapore and the Monetary Authority of Singapore AML/CFT Industry Partnership - *Legal Persons - Misuse Typologies and Best Practices*: https://abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf
[4] FATF - Beneficial Ownership: https://www.fatf-gafi.org/en/topics/beneficial-ownership.html
[5] FATF - *The FATF Recommendations*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html

- Providing asset protection for assets acquired using the proceeds of crime.

This year, the APG Secretariat asked APG members to provide information on their experience with misuse of legal persons. Members provided extensive responses and therefore, we structured this chapter to focus upon the intersection between misuse of legal persons and money laundering, and to highlight APG observer organisations and additional government/non-government organisations efforts in this area. Members also provided 138 case studies describing the latest ML/TF/PF methods and trends, including case studies illustrating the misuse of legal persons. Members responses regarding the misuse of legal persons and terrorist financing is captured separately in Chapters 2 and 3, and the misuse of legal persons and proliferation financing, and evasion of targeted financial sanctions, is captured in Chapter 4.

1.2 Members' understanding of the ML/TF risks posed by the misuse of legal persons

Assessing the ML/TF risks, including those associated with the different types of legal persons is a fundamental FATF requirement for jurisdictions to safeguard the integrity of both their, and the global financial system. Jurisdictions can only effectively mitigate and manage their ML/TF risks, when they have adequately identified them initially. In conducting thorough initial and ongoing risk assessments, jurisdictions' competent authorities are required to identify vulnerabilities and implement effective countermeasures. This assists jurisdictions to understand how criminals can misuse legal persons for ML/TF purposes in their jurisdiction/region, which enables them to develop targeted regulation and oversight mechanisms that can effectively mitigate and manage those risks.

The *FATF Recommendations* require jurisdictions to assess the ML/TF/PF risks under Recommendation 1, and ML/TF risks associated with legal persons under Recommendations 24. Recommendation 24 requires jurisdictions to assess the ML/TF risks of domestic legal structures that can be created or administered in the jurisdiction as well as foreign legal structures that have sufficient links to the jurisdiction. Of APG's 42 members, 38 (90%) have been subject to mutual evaluations under the updated 2012 *FATF Methodology*.[6] We set out the findings of these mutual evaluation reports below, noting some of these were published several years ago and jurisdictions have taken significant steps since then.

With regard to members' understanding the ML/TF risk associated with legal persons:

- Six members (14%) had assessed the ML/TF risk associated with legal persons at the time of their mutual evaluation.[7]
- 20 members (48%) had assessed the ML/TF risk associated with legal persons at the time of their mutual evaluation. However, the assessment teams deem their assessments deficient in a number of ways. They were either at a too basic/general level, not comprehensive, did not cover *all types* of legal persons, did not assess both domestic and/or international legal persons, or did not assess the ML and/or TF risks.[8]
- Six members (14%) had not assessed the ML/TF risk associated with legal persons at the time of their mutual evaluation. However, they have assessed the risk since.[9]
- Six members (14%) had not assessed the ML/TF risk associated with legal persons at the time of their mutual evaluation.[10]

While members have progressed their understanding of ML/TF risks generally, the data identifies that many are still grappling with understanding the ML/TF risks associated with legal persons.

[6] The Maldives and Niue are currently going through their mutual evaluations, and only Afghanistan and Tuvalu have not been assessed.
[7] Canada, India, Indonesia, Korea, New Zealand and United States.
[8] Bangladesh, Chinese Taipei, Cook Islands, Hong Kong, China, Japan, Macao, China, Malaysia, Marshall Islands, Mongolia, Myanmar, Nauru, Pakistan, Palau, Samoa, Solomon Islands, Timor-Leste, Thailand, Tonga, Vanuatu and Vietnam.
[9] Australia, Bhutan, Brunei Darussalam, Philippines, Singapore and Sri Lanka.
[10] Cambodia, China, Fiji, Lao PDR, Nepal and Papua New Guinea.

Some members have updated their understanding of ML/TF (and PF) risks through conducting new national risk assessments (NRA), and/or threat or sector-based risk assessments. Some examples of such initiatives are set out below.[11] Notably, one member assessed the misuse of legal persons and arrangements in its offshore financial sector as its primary ML/TF threat[12].

Australia

Australia, in its *Money Laundering in Australia National Risk Assessment*[13] assessed legal persons and legal arrangements as posing a **high and stable money laundering vulnerability**. Key judgments include:

- Legal persons (and legal arrangements) and associated banking arrangements are persistently exploited by criminals to store and move large volumes of criminal proceeds, including offshore.
- Legal persons (and legal arrangements) can be established with relative ease and can help mask beneficial ownership.
- Australia does not have comprehensive mechanisms for the systematic collection, verification and release of beneficial ownership information. This restricts government agencies' ability to detect and investigate money laundering through legal structures. Restraining and confiscating criminal assets held by companies or trusts can also be challenging and resource intensive.
- Offshore legal persons (and legal arrangements) can help further obscure financial flows and beneficial ownership, particularly when legal structures are established in secrecy jurisdictions or across multiple jurisdictions.
- Professional service providers play a key role in establishing and managing complex legal persons and legal arrangements used to conceal wealth and launder funds.

[11] In addition, members advised; Lao PDR is conducting an ML/TF risk assessment of all legal persons, due for publication late 2024; Malysia is finalising its fifth iteration of its NRA; Maldives recently rated legal persons as medium lave for ML/TF in its NRA; Singapore is currently updating its ML/TF risk assessment of legal persons which have remained at priority level risk; Vietnam has undertaken its NRA for ML/TF which includes assessment of legal persons.

[12] Asia/Pacific Group on Money Laundering - *Cook Islands Mutual Evaluation Report:* https://apgml.org/members-and-observers/members/member-documents.aspx?m=5c63cd37-73a2-4a45-aac3-f6e5b8ec0594

[13] AUSTRAC - *Money Laundering in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

Notably, Australia highlighted the **persistent involvement of professional service providers** to help establish complex business structures and associated banking arrangements to help individuals launder funds and conceal wealth.[14]

Canada

Canada recently published its Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada[15] which includes ML/TF risk assessment for corporations, partnerships, and non-profit organisations (NPO).

- Canada assessed the **ML/TF vulnerability of corporations and partnerships as very high and high** respectively.

China

China recently conducted an ML/TF risk assessment of all legal persons, including all types of domestic legal persons, and foreign legal persons carrying out businesses in China.

- Major typologies involve obtaining and laundering illegal proceeds through **concealing the identity** of money launderers via legal entities, or **through fictitious transactions using shell companies** or front companies.

Indonesia

Indonesia completed its *Sectoral Risk Assessment of Money Laundering and Terrorist Financing on Legal Person 2022*. The assessment reviewed data from 2019 to 2022 and is an example of how targeted sectoral and/or threat assessments can keep a jurisdiction's understanding of ML/TF risk up to date. Key findings include:

- Based on the type of predicate crime, corruption and narcotics are predicate crimes with a high risk of money laundering in legal persons.
- Based on the type of legal person, Limited Liability Companies-domestic ownership and funding are considered to have a high risk of money laundering.
- Based on the type of business sector, it is known that construction, trade, investment and finance, mining and distribution have a high risk of money laundering in legal persons.
- Based on the reporting party's sector, banks are considered to be at high risk of being used as a channel for money laundering in legal persons.
- Based on transaction delivery channels, cash deposits, transfers in and out of the country are considered as high risk for money laundering in legal persons.
- The emerging trend on money laundering in legal persons is exploitation vulnerability of appostille[16] documents used for investment purposes from the state who have not complied with the apostille convention and the use of virtual corporations or virtual office.

[14] As publicly identified on its website, the multi-agency Serious Financial Crime Taskforce that the ATO leads has one of its focuses on 'professional enablers': https://www.ato.gov.au/about-ato/tax-avoidance/the-fight-against-tax-crime/our-focus/serious-financial-crime-taskforce/how-the-taskforce-operates

[15] Government of Canada - *Updated Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*: https://www.canada.ca/en/department-finance/programs/financial-sector-policy/updated-assessment-inherent-risks-money-laundering-terrorist-financing-canada.html

[16] A form of authentication that seeks to simplify the process of legalising and authenticating public documents so that they can be recognised internationally.

Macao, China

Macao, China recently completed the *Macao Special Administrative Region Risk Assessment Report on Money Laundering/Terrorist Financing/Financing of Proliferation of Weapons of Mass Destruction (2022)*. Macao, China noted the Financial Intelligence Office of Macao, China (GIF) was closely monitoring probable misuse of legal persons or TCSP services.

Further, in 2023 GIF's Financial Information Analysis Team conducted **special strategic review and identified suspicious shell companies**. The team prepared summarised results of specific cases and referred them to the supervisor - the Legal Affairs Bureau. GIF is currently conducting another thematic strategic analysis with suspicious transaction report (STR) information to identify probable TCSP services which may have relation to shell companies. GIF has been periodically sharing strategic analyses results with reporting entities through its **public/private partnership** to enhance their prevention and mitigation measures.

Emerging trends, declining trends, and/or continuing trends related to the misuse of legal persons

Regarding trends related to the misuse of legal persons, members uniformly identified that legal persons were used in the commission of fraud offences, including email and telephone scams, investment frauds, and business email compromise, and in tax evasion offences.[17]

Other observed predicate offences included theft, misappropriation, embezzlement, bribery and corruption, securities and market manipulation, smuggling, drug trafficking, and distribution of obscene material.[18] General observations were made about the use of legal persons to undertake ML, in particular Trade based money-laundering.[19]

Some members noted a transnational component in the observed trends. The Cook Islands received nine international requests for information concerning legal persons registered in their jurisdiction in 2023. Japan commented on the connections with foreign jurisdictions in fraud cases. Chinese Taipei observed that foreign legal persons establish subsidiaries within their jurisdiction for the purpose of stealing trade secrets, whilst Chinese Taipei nationals also established companies in overseas tax havens and offshore financial centres, or controlled these through management/consulting companies, to commit crimes.

Members generally identified the forms of misuse as the use of shell companies, the use of stooge directors (nominees), and use of business accounts to move and co-mingle funds or to set up loan arrangements. Indonesia observed the use of fictitious entities, legal persons having unclear legality, such as not having a business license or institutional permit (or both), and the use of nominees/front men/straw men such as registered close associates and family members in legal persons to hide the identity of the true beneficial owner.

Japan also noted that sometimes the legal person has no status or its status was unclear. Red flag indicators regarding misuse of legal persons included companies established with a very small amount of initial capital (tens of thousands to hundreds of thousands of yen), and companies that frequently change locations or officers and companies with suspicious operations, such as those that conduct business, that are not closely related to each other. Japan and Indonesia noted that misused legal persons often have other regulatory problems, for example, they do not hold the appropriate business licences, and in Japan - violations of the laws regulating the receipt of contributions, the receipt of deposits, violations of the *Interest Rates/Money Lending Business Act*.

Legal persons - risk assessment methodologies

Several technical assistance providers have focused on the gaps in jurisdictions' risk assessments with respect to legal persons. The following are key insights from the World Bank Group and the EU Global Facility on methodologies of risk assessment and challenges in applying these in jurisdictional contexts.

[17] Cook Islands, Hong Kong China, Japan, Singapore. Chinese Taipei, Vietnam.
[18] Cook Islands, Hong Kong China, Japan, Maldives, Singapore, Chinese Taipei.
[19] Maldives.

World Bank Group - *National Money Laundering and Terrorist Financing Risk Assessment Toolkit* *(2022)*

In 2022, the Financial Market Stability and Integrity (FSI) unit of the World Bank Group (WBG) and the Stolen Asset Recovery Initiative (StAR), a partnership between the WBG and the United Nations Office on Drugs and Crime (UNODC) developed *the National Money Laundering and Terrorist Financing Risk Assessment Toolkit*[20] (NRA Toolkit).

Understanding and mitigating the ML/TF risks associated with the misuse of legal persons requires a structured framework for self-assessment, This enables jurisdictions to identify threats and vulnerabilities and develop targeted mitigation strategies. The NRA Toolkit contains guidance manuals, Excel worksheets; PowerPoint presentations; and other supporting materials.

In the self-assessment process, the WBG's tool places great emphasis on the *international nature of the misuse of legal persons, since criminal networks exploit legal loopholes across multiple jurisdictions* to conceal their illicit activities. Therefore, it's important for jurisdictions to understanding both "exported" risks (misuse of legal structures created within the jurisdiction by non-residents) and "imported" risks (misuse of foreign legal structures with links to the home jurisdiction).

The NRA toolkit explicitly requires jurisdictions to determine its attractiveness for non-resident incorporation of legal persons, which includes features related to a jurisdiction's general legal, institutional, economic, regulatory, and political frameworks that impact its attractiveness for the provision of company formation services (and related professional services) to non-resident individuals and non-resident legal persons.

Red flag indicators

The assessment should consider red flag indicators that assist in identifying potential gaps in a jurisdiction's legal and regulatory frameworks, that criminals could exploit for ML/TF purposes. These include:

- Ease of formation and registration: Lax registration requirements, low costs, and fast processing times for legal structures may be more attractive to criminals.
- Beneficial ownership transparency: Weak or non-existent beneficial ownership disclosure requirements, limited access to beneficial ownership information, and ineffective verification mechanisms create opportunities for concealing true ownership and control.
- Nominee arrangements: The use of nominee directors and shareholders, without proper controls and transparency, can facilitate the concealment of beneficial ownership.
- Opaque structures: Jurisdictions that allow for or fail to effectively regulate opaque structures like bearer shares, trusts, and foundations, increase the ML/TF risk.
- International cooperation: Weak international cooperation mechanisms, including information exchange and mutual legal assistance, hinder effective investigations and prosecutions of cross-border financial crimes.
- Regulation and supervision of TCSPs: Insufficient regulation and supervision of TCSPs can lead to their involvement in facilitating illicit activities.

By considering these red flag indicators, jurisdictions can identify specific vulnerabilities in their AML/CFT system and develop targeted mitigation and management measures. This includes strengthening legal frameworks, improving data collection and sharing, enhancing regulatory oversight, and fostering international cooperation.

EU Global Facility - Challenges and FSRB support

The EU Global Facility has observed, in the context of its technical support to partner countries on the implementation of the EU Global Facility Methodology for Assessing risk of LP/LA, that countries usually share the following challenges:

[20] World Bank Group - *Legal Persons and Arrangements Money Laundering Risk Assessment Tool*: https://star.worldbank.org/publications/legal-persons-and-arrangements-money-laundering-risk-assessment-tool

- **Comprehensiveness of the assessment and appropriateness of the risk assessment methodology**

  FATF guidance on the beneficial ownership of legal persons recommended jurisdictions: collect registration statistics; analyse STRs and enforcement/prosecutorial cases; identify most common typologies; investigate TCSP practices; conduct expert consultations and perform other important steps to better understand risks associated with each type of legal persons. In addition, the FATF revised its Recommendations 24 and 25 to also cover foreign legal structures that present ML/FT risk and have sufficient links to the country. To effectively perform this analysis, jurisdictions need to develop a methodology/use an existing methodology that will clearly explain the approach, the method, and the different risk assessment criteria used to assess the threat, vulnerabilities and mitigation measures for different types of domestic and foreign legal persons. Crucially, this methodology must be tailored to the jurisdictions' risk and context, and include all mandatory FATF requirements.

- **Availability of an accurate risk assessment tool**

  Jurisdictions need to use a risk assessment tool, that not only accurately takes into account the comprehensiveness of the jurisdiction's risk assessment methodology, but accurately follows that methodology.

- **Flexibility and adaptability of the risk assessment methodology to the jurisdiction's risk profile and existing preventive measures and tools**

  Jurisdictions have different risk profiles and use different mitigation measures. Therefore, it is challenging to design a one-size-fits-all risk assessment methodology that can be used by multiple jurisdictions. There are a number of different methodologies and tools available. Therefore, it's important for jurisdictions to confirm whether the methodologies and tools are flexible and allow for customisation.

- **Practical knowledge, experience, and coordination**

  International best practice includes jurisdictions establishing a Risk Assessment Working Group comprising representatives from relevant competent authorities. This may involve representatives from the FIU, law enforcement agencies (LEAs), company and beneficial ownership registrars, tax office, anticorruption office, customs office, AML/CFT supervisors of TCSPs, financial and other non-financial sectors, etc. All members of the working group should be trained to understand the methodology, and one party should be responsible for its coordination.

- **Further FSRB guidance and support**

  Currently, jurisdictions face challenges such as a lack knowledge and experience in conducting the legal persons risk assessment. Therefore, there is an opportunity for FSRBs to provide their members additional guidance and support, such as assisting jurisdictions in developing a risk assessment methodology and tools, and share this among their members. For example, in 2022 the EU Global Facility provided support to the Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) to develop a risk assessment tool for assessing ML/TF risks of legal persons (and legal arrangements), which incorporated the EU Global Facility's legal persons and legal arrangements risk assessment methodology. ESAAMLG adopted this toolkit and recommended its use to its members.

Beneficial ownership

"The purpose of concealing beneficial ownership is simple: to ensure that the true owner of an asset or revenue stream cannot be associated with it."

This observation was made in the APG and ATO co-authored paper in relation to Tax crimes and ML in the Asia-Pacific region.[21] In that context, concealment of beneficial ownership led to non-payment of taxable income and frustration of confiscation/forfeiture processes, but this observation is arguably also true for all predicates and stand-alone ML. Complex legal structures using companies and trusts, often spanning across multiple jurisdictions are a common feature in tax crimes and related ML schemes. For example, they are also used to obfuscate beneficial ownership of vessels and companies used in illegal fishing.[22]

In both of these contexts, surveys of APG members found that only half of surveyed members require the beneficial ownership of legal persons to be recorded in a central registry. Basic and beneficial ownership information for legal persons was either unavailable, incomplete or inaccessible, hampering investigations and effective information sharing.[23] Most information obtained about beneficial ownership was collected through information held by financial institutions. It was also observed that a belief exists amongst the private sector that failure to fulfil information requirements does not result in dissuasive penalties.

…a complex ownership structure shifts the cost from the beneficial owner (who will likely pay the exact same incorporation fee, regardless of whether the company has a simple or a complex structure), to a jurisdiction's competent authorities and/or reporting entities when determining the beneficial owner.

Beneficial ownership transparency of legal persons is a tool competent authorities can use to identify criminals who exploit these structures, and provide them with rapid information in the context of their analyses and investigations.[24] Accordingly, the misuse of legal persons can be significantly reduced if information regarding both the legal owner and the beneficial owner, the source of the legal person's assets, and its activities are available to competent authorities in a timely manner.[25]

Complex ownership structures

One of the main challenges to accurately identifying a legal person's beneficial owners is the use of complex ownership structures, where the beneficial owner may hide behind several layers of entities, offshore entities and/or use sophisticated control mechanisms. It is usually legal to create a structure as complex as the beneficial owner wishes. Jurisdictions tend not to put limits on the number of layers, the nationality of the entities involved in the ownership chain, or the residence of the beneficial owners. Similarly, jurisdictions tend not to explicitly prohibit circular ownership structures (where Company A is owned by Company B and vice-versa) even though such structures hinder identification of beneficial owners, and/or holding any natural person to account. Further, it may be impossible to distinguish between complex structures that attempt to conceal the beneficial owner from those complex structures that are the result of legitimate business activities (e.g. a multinational company that becomes complex through acquiring other companies).

Either way, a complex ownership structure shifts the cost from the beneficial owner (who will likely pay the exact same incorporation fee, regardless of whether the company has a simple or a complex structure), to a jurisdiction's competent authorities and/or reporting entities when determining the beneficial owner. I.e. they spend considerable time and resources to determine the legal and beneficial owners of each layer in the ownership chain.

[21] Asia/Pacific Group on Money Laundering and Australian Taxation Office - *Money Laundering Associated With Tax Crimes in the Asia Pacific*: https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=5206

[22] Asia/Pacific Group on Money Laundering - *APG Issues Paper: Illicit Financial Flows Generated from Illegal Fishing*: https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=6206#:~:text=The%20paper%20notes%20that%20illegal,to%20national%20and%20regional%20security.

[23] Ibid, and FATF - *Guidance on Beneficial Ownership for Legal Persons*: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf

[24] Asia/Pacific Group on Money Laundering and Australian Taxation Office - *Money Laundering Associated With Tax Crimes in the Asia Pacific*: https://apgml.org/methods-and-trends/news/details.aspx?pcPage=1&n=5206

[25] FATF - *Guidance on Beneficial Ownership for Legal Persons*: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Guidance-Beneficial-Ownership-Legal-Persons.pdf.coredownload.pdf

It is up to each jurisdiction or reporting entity to determine what they consider as 'complex'. This may depend on several factors, such as the legal person's sector, industry, number of employees or income. For example, it may be expected/normal for a multinational company to have a complex structure, while it may be suspicious for a PEP to create a similar structure just to hold real estate assets.

In discussions facilitated by the EU AML Global Facility,[26] experts identified the following **indicators and strategies that assist competent authorities and reporting entities identify complex structures**:

- Length of the ownership chain, both vertical and horizontal.
- Use of nominees.[27]
- Foreign entities, especially from higher-risk or blacklisted jurisdictions.
- Presence of legal arrangements (trusts)[28] and their combination with legal persons.[29]
- Ownership by investment funds or companies listed on the stock exchange, especially from foreign jurisdictions.
- Holdings slightly below the beneficial ownership transparency threshold, e.g., 24.98% of shares.
- Listing the senior manager rather than the beneficial owner in registration information.
- Lack of written documents naming the beneficial owner (e.g. oral communications between nominees and beneficial owners, the use of power of attorney so that the beneficial owner does not hold shares, even indirectly).
- Use of 'generic terms' in public documents. For example: 'John Smith means John Smith; or his family members; trusts, partnerships or LLCs for the benefit of John Smith or his family members, and their heirs, executors, estate, successors and legal representatives'.

Further, the experts proposed several **measures that jurisdictions could undertake to reduce the secrecy risks of complex ownership structures**. These include:

- Requiring legal persons to disclosure their full ownership chain (up to the beneficial owner, and those who are not).
- Analysing and statistically exploring domestic legal persons to determine 'a common/normal structure' (to enable competent authorities and reporting entities to easily detect outliers).
- Establishing public online access to open-data on beneficial ownership information, via interconnected registries.
- Applying enhanced due diligence, refusing the incorporation of legal persons or the opening of bank accounts if the legal persons' structure appears unreasonably complex or risky.
- Using new technologies, such as artificial intelligence and/or big data to relate databases (e.g. tax information, residence databases, etc.).
- Shifting the burden of proof onto legal persons (i.e. if challenged, the legal person has to prove that its structure is legitimate and declare information they provide is correct).
- Implementing whistle-blower programmes.

In its *Money Laundering in Australia National Risk Assessment*,[30] Australia noted that complex ownership structures can be established through one or more of the following lawful activities:

- The use of parent and subsidiary entities.
- The establishment of trust, trading and operational business accounts.
- The use of 'holding companies', joint ventures, partnerships, inter-party 'loans', service agreements and 'lines of credit'.

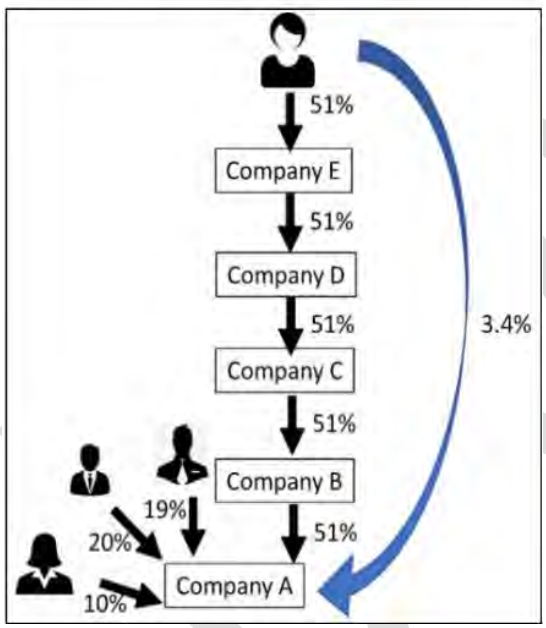
[26] EU Global Facility - *Beneficial Ownership And Complex Ownership Structures*: https://www.global-amlcft.eu/wp-content/uploads/2023/01/BO-Series-1-Webinar-pages-2022.pdf
[27] Informal nominees are more difficult to find, especially if they involve illegal payments or coercion rather than family relationships.
[28] Trusts need not register in many countries, so records of their existence or information about them may be unavailable).
[29] Although trusts usually require all parties to the trust to be identified without applying thresholds, adding a company as a party to the trust would de facto add thresholds (only those who pass the threshold would be identified as beneficial owners of the corporate party to the trust, and thus of the trust).
[30] AUSTRAC - *Money Laundering in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

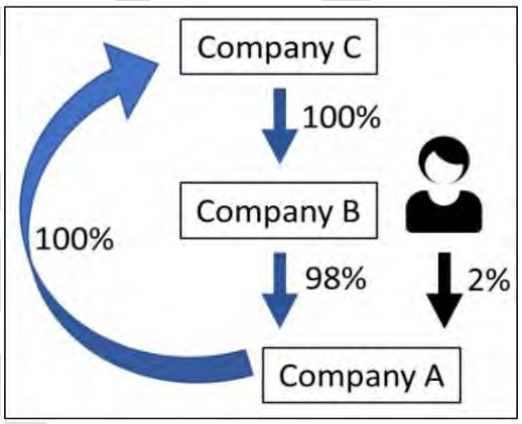
- The use of other structures or arrangements such as franchisor/franchisee structures, multi-level marketers, licensor/licensee arrangements and financial and legal instruments (e.g. powers of attorney, deeds and contracts).

Complex ownership structures can also be established using 'de facto' or 'shadow' directors. A de facto director is a person who operates in the capacity of a director but is not named on corporate regulator's records. They may have titles such as 'business development director', 'chairman' or 'principal'. A shadow director is a person who operates through a straw or dummy director. In Australia, it is illegal for legal persons to use de facto or shadow directors.

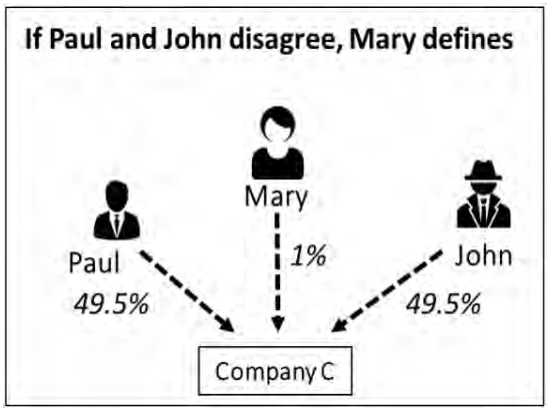
Tax Justice Network - *Complex Ownership Structures Addressing the Risks for Beneficial Ownership Transparency (2020)*

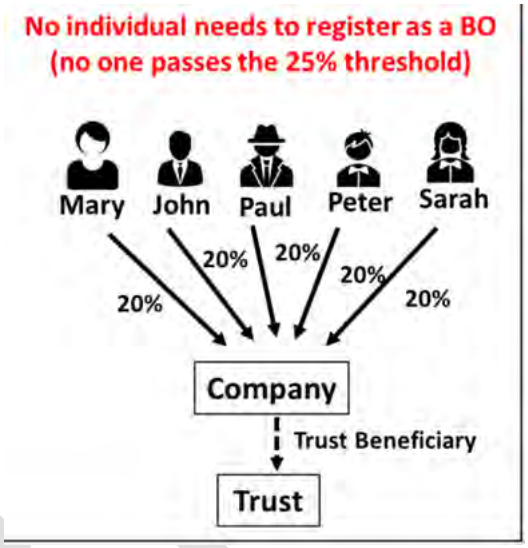
In 2020, the Tax Justice Network, together with City University London, the Independent Commission for the Reform of International Corporate Taxation, Transparency International, and the Financial Transparency Coalition hosted a roundtable event to discuss complex ownership chains, their risks for transparency and tax abuse, and the potential for regulation. 52 experts and researchers from academia, international organisations, civil society, jurisdiction authorities and the private sector attended the roundtable. The resulting brief - *Complex Ownership Structures Addressing the Risks for Beneficial Ownership Transparency*[31] contains relevant charts outlining common complex ownership structures, such as:





[31] Tax Justice Network - *Complex Ownership Structures: Addressing the Risks for Beneficial Ownership Transparency*: https://taxjustice.net/wp-content/uploads/2022/02/Complex-ownership-chains-Reduced-Andres-Knobel-MB-AK.pdf





Nominees

A nominee as a natural or legal person, holding a role in a legal person as an agent acting upon instructions of a nominator who has a more substantive claim to control and/or ownership of the legal person. Commonly, the nominator is the beneficial owner of the legal person. While many types of nominee arrangements have legitimate business purposes, people can use nominees as a deliberate device to evade beneficial ownership transparency initiatives, and thereby facilitate the misuse of legal persons for ML/TF purposes. The most common types of nominees are nominee directors and nominee shareholders.[32]

Case Study # 1: Money laundering investigation involving hawala

Fraud, including forgery; self-laundering; money value transfer services; use of legal persons and arrangements

In 2018, the Enforcement Directorate (ED) investigated a case under the *Foreign Exchange Management Act 1999* which identified that the mastermind of a criminal syndicate and his associates had established a web of shell companies in India and abroad (450 entities in India; 104 entities mostly in Dubai and Hong Kong, China; and 102 entities based on forged documents). The Economic Offences Wing of Delhi Police registered predicate offences relating to fraud, forgery, counterfeiting of documents and organised criminal conspiracy, based on a preliminary inquiry from the ED.

The syndicate's scheme involved recruiting dummy directors for shell companies. They also created fictitious persons using fabricated photographs and ID documents for the purpose of company incorporation, opening bank accounts and for fraudulent transactions.

Key accomplices managed offices, recruited employees and handled bank account transactions as per the mastermind's instructions. The syndicate used circular trading and provided accommodation entries to facilitate domestic operations. They also created fictitious turnovers from multiple accounts of shell companies.

The mastermind also created dummy travel companies to send money overseas to jurisdictions including Dubai, Hong Kong China and Singapore. These overseas entities then sent forged documents related to fictious foreign travellers to Indian authorised foreign exchange dealers to facilitate foreign exchange remittance.

Investigations included accessing the Ministry of Corporate Affairs portal, income tax returns, passport and travel details from the Bureau of Immigration, suspicious transaction report and cash transaction report information from the financial intelligence unit as well as bank account information from banks.

The investigation identified INR 5.65 billion (~ USD 67.29 million) generated from ML activity. The Adjudicating Authority confirmed an attachment order for INR 800 million (~ USD 9.5 million) and authorities filed charges against the mastermind. Authorities filed a prosecution complaint in 2020 and 2022. The

[32] FATF - *Guidance on Beneficial Ownership of Legal Persons* - https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html

hearing regarding the charges to be framed against sixteen suspects, including the hawala operator, as well as bail hearings took place in 2023 and are ongoing.

This case also led to a series of investigations into at least two other hawala operators and their associates who were using similar methods.

Source - India

Case Study # 2: Money laundering syndicate

Illicit gambling/gaming; self-laundering; use of legal persons and arrangements

On 10 November 2022, Chinese Taipei's FIU disseminated a financial intelligence report to the Criminal Investigation Bureau (CIB). In-depth analysis discovered 22 people involved in an online gambling syndicate, including Person A, who had successively opened multiple shell companies such as companies A, B and C, under the name of several figureheads. From May 2022, the syndicate used the shell companies as ML facilities.

When the syndicate recruited new employees, they first arranged them to hide them in a rented high-end residential building for centralised training and management. After the employees were familiar with the syndicate's online banking transfer process and could operate quickly, Person A asked the employees to hide in their own homes to wait for instructions via message, to launder the syndicate's funds, in an attempt to avoid detection by the police. To conceal the large amount of illegal gambling funds, the employees conducted a series of transactions through numerous dummy bank accounts. The syndicate's cadres regularly asked employees to report their status in a group chat, so to calculate each member's share of proceeds of crime accordingly.

After a long investigation including extensive evidence collection, the task force, conducted two waves of arrests and searches in February and June 2023. In the first wave, the task force arrested and brought to justice 13 people, in the second wave, the task force arrested nine people, including the Person A. Throughout the case, the task force seized mobile phones, laptops, computers, passbooks and other ML evidence. The proceeds of crime involved reached TWD 1.5 billion (~ USD 46.9 million), and the task force seized real estate owned by the syndicate valued at TWD 44.4 million (~ USD 1.4 million). In addition, during the search process, the task force discovered there was nearly TWD 30 million (~ USD 938,000) remaining in the dummy accounts used for ML, and the task force immediately reported it to the prosecutor and applied to the court for emergency seizure.

Source - Chinese Taipei

Trade-based money laundering

Trade based money-laundering (TBML) is broadly defined as disguising the proceeds of crime and moving value using trade transactions in an attempt to legitimise their illicit origins. In practice, TBML is frequently used in combination with other ML activities and criminal conduct.

TBML operates in the highly specialised global environment of customs, excise and revenue collection. The international trade system is subject to a range of vulnerabilities that criminals can exploit. Large volumes of global trade flows provide opportunities to obscure individual illicit transactions, particularly when combined with foreign exchange transactions or diverse trade-financing arrangements[33].

The World Customs Organisation identified the following two common methodologies associated with the misuse of legal persons and TBML:

- Use of straw directors (nominees) and related legal persons to conduct TBML.
- Entities that conduct tax fraud whilst laundering funds using bearer negotiable instruments before exporting the goods (the tax fraud was perpetrated on) overseas and mis-declaring the quantity.

Straw directors and TBML

Criminals set up two similar named legal persons in two jurisdictions. The legal person names often mimic names of well-known companies. One legal person acts as the main entity and the other acts as a pass-through account. The legal person's ownership is then transferred to other individuals who act as straw directors. However, the original directors continue to run the day-to-day operations and accounts. Goods are purchased

[33] AUSTRAC - *Money Laundering in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

using suspected proceeds of crime and exported overseas. These goods are then undervalued, thus transferring proceeds of crime offshore.

Carousal VAT fraud and TBML

Criminals covert money from an unknown source (likely proceeds of crime) into stored value cards and use these to purchase high-end electronics such as mobile phones, vacuums, computers and game consoles from retail outlets. They then raise invoices to 'sell' the goods to legal persons owned and controlled by criminals known to each other. No goods actually change hands but the criminals seek fraudulent refunds from the Taxation Authority for the non-existent 'payment' of goods and services tax. They then send the high-end electrical goods overseas with their value under-declared and quantity under-stated, allowing them an extra opportunity to launder/benefit through TBML.

Case studies

As illustrated by the following case studies members provided, criminals are increasing misusing legal persons in conjunction with TBML.

Case Study # 3: Diamond trade-based money laundering scheme

Trade based money laundering; dealers in precious metals and stones

Upon information exchange with Jurisdiction A, in early 2023 Hong Kong Customs uncovered a transnational TBML syndicate engaging in diamond trading for the purpose of laundering HKD 500 million (~ USD 64 million) between January to December 2021. The syndicate set up five companies to export low-value synthetic diamonds to Jurisdiction A in the guise of high-value, cut and polished natural diamonds for laundering purposes.

In a bid to move the illicit funds, the value of the synthetic diamonds was highly exaggerated in the trade declarations. Through inflating the declared value, the syndicate subsequently transferred their proceeds of crime from Jurisdiction A to Hong Kong, China as "legitimate payments" for the diamonds. The syndicate used the five companies' corporate bank accounts to handle the proceeds of crime and disbursed it to over 100 local companies for further dealings. Between December 2023 and February 2024, Hong Kong Customs neutralized the syndicate by arresting five persons for ML in Hong Kong, China and seized HKD 1 million (~ USD 0.13 million). The investigation is ongoing.

Source - Hong Kong, China

Case Study # 4: Trade-based money laundering

Trade-based money laundering; misuse of corporate vehicles; document forgery; tax offences; layering; structuring

Authorities identified four individuals with various law enforcement records, forming and misusing corporate vehicles as well as sole proprietorships, and conducting transactions indicating TBML activities. The individuals used banking services including internet banking and outward remittance services. The individuals submitted forged or invalid documents to the bank to conduct some of these outward remittances.

This case was initiated from STRs a bank submitted to the Maldives FIU. The reason for filing STRs was mostly related to customers conducting transactions inconsistent with their customer due diligence (CDD) and know your customer information. This case is currently under investigation by the law enforcement agencies.

Source - Maldives

Case Study # 5: Trade-based money laundering and dubious beneficial ownership

Trade-based money laundering

A number of STRs were filed against Company A, owned by Person C and Person D. Company A was involved in importing solar panels from jurisdiction B and sold them locally. The company opened five accounts with different banks and routed around PKR 2 billion (~ USD 7 million) through these accounts over three years. As per its trade invoices, the company imported solar panels valued at USD 20,150,

however, the customs authority assessed the value of the shipment at USD 91,233. This discrepancy suggested undervalued invoicing raising concerns about the authenticity of the transactions.

Pakistan's FIU, the Financial Monitoring Unit of Pakistan (FMU) identified Person E through its analysis, who had deposited PKR 50 million (~ USD 179,573) in cash and PKR 19 million (~ USD 68,238) through clearing transactions in one of the bank accounts maintained by Company A. Further analysis revealed that Person E was employed as salesman at Company B and had also deposited more than PKR 4.5 billion (~ USD 16 million) in cash in multiple accounts maintained by that company. The FMU identified that it had already disseminated financial intelligence about Company B to LEAs regarding under invoicing by Company A and TBML related to imports of solar panels. A First Information Report (FIR) was registered against the directors of Company B by one LEA following feedback from LEAs and an investigation is underway.

Additionally, Person F (identified as Person E's brother) acted as a signatory on one of the accounts held by Company B. The accounts maintained by Company A raised concerns that they might be used for benami[34] transactions (transacted in the name of another person) and also created doubts on the actual beneficial ownership of the company. However, an adverse media news surfaced, where a government audit department uncovered a large-scale over-invoicing and TBML in the solar panel import business where companies were exploiting tax rebate system on solar panel imports.

Tax records showed that Company A had paid minimal taxes during the same period when the suspicious account activity occurred. The FMU disseminated its financial intelligence to relevant LEAs for further investigation of the TBML element and to uncover the ultimate beneficiaries of the funds routed through the accounts of Company A.

Source - Pakistan

1.3 Professional enablers

In examining the misuse of legal persons, a consistent actor is the professional individual, organisation or network providing professional services that enable criminals to launder their proceeds of crime. Such entities have become known as "professional enablers".[35] Their behaviour is commonly deliberate, reckless, improper, dishonest and/or negligent through a failure to meet their professional and regulatory obligations. These 'criminalised professionals' play a key role in helping to create or operate legal persons (and arrangements) to conceal their criminal clients' control and beneficial ownership.

…the professional individual, organisation or network providing professional services that enable criminals to launder their proceeds of crime.

In 2018, FATF published guidance on *Professional Money Laundering*[36], which identifies the key characteristics of professional enablers, including:

- The individual professional money launderer.
- The professional money laundering organisation.
- The professional money laundering network of associates and contacts that work together to facilitate money laundering.

These professionals use a variety of money laundering tools and techniques including TBML, account management mechanisms, underground banking and alternative banking platforms. To lend a veneer of legitimacy to their activities, they work with corrupt individual(s) who specialise in the provision of otherwise legitimate services (e.g. bankers, lawyers, accountants, real estate agents).

[34] An informal nominee arrangement

[35] The Law Society (United Kingdom) - Professional enablers: https://www.lawsociety.org.uk/topics/anti-money-laundering/professional-enablers#:~:text=%E2%80%9CA%20professional%20enabler%20is%20an,their%20professional%20and%20regulatory%20obligations.%E2%80%9D

[36] FATF – *Professional Money Laundering*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Professional-money-laundering.html

Royal United Services Institute - *Disabling the Enablers of Sanctions Circumvention: Policy Brief*

In May 2024, the Royal United Services Institute's (RUSI) Centre for Finance and Security (CFS) published a policy brief[37] identifying common mechanisms by which professional service providers, such as lawyers, facilitate sanctions evasion. The policy brief concludes by making recommendations for how policymakers can work together to minimise enabling activities and thus strengthen sanctions implementation.

The work of investigative journalists, including those of the Organised Crime and Corruption Reporting Project (OCCRP), provides valuable insights into the activities of professional service providers. To extract the relevant policy lessons from this body of reporting, CFS at RUSI partnered with OCCRP to analyse over 100 relevant recent investigative reports on Russian individuals and entities who have been aided by professional service providers in their attempts to circumvent sanctions; as well as official US, UK and EU actions taken against professional enablers since the full-scale invasion of Ukraine in February 2022.

Key findings and recommendations

The investigative reports analysed by CFS revealed that enablers acting for Russian clients generally operate as 'one-stop-shop' consultants, offering a range of professional services including legal, accountancy, investment, real estate, and trust and company formation services. As enablers do not adhere to neatly defined professional roles, the Policy Brief recommends identifying and regulating enablers by typologies of activity.

The Policy Brief identifies five main categories of activities undertaken by professional enablers:

- Hiding wealth through convoluted corporate structures and working with money-laundering networks.
- Maintaining control by diluting ownership to avoid financial sanctions thresholds.
- Thinking globally by taking advantage of jurisdictions with lax regulatory oversight.
- Deflecting scrutiny by aggressively dealing with those who take an interest in their clients' affairs.
- The final enabler behaviour identified was described as 'being prepared', in that the most accomplished professional service providers engage in all typologies of enabler activity before their client is even sanctioned.

CFS's analysis found these typologies appeared consistently across the investigative reports, which illustrates that fundamental policy and practice gaps continue to allow professional service providers to help their clients improperly protect their assets and interests from sanctions.

The policy brief concludes by making twelve recommendations designed to close existing loopholes and combat professional enabler obfuscation tactics. These recommendations include:

- Increased enforcement actions against professional enabler networks and thus, increased deterrence.
- Enhanced coordination of sanctions designations and the harmonisation of rules and standards across likeminded jurisdictions.
- Imposing AML obligations on those who provide financial and related services.
- Developing more inclusive information sharing mechanisms.
- Boosting beneficial ownership and control transparency.

[37] Royal United Services Institute - *Disabling the Enablers of Sanctions Circumvention*: https://www.rusi.org/explore-our-research/publications/policy-briefs/disabling-enablers-sanctions-circumvention

World Bank Group - *Signatures for Sale: A Case Study of Criminalised Professionals Facilitating Money Laundering (2022)*

The *Signatures for Sale* report by the Stolen Asset Recovery Initiative (StAR)[38] examines the use of nominee services by corporate service providers (CSPs) to facilitate ML by protecting privacy and allowing individuals to conceal their true ownership of shell companies, effectively obscuring their identities from competent authorities. The report highlights the role of CSPs, in facilitating this illicit activity. These enablers, leveraging their knowledge and professional skills, actively promote and provide nominee services, often in conjunction with other secrecy-enhancing tools like powers of attorney.

The report draws on more than 3,300 responses gathered as part of a global mystery shopping exercise where researchers posed as clients seeking to establish shell companies. The results showed that 14% of CSPs offered nominee services without prompting and 15% mentioned powers of attorney or legal professional secrecy. This suggests that nominee services are readily available and used widely, particularly in jurisdictions known for facilitating financial secrecy.

Key findings

- Nominee services offered by CSPs can have many different uses, extending from those that are routinely used for legitimate business purposes, to those that have legitimate purposes but are vulnerable to misuse, to those where the primary purpose is to hide the beneficial owner.
- Their legitimate uses notwithstanding, nominee arrangements are one of the most common devices for hiding the identity of those controlling shell companies, and are especially prevalent among the most problematic parts of the company formation industry.
- Currently, the lack of attention to the potential and actual misuses of nominee arrangements constitutes a major vulnerability to curb the use of untraceable shell companies in financial crime. Greater attention to enforcement is necessary, and this point applies in particular to beneficial ownership registries.
- On the illicit end of this spectrum, nominee services are often explicitly marketed to clients shopping for shell companies as a device to keep the identity of the beneficial owner off the public record.
- Networks of shell companies with nominees pose a threat to corporate transparency primarily because of their inherently multi-jurisdictional nature. Yet there is a fundamental disconnect between the multi-jurisdictional threat and the single-jurisdiction rules to address this.
- Enforcing effective regulation of CSPs and regulation of nominee arrangements is critical to increasing transparency of beneficial ownership.

Enablers

The CSPs offering these kinds of services are often lawyers, acting as nominee directors or shareholders, providing their names and signatures for a fee. They may also draft power of attorney agreements that allow the true beneficial owner to control the company while remaining hidden. Legal professional privilege may act as an extra layer of protection. CSPs may also offer "shelf companies" with pre-existing bank accounts and nominee signatories, allowing clients to immediately access the financial system without revealing their identities.

The use of nominee services creates a significant vulnerability in the fight against ML. It allows criminals to operate with impunity, hiding their identities and assets from authorities. This undermines the effectiveness of beneficial ownership registers and other transparency measures.

The report emphasises the need for stronger regulation and enforcement of nominee services, including:

- Increased transparency: requiring nominees to disclose their nominators and the purpose of the nominee arrangement.
- Licensing and supervision: licensing professional nominees and subjecting them to rigorous supervision.
- Enhanced due diligence: requiring CSPs to conduct thorough due diligence on their clients and the purpose of the nominee arrangement.
- International cooperation: strengthening international cooperation to address the multi-jurisdictional nature of nominee services.

By addressing these vulnerabilities, authorities can effectively combat the use of nominee services and prevent criminalised professionals from facilitating ML.

[38] World Bank Group - *Signatures for Sale (2022), available at* https://star.worldbank.org/publications/signatures-sale-how-nominee-services-shell-companies-are-abused-conceal-beneficial

Case studies

Members and observers provided the following case studies that illustrate the ways professional enablers in the region facilitate the misuse of legal persons for ML/TF purposes.

Case Study # 6: Seven people charged in connection to sophisticated world-wide cyber scam

Investment scams; use of legal persons; use of the internet; use of virtual assets; use of financial services

A counterpart law enforcement agency in Jurisdiction S alerted the Australian Federal Police (AFP)-led Joint Policing Cybercrime Coordination Centre (JPC3) to Australian links to a scam based predominantly in Jurisdiction S. The AFP then began a parallel investigation with the foreign law enforcement agency (Operation Wickham).

The sophisticated scam involved the unlawful manipulation of legitimate electronic trading platforms. An organised crime syndicate conducted a 'Sha Zhu Pan style' scam using a mix of social engineering techniques, including the use of dating sites, employment sites, and messaging platforms to gain a victim's trust before mentioning investment opportunities. Once subscribed to a financial investment service, the syndicate is alleged to have manipulated the data provided through the legitimate application to encourage further investment, while concealing the fact the money had been stolen. More than USD 100 million in losses world-wide have been attributed to this organised crime syndicate, with the majority of victims being based in Jurisdiction S.

The syndicate used foreign nationals living in Australia to set up the infrastructure required to facilitate their fraudulent activities. The syndicate used the foreign nationals to register Australian companies and to establish Australian business bank accounts to launder the proceeds of crime. The funds were laundered through a remittance business and layered through the bank accounts linked to the registered Australian businesses.

One of the offenders, while working at the remittance business, is alleged to have had links with the organised crime syndicate and was directly involved in the procurement of straw directors and dummy account holders for the ML entities. He allegedly oversaw the establishment of fake companies, and their associated bank accounts, in an attempt to circumvent AML/CTF laws.

Seven people have been charged under Operation Wickham for various offences including dealing in the proceeds crime (money or property worth AUD 10 million or more) (~ USD 6.8 million). Further, the AFP-led Criminal Assets Confiscation Taskforce (CACT) also obtained restraining orders over bank accounts related to the syndicate, with a total value of over AUD 21 million (~ USD 14 million).

Source - Australia

Case Study # 7: Australian company entity being used by an offshore cybercriminal syndicate

Fraud including business email compromise; misuse of legal persons; use of virtual assets (cryptocurrencies or other virtual assets)

The Australian FIU, AUSTRAC identified an Australian company being used by an offshore cybercriminal syndicate to move their business email compromise-derived proceeds of crime, offshore. They did this using international shell companies, digital currency and professional service providers, including an accountant. The listed director of the company was highly likely the victim of identity theft or mule activity.

The company attempted to receive the fraudulently obtained proceeds into an Australian bank account, including over AUD 92,000 (~ USD 61,424) from a property settlement-related business email compromise in 2020. The funds were frozen and returned to the victim before they could be sent offshore. However, the account successfully received more than AUD 290,000 (~ USD 193,611) from several different overseas victims over four months in 2020, before layering and moving the funds offshore.

It is highly likely the company used digital currencies[39] to launder the proceeds of crime. The company deposited funds with a digital currency exchange provider[40] (DCE), that were immediately converted into digital currency and withdrawn from the DCE's custodial account. Two additional offshore corporate accounts were linked to the entity through the DCE and likely used to launder the proceeds of crime through shell companies[41].

Source - *Money Laundering in Australia National Risk Assessment* (with minor amendments)

[39] Virtual assets
[40] Virtual asset service provider
[41] AUSTRAC - *Money Laundering in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

Case Study # 8: Money laundering through shell companies

Misuse of legal persons

Between April 2019 and April 2021, 11 members of a criminal syndicate established approximately 340 shell companies together with approximately 900 bank accounts in the name of these shell companies. The bank accounts were "sold" to criminals who needed bank accounts to manage and conceal illegal funds obtained from running illegal gambling websites. In October 2012, Korean prosecution authorities prosecuted the 11 members of the criminal syndicate and obtained a dissolution order to dissolve the shell companies.

Source - Korea

Case Study # 9: Receive government funding using fraudulent documents and cash withdrawal

Fraud; self-laundering; financial institutions; cash; use of cheques; COVID-19; use of legal persons; suspicious transaction reporting

Between December 2021 and February 2023, four suspects in Macao, China opened corporate bank accounts for over 140 companies at five different domestic banks. The four suspects deposited cheques issued by the Government of Macao, China for subsidising small and medium sized enterprises as well as freelancers to cope with COVID-19 hardship. All the funds, totalling approximately USD 200,000 were withdrawn in cash shortly after the cheques cleared. When queried by the banks during their CDD procedure, the four suspects stated the cash would be used for business purposes. The banks submitted STRs based upon similar suspicious factors. Further analysis conducted by the FIU of Macao, China revealed that almost all of the companies shared the same correspondence address and the STR cases were then passed to the Public Prosecutions Office for further investigation.

Source - Macao, China

Case Study # 10: 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.

The criminal syndicate based in Malaysia was in operation only for a few years yet had allegedly amassed close to RM 200 million (~ USD 42.6 million) of proceeds of crime. Despite the operation being based in Malaysia, 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

Case Study # 11: Network of more than 3,000 companies used as conduits for business email compromise fraud

Fraud; foreign predicate offence; third party laundering; company service providers; use of legal persons and arrangements; suspicious transaction reporting

In 2020, the Commercial Affairs Department (CAD) of the Singapore Police Force observed a sudden rise in Singapore-incorporated companies that were used as conduits for business email compromise fraud targeted at victims overseas. The companies shared common characteristics and investigations by the CAD uncovered a network of more than 3,000 companies suspected to be incorporated for the purpose of laundering the proceeds of crime.

Recognising the importance of disrupting this criminal syndicate, the CAD engaged key stakeholders from the banking sector to share its observations and to exchange insights on this case. This included the issuance of an advisory by Singapore's FIU, the Suspicious Transaction Reporting Office (STRO), to the

banking sector on the emerging typology involving these Singapore companies. Such exchange of intelligence and insights have proven instrumental in expediting investigations as the STRO received and subsequently disseminated actionable financial intelligence which facilitated CAD's investigations.

Investigations revealed that foreign agents with links to foreign criminal syndicates engaged corporate service providers (CSPs) in Singapore to incorporate companies and recruit third party individuals to act as local directors for the companies they incorporated. These local directors, who each held directorships ranging from 57 to 1,002 companies, had allowed the companies and their bank accounts to be operated by the foreign agents, and were therefore found to be negligent in their duties as directors.

To date, seven individuals associated with the companies have been convicted of various offences under the Companies Act and sentenced to imprisonment or fined. Prosecution is ongoing for another five individuals involved.

Common traits observed among these companies include the following:

- The companies typically have both a local director and a foreign director, the latter who also acts as the sole shareholder of the company.
- The companies share a common registered address or local director. The local directors involved typically held multiple directorships across the network of companies.
- The companies were incorporated in the same time period.
- Limited online presence and, different nature of business despite large amounts transacted, high transaction volume for newly incorporated businesses.

Source - Singapore

Case Study # 12: Foreign exchange fraud

Fraud including phone/SMS/email fraud/social media; third party laundering; use of legal persons and arrangements

Person A and his criminal group established 42 shell companies and separately operated illegal foreign exchange and futures trading businesses while claiming to be a foreign exchange trader from jurisdiction X. They established branch offices in various regions, hired staff to expand their operations, implemented a broker system and conducted promotions through brokers or online platforms such as Facebook, WeChat, QQ, or Telegram. They also offered a "6% bonus program" to guarantee profits, aiming to attract people to trade on the group's fraudulent website. Between 2012 and May 2022, they defrauded a total of TWD 24.98 billion (~ USD 832 million).

To recover the proceeds of crime, the Ministry of Justice Investigation Bureau (MJIB) seized 93 real estate properties, valued at around TWD 149 million (~ USD 4.6 million), owned by Person A. Through tracing the flow of overseas fund transfers, the MJIB identified that Person B (and others) provided accounts for Person A to transfer illicit proceeds, amounting to TWD 115.69 million (~ USD 3.73 million). With the court's approval, the MJIB seized real estate properties under Person B's name, valued at around TWD 1.3 million (~ USD 406,250). The MJIB referred Person A and his criminal group to the prosecutor's office in Mar 2023, and they are now on trial.

Source - Chinese Taipei

Case Study # 13: Australia's most complex AFP-led money laundering investigation

Organised crime; currency exchange; money value transfer services; international cooperation; third party laundering; stand-alone laundering

Operation Avarus-Nightwolf was a 14-month AFP-led investigation supported by AUSTRAC, Australian Border Force (ABF), Australian Criminal Intelligence Commission (ACIC), the Australian Securities and Investments Commission (ASIC), the Australian Taxation Office (ATO) and the United States Department of Homeland Security.

Seven members of the Long River money laundering syndicate, and an alleged Australian organised crime syndicate with global reach, were investigated and charged in relation to secretly running a prominent, multi-billion-dollar money remitting chain in Australia: the Changjiang Currency Exchange. The AFP will allege that in an attempt to look and act like a law-abiding remittance company, the Changjiang Currency Exchange even supplied resources to educate customers about Australia's AML laws.

Between 2020-2023, the Changjiang Currency Exchange transferred more than AUD 10 billion (~ USD 6.8 billion) in and out of Australia. While most of these funds were from customers engaged in lawful actions,

the AFP will allege the company also secretly transferred unlawfully gained money in and out of Australia. The AFP will allege that between 2020-2023, the Changjiang Currency Exchange laundered over $228 million.

The AFP alleges some of the money laundered by the syndicate was from the proceeds of crime, including from cyber-enabled scams, and the trafficking of illicit goods. The AFP also alleges the syndicate would coach its criminal customers how to create fake business paperwork, such as false invoices and bank statements. This was to enable criminal customers and the Changjiang Currency Exchange to show authorities that unlawfully gained money was from lawful sources if the transfers ever came to the attention of authorities.

The AFP charged four foreign nationals and three Australian citizens for their alleged involvement in the money laundering syndicate and restrained more than $50 million in property and vehicles. In October 2023, AUSTRAC also suspended the registration of six remittance service providers.

Source - Australia

Case Study # 14: Stock market manipulation and asset misappropriation at a joint stock company

Fraud; insider trading and market manipulation

Person A and his accomplices conducted a case of stock market manipulation and asset misappropriation at a joint stock company.

Person A established a joint stock company and to increase charter capital, he turned this company into a public company to be listed on the stock exchange. Related to this case, a number of former public leaders were prosecuted for the crime of 'abusing position and power while performing official duties'. Some officials were prosecuted for the crime of 'publishing false information or concealing information in securities activities'.

The defendants paid VND 195 billion (~ USD 8 million) to the state to overcome the consequences; the Investigation Agency seized nine real estate properties and total damage amounted to VND 1,830 billion (~ USD 75.5 million).

Source - Vietnam

A key challenge with professional enablers: privacy and legal professional privilege

Recent transparency advancements to tackle illicit financial flows have involved an expansion in the collection and exchange of information among competent authorities. Examples of these new policies include the establishment of central registries of beneficial ownership information, the global automatic exchange of bank account information, and/or mandatory rules[42] for intermediaries to disclose schemes that circumvent exchanges of information or hide the beneficial owner.[43] This expansion of the collection, handling and exchange of information among governments has caused opposition, particularly in relation to the rights to privacy and information/data protection and legal professional privilege.

One of the most significant developments in this regard was the European Court of Justice's ruling[44] in November 2022, which invalidated public access to beneficial ownership information in relation to the fight against ML. The primary rationale related to individuals' right to privacy. Also, in connection to the right to privacy, legal professionals have also invoked their clients' legal professional privilege. For instance, the European Court of Justice recognised legal professional privilege to invalidate certain reporting of information based on *The EU Council Directive 2011/16* (known as DAC6) in relation to cross-border tax arrangements' mandatory disclosure rules[45]. A 2024 legal opinion[46] by the Advocate General to the European

[42] Tax Justice Network - *The unexploited silver bullet to tackle enablers: mandatory disclosure rules* blog: https://taxjustice.net/2023/07/14/the-unexploited-silver-bullet-to-tackle-enablers-mandatory-disclosure-rules/

[43] [43] The amendments to the EU Directive Administrative Cooperation (DAC 2 and 6) required the automatic exchange of bank account information and the mandatory disclosure of schemes by intermediaries.

[44] Court of Justice of the European Union - *Press Release No 188/22 - Judgment of the Court in Joined Cases C-37/20 | Luxembourg Business Registers and C-601/20 | Sovim:* https://curia.europa.eu/jcms/upload/docs/application/pdf/2022-11/cp220188en.pdf

[45] InfoCuria Case-law - *Judgement of the Court (Grand Chamber) In Case C-694/20:* https://curia.europa.eu/juris/document/document.jsf?text=&docid=268430&pageIndex=0&doclang=EN&mode=lst&dir=&occ=first&part=1&cid=27401

[46] InfoCuria Case-law - *Opinion of Advocate General Kokott delivered on 30 May 2024 Case C-432/23*: https://curia.europa.eu/juris/document/document.jsf?text=&docid=286580&pageIndex=0&doclang=en&mode=req&dir=&occ=first&part=1&cid=7340756

Court of Justice recognised legal professional privilege to oppose submitting information on the creation of companies, also within the right to privacy. Civil society organisations have criticised this ruling.[47]

The FATF and the Global Forum on Transparency and Exchange of Information for Tax Purposes (Global Forum) have been warning against these developments and arguing for limits on legal professional privilege. For instance, the 2019 FATF report *Guidance for a Risk-based Approach Legal Professionals*[48] noted that:

> *"criminals may also seek out legal professionals (over other non-legal professions) to perform the services listed in Recommendation 22 with the specific criminal intent of concealing their activities and identity from authorities through professional privilege/secrecy protections"* (page 23).

Likewise, the 2013 FATF report *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*[49] noted that:

> *"claims of legal professional privilege or professional secrecy could impede and delay the criminal investigation… In many instances this means that the claim of legal professional privilege or professional secrecy will need to be resolved by a court, which can delay the investigation process for a substantial period of time. As time is a critical factor in pursuing the proceeds of crime, this may influence the decision of investigators of whether to investigate the possible involvement of the legal professional or to seek evidence of their client's activities from alternative sources"* (pp 31-32).

Further, the report's Annex included 45 cases of legal professionals obscuring ownership through the creation of companies, trusts, use of bearer shares or acting as trustees. Case 59 of the Annex involved a legal professional creating complicated foreign structures and transferring funds through the client account while claiming privilege to prevent discovery.

While noting there are differing views on this issue, there is an argument that the protection provided to clients under legal professional privilege should be specific to communications and information generated by legal professionals acting *in their capacity as legal professionals*. For instance, the *Handbook for Peer Reviews on Transparency and Exchange of Information on Request*[50] describes that:

> *"Communications between a client and an attorney, solicitor or other admitted legal representative are only privileged if, and to the extent that, the attorney, solicitor or other legal representative acts in his or her capacity as an attorney, solicitor or other legal representative. For instance, to the extent that an attorney acts as a nominee shareholder, a trustee, a settlor, a company director or under a power of attorney to represent the company in its business affairs, he cannot claim the attorney-client privilege with respect to any information resulting from and relating to any such activity*" (paragraph 88).[51]

According to the Global Forum, ownership information would in principle not be subject to confidentiality. Further, the *Model Tax Convention on Income and on Capital 2017*[52] that serves as a legal basis for exchange of information describe that:

> *"such protection does not attach to documents or records delivered to an attorney, solicitor or other admitted legal representative in an attempt to protect such documents or records from disclosure required by law. Also, information on the identity of a person such as a director or beneficial owner of a company is typically not protected as a confidential communication"* (paragraph 19.3).

[47] Tax Justice Network - *Another EU court case is weaponising human rights against transparency and tax justice* blog: https://taxjustice.net/2024/06/28/another-eu-court-case-is-weaponising-human-rights-against-transparency-and-tax-justice/
[48] FATF - *Guidance for a Risk-Based Approach Legal Professionals*: https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Legal-Professionals.pdf.coredownload.inline.pdf
[49] FATF - *Money Laundering and Terrorist Financing Vulnerabilities of Legal Professionals*: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/ML%20and%20TF%20vulnerabilities%20legal%20professionals.pdf.coredownload.pdf
[50] OECD Global Forum on Transparency and Exchange of Information for Tax Purposes - *Handbook for Peer Reviews on Transparency and Exchange of Information on Request*: https://web-archive.oecd.org/tax/transparency/documents/handbook-for-peer-reviews-on-transparency-and-exchange-of-information-on-request.pdf
[51] Generally in common law countries, privilege attaches to confidential communications, between lawyer and client, created for the dominant purpose of providing advice or in respect of litigation. Also, where that communication is for an illegal purpose, privilege can be struck down.

[52] OECD - *Model Tax Convention on Income and on Capital 2017*: https://www.oecd-ilibrary.org/docserver/g2g972ee-en.pdf?expires=1722597850&id=id&accname=guest&checksum=FA165AD67AA8EF4BE6F09EA6EB60E69F

1.4 Defenders

Competent authorities can use a range of mechanisms to mitigate professional enablers and the misuse of legal persons. Having timely access to basic and beneficial ownership through such mechanisms as publicly available registers is critical to competent authorities' efforts. Further, given that professional enablers can commonly be TCSPs, jurisdictions effectively regulating TCSPs alongside other mechanisms is also critical. There are also other mechanisms such as implementing proportionate and dissuasive sanctions, whistleblower protections and public/private partnerships. Finally, given the challenges that an international element to a legal person's beneficial ownership presents, international cooperation among competent authorities becomes crucial.

This section outlies both members' and observers' efforts, international best practice and lessons learned with these implementing these mechanisms.

Royal United Services Institute - *Anti-Money Laundering and Professional Service Providers, Conference Report (2024)*

Between April and June 2024, the Centre for Finance and Security (CFS) at the Royal United Services Institute (RUSI) organised three workshops exploring the role of AML regulation, supervision and enforcement activity in preventing, detecting and punishing so-called 'enabling' behaviour by lawyers and accountants, and examined the role of good practices incentives in the United Kingdom (UK) and the European Union (EU).

RUSI organised the workshops in partnership with the *Delegation of the European Union to the United Kingdom of Great Britain and Northern Ireland*, and brought together industry, regulators, law enforcement and academics across the UK and the EU. In July 2024, CFS published a Conference Report[53] summarising the main findings of the discussions.

Each workshop focused on specific challenges related to different elements of the supervisory process with respect to professional service providers: effectiveness, enforcement and incentives. The report outlines in comprehensive detail, each workshop's findings. The three workshops highlighted that there are many common challenges in enforcing AML obligations in professional service providers, notably:

- The lack of consistent supervisory structures both within some jurisdictions and across different jurisdictions; this hinders cross-border collaboration and potentially introduces gaps which criminals can exploit.
- The need for greater information sharing across all parts of the ecosystem, particularly in relation to suspicious transaction reports/suspicious activity reports, where both professionals and supervisors felt that more feedback would be hugely advantageous.
- The need for supervisors to have access to a wide range of regulatory tools, including different ways to incentivise professionals to comply with their AML obligations. These tools should also be tailored to different types of professional service provider and different geographies.

All participants agreed that lawyers and accountants have a very important part to play in preventing and detecting ML, but that the challenges identified hinder both the effective implementation of AML controls and effective enforcement when professionals or professional service providers are non-compliant.

United Nations Office on Drugs and Crime's work on preventive measures associated with professional enablers

The United Nations Office on Drugs and Crime (UNODC) is actively working on preventive measures associated with professional enablers. At a panel on measures to prevent ML, with a focus on the role of intermediaries in the transfer of proceeds of crime, under item 6 on the follow-up to Special Session of the

[53] Royal United Services Institute - *Anti-Money Laundering and Professional Service Providers: Conference Report*: https://www.rusi.org/explore-our-research/publications/conference-reports/anti-money-laundering-and-professional-service-providers-conference-report

General Assembly (UNGASS) against corruption during the 14th resumed session of the Implementation Review Group (4-8 September 2023), UNODC provided the following update:

> *"The laundering and hiding of proceeds of crime is a complex and evolving problem and a serious threat to both the integrity of the financial system and the rule of law. It enables criminals to conceal the origin and ownership of their illicit proceeds, and to enjoy the benefits of their illegal activities. Intermediaries, or gatekeepers, are frequently involved in money-laundering schemes, either knowingly or unwittingly. They provide services that can help launderers to disguise the source and destination of their funds, such as creating shell companies, opening bank accounts, transferring assets, or conducting transactions."*

UNODC addresses challenges identified by Member States and through the United Nations Convention against Corruption (UNCAC) Review Mechanism. Some of these key challenges include:

- Closing legal and regulatory gaps and ensuring the effective supervision of intermediaries by the appropriate bodies, and in that regard: developing capacity and effective mechanisms for monitoring and enforcing compliance with AML standards.
- Enhancing the awareness and understanding of intermediaries about their role and responsibilities in preventing and detecting money-laundering.
- Improving cooperation and information-sharing between intermediaries, law enforcement and regulatory authorities.
- Ensuring that intermediaries who report suspicious transactions are protected from retaliation or intimidation.

A key challenge lies in designing the appropriate responses that take into account the specificities of different sectors and professions. While preventive approaches are more useful where intermediaries are vulnerable to being used for ML purposes, this will not be enough where it comes to professional enablers.

New Zealand's efforts with professional enablers

New Zealand noted vulnerabilities associated with the provision of nominee services by its professional service providers. For example, a New Zealand TCSP that provided nominee services for more than 1,000 companies registered in New Zealand on behalf of overseas clients, and other examples included criminals using informal nominees (family members and strawmen) to conceal their beneficial ownership.

In response, New Zealand took a number of actions, particularly through accelerating the inclusion of TCSPs in its AML/CFT system, creation of a register of New Zealand Foreign Trusts, the creation of a dedicated Integrity and Enforcement Team responsible for ensuring the integrity of corporate registries, and amendments to the Companies Act to require companies have a resident director. Further, New Zealand also undertook consultation on beneficial ownership reforms in relation to companies and partnerships.

Beneficial ownership registers

Characteristics of an effective AML/CFT/CPF system include a jurisdiction implementing measures to:

- Prevent legal persons and arrangements from being used for criminal purposes.
- Make legal persons and arrangements sufficiently transparent.
- Ensure that adequate, accurate and up-to-date basic and beneficial ownership information is available on a timely basis.
- Beneficial ownership information is available to competent authorities[54].
- Persons who breach these measures are subject to effective, proportionate and dissuasive sanctions.

Effective implementation of these measures makes the misuse of legal persons less attractive for criminals.[55]

Many jurisdictions have created, are in the process of creating, or are considering, centralised repositories for holding beneficial ownership information. Beneficial ownership registers can take different shapes and

[54] FATF - *Guidance on Beneficial Ownership of Legal Persons* - https://www.fatf-gafi.org/en/publications/Fatfrecommendations/Guidance-Beneficial-Ownership-Legal-Persons.html
[55] FATF *Methodology for Assessing Technical Compliance with the FATF Recommendations and the Effectiveness of AML/CFT/CPF Systems* - https://www.fatf-gafi.org/en/publications/Mutualevaluations/Assessment-Methodology-2022.html

forms, and jurisdictions have significant flexibility to adjust their set-up to match the institutional context in which the registers operate, as well as the variety of legal persons whose beneficial ownership is recorded.

Data collected from members regarding beneficial ownership information demonstrates that this is an area that requires significant uplift. Generally, there is little information available on the beneficial ownership of legal persons in the Asia/Pacific region. Where members do have a central public register for legal persons, commonly only basic information is maintained and does not include beneficial ownership information as defined by the FATF Standards. Across the global network, the quality of the information held on existing registers is often unverified and not kept up to date. Legal frameworks may not even require legal persons themselves to maintain beneficial information beyond immediate shareholders.

However, on a positive note, some jurisdictions are leading the way in implementing reforms, and offer opportunities for other jurisdictions to model at an appropriate scale for their own risk and context.

Canada's beneficial ownership registers

On 22 January 2024, Canada launched a public beneficial ownership register for companies incorporated federally under the *Canada Business Corporations Act* (CBCA). In Canada, beneficial owners are also known as individuals with significant control (ISC). Canada is using Open Ownership's (a non-profit organisation focused on beneficial ownership transparency) *Beneficial Ownership Data Standard*[56] the international standard, to structure the collected data. This will allow its beneficial ownership register interoperability with other beneficial ownership registries worldwide, which will allow for more timely data sharing. Canada required corporations governed by the CBCA to file beneficial ownership information with Corporations Canada. Information that is publicly available include[57]:

- Full legal name.
- Date the individual became an ISC and ceased to be an ISC, as applicable.
- Description of the ISC's significant control.
- Residential address (will be made public if no address for service is provided).
- Address for service (if one is provided).

Further, on 31 March 2023, the province of Quebec launched a public beneficial ownership registry, which covers corporations incorporated in Quebec and all other legal entities registered to do business there. On 11 May 2023, the province of British Columbia passed legislation to create a public beneficial ownership registry, which they plan to launch in 2025.

The Philippines' reform of its companies register

The Philippines recently initiated a program to reform its companies register to enhance and streamline LEA's access to beneficial ownership information, primarily with the Philippines' Securities and Exchange Commission (SEC). Actions include:

- The SEC introduced automatic enrolment in *eFAST* and mandatory disclosure of beneficial ownership, during the incorporation process. The SEC complemented this by implementing the *SEC Memorandum Circular (MC) No. 19, Series of 2023,* which provides guidelines on placing corporations in delinquency status for non-submission of reporting requirements, in accordance with Sections 21 and 177 of the Revised Corporation Code.
- As of April 2024, there are over half a million active corporations, of which 68% are now compliant with beneficial ownership disclosure requirements. The SEC placed the remaining 32% under 'delinquency status'. The SEC conducted a scoping exercise that showed that 97% of these delinquent entities belong to the micro, small, and medium enterprise sector.
- The SEC has likewise suspended 117,885 corporations monitored and non-operating for at least eight years. It is notable that all (100%) of these suspended corporations have neither engaged in nor reported any commercial activity over that time.

[56] Open Ownership - *Beneficial Ownership Data Standard*: https://standard.openownership.org/en/0.4.0/
[57] Government of Canada - *Individuals with significant control - File your information*: https://ised-isde.canada.ca/site/corporations-canada/en/individuals-significant-control-file-your-information?utm_campaign=ised-isde-cc-isc-23-24&utm_medium=link&utm_source=notice

- The SEC has worked closely with its 19 partner agencies, processing 734 requests for information related to corporate information, including beneficial ownership, on 4,989 corporations and 1,099 individuals.

Australia's proposed beneficial ownership register

In November 2022, the Australian Government opened consultation on the design features for the first phase of a publicly available beneficial ownership register. The aim is to increase transparency of beneficial ownership and discourage the use of complex ownership structures that avoid legal requirements and obscure tax liabilities. It also seeks to support stronger regulatory and law enforcement responses to tax and financial crime, assist foreign investment applications, and facilitate the enforcement of sanctions.

The first phase of consultation sought views on a proposal to require specified unlisted entities regulated under Australia's *Corporations Act* to maintain accurate, up-to-date and publicly accessible beneficial ownership registers. Future consultation phases will seek views on approaches to disclosure of beneficial ownership held through other legal vehicles, such as trusts, and the centralisation of information in a single public registry[58].

Lessons learned: best practices and challenges when establishing a beneficial ownership register

As reflected in the EU Global Facility's report *Building a Country Roadmap for Beneficial Ownership Disclosure Regime*[59], there are many lessons learned and issues to consider when establishing a Beneficial Owner Register (BOR). Best practice headlines from this report examine; legal framework design, intergovernmental coordination, technological solutions for streamlining interconnectivity, and effective training.

The report also identified_major challenges that need to be addressed when setting up a BOR, including; underestimating time and resources required, unclear or ambiguous legislation, and low-quality data produced by insufficiently robust systems.

United Nations Office on Drugs and Crime - *Implementation of Beneficial Ownership Transparency in ASEAN Member States and Timor-Leste*
In 2024, UNODC published a report[60] which covered a comparative study on the implementation of beneficial ownership transparency in Member States in the Association of Southeast Asian Nations (ASEAN) and Timor-Leste. This report explored legal definitions on beneficial ownership in ASEAN and Timor-Leste, as well as key elements in their beneficial ownership disclosure frameworks. Key elements studied and compared included the collection and maintenance of beneficial ownership data where, UNODC identified that six ASEAN Member States had established registers to collect and maintain beneficial ownership data with discrepancies in relation to their coverage. Other elements studied and compared included sanctions for non-compliance and the scope of legal entities covered by beneficial ownership disclosure frameworks in ASEAN and Timor-Leste.

The positive role TCSPs can play in beneficial ownership registration

When companies and other entities engage with TCSPs, this can offer advantages to the beneficial ownership registration process. Compared to their customers (e.g. a legal person subject to beneficial ownership registration), TCSPs commonly have a better knowledge and understanding of beneficial ownership requirements under the relevant legislation.

If the TCSP is considered a reporting entity under the jurisdiction's AML/CFT legislation (e.g. a DNFBP), they are required to apply robust CDD processes, including identifying the beneficial owner of their customers. Having collected this information to comply with their CDD requirements, TCSPs will be in a better position

[58] Australian Government, The Treasury website - *Multinational tax integrity: Public Beneficial Ownership Register*: https://treasury.gov.au/consultation/c2022-322265
[59] EU Global Facility - *Building a Country Roadmap for Beneficial Ownership Disclosure Regime*: https://www.global-amlcft.eu/wp-content/uploads/2024/05/BO-Country-Roadmap-vfinale.pdf
[60] United Nations Office on Drugs and Crime - *Implementation of Beneficial Ownership Transparency in ASEAN Member States and Timor-Leste:* https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_Beneficial_Ownership_Transparency_in_ASEAN_Member_States_and_Timor-Leste.pdf

to register accurate information with the beneficial ownership registry. Further, unlike a company registrar, TCSPs are commonly in close and extensive contact with their customer, allowing them to be aware of changes in the ownership or control to keep beneficial ownership information updated. Notably, one member who regulated TCSPs under their AML/CFT system noted that in 2023, TCSPs reported a total of 35 STRs to the FIU.

In examples of where TCSPs have been involved in beneficial ownership registration, the follow advantages have been observed:

- Better compliance and understanding of beneficial ownership requirements. For example, in Belgium 70% of companies register their information through their accountant, and others do it directly through their legal representative.
- Awareness campaigns and training. From the perspective of the beneficial ownership register (BOR), concentrating training efforts on those TCSPs involved in beneficial ownership registration is more efficient than reaching out to all legal persons or arrangements directly.
- Communication. By dealing with a relatively small number of TCSPs (as opposed to all legal persons or arrangements), the BOR can offer integrated technological solutions, such as secure online portals and automated data transfer systems (e.g. an API) to facilitate seamless information sharing between TCSPs and the BOR.
- Verification. TCSPs subject to CDD requirements are also required to verify the accuracy of beneficial ownership information. Based on their verification of this information, TCSPs may be allowed (or required by law), to report discrepancies to the BOR to improve the accuracy of registered information. This will enable the BOR to initiate an investigation, request additional information, correct any inaccuracies, and/or apply enforcement measures.
- Human resources. There is a significant advantage when comparing the number of full-time equivalent employees assigned to compliance and due diligence within TCSPs, when compared to the number of employees working for a jurisdiction's public authority.

While there are advantages involving TCSPs in the beneficial ownership registration process, it does not guarantee full compliance. Therefore, the BOR should implement oversight mechanisms such as regular audits, inspections, and penalties for non-compliance to monitor and enforce TCSPs adherence to their gatekeeping responsibilities.

Singapore's regulatory efforts with company service providers

Singapore identified that criminals commonly exploit legal persons to facilitate illicit transactions and/or control and move illicit assets. In Singapore, most people form legal entities through corporate service providers (CSPs). Before forming a legal entity for a client, CSPs are required to conduct CDD, identify and verify the identities of the customer, and identify and verify the identities of the beneficial owners associated with the proposed legal person.

The Accounting and Corporate Regulatory Authority (ACRA) oversees and regulates CSPs and takes supervisory actions against CSPs found to have breached their CDD obligations, or have facilitated or assisted in the misuse of legal persons. Possible sanctions on CSPs include financial penalties, and suspensions or cancellations of their registrations. ACRA also maintains a list of CSPs whose registrations have been suspended or cancelled on its website.

Singapore is currently updating its ML/TF risk assessment for legal persons (last completed in 2019), and in early 2024, Singapore's public-private partnership, the AML/CFT Industry Partnership, published the *Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risks Associated with Receiving Referrals from Corporate Service Providers*[61].

Further, in March 2024, Singapore launched a public consultation to enhance its CSP regulatory regime. The proposals include increasing the penalties applicable to CSPs and their senior management for breaches of AML/CFT obligations and prohibiting persons from acting as nominee directors by way of business unless registered CSPs arrange the appointments, and they have been assessed as fit and proper by the registered CSPs. These proposals were incorporated within the CSP Bill and the Companies

[61] Monetary Authority of Singapore - *Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risks Associated with Receiving Referrals from Corporate Service Providers:* https://www.mas.gov.sg/regulation/external-publications/best-practices-for-banks-to-manage-ml-and-tf-risks-associated-with-receiving-referrals-from-csps

and Limited Liability Partnerships (Miscellaneous Amendments) Bill, which were passed in Parliament on 2 July 2024.

Singapore AML/CFT Industry Partnership - *Legal Persons - Misuse Typologies and Best Practices (2018)*

In April 2017, Singapore set up the AML/CFT Industry Partnership, a public-private partnership that brings together the financial sector, regulators, law enforcement agencies and other government entities to collaboratively identify, assess and mitigate key and emerging ML/TF risks facing Singapore.

In May 2018, the AML/CFT Industry Partnership published the *Legal Persons - Misuse Typologies and Best Practices*[62] best practice paper. The AML/CFT Industry Partnership best practice papers highlight red flag customer behaviours or transaction patterns that financial institutions can look out for to detect illicit financial activities. They also recommend measures that financial institutions can take to identify or prevent such activities.

Many professional intermediaries are key to setting up legal persons, as well as the provision of ongoing corporate secretarial services. Therefore, they form the first line of interaction with the legal persons. Highlights from the best practice paper include:

- Legal persons misuse typology in law firm: provision of legal assistance to establish legal persons for possible ML/TF purposes. In the context of legal persons, it is not uncommon for law firms to act on behalf of legal persons, or be asked to assist with the establishment of legal persons or arrangements.

  Client A meets with Solicitor A requesting legal advice and assistance with potential litigation because of a dispute with a business based in the jurisdiction of Solicitor A's practice. No documents are exchanged at the meeting, but Client A describes the facts surrounding the dispute. After the meeting, and in accordance with Solicitor A's procedures for on-boarding new clients, Solicitor A identifies the beneficial owners of Client A and performs screening and nothing appears amiss.

  Client A then proceeds to request for the terms of engagement and to set up a retainer arrangement with Solicitor A, and wires monies into Solicitor A's client account on account of costs. Shortly after, Client A writes to Solicitor A to notify Solicitor A that the claim has been settled. Solicitor A has not carried out work for the client, but a small fee for the initial time spent is deducted. Client A requests for the balance to be sent back to it, but to a different account from which the monies were originally wired from Client A.

  Unbeknownst to Solicitor A, Client A had made up the existence of the claim. Despite the conduct of AML/KYC checks on Client A by Solicitor A, no adverse information was identified. If Solicitor A had returned the balance of the monies to Client A, it would have facilitated a sham- litigation ML. However, any delay in returning the balance of the monies may tip-off Client A.

- Legal person misuse typology in (trust and) company service providers: dual nationalities. Professional advisors, like consulting companies and auditing firms, also observe typologies of ML/TF risk linked to Legal Persons in the course of their work.

  Client A, who is a foreign passport holder of Jurisdiction A, approached a company service provider to incorporate a company in an Offshore Company Location. After a period of time, Client A requested the dissolution of the overseas company. At the same time, he requested to incorporate a South-East Asian company with similar name as the overseas company with his foreign passport issued by another jurisdiction, Jurisdiction B.

- Managing ML/TF risks in the context of company service providers.

  The majority of the company service providers' involvements with legal persons occur during the incorporation of a company (Day 1), the change of a company's structure (ad-hoc) and during the filing of an annual return (periodic basis). As such, the on-boarding stage presents highest ML/TF risks to company service providers.

[62] The Association of Banks in Singapore and the Monetary Authority of Singapore AML/CFT Industry Partnership - *Legal Persons - Misuse Typologies and Best Practices*: https://abs.org.sg/docs/library/legal-persons-misuse-typologies-and-best-practice.pdf

The following are examples of best practices shared by the company service provider members to mitigate the associated ML/TF risks:

- Identification and verifications of controllers, beneficial owners, shareholders, directors and/or authorised signatories
    - For companies with nominee directors, some examples of additional controls in place include ensuring that the financial accounts of the companies are prepared by the company service providers or are audited by a certified public accounting firm.
    - If original documents are not sighted by company service providers during the client due diligence process, they can accept a copy of the document that is certified to be a true copy by a suitably qualified person (e.g. a notary public, a lawyer or certified public or professional accountant).
- Screening of controllers, beneficial owners, shareholders, directors and/or authorised signatories.
    - Company service providers can use trusted commercially available screening databases during the on-boarding process to identify risk indicators (e.g. adverse news, politically exposed person, etc.).
- Understanding the customer's purpose of setting up an account and/or nature of business, controllers/ ultimate beneficiary owners.
    - Company service providers can conduct interviews to understand the proposed business operations and the purpose of setting up the company.
    - Additional information from the client may provide insights to determine the risk level associated with the client, such as the geographical locations of their client's existing main customers and suppliers, the beneficial owner's occupation and SOF for capital injection. For significant share allotments, they may also request bank statement records or bank-in slips for monies injected into the company account from the customer.
- Procedures on suspicious activities indicators/ red flags/ thresholds.
    - The company service provider should formalise procedures for reporting suspicious activities to relevant government agencies through suspicious transaction reports.

United Kingdom - *Office for Professional Body Anti-Money Laundering Supervision*

The UK's Office for Professional Body Anti-Money Laundering Supervision (OPBAS) was established in 2018 as part of reforms to strengthen the UK's anti-money laundering supervisory regime, to tackle vulnerabilities identified in the UK's first national risk assessment of money laundering and terrorist financing (NRA). OPBAS supervises the 25 professional body supervisors (PBSs) in the legal and accountancy sectors. Its objectives are to drive effective supervision by the PBSs and improve information sharing between PBSs, law enforcement and other public bodies[63].

Housed within the UK's Financial Conduct Authority (FCA), OPBAS's approach to supervision is aligned to that of the FCA but also FATF, with an intentional focus on both compliance and effectiveness (outcomes).

As well as conducting cycles of onsite risk-based supervisory assessments of PBSs, OPBAS undertakes thematic and risk-based project work - examples including TCSPs[64] and risk identification and verification work[65]. OPBAS focuses across sectors and sub-sector clusters including barristers, bookkeepers, conveyancers and taxation. This approach allows it to form a holistic view on the relative risks present in underlying populations, so it can target resources to be most impactful in tackling the harm.

OPBAS works collaboratively and proactively with many partners including law enforcement and central government, as well as internationally, to tackle the threat of professional enablers, that is, regulated professionals whose activities facilitate criminal activity, whether the professional is complicit or unwitting. Further, in fulfilling its second objective, OPBAS drives information and intelligence sharing

[63] Financial Conduct Authority - *Office for Professional Body Anti-Money Laundering Supervision (OPBAS)*: https://www.fca.org.uk/about/how-we-operate/who-work-with/opbas
[64] Financial Conduct Authority, Office for Professional Body Anti-Money Laundering Supervision - *Multi-PBS review, Multi-PBS project on TCSP risk*: https://www.fca.org.uk/publication/multi-firm-reviews/opbas-multi-pbs-project-tcsp-risk.pdf
[65] https://www.fca.org.uk/publication/corporate/opbas-supervisory-update-risk-identification-verification.pdf

between PBSs and law enforcement forward, for example by the creation of Intelligence Sharing Expert Working Groups[66, 67].

The UK's *Economic Crime Plan 2*[68] includes actions to reduce the threat from professional enablers, and it developed a *Professional Enablers Strategy*[69] to achieve this. Actions within the strategy include intensified work to foster trust and increase levels of information and intelligence sharing between the public and private sectors, which is a key focus for OPBAS.

Two recent Economic Crime Acts*: Economic Crime (Transparency and Enforcement) Act 2022* and *Economic Crime and Corporate Transparency Act 2023* have made ground-breaking laws to increase corporate transparency, improve beneficial ownership registers, and tackle the misuse of legal persons. OPBAS is working with the UK's Companies House, currently implementing these reforms, to effectively contribute to the fight against such misuse.

The UK's cross-system approach demonstrates the value of public-private partnerships. The UK recognised that silo working is ineffective, and that all parts of the system have a role in reducing ML risks. In addition, civil society and academia are welcome partners, bringing different perspectives, challenge and expertise to the table. OPBAS is an external-facing organisation. It recognises that risks are cross-border and is, therefore, keen to do even more internationally, by sharing the UK's experiences and good practice, and learning from others.

Proportionate and dissuasive sanctions

To ensure competent authorities have timely access to beneficial ownership information, it is crucial for jurisdictions to consistently apply proportionate and dissuasive sanctions to all legal persons for non-compliance with requirements to maintain and disclose beneficial ownership information.

Pakistan's improvements with applying sanctions to legal persons and legal arrangements for non-compliance with beneficial ownership information requirements

Pakistan recently made positive and tangible progress in increasing effectiveness of its AML/CFT/CPF system through applying proportionate and dissuasive sanctions to legal persons (and legal arrangements) for non-compliance with beneficial ownership requirements.

Pakistan recently completed one full cycle of inspections in respect of all categories of legal persons (and legal arrangements) during which it imposed sanctions for a total of PKR 2,385.58 million (~ USD 85.6 million) against 54,593 entities, the majority of which were companies, but also included limited liability partnerships and waqfs (charitable or philanthropic foundations), trusts and cooperatives. Pakistan also imposed other types of enforcement measures such as suspensions, de-registrations, etc. Further, it implemented a WTC portal, enabling the collection of information, including beneficial ownership information of all waqf, trusts and cooperatives in the country, which is accessible by Pakistan's competent authorities.

Macao, China's supervision and sanction of legal persons

In 2023, Macao, China published the *Macao Special Administrative Region Risk Assessment Report on Money Laundering/Terrorist Financing/Financing of Proliferation of Weapons of Mass Destruction (2022)*. In early 2024, Macao, China's competent authorities released this report to and arranged outreach initiatives, which included outreach for the TCSP sector (notaries and lawyers).

The Financial Intelligence Office of Macao, China (GIF) has been closely monitoring the probable misuse of legal persons or TCSP services. In 2023, GIF's Financial Information Analysis Team conducted a special strategic review and identified suspicious shell companies. The team prepared summarised results of specific cases and in August 2023, referred them to the sector's supervisor: the Legal Affairs Bureau (DSAJ).

[66] Financial Conduct Authority, Office for Professional Body Anti-Money Laundering Supervision - *Accountancy Sector Intelligence Sharing Expert Working Group Terms of Reference*: https://www.fca.org.uk/publication/opbas/accountancy-sector-isewg-terms-of-reference.pdf
[67] Financial Conduct Authority, Office for Professional Body Anti-Money Laundering Supervision - *Legal Sector Intelligence Sharing Expert Working Group Terms of Reference*: https://www.fca.org.uk/publication/opbas/legal-sector-intelligence-sharing-expert-working-group-terms-of-reference.pdf
[68] His Majesty's Government - *Economic Crime Plan 2 2023-2026*: https://assets.publishing.service.gov.uk/media/642561b02fa8480013ec0f97/6.8300_HO_Economic_Crime_Plan_2_v6_Web.pdf
[69] National Crime Agency, National Economic Crime Centre and the Office for Professional Body AML Supervision - *Cross-System Professional Enablers Strategy 2024-2026*: https://www.nationalcrimeagency.gov.uk/who-we-are/publications/724-cross-system-professional-enablers-strategy/file

GIF is currently conducting another thematic strategic analysis with STR information to identify probable TCSP services which may have relation to shell companies. The result will be shared with competent authorities once completed.

Through Macao, China's public-private partnership, GIF has also been periodically sharing strategic analyses results with the private sector to enhance their prevention and mitigation measures to prevent the abuse of legal persons. In 2020 and 2021 during the COVID-19 period, GIF shared a list of probable shell company names with FIs so they could apply their mitigation controls. GIF is currently preparing a new list for sharing with FIs and the supervisor.

Macao, China has a range of proportionate and dissuasive sanctions its competent authorities can access for ML under the *Law no. 2/2006 (Prevention and suppression of the crime of money laundering)* and TF under *Law no. 3/2006 (Prevention and suppression of the crimes of terrorism)*. This includes monetary fines or judicial dissolution. Fines can range from MOP 10,000 (~ USD 1,250) to MOP 20 million (~ USD 2.5 million), and a judicial dissolution can be imposed when the legal person was established with the intention of committing ML/TF, or when the repeated commission of such criminal offence demonstrates that the legal person is being used for that purpose, by its members or its management.

Further, legal persons can also incur several accessory penalties which may be applied cumulatively. This includes:

- Prohibition of the exercise of certain activities for a period of 1 to 10 years.
- Deprivation of the right to subsidies or subventions granted by government departments or public entities.
- Closing of the establishment for a period of 1 month to 1 year.
- Definite closing of the establishment.
- Judicial injunction.
- Publicity of the sentence.

In addition to criminal liability for ML/TF, there are also administrative infractions for those entities which fail to comply with the ML/TF preventive obligations, even if they act negligently. These infractions are punishable with a fine MOP 100,000 (~ USD 12,500) to MOP 5 million (~ USD 625,000). Furthermore, when the criminal obtains an economic benefit from the infraction that exceeds half of the maximum limit established under the law, the limit shall be raised to double the amount of the benefit.

A multi-jurisdictional defence

Law enforcement faces significant challenges in combating the misuse of legal entities for ML, particularly when it involves cross-border activities. Criminal networks often employ a tactic known as 'multi-jurisdictional splitting', where they strategically disperse company formation, asset ownership, intermediaries, and bank accounts across different jurisdictions to evade regulations. This fragmentation makes it extremely difficult for authorities in any single jurisdiction to obtain a complete picture of the legal person's misuse, necessitating international information exchange for effective detection, investigation, and prosecution. Further, some jurisdictions struggle with insufficient enforcement against ML offences due to capacity constraints or policy choices. This lack of robust enforcement hinders the accurate assessment of the problem's extent and the identification of emerging trends.

Effective preventive actions and investigations necessitate international cooperation. Utilising both informal and formal channels for cooperation enables timely access to beneficial ownership data from foreign jurisdictions, expediting the investigation process and enhancing the ability to trace, freeze, and ultimately confiscate the proceeds of ML before further dissipation.

A crucial element of the *FATF Recommendations* is for jurisdictions to have a legal basis for international cooperation, and to provide appropriate information, financial intelligence, and evidence and facilitate action against criminals and their assets. Under R. 24, jurisdictions should rapidly, constructively and effectively provide the widest possible range of international cooperation in relation to basic and beneficial ownership information, on legal persons.

United Nations Office on Drugs and Crime - *Implementation of UNCAC chapter IV: International cooperation in ASEAN States parties and Timor-Leste*

This report presents an overview of the challenges and good practices by ASEAN States parties and Timor-Leste in implementing provisions under chapter IV of UNCAC, which covers international cooperation mechanisms such as the extradition, mutual legal assistance, law enforcement cooperation, joint investigations and special investigative techniques. States which did not recognise the criminal liability of legal persons and/or required dual criminality for executing mutual legal assistance requests could face challenges in providing assistance to other States in relation to legal persons.

Overall, implementation is varied in the region, given differences in legal frameworks and existing capacities, experiences in international cooperation, and pre-existing international arrangements. The region received the highest number of recommendations in relation to mutual legal assistance - and while some States were able to afford mutual legal assistance in relation to UNCAC offences committed by legal persons, the ability to do so was less clear for other States.

Case studies

Members contributed the following case studies as examples of how they have applied the components of an effective AML system, including international cooperation to respond to the misuse of legal persons (and one case involving legal arrangements).

Case Study # 15: Money Laundering through shell companies

Fraud; transnational organised crime group; foreign predicate offence

An investigation in Jurisdiction A revealed two criminals conspired with other syndicate members to falsely represented a fund to have good prospects by presenting fraudulent figures and documents, which led to a number of victims to invest in the fund. Over USD 1.63 million was deceived and remitted into the criminals' bank accounts in Jurisdiction A. Authorities eventually arrested the criminals, and the subsequent investigation revealed that they had set up several bank accounts in Hong Kong, China using several shell companies (in the finance and securities industry) for laundering part of the proceeds of crime.

After executing a mutual legal assistance request and repatriating most of the funds back to the Jurisdiction A, in 2023 the Hong Kong Police obtained confiscation order domestically to confiscate the proceeds of crime totalling HKD 2.5 million (~ USD 347,850) remaining in the shell companies' bank accounts.

Source - Hong Kong, China

Case Study # 16: Successful repatriation of funds to Jurisdiction L

Corruption; international cooperation; self-laundering; third party laundering; purchase of real estate; asset recovery

In 2015, the Corrupt Practices Investigation Bureau (CPIB) received information that Company U, an aircraft manufacturer from Jurisdiction X, had engaged an 'adviser' in Jurisdiction L to pay bribes to officials from the national airlines of that jurisdiction to secure contracts for the provision of aircrafts and aftermarket service of the aircraft engines. Investigations identified the adviser to be Person A, those who had allegedly received bribes to be Persons B, C and D, senior executive officials from the stated airlines.

CPIB also received information that all the individuals mentioned have a banking presence in Singapore and that bribes might have been paid and laundered through the Singapore financial system. Funds tracing revealed that Person A had transferred monies to Persons B, C and D by layering through accounts belonging to him or companies beneficially owned by him.

Authorities in Jurisdiction X, Jurisdiction L, and CPIB conducted a joint investigation on the corruption as well as subsequent ML offences.

Seizure of Accounts and Property

CPIB exercised its powers under Criminal Procedure Code and seized 32 relevant bank accounts and a private (real estate) property registered under the name of Person B on 16 January 2017. The purchase price of the property was approximately SGD 2.6 million (~ USD 1.9 million).

Other Information

On 17 January 2017, authorities in Jurisdiction X reached a Deferred Prosecution Agreement (DPA) with Company U. The indictment, which was suspended for the term of the DPA, covered 12 counts of conspiracy to corrupt, false accounting, and failure to prevent bribery. In the DPA, it was stated that the corrupt conduct had spanned three decades and involved several jurisdictions including Jurisdiction L.

In late 2019, authorities in Jurisdiction L obtained the cooperation of Person D to surrender the funds he had remaining in his Singapore bank account to the authorities. CPIB coordinated with the Attorney-General's Chambers (AGC) and the authorities in Jurisdiction L and successfully transferred approximately USD 1.4 million on 3 September 2020 from Person D's Singapore bank account to Jurisdiction L by way of voluntary repatriation of funds.

On 8 May 2020, Persons A and B were convicted on corruption and ML charges in Jurisdiction L. In April 2021, Singapore received a foreign confiscation order from the authorities of Jurisdiction L against the private property. Singaporean authorities are currently working towards obtaining a confiscation order from the High Court to proceed with realisation of the property for repatriation to Jurisdiction L.

Source - Singapore

Case Study # 17: Concealment of assets in Singapore through the use of trusts

Tax crimes; trust and company service providers; use of legal persons and arrangements; International cooperation

In 2015, Singapore's FIU, the Suspicious Transaction Reporting Office (STRO) proactively shared financial intelligence with Jurisdiction X's FIU that Person A was the beneficiary of two trusts incorporated in Jurisdiction Y. These trusts held two bank accounts in Singapore with funds amounting to about USD 700 million. The trustee of both trusts is a foreign-incorporated company (i.e. a corporate trustee).

At the material period of time, Person A was under investigation in Jurisdiction X for alleged tax and ML offences, and it was found that Person A had not declared the two Singapore bank accounts and the related income earned from the trusts in Jurisdiction Y between 2013 and 2016.

Singapore authorities supported these ongoing investigations by urgently processing and sharing voluminous bank records of the Singapore bank accounts with Jurisdiction X pursuant to requests from overseas authorities. This was supplemented by close cooperation between the Commercial Affairs Department of the Singapore Police Force and Jurisdiction X's law enforcement agencies.

In October 2023, Person A was convicted of one count of fraud by false representation. A settlement was agreed between Person A and Jurisdiction X for the sum of about USD 803 million to be paid to Jurisdiction X's government. The payment of the settlement sum was successfully made following close coordination between law enforcement agencies in both jurisdictions.

Source - Singapore

1.5 Common threads

Red flag indicators

Key to a jurisdiction's competent authorities' ability to effectively address ML/TF/PF is having access to quality information that they can act upon. Quality information is information that is detailed, accurate and timely. Access to information can be addressed through effective domestic and international cooperation among competent authorities, and they can improve the quality of information through educating their reporting entities through publishing red flag indicators. Red flag indicators demonstrate or suggest the likelihood of the occurrence of unusual or suspicious activity.

Red flag indicators assist reporting entities understand, identify and report suspicious financial activity to a jurisdiction's FIU, to detect and prevent criminal activities. The FIU can use the reported information to generate actionable financial intelligence that competent authorities can act upon. To that end, a number of members produced red-flag indicators.

Australia's AML/CFT regulator and FIU, AUSTRAC recently redrafted all of its red flag indicator papers[70], while its public/private partnership, the Fintel Alliance continues to publish financial crime guides.

Singapore's central bank and integrated financial regulator, the Monetary Authority of Singapore (MAS) recently published a guidance paper: *Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons*[71]. The guidance paper sets out MAS' supervisory expectations of sound practices, for effective AML/CFT frameworks and controls to address misuse of legal persons risks. In addition, it illustrates a number of case studies and best practices that would be relevant and applicable to other FIs with appropriate tailoring. MAS recommended FIs to study and incorporate the guidance's learning points in a risk-based and proportionate manner, giving proper regard to the ML/TF risk profile of their business activities and customers, including:

- Strengthening FIs detection capabilities, including enhancements to on boarding and ongoing controls.
- Augmenting FIs detection with use of data analytics tools.
- Employing timely, effective risk mitigation measures.

Further, APG's observers have also recently completed significant work with red flag indicators.

The World Bank Group completed a body of work that investigated the misuse of legal persons and arrangements, which identified a number of red flags related to their ownership and control. These indicators are useful those involved in supervisory activities as it helps to identify legal structures that may be more susceptible to ML, thereby target supervisory efforts on these types to ensure compliance and mitigate the risks (inspections / develop guidance). From a law enforcement perspective, understanding the types of legal persons most frequently used for ML enables the development of effective investigative strategies and allocation of resources. Indicators include:

Ownership and control

- Anomalous complex ownership/control structures: complex ownership structures that don't appear to serve any legitimate business purpose but are primarily designed to conceal true ownership.
- Control through power of attorney: use of power of attorney arrangements that are overly broad or lack clear purpose, potentially allowing for control by individuals not readily identifiable.
- Use of trusts or foundations in ownership/control structures: trusts or foundations used in ownership structures, especially if they are located in jurisdictions with weak transparency rules, can obscure beneficial ownership.
- Use of nominee directors/nominee shareholders/"front men": using individuals as directors or shareholders who are not the true beneficial owners, often to hide the identity of the actual controller.
- Use of legal persons as company directors: using legal persons as directors, which can further obscure the identity of the ultimate beneficial owner.
- Use of bearer shares: ownership held in the form of bearer shares, where the person possessing the share certificate is considered the owner, making it difficult to trace ownership.

Red flags related to formation and operations:

- Use of international business companies (IBCs)/exempt companies: using IBCs or exempt companies to avoid registration or disclosure obligations, potentially concealing illicit activity and beneficial ownership.
- Use of fictitious entities: using entities that are not legally formed or registered anywhere, lacking legal personality, to facilitate ML or predicate crimes.
- Use of private investment funds/hedge funds: channelling illicit funds through private investment funds or hedge funds to circumvent AML controls, commit ML, evade sanctions, or invest proceeds of crime.
- Use of large professional firms: using large professional firms (law, accounting, TCSPs, banks) to form or administer legal persons, open accounts, transfer funds, or perform other services, potentially exploiting professional privilege or confidentiality.

[70] AUSTRAC – *Indicators of suspicious activity*: https://www.austrac.gov.au/business/industry-specific-guidance/all

[71] Monetary Authority of Singapore - *Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons*: https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk-from-misuse-of-legal-persons

- Use of fake IDs for formation/registration: providing fake identification documents during the formation process or account opening to evade CDD and ML controls.
- Use of deceptive names of legal persons: intentionally giving legal persons deceptive names to mislead business partners, compliance officers, and others, obfuscating the true nature and beneficial owners.

Red Flags Related to Cross-Border Activities:

- Multi-jurisdictional splitting: splitting company formation, asset ownership, professional intermediaries, and bank accounts across different jurisdictions to evade regulations.
- Links to secrecy jurisdictions: ownership or control links to jurisdictions with weak corporate and financial transparency rules, often associated with opaque offshore structures.
- Exposure to jurisdictions of origin for proceeds of crime: links to jurisdictions known for generating proceeds of crime, suggesting potential involvement in illicit activities.

Additional Considerations:

- Sector involvement: certain sectors, such as real estate, consultancy services, export/import, and offshore activities, may be more prone to ML misuse.

TBML red flag indicators

FATF has systematically completed work on red flag indicators, including ongoing work on TBML red flag indicators. Common TBML indicators include:

- Significant discrepancies appear between the description of the commodity on the bill of lading and the invoice.
- Significant discrepancies appear between the description of the goods on the bill of lading (or invoice) and the actual goods shipped.
- Significant discrepancies appear between the value of the commodity reported on the invoice and the commodity's fair market value.
- The size of the shipment appears inconsistent with the scale of the exporter or importer's regular
- business activities.
- The type of commodity being shipped is designated as high risk for ML activities.
- The type of commodity being shipped appears inconsistent with the exporter or importer's regular business activities.
- The shipment does not make economic sense.
- The commodity is shipped to, or from a jurisdiction designated as high risk for ML activities.
- The commodity is transhipped through one or more jurisdictions for no apparent economic reason.
- The method of payment appears inconsistent with the risk characteristics of the transaction.
- The transaction involves the receipt of cash, or other payments from third party entities that have no apparent connection with the transaction.
- The transaction involves the use of repeatedly amended or frequently extended letters of credit.
- The transaction involves the use of front (or shell) companies[72].

In 2021, FATF published its most recent TBML guidance: *Trade-Based Money Laundering: Risk Indicators*[73] that builds upon these and includes more detailed red flag indicators.

[72] FATF - *Trade-Based Money Laundering*: https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Trade%20Based%20Money%20Laundering.pdf.coredownload.pdf
[73] FATF - *Trade-Based Money Laundering: Risk Indicators*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/Trade-based-money-laundering-indicators.html

1.6 Conclusion

In mid-2024, the heads of the FATF, INTERPOL and UNODC put out a call to action to FATF Member States to urgently step up their efforts to target the huge illicit profits generated by transnational organised crime.[74] A key methodology used by transnational organised crime is the misuse of legal persons.

The *FATF Recommendations* give jurisdictions the tools to effectively combat the misuse of legal persons for ML/TF/PF purposes. The information set out in this chapter attempts to chart the typologies of abuse of legal persons for ML/TF, including the use of professional enablers and individual rights such as privacy protections and legal professional privilege. The analysis supports the critical need for jurisdictions globally to implement the ML/TF/PF risk requirements in R.1, the legal persons transparency requirements set out in R. 24 (and R. 25 for legal arrangements) and international cooperation requirements in R. 40. Contributions from APG delegations also articulate some of the components of an effective AML/CFT/CPF system such as beneficial ownership registers, partnerships with the TCSP sector and international cooperation that jurisdictions can implement to combat the misuse of legal persons for ML/TF/PF purposes.

[74] FATF - *Urgent action needed to fight money laundering and terrorist financing, say Heads of FATF, INTERPOL and UNODC*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/FATF-INTERPOL-UNODC-Call-to-action.html

2 - MONEY LAUNDERING AND TERRORISM FINANCING METHODS

APG members provided the following case studies which we have set out in alphabetical order by reference to the source jurisdiction. Under the title of each case study, we have included relevant accepted terms referring to predicate offences, methods of payment or other context. We further referenced these terms in the index in section 8 of this report.

2.1 Australia

Case Study # 18: More than a billion dollars in fraudulent GST refunds stopped

Tax Crimes; tax or GST refund fraud; use of the internet (social media)

Operation Protego is an Australian Tax Office (ATO)-led investigation into large-scale goods and services tax (GST) refund fraud that was promoted particularly on social media. The ATO announced the launch of Operation Protego on 6 May 2022 to investigate and disrupt the large-scale fraud.

This fraud was first detected in early 2022 and involves offenders inventing fake businesses and Australian business number (ABN) applications, then submitting fictitious Business Activity Statements (BAS) in an attempt to gain a false GST refund. The fraud's promoters used social media and other channels to recruit participants. The ATO referred Operation Protego to the ATO-led Serious Financial Crime Taskforce (SFCT), a domestic multi-agency taskforce, which was established to tackle the most serious forms of financial crime.

To date, the ATO has taken compliance action on more than 56,000 alleged offenders, issued approximately $300 million (~ USD 202 million) in penalties, and stopped approximately $2.7 billion (~ USD 1.82 billion) in fraudulent GST refunds from being paid to individuals seeking to defraud the system. The ATO continues to work with the Australian Federal Police (AFP)-led Criminal Asset Confiscation Taskforce to ensure that illegally obtained funds, and property bought with the proceeds of GST fraud, are forfeited.

Examples of successful prosecutions include:

- Person A reactivated an ABN for a jewellery and silver manufacturing business on 7 February 2022. Between 21 February 2022 and 26 July 2023, Person A lodged 63 fraudulent BAS obtaining $73,650 (~ USD 49,693) that she was not entitled to. Person A also attempted to claim a further $192,983 (~ USD 130,201) in fraudulent GST refunds. Person A was sentenced to one year and eight months imprisonment after being charged with four counts of obtaining benefit by deception.

- Person B lodged fraudulent BAS between 22 October 2021 and 23 November 2021 to claim $834,437 (~ USD 562,976) in GST refunds for a business that did not exist. Person B used most of that sum to purchase a property and a luxury car. Following a plea of guilty to four charges related to 'Obtaining financial advantage by deception', 'Attempt to obtain financial advantage by deception', and 'Deal with the proceeds of crime', Person B was sentenced to seven years and six months' imprisonment with a non-parole period of five years. The Court also ordered Person B to make reparations to the Commonwealth for the sum of $834,437 (~ USD 562,976). In early 2024, Person B appealed the sentence however, a hearing date for the appeal has not yet been set.

- Person C had an ABN which had been registered between 28 March 2009 and 13 February 2015. He then re-registered this ABN on 11 February 2022 with the intent to lodge BAS for a business that did not exist and to claim GST on purchases that were never made. As a result of the false information reported in each BAS, Person C obtained $109,278 (~ USD 73,721) in GST refunds that he was not entitled to. Following a plea of guilty to five charges of 'Obtain financial advantage by deception,' Person C was sentenced to two years' imprisonment, to be released after twelve months upon entering an 18-month good behaviour bond. The Court also ordered Person C to make reparations to the Commonwealth for the sum of $109, 278 (~ USD 73,721).

- Between January and March 2022, Person D lodged fraudulent BAS to claim $282,914 (~ USD 190,771) in GST refunds that she was not entitled to. Person D pleaded guilty to 11 charges of 'Obtain financial advantage by deception' and was sentenced to three years imprisonment, to be released after ten months upon entering a four-year good behaviour bond (subject to a two-year period of supervised probation including mandatory drug/alcohol rehabilitation and gambling courses). The Court also ordered Person D to make reparations to the Commonwealth for the sum of $89,767 (~ USD 60,531).

- Between 17 February 2022 and 28 April 2022, Person E lodged fraudulent BAS to claim $246,463 (~ USD 166,183) in GST refunds he was not entitled to. Person E pleaded guilty to three charges relating to 'Obtain financial advantage by deception', 'Attempt to obtain financial advantage by deception' and 'Attempt to obtain a financial advantage by deception in joint commission'. Person E was sentenced to three years and four months' imprisonment with a non-parole period of one year and nine months. The Court also ordered Person E to make reparations to the Commonwealth for the sum of $180,095 (~ USD 121,436). Note: Person E is intending to appeal the sentence.

The ATO also commenced writing to more than 20,000 individuals involved in the fraud, warning them of the impending serious consequences unless they voluntarily come forward and repay the defrauded money. Further, the ATO has strengthened its controls to prevent this fraud and its treatments of those participating in the fraud.

Source - Australia

Case Study # 19: The fight to stop international organised criminals sexually extorting Australian children

Sexual exploitation, including sexual exploitation of children; use of the internet

In June 2022, Australian authorities commenced Operation Huntsman to target offshore organised criminals sexually extorting Australian children for financial gain. As part of Operation Huntsman, AUSTRAC, the Australian Federal Police (AFP) and the AFP-led Australian Centre to Counter Child Exploitation (ACCCE) partnered together to stop criminal networks, by targeting Australian-based money mule accounts sending money from domestic victims to international syndicates.

Operation Huntsman targeted international criminals who fraudulently claimed to be teenagers, who coerced Australian children into sending them sexualized images, videos and payments online. Once they had the victim's materials, the criminal syndicates then blackmailed the child victims with threats to share their pictures and videos unless they send them money, gift cards, or online gaming credits. In some instances where the victim was unable to pay, they are instructed to become a money mule and open bank accounts to enable the criminals to move the proceeds of crime through these accounts.

To date, Operation Huntsman has disrupted more than 1,000 people operating more than 1,500 Australian bank, financial services and digital currency accounts linked to international organised criminals sexually extorting Australian children.

AUSTRAC is working with financial services providers to obtain hundreds of additional Australian bank and financial services account details with links to international criminals, to take action against hundreds more people facilitating the flow of money out of Australia.

AUSTRAC, ACCCE, AFP intelligence is continuing to target criminals in Australia and internationally, taking away their ability to move money offshore gained through targeting and exploiting Australian children. Further, AUSTRAC and AFP are also continuing to work with domestic and international law enforcement partners on several investigations.

Source - Australia

2.2 Cook Islands

Case Study # 20: Ministry of Social Development fraud

Forgery; obtaining by false pretence; money laundering

In February 2017, the Cook Islands' FIU disseminated an intelligence report to the investigating authority informing them of a potential benefit fraud case. The FIU disseminated the intelligence report following an investigation triggered by an STR from a financial institution in relation to superannuation payments paid to a deceased person's account.

The superannuation payments were coming from New Zealand's Ministry of Social Development, notwithstanding the pensioner recipient had passed away in January 2011, and an administrator/executor appointed in April 2011. The New Zealand's Ministry of Social Development paid the deceased pensioner's account a total of $116,002.32 (~ USD 71,808) until it was suspended in January 2017.

During 2017 and 2018, Cook Islands and subsequently New Zealand authorities conducted investigations into the matter. Jurisdictional issues complicated the matter, required obtaining a legal, and further investigations in relation to potential forgery of legal documents were initiated in 2021.

Ultimately in 2023, two suspects were charged and entered guilty pleas before the High Court of the Cook Islands. The first suspect was a law enforcement officer and the deceased pensioner's nephew. The second suspect was the first suspect's partner. The two suspects admitted receiving and withdrawing the pension funds.

- Suspect 1 was charged with the predicate crime of Forgery and Obtaining by false pretence. Suspect 1 was sentenced to 2 years and 3 months imprisonment and ordered to pay jointly with Suspect 2 the total amount of NZD118,000 (~ USD 73,035) to the NZ Ministry of Social Development.
- Suspect 2 was charged with money laundering. Suspect 2 was sentenced to 9 months' probation and ordered to pay jointly with Suspect 1 the total amount of NZD1118,000 (~ USD 73,035) to the NZ Ministry of Social Development.

As a result of the above prosecution outcome, the Ministry of Social Development has been able to continue its Principal Arrangements with returning Cook Island residents in accessing their superannuation funds and benefits, which were suspended during the police investigation.

Source – Cook Islands

2.3 Hong Kong, China

Case Study # 21: Money laundering through the use of debit cards

Fraud; transnational organised crime group; foreign predicate offence

In early 2023, Jurisdiction A identified over HKD 100 million (~ USD 12.8 million) worth of proceeds of crime from telephone frauds that occurred locally were subsequently dissipated in Hong Kong, China through purchases made with debit cards which held the proceeds of crime. The investigation in Jurisdiction A revealed that a syndicate procured stooges' (third parties') personal bank accounts with linked debit cards and instructed the victims to deposit funds into those stooge accounts. Shortly after the victims deposited the funds, the syndicate coordinated its members to use the physical debit cards in Hong Kong, China to purchase high-value goods.

The Hong Kong Police intercepted the nine syndicate members in the act of conducting transactions with the stooges' debit cards. The Hong Kong Police seized the stooges' debit cards together with luxury watches and other valuables. Investigation into the case is ongoing.

Source - Hong Kong, China

Case Study # 22: Laundering of the proceeds of crime via cryptocurrency

Third party laundering; fraud; foreign predicate offence

In 2022, intelligence disseminated between two LEAs suggested people controlling a group of suspicious bank accounts (of individuals) in Hong Kong, China had made frequent ATM cash withdrawals after receiving proceeds of crime originating from local and overseas frauds. During the offence period, the people controlling the accounts had laundered over HKD 111 million (~ USD 14.2 million) of suspicious funds. The subsequent investigation identified a local money laundering syndicate had utilized the stooge accounts to dissipate the proceeds of crime. Once the proceeds of crime were remitted into the accounts, the syndicate immediately tasked their members to make withdrawals at ATMs. Through this methodology, the syndicate accumulated a large cash lump sum, which they then used to purchase cryptocurrency in an effort to conceal the origin of the funds. In total, the Hong Kong Police arrested 10 syndicate members. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 23: Cold call loan fraud employing bogus websites

Loan fraud; third party laundering

Between September 2022 and October 2023, a criminal syndicate defrauded 49 victims in Hong Kong, China though cold calls promoting low interest loans. The victims were directed to bogus websites under the presence of licensed money lenders and were asked to transfer a total of HKD 15.3 million (~ USD 2.128 million) to 111 local bank accounts (of individuals) as guarantee fees to facilitate their loan applications. None of the victims received any loans. The investigation led to the arrests of 14 individuals

including the web host subscriber of the bogus websites and stooge account holders. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 24: Cross-border scam syndicate

Romance scam; investment fraud; compensated dating scam; employment fraud; third party laundering

In early 2023, an arrest operation in Jurisdiction A unveiled a naked-chat syndicate operating a scam centre that had a nexus with a money laundering syndicate in Hong Kong, China, which involved 149 scam cases with a total loss of HKD 68.2 million (approx. USD 8.7 million). Jurisdiction A referred intelligence to the Hong Kong Police, and the investigation identified five core members in Hong Kong, China who operated various stooge bank accounts (of individuals) for receiving and laundering the proceeds of crime from the scams. The Hong Kong Police arrested nine stooge account holders who sold their bank accounts to the syndicate and one SIM card subscriber whose SIM card was used by a fraudster to communicate with victims. Two stooge account holders were prosecuted and convicted for "Conspiracy to deal with property known or believed to represent proceeds of an indictable offence". The investigation against the remaining arrestees is ongoing.

Source - Hong Kong, China

Case Study # 25: Instant messaging app hijacking fraud

Third party laundering; fraud

Between October and November 2023, a local fraud syndicate deceived 326 local victims into transferring a total of HKD 3.96 million (~ USD 550,995) to stooge bank accounts by impersonating victims' relatives or friends via hijacking their instant messaging accounts. Fund flow analysis revealed that the proceeds obtained from victims were transferred to a total of 18 virtual bank accounts (of individuals) held by 10 stooges and further investigation showed that multiple stooge accounts were controlled by the same IP address. An arrest operation was conducted with 13 syndicate members arrested. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 26: Money laundering through stored value facility (Note: the term 'facility' includes products such as e-wallets and pre-paid cards etc.)

Third party laundering; fraud

Between November and December 2023, a total of 143 victims reported that they had received phishing SMS purportedly sent by a stored value facility (SVF), which requested them to access to a bogus website and input the login credentials of their SVF wallets or credit cards for redemption of rewards. After complying with the instructions, the victims soon discovered unauthorised money transfers to other bank accounts/transactions were made from their SVF wallets or credit cards, which totalled HKD 680,335 (~ USD 94,662) of losses. Authorities took down a total of 71 bogus websites that surfaced from the scams. In December 2023, two culprits who took over victim's accounts, and five stooge bank accounts holders were arrested. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 27: Deepfake video scam

Fraud; use of online applications; third party laundering

Between September 2022 and July 2023, a local loan fraud syndicate used stolen or forged identity cards of victims and exploited 'Deepfake' technology to bypass facial verification in applying loan or bank accounts in 144 occasions. The loan fraud syndicate successfully applied for four loans totalling HKD 200,000 (~ USD 25,670) and five bank accounts, and the fraudulent loans were transferred to various stooge accounts (of individuals). In August 2023, the operation turned overt with eight syndicate members including the mastermind arrested for 'Conspiracy to cheat and defraud'. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 28: Online casino hosted overseas

Illicit gambling; use of virtual assets; third party laundering

Intelligence suggested that an illegal gambling website hosted in Jurisdiction A had actively promoted online gambling to Hong Kong, China citizens by sending spam messages through a social media platform. The message stated that registered gamblers are required to acquire gambling credits by bank transfer or cryptocurrency and 5% of game credits would be charged as commission for each win. The investigation identified that the syndicate members were actually controlling the platform through local operating centres and using stooge account for top-up or cash-out of gambling credits in Hong Kong, China. Eventually, 32 Hong Kong, China citizens were arrested for "Conspiracy to Engage in Bookmaking" and 15 were arrested for "Conspiracy to Money Laundering" in late August 2023. Between October 2022 and July 2023, the syndicate laundered a total of USD 38.5 million with an estimated betting amount of USD 3.3 million per month.

Source - Hong Kong, China

Case Study # 29: ML syndicate engaging cash couriers

Cross-border cash couriers; organised crime

Through proactive analysis of declarations of cross-boundary movements of currency and bearer negotiable instruments after the full resumption of travel in early 2023, the Hong Kong, China Customs uncovered a ML syndicate engaging cash couriers to launder about HKD 700 million (~ USD 89.7 million) between May and June 2023. Since January 2023, Hong Kong, China Customs identified that a ML syndicate recruited cash couriers to bring in large quantities of US dollars into Hong Kong, China. During the Customs clearance process, the cash couriers declared that they were employees of two companies in Jurisdiction A and they carried the cash to source jewels and diamonds in Hong Kong, China. Upon investigation, the cash couriers were unable to provide any details of the purchases, while intelligence exchange with Jurisdiction A via Egmont Group revealed that the two companies were not engaged in the jewels and diamonds trade. In May 2023, Hong Kong, China Customs smashed the ML syndicate by arresting 23 people and seizing HKD 43 million (~ USD 5.5 million) of suspected proceeds of crime in cash. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 30: Residential premises as an operation centre

Standalone money laundering; suspicious transaction reporting

Upon analysis of STRs received from a local bank, the Hong Kong, China FIU identified an ML syndicate operating multiple bank accounts at various local banks, and frequently retrieving cash from an unwitting money service operator to deal with suspicious funds of about HKD 6 billion (~ USD 767 million) from various suspicious counterparties between 2020 and 2022. The investigation revealed that the ML syndicate rented a residential premises at a large private housing estate to camouflage the operation of their ML activities. In January 2023, the Hong Kong, China Customs arrested nine people for ML and seized a total of HKD 3.9 million (~ USD 500,000). The investigation is ongoing.

Source - Hong Kong, China

2.4 India

Case Study # 31: Money laundering with shell companies

Fraud including phone/sms/email/social media; self-laundering; new payment method; use of legal persons and arrangements

In January 2021, following the filing of a first information report with the police of the State of Hyderabad and subsequent searches, the police unearthed a network of persons and mobile applications engaging in micro-lending at exorbitant rates. The mobile applications were operated by foreign individuals through a web of shell companies in India. These mobile applications provided loans to victims at high interest rates, while also collecting personal data of victims from mobile phones, using the personal data to blackmail victims and recover the loan amount with interest. The modus operandi involved:

- Foreign individuals incorporated shell companies in India to receive money from their home jurisdiction. These companies had both foreign and locally hired Indian directors.
- These shell companies then entered into a memorandum of understanding (MoU) with non-banking financial companies (NBFCs) in India. Under the MoU, they provided security deposits to NBFCs which in turn opened multiple Merchant IDs with payment gateways which allowed the shell companies to run mobile applications. Such applications were listed on major mobile app stores.
- Loans were provided through the app, and recovery was done through the app/payment gateway and transferred back to the shell companies by the NBFCs through the Merchant IDs after deducting a commission.

The ML investigations resulted in attachment/seizure of INR 7.8 billion (~ USD 93 million) as well as prosecution against 521 (legal and natural) persons. The investigations are ongoing.

Source - India

Case Study # 32 Terrorism financing investigation on the basis of a suspicious transaction report

Terrorism, including terrorist financing; trade-based money laundering; use of legal persons & arrangements

In June 2020, India's National Intelligence Agency (NIA) received a suspicious transaction report (STR) from the Financial Intelligence Unit - India regarding Person A. A financial institution (FI) filed the STR on the basis of adverse media reports and irregular transaction patterns where Person A operated a business account with only cash withdrawals and no business transactions. The FI shared details of his other accounts along with identifiers in the STR.

The STR initiated an investigation into Person A's business activities (and others), which led to the NIA uncovering a number of terrorist financiers. These terrorist financiers were involved in under-invoicing that created a trade imbalance, and generated profits that they used to support the sustenance and operations of terror organisations of the Hizbul Mujahideen and Lashkar-e-Tayyiba. The terrorist financiers were involved in the generation and distribution of funds for the terrorist organisations, but not directly involved in terrorist activity. They are currently facing prosecution for TF charges under the *Unlawful Activities (Prevention) Act, 1967*.

Source - India

2.5 Indonesia

Case Study # 33: State financial loss from bribery

Corruption and bribery; mingling; financial institutions

The convicted legal person (Company X) was appointed as a supplier of goods/services for a project for City Z Government, in the fiscal year of 2014. The contract value amounted to USD567,000. The project was to be completed between April 1, 2014, and December 1, 2014. The project works were not carried out in accordance with the contract term, yet Company X received full payment before completing its obligations under the contract. An audit discovered that some of the tender documents submitted in the Government procurement process were fake qualification documents.

The audit report found the actions of the defendant as a supplier of goods/services in the project had enriched Company X and harmed the state finances in the amount of USD236,000. The money obtained from such criminal acts of corruption had been transferred/incorporated by the goods/services user to the account of the defendant Company in Bank C, so that the funds were co-mingled with money already saved in the account with the aim of concealing and disguising the origin of the assets originating from the corruption crime. Company X was charged with corruption and money laundering and was fined USD47,000.

Source - Indonesia

Case Study # 34: State financial loss from bribery

Corruption and bribery; co-mingling; financial institutions; politically exposed persons

The defendant, Company B, and two affiliated companies were beneficially owned and controlled by a public official Person A (a PEP). Person A used Company B as a front to collect bribes from government

project partners and to receive profits from government work projects where Person A regulated the procurement process. During 2016 and 2017, Person A co-mingled Company B's funds with accounts of the affiliated companies and then withdrew it for Person A and his family's benefit. The authorities' investigation into Company B examined its deed of establishment, articles of association and amendments, power of attorney for the company's checking account and bookkeeping records, and its financial transactions. The investigation showed that even though an employee was legally appointed to control Company B, Person A was in fact its controller and beneficial owner.

The defendant, Company B, was convicted of money laundering and fined USD3,145 and additional punitive damages of confiscation of corporate assets to the state amounting to USD226,000 and USD144,000, and banned from bidding in the procurement of government goods and services for three years.

Source - Indonesia

Case Study # 35: Money laundering and fraud via fake foreign currency trading

Fraud; self-laundering; mingling; virtual asset service providers; use of virtual assets (cryptocurrencies or other virtual assets); purchase of real estate

Person X registered on the website "Y" in 2018. "Y" is a game where the player chooses a commodity and bets on whether the commodity will go up or down in value during a chosen time period. One of the commodities is foreign currency. If the player's choice is correct, they receive a profit of 80% on the bet amount, whereas if they are wrong, the player loses 100% of the bet amount.

Person X then became an affiliate of "Y". Affiliates can invite prospective players to register at "Y". Affiliates receive benefits in the form of payments based on a percentage of revenue sharing. Person X created educational videos about "trading" on "Y" which he posted on his YouTube channel, Instagram and Telegram accounts to promote registration with "Y" via his referral link.

To further convince the public that the "Y" game was really a "trading platform", Person X also founded Company Z which operates in the education sector. Person X was the director and majority shareholder. Company Z's activities included Person X opening classes or training by selling educational services where he provided information in the form of videos related to crypto trading, stocks, financial education and video games. Company Z asked course participants to pay a course fee of USD 94 to 125 per year, per person and by the beginning of 2022, the trading course had attracted approximately 3,000 participants.

Through his social media, Person X made a number of false assertions, such as; "it is trusted" and "Y is already legal in Indonesia" and "Y is official in Indonesia in 2015 and it has been 4 years" even though in reality "Y"'s activities were neither legal nor official in Indonesia because it had not received permission from the Commodity Futures Trading Supervisory Agency (BAPPEBTI). As a result of Person X's actions, 144 people suffered losses of around USD 5.2 million.

As a "Y" affiliate, Person X received profits from "Y"'s profit sharing, which were paid through his bank accounts, several virtual account payment gateways and via crypto digital assets such as Bitcoin, Ethereum and others contained in his account, or in the name of another person. Between June 2020 and January 2022, Person X received cryptocurrency into his VASP account in Bitcoin and Ethereum, amounting to 105 transactions totalling 395 BTC. Person X withdrew Bitcoin which was disbursed to a bank account amounting to USD 6.5 million. From the affiliate's profits, Person X purchased several assets in the form of houses and land, luxury goods in the form of luxury cars and watches, and transferred the money to his family, his girlfriend and her family, other third parties, Company Z (his company) and Company B (another company in which he is a director).

Person X has been proven legally and convincingly guilty of committing the criminal act of spreading false and misleading news which resulted in consumer losses in electronic transactions, and money laundering. Person X was sentenced to 10 years' imprisonment and a fine of USD 615,000 with the provision that if the fine is not paid it will be replaced by an additional term of imprisonment for ten months.

Source - Indonesia

Case Study # 36: Pharmaceutical company fraud

Fraud; COVID-19

Person C was the Business Manager of a pharmaceutical company, Company K, which provided Rapid Antigen Test screening (for Covid-19) at the airport. Person C ordered several employees to reuse Dacron swabs and tubes. The profit generated from re-using the equipment totalled approximately IDR 2.2 billion (~ USD 137,500). To cover up his illegal actions, Person C also ordered his employees to manipulate reports on the results of the Covid-19 Antigen Swab Rapid Tests by reducing the number of test results

reported to relevant agencies. Person C used the profits from his illegal actions for his personal gain and placed the money in several accounts, including those of his employees which he controlled. Authorities charged Person C with violations of health laws, consumer protection laws, and money laundering, and he was sentenced to imprisonment for ten years and a fine of IDR 1,000,000,000 (~ USD 65,208). Authorities confiscated the proceeds of crime, including funds held in third persons' bank accounts.

Source - Indonesia

Case Study # 37: Terrorism financing with loans from bank and online loans

Terrorism, including terrorist financing; financial institutions

In 2019, the police conducted a search on Person B's house and found that Person B obtained loans from Bank X and several fintechs (online loans/peer to peer lending) ranging from USD37 to USD628, and totalling USD1,000. Person B used these funds for terrorist group purposes (organisation funds and giving to members) and a terrorist act (buying weapons to be used in a terror act), and he used USD 314 for personal interests.

Source - Indonesia

2.6 Japan

Case Study # 38: Concealing the proceeds of crime from an international romance scam as proceeds from a car sale

Fraud; third party laundering; financial institutions; suspicious transaction reporting

Japan's FIU (JAFIC) analysed information in numerous suspicious transaction reports using key phrases such as "after a small amount of money was suddenly deposited in a long-term inactive account, a large amount of money was transferred from multiple accounts". In one case, JAFIC found that the money transferred to Person A was proceeds from international romance fraud and investment fraud. The police investigated the case and found that Person A deposited the proceeds of crime into a company bank account by falsely claiming it was the proceeds of a car sale. The police arrested Person A for fraud and violation of the Act on Punishment of Organized Crimes and Control of Proceeds of Crime (concealment of criminal proceeds).

Source - Japan

Case Study # 39: Smuggling of methamphetamine by remittances to high-risk jurisdictions

Drug related crime; smuggling; financial institutions; wire transfer; suspicious transaction reporting

The police launched an investigation based on suspicious transactions reports delivered by financial institutions, which contained key phrases such as "sending money from multiple branches on the same day to jurisdictions with a high risk of fraudulent remittances" and "applying for foreign remittances under the direction of a companion," as well as information about suspicious imported packages. As a result of the investigation, the police identified a group of suspects of multiple nationalities who imported methamphetamine from foreign jurisdiction. The police arrested the suspects for violating Act Concerning Special Provisions for the Narcotics and Psychotropics Control Act, and Other Matters for the Prevention of Activities Encouraging Illicit Conducts and Other Activities Involving Controlled Substances through International Cooperation (joint possession).

Source - Japan

Case Study # 40: Selling counterfeit brand-name goods using flea market apps

Counterfeiting and piracy of products; self-laundering; financial institutions; new payment method; suspicious transaction reporting

Japan's FIU analysed information in numerous suspicious transactions identified using key phrases such as "transfers from multiple flea market apps are transferred to individuals via Internet banking, and the purpose of use of the account and the transaction status are discrepancies," and where it suspected that an individual was selling counterfeit brand-name goods. The police investigated and found Person A was selling counterfeit brand-name goods and received bank cards from Person B. The police referred Person

A to the public prosecutor for violating Trademark Act and the Criminal Proceeds Act (gratuitous receiving).

Source - Japan

Case Study # 41: Transfer of criminal proceeds to a foreign jurisdiction by crypto assets

Fraud; third party laundering; VASP; use of virtual assets; suspicious transaction reporting

Japan's FIU analysed key phrases in suspicious transactions reports, such as "depositing a large amount of cash at an ATM and then transferring funds to a foreign jurisdiction through a specific crypto asset exchange company" and "the account holder is a party to the fraud case."

Japan's police service investigated and after Person B notified them of a delivery location for the fraudulently obtained money, they identified Person A as the person who received it. Person A let the clerk of his store (who was unaware the funds were fraudulently obtained) receive the money, Person A then exchanged the money for crypto assets and transferred the funds to a foreign jurisdiction. Japan's police arrested Person A for violating Act on Punishment of Organized Crimes and Control of Proceeds of Crime (receipt of criminal proceeds).

Source - Japan

Case Study # 42: Concealment of fraud damage using electronic money

Fraud; third party laundering; financial institutions; new payment method

Person B, a member of a fraud syndicate phoned a victim and defrauded them into handing over their bank card. Person A (another member of the syndicate) then withdrew cash from an ATM machine using the bank card. Person A then purchased electronic money using a portion of the cash, and transferred the right to use the electronic money to Person C, by sending an e-money usage code number to Person C's account via Telegram. Japan's police service arrested Person A for violating the Organized Crime Punishment Act (concealment of criminal proceeds, etc.).

Source - Japan

Case Study # 43: Computer fraud using remote control apps and concealment of proceeds of crime

Fraud; self-laundering; financial institutions

Person A displayed a fake IT security message on Person B's computer screen, which prompted Person B to call the phone number displayed. Person A took the phone call, introducing himself as a worker for the IT Security company. Person A forced Person B to download a remote-control application and enter his ID and password for his internet banking. Person C (who managed an account in the name of a third-party individual) received a unauthorised funds transfer from Person B's account and was arrested for violating the Organized Crime Punishment Act (concealment of criminal proceeds, etc.).

Source - Japan

Case Study # 44: Receipt of bank cash cards for debt forgiveness

Fraud; financial institutions

Person B owed Person A money, so Person B opened a bank account and deposited the amount of money he owed and gave Person A the cash card linked to the bank account. Person B gave Person A an undertaking that he would not use the bank account, thus repaying the debt to Person A. Japan's police arrested Person A for violating the Organized Crime Punishment Act (receipt of criminal proceeds, etc.).

Source - Japan

2.7 Korea

Case Study # 45: Trade-based money laundering via shell company

Tax crimes; trade-based money laundering; wire transfers; use of credit/debit cards; purchase of real estate

The Korean Customs Service detected suspicious activity by Company A through the collection and analysis of financial transactions and trade records. Company A, based in the Republic of Korea, was involved in the business of exporting pharmaceutical packaging materials. Company A established a shell company - Company B in another jurisdiction (Jurisdiction C) and deceived the Korean Customs Service by falsifying its records to make it appear as if shell Company B was facilitating its trade. Company A exported USD $14 million worth of products directly to Jurisdiction D but only declared the value as USD $12 million.

Company A diverted USD $2 million to Company B in Jurisdiction C. These diverted profits were then laundered back to the Republic of Korea via small transfers through 40 undisclosed accounts (accounts used to hide the activity from Korean authorities) and by withdrawing it in cash via ATMs. The 40 accounts were in the name of other people (such as their acquaintances), and not in the criminal's own name.

Through this falsification of trade profits, Company A evaded paying taxes. During the investigation, Korean authorities also discovered that a representative of Company A had also used some of the diverted funds to purchase real estate (an apartment).

In January 2023, Korean authorities prosecuted Company A under the Korean Republic's customs laws, and laws related to concealing criminal proceeds. Korean authorities also filed an application for provisional attachment against the representative of Company A's apartment before the prosecution, to prevent its disposal. The prosecution is ongoing.

Source - Korea

2.8 Macao, China

Case Study # 46: Corruption and money laundering by ex-government officials and businessmen

Corruption and bribery; abuse of power; politically exposed persons; third party laundering; real estate; wire transfer; company shares

While serving as government officials of Macao, China, Persons A and B abused their power to assist property developers C, D and E in the vetting and approval of local construction projects and they gained an illegal and improper advantage. As a reward, the property developers C, D and E, paid Persons A and B unlawful bribes through the sale and purchase of immovable properties at below/above market price values, transferred shares in jointly established companies, and obtained benefits by other persons. During this process, Persons A and B, were aided by their accomplices and family members, who received and disposed of the relevant unlawful advantages in an obscure manner to conceal the illegal nature and source of the assets.

In 2022, the Public Prosecutions Office of the Macao, China charged Persons A and B, and property developers C, Dand E and the rest of their criminal associates with offences such as accepting bribery for illicit acts, offering bribery, and money laundering. In 2023, after the trials in the Court of First Instance and the Court of Second Instance of Macao, China, Persons A and B, and property developers C, D and E and others were convicted of the offences and sentenced to imprisonment ranging from several to 20 years.

Source - Macao, China

Case Study # 47: Laundering of drug-trafficking proceeds through new electronic payment method

Drug-related crime; self-laundering; third party laundering; cash; wire transfer; use of debit cards; new payment method

In 2021, Persons A and B were instructed to engage in drug trafficking activities in Macao, China. To conceal and disguise the proceeds of crime gained from this, they were asked to arrange a bank account to receive payments. Person B later negotiated with Person C to use their bank account to receive money transfers from drug buyers.

After withdrawing the proceeds of crime using the debit card linked to his account, Person C then transferred the proceeds of crime to Person A, either in cash or through other electronic payment

platforms. Person A then approached a staff member of a pawnshop to transfer the proceeds of crime to the drug suppliers in Jurisdiction D through overseas mobile payment service of a messaging application.

The Public Prosecutions Office of the Macao, China charged Persons A, B and C with money laundering offences in 2023, while Persons A and B had already been convicted by the Court of First Instance of Macao, China for drug trafficking and related offences in 2022.

Source - Macao, China

Case Study # 48: Illegal gambling syndicate apprehended for organised crime, fraud and money laundering

Transnational crime syndicate; illicit gambling; fraud; third party laundering; structuring/smurfing; casinos; cash; virtual assets (cryptocurrencies)

In January 2023, the Judiciary Police cracked down a trans-border criminal syndicate which had been operating illegal online gambling platform in China, Macao, China and Chinese Taipei. The illegal online gambling platform offered multiple gaming accounts and various online betting options with backend servers located outside Macao, China. The members of the syndicate or its subordinate agents solicited the patrons.

The syndicate laundered proceeds of crime gained from online gambling through stooge accounts or cryptocurrencies. In addition, the syndicate transferred proceeds of crime of approximately USD 3.5 million to the members' bank accounts at the same time the funds were being transferred to China through smurfing. The Judiciary Police seized approximately USD 1.3 million in cash during the operation and subsequently charged several suspects for the offences of criminal syndicate, illicit gambling and money laundering and passed the case to the Public Prosecutions Office.

Source - Macao, China

Case Study # 49: Three local suspects apprehended for money laundering, criminal syndicate and fraud in felony

Phone fraud; self-laundering; third party laundering; financial institutions; cash; use of debit cards; regional cooperation; purchase of high value products

In June 2023, the Anti-Fraud Coordination Centre of the Judiciary Police received intelligence that the criminal proceeds of USD 190,000 related to a telecom fraud case in China was transferred to Macao, China and they launched an investigation forthwith.

According to investigation, the syndicate laundered the proceeds of crime first by using overseas bank cards and then using those cards to purchase luxury items at jewellery shops in Macao, China with the transaction amount totalling over USD 90,000. The Judiciary Police was capable to identify those members at jewellery shops and notified immediately the law enforcement agency in China. The police officers in China arrested those members the following day. In addition, the Judiciary Police successfully intercepted three other suspects and seized approximately USD 93,000 and a vehicle. The Judiciary Police charged the three suspects for the offences of criminal syndicate, fraud and money laundering and passed the case to the Public Prosecutions Office.

Source - Macao, China

Case Study # 50: Two suspects arrested for virtual currency fraud and money laundering

Fraud; self-laundering; casinos; virtual assets service providers; cash; use of virtual assets; regional cooperation

The Judiciary Police received intelligence as well as request for assistance from the neighbouring jurisdiction which related to a huge fraud case using virtual currency trading platform.

They immediately launched the investigation, and the further information revealed that the virtual currency trading platform was falsely claiming to be a legitimate licensed company with multiple over-the-counter currency exchange locations. To attract investors, the platform also hired high-profile celebrities for its publicity campaign on the internet where it claimed to provide unreasonably, high returns on investment. However, the virtual currency issued by that platform could not be traded over-the-counter due to its extremely low liquidity. In addition, the platform charged investors handling fees for withdrawals which could be altered at any time. As a result, the investors filed to retrieve their capital. According to the law

enforcement agency from the neighbouring jurisdiction as of September 2023, there were over 2,000 victims filed a police record which involved approximately USD 190 million in funds.

After investigation, the Judiciary Police identified two suspects related to the case located in Macao, China with possession of approximately USD 830,000 in the form of gaming chips and USD 9,000 in cash. The Judiciary Police later froze the suspects' casino front money account which had approximately USD 1 million in it.

Despite refusing to disclose any details, the Judiciary Police found the two suspects were the core members of the fraud case involving in the virtual currency trading platform and they used the casino front money account to transfer, conceal and launder the proceeds of crime. The Judiciary Police charged the two suspects for the offences of criminal syndicate, computer fraud and money laundering and passed the case to the Public Prosecutions Office.

Source - Macao, China

Case Study # 51: Illegal gaming operations and money laundering through legitimate junket operations

Criminal syndicate; illegal gaming operations; under-table bets; overseas on-line casinos; fraud; triad; junkets

In November 2021 and January 2022, a law enforcement agency arrested two businessmen for two criminal cases in Macao, China, together with numerous associates, including some high-position employees of junket companies. The two businessmen were the owners of two large junkets in Macao, China and accused of utilising the legitimate licensed junket businesses to operate illegal gaming. This illegal gaming included under-table bets utilising legal table gaming results in Macao casinos, and overseas online casinos utilizing the existing junket company resources (employees, front money accounts and client base) in Macao, China.

The two businessmen utilised junket-operated front money accounts, gaming credits, companies (legal persons) in Macao, China and overseas and bank accounts as vehicles to transfer proceeds of illegal gaming.

Between January 2023 and January 2024, the two junket owners were convicted by the Courts of Macao, China for 18[75] and 13[76] years' imprisonment respectively, for operating illegal gaming (side-table betting and overseas online casinos) and leading triad criminal syndicates, as well as the conviction for the aggravated offence of money laundering.

Source - Macao, China

2.9 Malaysia

Case Study # 52: Criminal breach of trust and activity money maundering by misusing non-profit organisation

Corruption and bribery; self-laundering; fraud; criminal breach of trust; abuse of non-profit organisations

The Malaysian Antti-Corruption Commission (MACC) charged Persons A, B, and C with 164 charges involving money laundering, fraud, and criminal breach of trust worth approximately MYR39.5 million (~ USD 8.2 million).

Persons A and B, both involved in managing a non-profit organisation (NPO) and serving as directors of Company A, were entrusted with managing the NPO's assets. Allegedly, they misused approximately MYR20.9 million (~ USD 4.4 million) belonging to the NPO, which was derived from public donations of which, the donation did not go to the intended recipients.

For this purpose, Persons A and B were each charged 52 counts of criminal breach of trust for the transfers conducted via a bank between 2018 and 2023. They are also jointly charged with 19 counts of cheating by deceiving the NPO's Board of Trustees into handing over MYR39.1 million (~ USD 8.1 million)

[75] In January 2023, the junket owner in the first criminal case was sentenced for 18 years of imprisonment. Source: Court of First Instance of Macao China, Case No CR2-22-0147-PCC, https://www.court.gov.mo/sentence/zh-9f8cd198757f3527.pdf
In October 2023, the Intermediate Court agreed with the advice of the Public Prosecutions Office to convict the junket owner for ML crime. The term of sentence remained unchanged with the ML charge. Source: Intermediate Court of Macao China, Case No. 162/2023, https://www.court.gov.mo/sentence/zh-6baa9952c1a81882.pdf

[76] In April 2023, the accused junket owner in the second criminal case was initially sentenced for 14 years of imprisonment. Source: Court of First Instance of Macao China, Case No. CR1-22-0166-PCC, https://www.court.gov.mo/sentence/zh-27669220ca401221.pdf
In the first appeal, the Intermediate Court of Macao reduced the term of imprisonment to 13 years in January 2024. Source: Intermediate Court of Macao China, Case No. TSI-461/2023, https://www.court.gov.mo/sentence/zh-aae7e384f7a73fda.pdf

in cash to Company A as a broker for the purchase of gold, whereby the purchase price was inflated higher than the market price. Persons A and B also each faced 19 separate money laundering charges as directors of Company A for allegedly using MYR12.8 million (~ USD 2.7 million) to purchase luxury vehicles, shop lots, warehouses, and land. It appears the money laundering activities only happened domestically with no indication of money laundering activities being carried out overseas.

Meanwhile, Person C, who is also a director of Company A, was charged with three charges of using the proceeds of illegal activities involving MYR6 million (~ USD 1.3 million) as payment for the purchase of a purchase shop lots and warehouses. The case is ongoing.

Source - Malaysia

Case Study # 53: Fraudulent pyramid scheme and unlicensed e-money services

Investment fraud

Company A set up a group of subsidiary companies and conducted a direct sales business using electronic transactions, without a valid license issued by the Controller of Direct Sales. It promoted a pyramid scheme where members would receive commissions or other benefits through direct sales of membership packages and recruitment of new members into the scheme as their downlines.

At the same time, Company A actively promoted their e-wallet application where users purchased Ringgit Malaysia-denominated 'vouchers' that can be used for the purchase of goods or services at registered merchants. Company A encouraged usage of their e-wallet by offering bonus vouchers to users who purchased vouchers during promotional periods. These bonus vouchers could also be redeemed in exchange for goods and services at registered merchants. Company A promised users they would be able to withdraw their unused purchased vouchers at any time.

The public started to lodge complaint reports to various regulatory and law enforcement agencies when Company A stopped enabling users to withdraw their purchased vouchers. In reality, Company A had closed its company and subsidiaries' bank accounts after suspected probing by law enforcement agencies on its operations. Despite being a relatively new setup, Company A's accounts showed extremely high transaction volumes with various counterparties and aggregated billions of transaction amounts. Authorities charged Company A and its directors for conducting direct sales business using electronic transactions without a valid license, promoting pyramid schemes, and money laundering. The case is ongoing.

Source - Malaysia

2.10 Maldives

Case Study # 54: Real estate fraud

Fraud; misuse of corporate vehicles; document forgery; tax offences; layering; structuring; real estate

Following media reports of Person A conducting fraudulent real estate activities in Jurisdiction A, the Maldives FIU conducted an analysis of their financial activities, their associates and the legal entities they used in the fraud. The FIU observed that Person A had collected large amounts of funds from various individuals as advance payment against sale of luxury apartments Company A was developing. Person A is a minority shareholder in Company A, who also forged company documents that enabled them to operate the company's bank accounts. In addition to the bank transfers from Company A to Person A's accounts, Person A collected funds from buyers in cash as well as in bank transfers. Person A is also purported to have sold an apartment to one buyer, and then sold the same apartment to additional buyers. He defrauded all of these buyers by making them pay advance payments in cash directly to him, and not Company A. Person A also formed various other companies and Company A's funds were layered and funnelled through those companies as well as through other associates.

The FIU's analysis of financial records and other information identified that Person A used the funds to buy other properties in the Maldives as well as in Jurisdiction B. In addition, Person A used some of those funds to buy luxury items. The FIU successfully traced those properties and luxury items of high value and provided information to the law enforcement agencies for investigation and prosecution. The law enforcement agencies prosecuted Person A and one associate for money laundering and associated predicate offences. Law enforcement agencies also seized the traced assets in the Maldives and Jurisdiction B, and together with the Prosecutor General's Office are currently working on seizing Person A's property in Jurisdiction B.

Source - Maldives

Case Study # 55: Misuse of non-government organisation

Misuse of NGO funds; illegal foreign exchange; abuse of authority; tax offences; layering; structuring

The Maldives FIU's analysis of financial records and other information of a prominent local non-government organisation (NGO) identified that Person A - the President of that NGO misused NGO funds to enrich himself by purchasing real estate. He also used some of the NGO funds for personal business investments. Person A misused his authority as the President of the NGO to falsify documents under the guise of USD sale transactions to disguise the true purpose of the funds. The FIU traced the real estate purchased, transactions related to business investments and transactions related to personal expenses.

After investigation by the relevant law enforcement agency, the Prosecutor General's Office is preparing to charge Person A for money laundering and associated predicate offences regarding the real estate. The Prosecutor General's Office has already charged Person A for money laundering and illegal foreign exchange and the case is currently ongoing at the Criminal Court.

Source - Maldives

2.11 Pakistan

Case Study # 56: Off-shore loan facility fraud

Fraud; tax evasion

The regulator of companies, the Securities & Exchange Commission of Pakistan (SECP) examined the annual audited accounts for three financial years and related quarterly accounts pertaining to Company A Limited and found that the accounts for the years 2018 and 2019 were prima facie materially misstated. The matter was reported to the Financial Monitoring Unit Pakistan (FMU) as a suspicious transaction report.

During a three-year period, Company A Limited and its directors and shareholders maintained 10 accounts with different banks having aggregate credit turnovers of PKR 1.50 billion (~ USD 5.4 million). The funds were mainly credited to the accounts of directors and associated businesses (sister concerns) and no business-related transactions were carried through these accounts.

In 2012, Company A received USD 1.1 million from an offshore company, Company B as advance money towards share application money. Later, Company A did not issue shares to Company B, and Company A converted the money into long term financing. However, at the year ended June 2019, the principal amount worth USD 1.1 million and interest of USD 60,000 were written off/written back without any due consideration being given and by just providing a notice that the investment company has closed its business.

Similarly, in 2016, Company A obtained a loan of USD 500,000 against a loan facility of USD 1 million from another offshore company, Company C. Then again, in the year ended 2017, it also received the remaining amount of USD 500,000 against the loan facility. Company A also wrote back the total loan at the year ended June 2020 without giving any due consideration.

As per the audited reports, Company A incurred losses over nine consecutive years and despite such history, purportedly received financial loans from the offshore companies, which were subsequently written off without any due consideration.

Despite Company A consistently experiencing losses in its primary business and the associated businesses showing minimal activity in terms of turnovers, the owner's (Company A's directors and shareholders) assets held abroad, as reported in tax returns, have seen a significant and unexplained increase over the years. This suggests a potential case of tax evasion, where losses may have been deliberately misreported over multiple years.

Additionally, authorities hold suspicions that profits from Company A and associated businesses may have been illicitly transferred abroad through undocumented methods. Furthermore, the injection of funds in the form of loans from offshore companies appears to be a method of repatriating profits or funds previously held in foreign assets.

The findings were shared with law enforcement agencies which has initiated its investigation and has also sent an informal international cooperation request through the FMU to the foreign jurisdiction's FIU where the two offshore companies are located.

Source - Pakistan

Case Study # 57: False advertisement on social media

Fraud through social media

Authorities identified three android applications in the names of A Trade, B Trade and C Trade to be providing digital investment and forex trading services. A Trade had been falsely advertising a picture of the Prime Minister of Pakistan to attract the investors. The image of the Prime Minister standing among foreign nationals was advertised on "Youtube.com" depicting the details of investments in small denomination like PKR 5 (~ USD 0.02), PKR 50 (~ USD 0.18) and PKR 500 (~ USD 1.80), resulting in hefty profits over two or three days of PKR 200 (~ USD 0.72), PKR 3,000 (~ USD 10.81) and PKR 40,000 (~ USD 144.10) respectively. The image of the Prime Minister was seemingly an alteration of an actual picture taken at the time of officials from a foreign based company handing over a cheque to the Prime Minister of Pakistan for flood affected people.

Up to 5 April 2023, members of the public had downloaded each of all three mobile applications more than 100,000 times. Upon selecting the deposit (investment) option, these applications offer a range of investments from PKR 500 (~ USD 1.80) to PKR 50,000 (~ USD 180.11). However, choosing any of these options often leads to payments diverted to individual accounts rather than paid to the respective business accounts of A Trade, B Trade, or C Trade.

Each deposit attempt through the application typically created a new individual account. Authorities identified hundreds of these branchless banking accounts and multiple accounts among them were commonly used by all three android applications.

Authorities analysed a total of 30 major accounts with an aggregate credit turnover of more than PKR 500 million (~ USD 1.8 million) which revealed that the accounts were opened in the same period, received small value funds and from the same regions. The account holders were mostly illiterate individuals under 30 years old, whose benami accounts were opened to route the investment funds. Two of these accounts were already under investigation by a law enforcement agency. Further, 11 of the 30 major accounts were found to have the highest turnover wherein most of the funds were withdrawn in cash, and authorities suspected these account holders to be the ultimate beneficiary of the scam.

Numerous investors reported the android applications as frauds and scams to Google Play Store.

The FMU disseminated its financial intelligence to the law enforcement agency and the case is currently under investigation.

Source - Pakistan

Case Study # 58: Ponzi scheme

Fraud; use of legal persons and arrangements

The FMU received multiple STRs from different banks on XYZ Group based on a warning advisory issued by the Securities and Exchange Commission of Pakistan (SECP) to the general public, advising against investing in fraudulent schemes by XYZ Group.

The directors of XYZ Group (Private) Limited (one of the companies in the XYZ Group) held shares as per following detail:

S. No.	Name	Designation / Position	Shareholding %	Age
1	Person A	Director/shareholder	99%	21 Years
2	Person B	Director/shareholder	1%	24 Years

Person A is 21 years old, and she is the daughter of Person C and sister of Person D while Person B is 24 years old and worked as Regional Manager at 'XYZ Group' and is currently a director in XYZ Group (Private) Limited.

XYZ Group's business model appeared similar to LMN Group of companies, which was owned by Persons C and D. Law enforcement agencies were already investigating LMN Group for alleged involvement in collecting deposits from the general public promising hefty returns on its website. the FMU had also shared financial intelligence on LMN Group with Law enforcement agencies and the regulator - the SECP.

The FMU searched Persons A and B's computerized national identification numbers (CNIC) in its database where it identified 491 currency transaction reports (CTRs), involving funds amounting to PKR 2.2 billion (~ USD 7.9 million) against Person A, and 413 CTRs involving funds amounting to PKR 1.9 billion (~ USD 6.8 million) against Person B, reported during 2023.

The FMU requested information from financial institutions in relation to all the accounts of XYZ Group identified in STRs/CTRs which revealed very high turnovers in a short span of time. The FMU observed

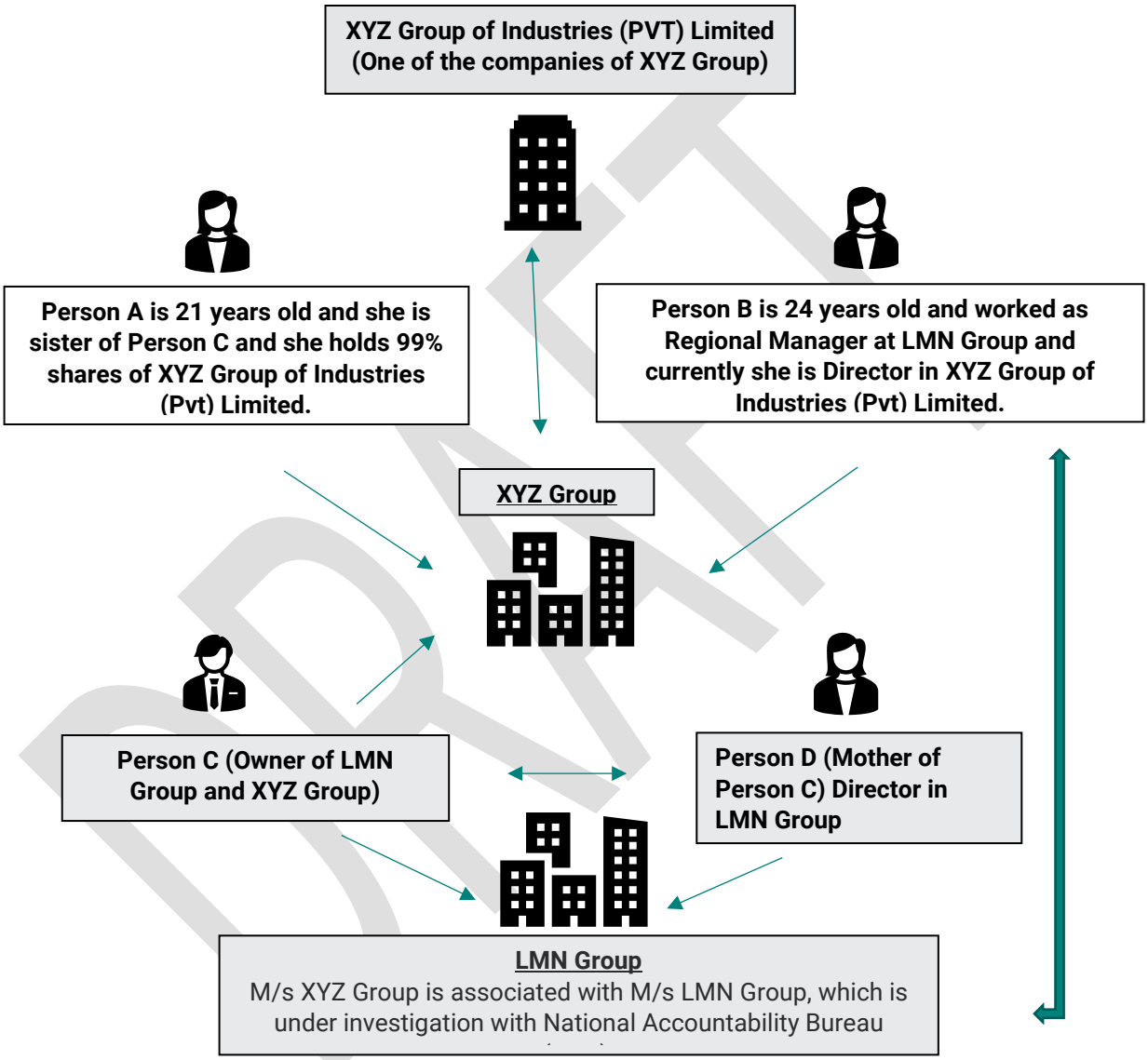
aggregate credit turnovers over PKR 26 billion (~ USD 93 million) in four bank accounts. XYZ Group opened these bank accounts between December 2022 to February 2023.

The FMU found 15 companies registered against Person A's CNIC number and 12 companies registered Person B's CNIC number in the company registry database.

Both Person A and Person B were not registered as income tax filers.

The FMU shared its financial intelligence with following designated agencies:

- The regulator - the SECP for regulatory action.
- Three law enforcement agencies for ground check (factual investigation), cheating the public at large scale and tax evasion.



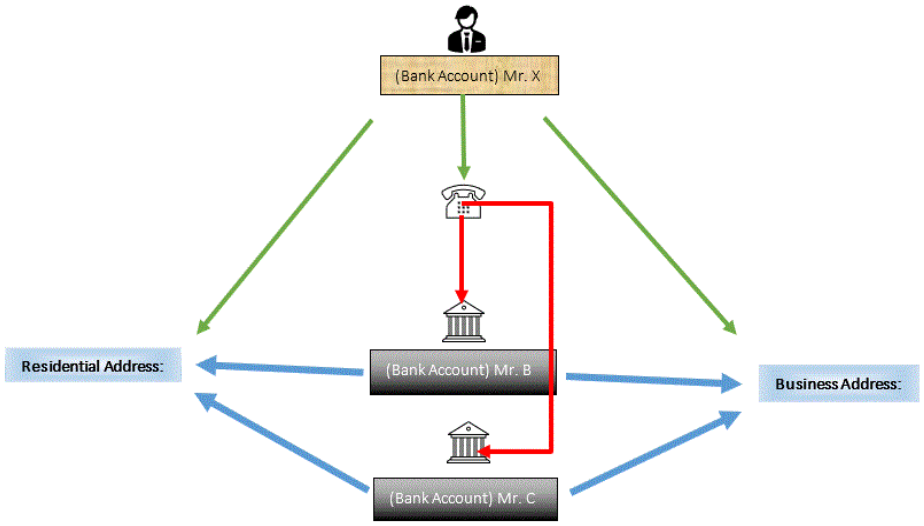
Source - Pakistan

Case Study # 59: Tax Evasion under the shadow of ultimate beneficial ownership

Tax evasion; beneficial ownership

The FMU received suspicious transaction reports from a reporting entity about a customer (a cosmetic business) with high value transactions that deviated from its business profile, owned by Person X. Person X appeared to be sole proprietor of a single entity however, his contact number was used in bank account details of Person B and Person C. In addition, the reporting entity found that the residential address and

business address of all three individuals were found to be the same across their bank account details. Based on the reporting entity's identification of positive contact numbers, residential and business addresses in different databases, Person X appears highly likely to be the beneficial owner of various accounts belonging to other individuals. Person X routed more than PKR 683.89 million (~ USD 2.45 million) from his reported and associated accounts. Moreover, the tax records for previous years showed that Person X had not paid any tax. The FMU disseminated the financial intelligence to relevant law enforcement agency for further investigation on ultimate beneficial ownership concerns in relation to Person X's business and bank accounts, and for tax evasion.



Source - Pakistan

Case Study # 60: Illegal money value transfer services in the garb of dry fruit business

Hawala; tax evasion; Beneficial ownership

A number of different banks reported multiple STRs to the FMU in relation to Person A. Person A was a resident of city B and the owner of a sole proprietorship business dealing in dry fruits and general food items. The banks raised suspicions about transactions on the accounts that Person A conducted with unrelated counter parties located at far-flung areas. Analysis of account opening forms from different banks showed that Person A had a clear and proper signature on his national identification card whereas he used immature and easy to copy signatures while opening of bank accounts, which raised the bank's concerns for the beneficial ownership of the bank accounts. The FMU's analysis of financial statements revealed turnover of PKR.3.48 billion (~ USD 12 million) and transactions with inconsistent counterparties that were inconsistent with Person A's business profile. Further, Person A's counter parties were located in far-flung areas, and he immediately withdrew the funds deposited into the accounts. The FMU had commonly observed these transaction patterns in hawala / hundi business. Moreover, Person A's tax records of previous years showed that he paid meagre amounts of income taxes despite having routed a huge volume of funds through his bank accounts.

Based on the above findings the FMU disseminated the financial intelligence to LEAs for investigation of tax evasion and hawala offences and potentially terrorist financing.

Source - Pakistan

Case Study # 61: Money Laundering through opening multiple accounts, trade-based money laundering and tax evasion

Hawala; tax evasion; trade-based money laundering

Customs authorities suspected Company A (family-owned business) of siphoning off funds by over-invoicing importation of solar panels from an offshore company - Company B. Customs authorities audited Company A's invoices related to it solar panel imports, which were not the company's actual business, revealed that Company A siphoned off PKR 4.78 billion (~ USD 17,169 ,485) in the context of the value of the imports. During 2022, Company A received funds amounting to PKR 22 million (~ USD 78,973)

from an unrelated counter party located in a different jurisdiction, raising suspicions that these funds were part of the value siphoned off. Moreover, Company A conducted multiple transactions with unrelated counter parties. Financial analysis showed that Company A and its directors opened 216 accounts, including personal and business accounts, through which it routed funds from company accounts to personal and sole proprietorship accounts. Aggregate activity in all the accounts amounted to PKR 77 billion (~ USD 276 million) which did not align with the company's profile. Company A and its directors' income tax payment records revealed they only paid nominal taxes during the period of financial activity. Subsequently, the FMU shared its financial intelligence with law enforcement agencies to probe Company A for over-invoicing and tax evasion. The case is currently under inquiry with the law enforcement agency.

Source - Pakistan

Case Study # 62: Defrauding public by offering lucrative returns on investment packages

Fraud through social media; real estate

In 2022, Company A was officially registered with the Securities and Exchange Commission of Pakistan (SECP), declaring its business as real estate activities. However, contrary to its stated business scope, three directors of the company engaged in unauthorised activities by soliciting investments and deposits from the general public through their websites and social media accounts. They promised fixed and excessively high returns of up to 60% annually. They falsely represented that the funds would be invested across various sectors such as real estate, media, information technology, and mineral water, and profits would be distributed among the investors. Analysis of the company and its directors' accounts revealed that multiple individuals deposited funds into the company account through online cash deposits and internet transfers, indicative of public investment. Subsequently, a total of PKR 6 million (~ USD 21,572) in cash was withdrawn and PKR 0.3 million (~ USD 1,079) transferred from the company account to personal accounts belonging to two of the directors (total ~ USD 22,600). Following the identification of these irregularities, the FMU's reported its financial intelligence findings to law enforcement agencies and regulatory bodies. As a result, the SECP imposed a penalty of PKR 0.3 million (~ USD 1,079) on the company and its directors, along with disqualifying the directors from holding office.

Source - Pakistan

Case Study # 63: Tax evasion through benami accounts

Smuggling; dubious beneficial ownership; hawala; trade-based money laundering

Person A holds a directorial position at Company A, a family-run enterprise located in Pakistan, primarily engaged in the distribution of liquefied petroleum gas (LPG). The company had sought bank assistance for importing LPG from Jurisdiction X via land transport. However, the bank declined the request as the jurisdiction falls under FATF's *Jurisdictions under Increased Monitoring* list ('high-risk jurisdictions list').

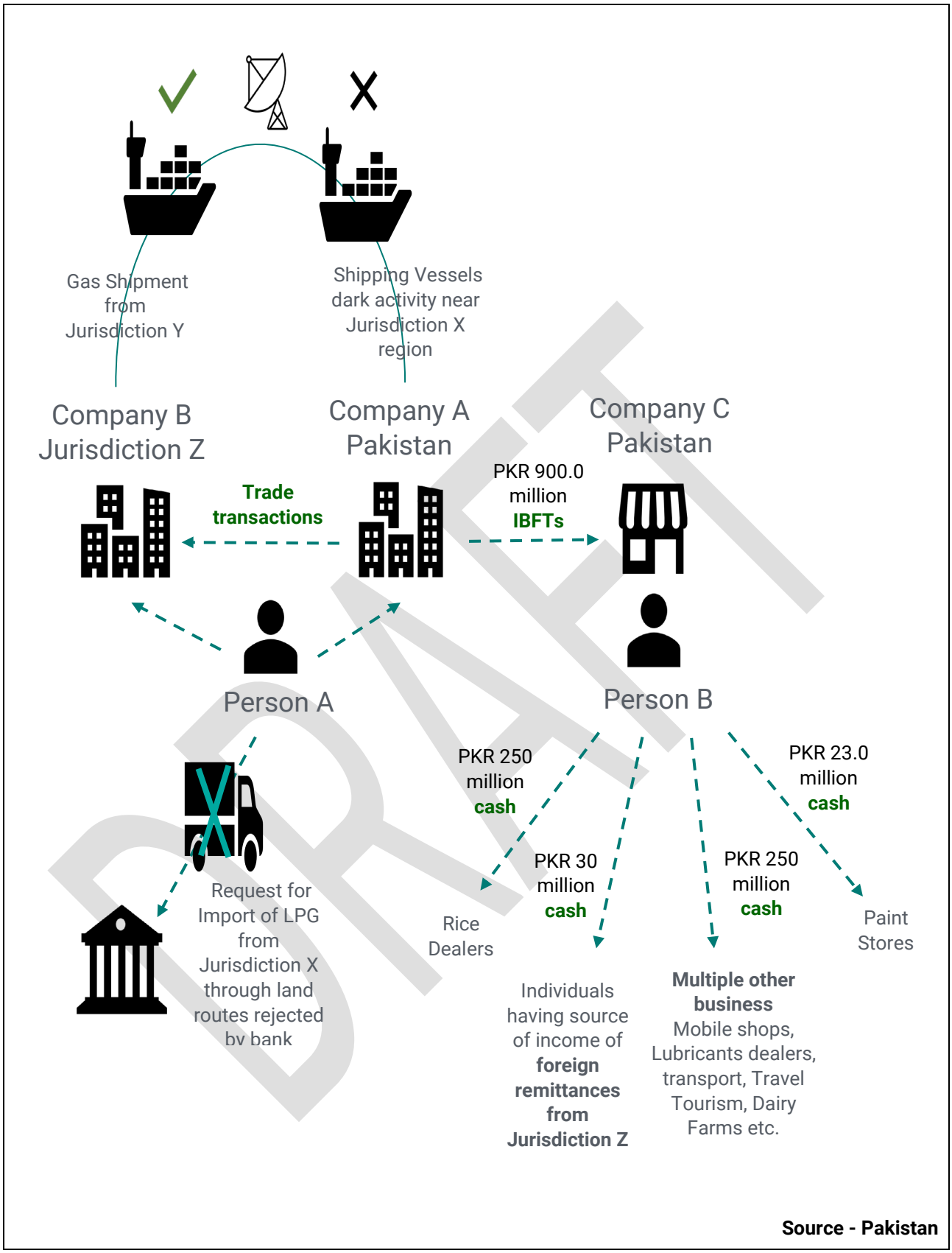
Subsequently, Person A initiated the import of LPG from Jurisdiction Y, through Company B based in Jurisdiction Z, where Person A also serves as a director. Notably, both companies are family-owned entities.

Aggregate credit turnovers of Company A's business identified in different banking accounts worth more than PKR 100 billion (~ USD 359 million) with a high volume of import-related transactions.

Moreover, Company A transferred funds totalling PKR 900 million (~ USD 3,231,837) to Company C, a sole proprietorship dealing in dry fruits in Pakistan. The sole proprietor, a young individual, possesses inconsistent signatures on his identity card and banking documents through signature indemnity, (form required by bank where signatures mismatch) raising questions about the beneficial ownership of Company C, as no previous financial activity of Person B was identified. The account's turnover exceeds PKR 1.0 billion, with PKR 900 million (~ USD 3,231,837) transferred from Company A within a year.

The transfer of funds from an LPG supplier to a dry fruit trader lacked economic rationale. Additionally, Company C has been disbursing funds to various unrelated entities such as paint stores, mobile shops, travel agencies, and rice dealers, especially to those whose family members are residing in Jurisdiction Z and are dependent upon foreign remittances.

Given these findings, the FMU shared its financial intelligence with relevant law enforcement agencies due to suspicions that Person A and Person B are involved in smuggling and illicit financial activities such as hawala/hundi transactions and TBML practices.



Source - Pakistan

Case Study # 64: Tax evasion through benami accounts

Tax evasion; dubious beneficial ownership; commingling of funds

Various banks filed several suspicious transaction reports against Person A. Allegedly, Person A was acting as a front man for a family business, which was managed by three brothers. Person A, who was employed as an accountant in the family business, opened 11 personal and business accounts across different banks during a period of three years (2016-2019). The accountant nominated his employer as the next of kin and routed approximately PKR 6 billion (~ USD 21,567,837) through these accounts over three years. The aggregate financial activity within these accounts amounted to PKR 7.73 billion (~ USD 27,964,473), *significantly* surpassing person A's documented profile and income. Additionally, his family members operated multiple companies and collectively opened 94 additional bank accounts, both business and personal. Tax records from previous years indicated that Person A and family members (his employer) had paid nominal income taxes during the same period when the suspicious account activity occurred. The FMU passed its financial intelligence to law enforcement agencies for investigation into potential tax evasion and to identify the ultimate beneficiaries of the funds routed through Person A's multiple accounts. The case is under inquiry with the law enforcement agencies.

Source - Pakistan

2.12 Philippines

Case Study # 65: Tax fraud/evasion using shell companies

Tax evasion

A law enforcement agency's investigation revealed a fraudulent scheme called "Input VAT Receipt for Sale". This scheme was committed by a certain organised crime group using a fraudster company and several ghost or dummy corporations, to sell fictitious receipts and invoices to large taxpayers (usually corporations; referred as clients), to evade payment of taxes due to the government. Allegedly, the operation has lasted for more than 15 years.

The fake receipts and sales invoices were allegedly procured by the clients, in exchange for a fee ranging from 0.4% to 1.25% of the total amount in the fictitious receipts and invoices. These fees were paid through cheques or cash collected by the same messenger or deliveryman, who handed over the procured receipts/invoices to the client, or through bank deposit using the bank accounts provided by the fraudster company. The receipts or invoices obtained were then used by clients to claim input VAT and/or to reduce their income tax by bloating their expenses. The matter is being investigated by law enforcement agencies and the Philippine's Tax Authority and some cases have been filed with the Department of Justice and the Courts.

Source - Philippines

Case Study # 66: Child sexual abuse in a religious organisation

Sexual exploitation, including sexual exploitation of children

Person Z is the head of Group X, a religious organisation[77]. The covered person noted unusual and questionable transactions through Person Z's account including high volumes of cash transactions with significant values, and dealings with several companies which do not belong to the same industry as Group X. Later on, Person Z became the subject of several adverse news articles due to his involvement in a fraud/scam. He was also charged by prosecutors of a foreign jurisdiction for sex trafficking activities and has been sanctioned by a foreign government agency for engaging in egregious human rights violations for more than a decade, including a pattern of systemic and pervasive rape of girls as young as 11 years old, as well as additional physical abuse.

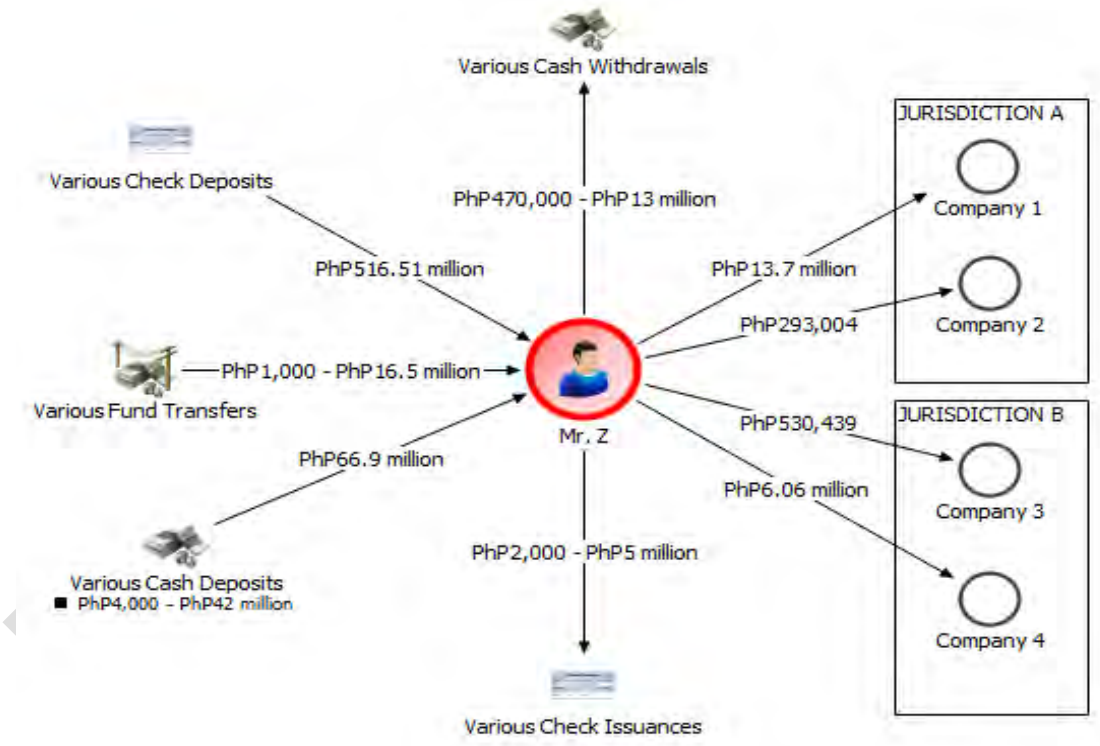
Reportedly, Person Z's USD and PhP accounts had large cheque deposits and funds transfers which had no economic justification. Credits to his personal accounts include numerous cash deposits ranging from PhP 4,000 to PhP 42 million (~ USD 70 to USD 730,000) and funds transfers ranging from PhP 1,000 to PhP 16.5 million (~ USD 18 to USD 751,490), while disbursements were conducted through outward remittances and fund transfer debits ranging from PhP 26.9 million to PhP 47 million (~ USD 481,488 to USD 841,102). Other disbursements observed were cash withdrawals ranging from PhP 470,000 to PhP 13

[77] Anti-Money Laundering Council - *Online Sexual Abuse and Exploitation of Children in the Philippines. An Evaluation Using STR Data*: http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf

million (~ USD 8,408 to USD 232,598), and cheque issuances ranging from PhP 2,000 to PhP 5 million (~ USD 36 to USD 89,440) allegedly intended for e-taxes and bills payments, operational expenses, worker compensation, and different materials for the continuous construction of Group X project. Likewise, Person Z has four active auto loan accounts with maturity dates in 2022, 2024, and 2025. Person Z's accounts have already been included in the covered person's internal watchlist and may be recommended for closure once the lawsuit in the foreign jurisdiction has progressed.

Additionally, Person Y, who is alleged to be the former leading church administrator in the foreign jurisdiction that manages the collection of financial data from worldwide church operations, figured in suspicious transactions related to Group X. Apparently, Person Y is the subject of an adverse media information in the foreign jurisdiction on allegations of being part of the dangerous and powerful criminal organisation engaged in child sex, human trafficking, bulk cash smuggling, ML, forced labour and immigration fraud. An arrest warrant has been issued in the foreign jurisdiction for Person Z and Person Y. Person Y's account is also under close monitoring by the covered person and subject to closure if she is prosecuted and found guilty.

Figure 1. Unusual Transactions of Person Z



Source - Philippines

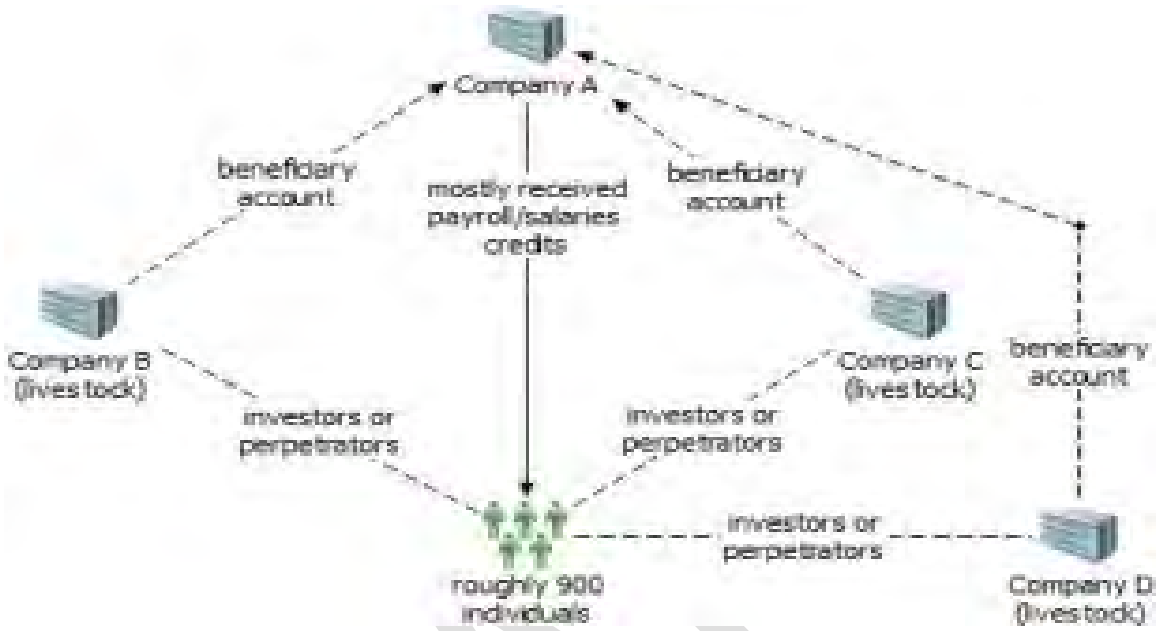
Case Study # 67: Companies involved in unauthorized investment taking activities

Fraud; investment scam; tax evasion

Roughly 900 individuals figured in voluminous suspicious transactions estimated at PhP 226 million (~ USD 3.9 million) relative to alleged involvement in unauthorised and fraudulent investment schemes[78]. The scheme reportedly involves investing in three companies: Company A, Company B and Company C, investing in livestock products with a promise of a 100% return in two months. The majority of the nearly 900 subjects received funds via payroll credits from a travel and tours agency, which is allegedly used as the beneficiary account of the investment-taking activities of three entities. An SEC advisory was released in 2019 against the three corporate entities, warning the public to stop investing with them. The SEC further warned that those involved will be reported to tax authorities, so that penalties and/or appropriate taxes will be correspondingly assessed. Relevant information has been shared with stakeholders including law enforcement agencies for investigation.

[78] Anti-Money Laundering Council - *An Analysis of Suspicious Transaction Reports with Possible Links to Tax Crimes*: http://www.amlc.gov.ph/images/PDFs/2021%20ANALYSIS%20OF%20STRS%20WITH%20POSSIBLE%20LINKS%20TO%20TAX%20CRIMES.pdf

Figure 2. Fraudulent Investment SchemeInvolving Legal Persons



Source - Philippines

Case Study # 68: Involvement of a casino junket in a criminal syndicate

Fraud; investment scam

Casino X reported several individuals as members of the ABC criminal syndicate[79]. Notably, Person D one of the identified members, is involved in various businesses, such as construction, cosmetics distributorship, and lending. He is also an official of one company that is allegedly running a Ponzi scheme and was involved in an adverse news article about casino junket operations. Person D had personal and corporate accounts with a domestic bank, both of which were closed due to unresolved red-flag transactions. Notably, Person D issued a bogus cheque in the amount of PHP10.50 million (~ USD 187,830) in another domestic bank. Given the circumstances, an STR pertinent to the fraudulent issue of the bogus cheque was warranted, and the checking account was closed.

Related to this, Casino Y received a letter from an Appropriate Government Agency for Casinos on the alleged investment fraud activities of the ABC syndicate. The letter indicated that the group is run by Person D, who, upon verification, is a member of Casino Y's rewards program. Person D allegedly entices investors into a contract of loan by promising them exorbitant returns or interest by issuing post-dated cheques that ultimately bounce. The ABC syndicate asserted that they had a junket deal with private casinos and the funds will be used to pay their international guests' gaming operations. In an effort to provide the appearance of a real organisation, the ABC syndicate uses names of legitimate businesses. Relevant information has been disseminated to various stakeholders including law enforcement agencies for investigation.

Source - Philippines

[79] Anti-Money Laundering Council - *Analysis of Suspicious Transactions Associated with Casino Junkets*: http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf

2.13 Singapore

Case Study # 69: Company charged for offences under the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act*

Use of legal persons and arrangements

On 29 September 2022, Company A was charged in the court for offences under the *Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act 1992* (CDSA). Company A was charged with 42 counts of acquiring property which it knew was another person's benefits from criminal conduct, under section 47(3) of the CDSA. Between 2014 and January 2018, Company A received on board its vessels a total of USD 56 million worth of marine gasoil, which had been dishonestly misappropriated from a petroleum refinery facility in Singapore. Each of the offences faced by Company A carries a penalty of a fine not exceeding SGD 1 million (~ USD 779,281) or twice the value of the property in respect of which the offence was committed, whichever is higher upon conviction.

The ex-managing director of the company, who allegedly consented to acquiring the misappropriated marine gasoil, has also been charged separately in court for his involvement. His case is also ongoing.

Company A operates in the marine industry and the acquisition of the misappropriated marine gasoil was driven purely by business interest. The court proceeding against Company A is ongoing.

Source - Singapore

Case Study # 70: Members of organised crime group charged

Organised criminal group and racketeering; self-laundering

In May and October 2023, a total of 16 individuals were charged for their alleged involvement in an organised criminal syndicate which was believed to be engaged in illegal remote gambling activities. They were among the 37 persons arrested in a Police operation targeting criminal syndicates. During the investigation, Police seized a total of SGD 4.53 million (~ USD 3.53 million) worth of cash and assets.

The subjects were charged for offences under the *Remote Gambling Act 2014* ("RGA") and the *Organised Crime Act 2015* ("OCA"). Among them, 3 men and a woman faced additional charges under the CDSA for laundering their own proceeds of crime. Person A has concealed criminal proceeds in another person's bank account and converted criminal proceeds as partial payment for a scooter. Person B had converted criminal proceeds as loans for his company while Person C abetted Person D in using criminal proceeds to pay for her vehicle's instalments. Court proceedings against these persons are ongoing.

Source - Singapore

Case Study # 71: 12 men charged for their Involvement in recent spate of banking-related malware cases

Fraud involving malware; self-laundering; third party laundering

Between June and August 2023, a series of banking-related malware cases were reported involving unauthorised transactions from victims' bank accounts where victims did not divulge their one-time passwords to anyone. Through extensive investigation, the police established the identities of 12 men responsible for the cases who were all arrested in an island-wide operation in September 2023. Authorities seized an array of items during the operation which included cash amounting to more than SGD 13,000, (~ USD 10,135) two laptops, 32 bank cards, 23 mobile devices, drug paraphernalia and a knife. In addition, authorities froze 60 bank accounts to prevent further misuse.

Nine men have since been charged in court while investigations against three others are ongoing for multiple offences such as assisting another to retain benefits from criminal conduct, possession and consumption of controlled drugs, possession of drug paraphernalia, unlawful possession of offensive weapon, unauthorised access to computer material and acting as a member of an unlawful society and locally linked organised criminal group. Court proceedings against the nine individuals are ongoing.

Source - Singapore

Case Study # 72: Money laundering from drug related offences

Drug-related crime

On 30 November 2023, authorities arrested Person A for trafficking in a controlled drug under *the Misuse of Drugs Act (MDA) 1973*. During investigations, authorities restrained one bank account with a total balance of SGD 1,324.20 (~ USD 1,032). During financial investigations, Person A claimed that only SGDS 700 (~ USD 546) were proceeds of crime from drug trafficking.

On 14 March 2024, he was convicted of his drug predicate and drug ML offences. Accordingly, he was sentenced to five years, eight months and three weeks of imprisonment, and five strokes of the cane. An application has been made to the court to forfeit SGD 700 (~ USD 546) to the state (the forfeiture is pending).

Source - Singapore

Case Study # 73: Money laundering from drug related offences

Drug-related crime

On 5 May 2022, authorities arrested Person A for trafficking in a controlled drug under the *Misuse of Drugs Act (MDA) 1973*. During his arrest, authorities seized cash amounting to SGD 19,717.60 (~ USD 15,372) and some pieces of jewellery. During investigations, authorities also restrained one bank account with a total balance of SGD 358.03 (~ USD 279). During financial investigations, Person A claimed that only SGD 1,100 (~ USD 858) were from proceeds of crime from drug trafficking.

On 26 September 2023, Person A was convicted of his drug predicate and drug ML offences. Accordingly, he was sentenced to 30 years' imprisonment. The SGD 1,100 (~ USD 858) was forfeited to the state.

Source - Singapore

Case Study # 74: Conviction of legal person

Fraud; third party laundering; use of legal persons & arrangements; foreign predicate offence; suspicious transaction reporting

The Suspicious Transaction Reporting Office (STRO) received information on Company X indicating that there were multiple funds recall requests on its bank account citing fraud. The STRO disseminated financial intelligence to the Commercial Affairs Department (CAD) of the Singapore Police Force after analysis, and investigations were commenced against Company X and Person Y, who was the sole director and shareholder.

Investigations showed that four victims of investment and love scams residing in Jurisdiction A, Jurisdiction B and Jurisdiction C were deceived to transfer monies totalling more than SGD 110,000 (~ USD 85,759) to two bank accounts held by Company X. Person Y was unable to provide a consistent and credible explanation why he continued to use the two bank accounts to receive monies despite being notified of the funds recall. Person Y even attempted to deregister Company X, but the application was rejected by authorities. Both Company X and Person Y were thereafter charged with ML offences. Person Y was eventually convicted in September 2023 and sentenced to six months imprisonment. Company X was convicted in September 2023 and fined a total of SGD 30,000 (~ USD 23,389).

Source - Singapore

Case Study # 75: Recalcitrant money mule

Fraud; third party laundering; financial institutions; remittance services; suspicious transaction reporting

Between February and July 2021, Person A deceived an overseas love-scam victim into transferring around SGD 74,000 (~ USD 57,694) to Person A's bank account. Investigation by the Commercial Affairs Department of the Singapore Police Force revealed that Person A was a money mule who had assisted an unverified individual, Person B, to receive the scam proceeds.

The investigation also revealed another instance in February 2021, where Person B had requested for Person A's assistance to receive funds from another unverified individual, Person C. Person C purportedly wanted to purchase property in Jurisdiction X but did not want to remit the money for the property directly to Jurisdiction X. Person A was suspicious of Person B's request and asked for supporting documents relating to the property but Person B was unable to furnish any documents. Despite this, Person A still

assisted to receive the funds and remit them to bank accounts in Jurisdiction X. Some of the funds were remitted to Jurisdiction X through a Singapore licenced money changer.

Person A was convicted of an offence under the CDSA in December 2023 and sentenced to seven months' imprisonment. The Singapore licensed money changer was also charged with a CDSA offence for failing to file a STR despite having reasonable grounds to suspect that the remitted funds were proceeds of crime. Court proceedings against the Singapore licensed money changer are ongoing.

Source - Singapore

Case Study # 76: Enabler who facilitated the use of a shell company to deal with proceeds of crime

Fraud; third party laundering; use of legal persons & arrangements

Acting on the instructions of an unknown third party, Person A proceeded to incorporate Company X and opened corporate bank accounts for the company. It was found that nearly USD 1.5 million was deposited into a Company X bank account, which was part of USD 4 million in fraudulent proceeds linked to a scam perpetrated against a bank in a foreign jurisdiction.

During investigations, Person A as the director of Company X, was unable to provide a satisfactory account of how Company X's bank account came to possess these suspected benefits of criminal conduct. For giving others access to Company X's bank accounts and his failure to use reasonable diligence in the discharge of his duties as director of the company, in December 2023, Person A was charged for offences under the *Companies Act 1967*, CDSA and *Computer Misuse Act 1993*. Court proceedings against Person A are ongoing. As a separate legal entity, Company X was convicted of a ML offence under S55 of the CDSA in March 2024 and was ordered to pay a penalty of SGD 50,000 (~ USD 38,980).

Source - Singapore

Case Study # 77: Tax money laundering

Tax crimes; tax money laundering; money value transfer services

As part of a joint investigation with the tax authority of Singapore into a tax fraud, it was revealed that a sole director had used two shell companies and created various fictitious invoices to submit fraudulent Goods and Services Tax (GST) refund claims to the tax authority. As a result, the tax authority made payments to the two companies which should not have been made. A follow-up ML investigation by the Commercial Affairs Department of the Singapore Police Force revealed that the director was residing in Jurisdiction C during the period of his offences and had no known sources of income. Between 1 January 2015 and 31 January 2020, the fraudulent GST refunds were credited into the Singapore bank accounts of the two shell companies on a quarterly basis. Around the end of every quarter, the director would return to Singapore, during which time he would engage the services of cross-border money transfer service providers to remit the fraudulent GST refunds to bank accounts belonging to him and his wife in Jurisdiction C. The director also used a portion of his GST refunds to make contributions to his Central Provident Fund ("CPF") account, which is Singapore's mandatory social security savings scheme, under one of the shell companies' names to create a facade that the shell company had active business operations. In so doing, the sole director had transferred and removed the benefits of his criminal conduct through GST evasion from Singapore – this constitutes the ML offences.

In December 2023, the director was convicted of 16 counts of GST evasion under section 62(1)(b) and section 62(1)(c) of the *Goods and Services Tax Act 1993* involving SGD 660,114.97 (~ USD 514,630) of fraudulent GST refunds. The director was sentenced to a total of 84 weeks' imprisonment and ordered to pay a penalty of SGD1,980,344.91 (~ USD1,543,853), representing three times the GST amount evaded. 33 additional GST evasion charges were taken into consideration in his sentencing.

Further, in December 2023 the director was convicted and sentenced to a total of 15 months' imprisonment for four counts of ML of SGD 523,459.90 (~ USD 408,045) by transferring the fraudulent GST refunds overseas and by using the fraudulent GST refunds to top up his CPF account. Six additional ML charges were taken into consideration in his sentencing.

Source - Singapore

Case Study # 78: Successful arrest of man alleged to have smuggled gold bars across different jurisdictions

Smuggling: trade-based money laundering; trade in precious metals and/or stones, international cooperation

In a long-running intelligence probe against a group of individuals from Jurisdiction A, which included financial intelligence, the Commercial Affairs Department (CAD) of the Singapore Police Force uncovered that two suspects from the group, Persons A and B, purchased at least 28,000 pieces of gold bars worth at least SGD 1.5 billion (~ USD 1.1 billion) from a jewellery wholesaler in Singapore between 2014 and 2017. They were suspected of concealing the gold bars within exports containing mechanical tools to overseas destinations, including foreign Jurisdictions A and C. Singapore convened regular virtual case discussions with law enforcement agencies in Jurisdictions A and C to share intelligence findings on the group to develop potential leads.

In mid-December 2023, the Customs authority in Jurisdiction C seized a shipment containing 15 pieces of gold bars concealed in the shipment sent by a suspected co-conspirator of Person A. In late December 2023, Person A was arrested by the CAD when leaving Singapore and was charged for one count of cheating under Section 417 of the *Penal Code 1871*. To date, he has been charged with 4 additional counts under Section 417 of the *Penal Code 1871* involving more than 17,000 pieces of 1kg gold bars. Investigations and court proceedings are ongoing.

Source - Singapore

Case Study # 79: Dissipation of scam proceeds via cryptocurrency conversion

Fraud; foreign predicate offence; third party money laundering; use of virtual assets

Due to intelligence probes, the Commercial Affairs Department (CAD) of the Singapore Police Force uncovered a criminal syndicate coordinated by Person A, which was responsible for the dissipation of scam proceeds of more than SGD850,000 (~ USD 662,598) via cryptocurrency conversions. Person A, a national of Jurisdiction X, had assisted an unverified individual, Person B, to

- Source cryptocurrency sellers.
- Purchase ATM cards from unknown individuals to be used to receive funds from Person B to pay for the purchase of the cryptocurrency.
- Purchase and transfer the purchased cryptocurrency into Person B's cryptocurrency wallet.

Person A also assisted Person B to obtain access to a Singapore bank account without due authorisation, which Person B used to receive and transfer more than SGD500,000 (~ USD 389,764) of scam proceeds.

In February 2024, Person A was convicted of various offences under the CDSA and the *Computer Misuse Act 1993* and sentenced to four-and-a-half year's imprisonment. Further, authorities seized cash amounting to SGD$15,715 (~ USD 12,250) from Person A during the investigation.

Source - Singapore

2.14 Chinese Taipei

Case Study # 80: Unlisted stock fraud

Fraud; cash; use of legal persons and arrangements

A bank reported a case to the Criminal Investigation Bureau (CIB) where a bank teller alleged that Person A was withdrawing large amounts of cash from various branches of the bank and was identified as a money mule. After investigation, members of the public started to report to the police one after another, claiming that Company O pretended to be engaged in the green energy industry and had promising prospects. Many victims were misled by Company O fraudulent claims and bought its unlisted shares.

In early 2024, a task force set up to investigate this. After more than a month of tracing and collecting evidence, they searched the office of Company O and the residences of 12 individuals. They arrested the relevant suspects (including Person A), and seized computer hosts, laptops, mobile phones, company files, seals, stamps and private seals of shareholders, one batch of company promotion documents, one batch of stock certificates, one batch of stock dividend collection form receipt notices, one batch of stock transfer application forms, one batch of tax payment forms, one batch of company contracts and more than TWD 320,000 (~ USD 10,000) in cash as evidence. More than 1,300 people were victims of this scam, and the amount of money defrauded exceeded TWD 400 million (~ USD 12.5 million).

Company O claimed to be cooperating with various listed companies and government departments in the field of thermal cracking regenerative power generation technology. However, the information they provided to the public was either exaggerated or fictitious - the company did not have any operating performance and cooperated with unlicensed securities dealers to send text messages and make calls to promote their unlisted stocks to the public. After the victims remitted money to purchase the unlisted stocks, the money mule group (including Person A) would withdraw cash at bank branches and hand it over to the leaders of the unlicensed securities dealers.

Source - Chinese Taipei

Case Study # 81: Suspected corruption by public official

Corruption and bribery; cash; third party laundering;

Person A was the Speaker of County Y Council. To conceal the bribes he received from vendors, he demanded they remit money to a co-conspirator: Person B's company under the guise of a scour protection project (a project that safeguards offshore wind turbine foundation piles from wave impact by placing stones around them). Person B then withdrew cash and gave it to Person A, which disguised the transfers and the fact that Person A took bribes. Person A received approximately TWD 25,404,899 (~ USD 793,900) of illicit proceeds.

Source - Chinese Taipei

Case Study # 82: Tunnelling listed company through fraudulent transactions

Fraud; cash; use of cheques; use of legal persons and arrangements

Company W is a listed company primarily engaged in construction, where Person A served as its representative. From 2010, Person A and their spouse Person B established three shell companies, Companies X, Y, and Z, under the name of Persons C, D and E. They then utilized Companies X, Y, and Z to sign fraudulent project sales contracts with Company W. In reality, either personnel from Company W or other commissioned companies sold the projects. Subsequently, Companies X, Y, and Z fabricated billing documents to request payment from Company W. This resulted in Persons A and B embezzling TWD 600 million (~ USD 18.75 million) from Company W.

Persons A and B also fabricated false accounting documents for Companies X, Y, and Z, then withdrew cash from the accounts of Company X, Y, and Z, with a portion being stored in the company's safe (Person B later withdrew these funds for personal use. They also issued cheques with payees listed as Persons C, D, and E, then deposited those cheques into the accounts of Persona C, D, and E, and subsequently withdrew all of the funds. This resulted in Persons A and B laundering TWD 395,183,223 (~ USD 12 million) of proceeds of crime.

In September 2023, the Ministry of Justice Investigation Bureau referred Person A and B to the prosecutor's office on charges of violating the *Business Entity Accounting Act*, the *Money Laundering Control Act*, the *Securities and Exchange Act* and the *Criminal Code*.

Source - Chinese Taipei

Case Study # 83: Bank employee bribery for money laundering

Fraud; bribery; wire transfers; use of legal persons and arrangements

Money laundering syndicate, Syndicate A acquired dummy and shell company accounts through intermediaries, with corporate accounts fetching higher prices than individuals' accounts. Syndicate A bribed some of Bank X's employees, including Person B, to facilitate the application process for multiple dummy accounts and shell company accounts, bypassing proper customer due diligence checks. Further, Person B and others assisted in adjusting online banking transfer limits and establishing designated overseas recipient accounts for these dummy and shell company accounts. Person B and others charged varying fees based on the services provided and aided Syndicate A in transferring illicit proceeds. After receiving fraudulent funds from victims, Syndicate A utilized multiple accounts to layer and transfer funds, ultimately directing the funds to designated overseas accounts. In total, Syndicate A obtained and transferred criminal proceeds amounting to TWD 115 million (~ USD 3.5 million).

Source - Chinese Taipei

Case Study # 84: Pig butchering scam

Virtual asset service providers

The Criminal Investigation Bureau (CIB) investigated an international pig butchering scam case and found that the suspects claimed to be an Iraqi military officer, a United Nations official or a netizen[80] who is willing to be the victim's wife. They lured the victims into a fake romantic relationship, and took them to Company J, a virtual asset service provider that did not complete the AML compliance statement, to buy cryptocurrency using cash. Company J cooperated with the suspects, sold cryptocurrencies to the victims at a price which was 10% higher than the market price, then transferred the cryptocurrencies to the suspects' overseas wallet.

After collecting the evidence, the CIB carried out a search in early 2024 and arrested 18 people including the main suspect, Person A. The CIB also seized more than TWD 26 million (~ USD 812,500) in cash, a Porsche vehicle, 23,912 Tether USDT (cryptocurrency), a safe deposit, money-counting machines, related mobile phones, computers and documents and other evidence.

Source - Chinese Taipei

Case Study # 85: Government official bribery case

Corruption and bribery; cash

Person A was the director of a unit within the Ministry of the Interior, overseeing the evaluation process of some of their projects. During the initial review meetings, relevant personnel from municipalities and jurisdictions presented their proposals for projects to Person A who would select which proposals could be submitted to the Ministry of the Interior for subsidy approval. To obtain approval of and the substantial subsidies available for local projects undertaken by Person B, he bribed Person A, by going through Person C - the chief executive officer of a legislator's office.

In order to conceal the bribes, Person A required they were paid in cash, and asked Person C to store it in his office where Person A could access it as needed. Person A also hid some of the cash in various corners of his residence or in tea canisters, and also deposited some of it into his bank account and the bank accounts of his spouse, mother, son, and others, by splitting the cash into smaller amounts. Between 2017 and 2023, the total amount of cash deposited exceeded TWD 10 million (~ USD 312,500). Further, Person A also bought a Mercedes-Benz sedan under Person B's name, and deposited some of the funds into the financial account of Company E, operated by his friend Person D.

In August 2023, Person A was indicted by Taipei District Prosecutors Office for violating the *Anti-Corruption Act* and the *Money Laundering Control Act*.

Source - Chinese Taipei

Case Study # 86: Suspected money laundering

Purchase of real estate

Person Y was an associate detective of a Criminal Investigation Division in a local police department. Person D was involved in organised fraud crimes. Person Y knowingly assisted Person D to conceal the illicit proceeds of his fraudulent activities, and to evade investigation, prosecution, and punishment by judicial authorities. Person Y deposited cash, which was the illicit proceeds Person D provided him, into their own bank accounts, then purchased properties under their names and paid for house decoration expenses. Through this Person Y created breakpoints in the financial flow to jointly disguise and conceal the proceeds of Person D's fraudulent activities totalling TWD 14,220,700 (~ USD 444,400) and their destination.

Source - Chinese Taipei

Case Study # 87: Suspected corruption by Persons A, B, and C which jointly violated the *Anti-Corruption Act*

Corruption and bribery; wire transfers

Persons A, B, and C were security guards at a detention centre, who elicited bribes received from detainees. To conceal these bribes, they contacted te detainees' relatives through a mobile phone registered under the name of Person D from Jurisdiction A, to transfer money to the account of Person A's

[80] A person met through the Internet.

daughter and to the account of Person E, a former detainee from Jurisdiction B. Persons A, B, and C managed those accounts and held the passbooks and the corresponding personal seals, so as to deposit the illicit proceeds received between 2020 and 2023 into those accounts. Persons A, B and C also instructed Person A's spouse and daughter to use these accounts for cash deposits and withdrawals irregularly, thus transferring or altering the illicit proceeds.

Through these approaches, persons A, B, and C concealed, transferred, and altered the true nature of the bribes and unlawful profits, amounting to at least TWD 810,100 (~ USD 25,315). Chinese Taipei authorities successfully prosecuted this case.

Source - Chinese Taipei

Case Study # 88: Embezzlement from a non-profit organisation

Self-laundering; cash; wire transfers

Person A served as the chairperson at Temple W, while Persons B and C (Person A's relatives), also held the position of financial manager and manager at Temple W. Between 2019 and 2020, Persons A, B, and C took advantage of their positions responsible for managing Temple W's passbooks, seals, and cheques, as well as the opportunity to freely access Temple W's funds. They gradually misappropriated funds from Temple W's accounts for personal use or diverted them to other companies operated by the three of them, including depositing cash or transferring funds between Temple W and other companies.

Ultimately, they used those funds to purchase personal life insurance for Person B, invest in managed funds, US dollar deposits, and buy a luxury car for Person C. In total, they embezzled TWD 45.2 million (about USD 1.41 million) from Temple W. In addition, from 2016 to 2022, Person A, B, and C also fabricated false financial statements to evade taxes, amounting to TWD 10.85 million (~ USD 339,000). In November 2023, Persons A, B, and C were prosecuted for violating the *Criminal Code* and *Tax Collection Act*.

Source - Chinese Taipei

Case Study # 89: Investment fraud

Fraud; wire transfers

Persons A, B, and C provided their bank account passbooks, ATM cards, ATM PINs, and online banking account passwords to members of a criminal syndicate whose real identities are unknown. From May 2022, the syndicate members sent investment advertisement links to victims, enticing them to join LINE investment chatrooms. The syndicate members falsely claimed to investors that after registering as members on the "Z app", investors could decide the investment amount themselves, then Company Z would gather the investment funds and use "Z app" to collectively buy stocks. They also claimed that after speculating the targeted stocks, Company Z would distribute the stocks to investors' "Z app" accounts according to their investment amounts, and investors could also participate in stock capital raising and buy unlisted stocks through "Z app".

If profits were made, an additional 20% of the investment amount would need to be paid for profit sharing. This led victims to mistakenly believe in the scheme and transferred funds into the accounts of Persons A, B, and C, totalling TWD 1.27 million (~ USD 39,688). The syndicate never invested any of the customer's money in any stocks, and Persons A, B, and C have been prosecuted for violating the *Criminal Code (Offenses of Fraudulence)* and the *Money Laundering Control Act*, and they are currently on trial.

Source - Chinese Taipei

Case Study # 90: Drug trafficking from Jurisdiction A

Drug related crime

Beginning in January 2021, Person A and their criminal syndicate began sending packages containing ketamine from Jurisdiction A to Jurisdiction B for sale. In an attempt to conceal the origin of the illicit funds, Person A used their mother's account to transfer WTD 1.63 million (~ USD 50,937) of the proceeds of the crime into her account before transferring it out again. Person A was prosecuted for violating the *Narcotics Hazard Prevention Act* and the *Money Laundering Control Act* and is currently on trial.

Source - Chinese Taipei

Case Study # 91: Drug trafficking from Jurisdiction B

Drug related crime

Beginning in March 2023, Person A and their criminal syndicate began mailing packages containing Marijuana from Jurisdiction A to Jurisdiction B for sale. Person A instructed members of the syndicate to deposit drug proceeds of TWD 762,500 (~ USD 23,828) into Person B's account, which is controlled by Person A, using a non-passbook deposit method, and subsequently transferred the funds to other people. Person A was referred to the prosecutor's office on charges of violating the Narcotics Hazard Prevention Act and the Money Laundering Control Act.

Source - Chinese Taipei

Terrorism financing

Members contributed the following case studies as examples of how legals persons have been misused for TF purposes.

Case Study # 92: Terrorism financing with loans from bank and online loans

Terrorism, including terrorist financing; financial institutions

In 2019, the police conducted a search on Person A's house and found that Person A planned to carry out a terror act and needed some equipment. To buy this equipment, Person A and his friends took out a loan from Bank X and also through other online loan applications. The conditions for borrowing from Bank X only require an ID card and a fingerprint scan. Other online loans with nominal amounts only require an ID card and bank/ATM account book. Person A obtained USD 596 from Bank X and approximately USD 486 from several financial technology (online loan) companies. The loan funds were used to buy an air rifle along with a gas cylinder and regulator to be used in a terror act (attacks on government, police, and military installations), and some was given to the terror group which Person A belonged to, as organisation funds.

Source - Indonesia

Case Study # 93: Foreign legal persons related to Chen Shih-Hsien

Terrorism financing

Chinese Taipei's Ministry of Justice convened the Terrorism Financing Review Committee meeting on 12 January 2018, in accordance with the provisions of the *Counter-Terrorism Financing Act*. During the meeting, based on international cooperation and United Nations resolutions, the TF review Committee resolved that:

- Chen Shih-Hsien
- Bunker's Taiwan Group Corporation
- Billions Bunker Group Corporation
- UMC Corporation Peru S. A. C.
- Oceanic Enterprise Ltd.

(one natural person and four foreign legal persons) be listed on the sanctions list.

Following Chen Shih-Hsien's passing on 22 June 2019, the Ministry of Justice announced on 25 November 2019 the removal of Chen Shih-Hsien from the sanctions list. However, the four sanctioned foreign legal persons remain on the sanction list.

Chen Shih-Hsien's widow reached out to the Ministry of Justice in 2020, expressing her intention to dissolve the four foreign legal persons. However, to date, Chen Shih-Hsien's widow has not submitted any relevant dissolution documentation. Consequently, the four foreign legal entities continue to be included on Chinese Taipei's designated sanctions list.

Source - Chinese Taipei

Case Study # 94: Legal persons related to Tsang Yung-Yuan

Terrorism financing

On 23 February 2018, The U.S. Office of Foreign Assets Control (OFAC) sanctioned Chinese Taipei national Tsang Yung-Yuan. Following the United Nations Security Council Resolution 1718 on 30 March 2018, the United Nations Security Council included:

- Tsang Yung-Yuan.
- Kingly Won International Co., Ltd.
- Pro-Gain Group Corporation

in the United Nations Security Council sanctions list. Therefore, on 31 March 2018, Chinese Taipei's Ministry of Justice included these three persons on Chinese Taipei's sanctions list.

This means any Chinese Taipei person is prohibited from providing any property or property interests to the sanctioned persons or engaging in any act involving changes in their property or property interests. Given that this case involves United Nations Security Council-imposed sanctions and designation by the Ministry of Justice, removal from Chinese Taipei's sanctions list cannot occur without following the UN Security Council's removal procedure. To date, the United Nations Security Council has not removed these three persons from the list, thus the sanctions remain in force domestically.

Source - Chinese Taipei

3 - MONEY LAUNDERING AND TERRORISM FINANCING TRENDS

This section of the typologies report includes information from members about research and studies being undertaken (part 3.1), members' reports about ML/TF trends observed over the 2023-2024 period (part 3.2) and their 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[81]. 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[82].

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

3.1.1 Australia

The *Money Laundering in Australia National Risk Assessment*[83] assessed crimes that generate illicit proceeds, as well as the methods and channels used to launder funds in Australia. It also examines the international and domestic drivers that influence the Australian environment and considers how Australia mitigates and combats money laundering activity, including where improvements could be made.

The key theme to emerge from the assessment is 'persistence': persistent exploitation of channels that have historically been used to launder funds (e.g. banks, remitters and casinos); persistent exploitation of high-value assets like luxury watches, vehicles and real estate; and persistent involvement of professional service providers to help establish complex business structures and associated banking arrangements to help individuals launder funds and conceal wealth.

Another theme to emerge from this assessment is the criminal exploitation of legitimate financial channels, assets and services. Core features of Australia's domestic economy, such as cash, bank accounts, payments technology, business structures and trusts, are also used by money launderers to place, layer and integrate criminal proceeds.

Underpinning many money laundering activities in Australia is opacity, anonymity and a lack of transactional visibility. The use of cash, trusts, identity crime, mule accounts and third-party transactions that obscure identity, beneficial ownership or financial flows, continues to be a mainstay of money laundering. Key findings:

- Australia's economy is exploited by money launderers. Lawful domestic financial channels remain fundamentally important pathways for money launderers to place, layer and integrate funds domestically and internationally.
- Australia remains an attractive destination to store and integrate criminal proceeds because of its stable political system, open and free economy, independent legal system, well-developed financial services sector and strong real estate market.
- Crimes generating the highest value of illicit proceeds that require laundering are assessed to be drug offences (including cultivation, manufacture and trafficking), tax and revenue crimes, as well as defrauding government-funded programs.
- Criminals continue to use established channels such as cash, luxury goods, real estate, domestic banks, casinos and remitters to launder funds in Australia.
- Criminal use of digital currency, digital currency exchanges, unregistered remitters and bullion dealers is increasing.

[81] 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
[82] Department of the Treasury - *2024 National Terrorist Financing Risk Assessment*: https://home.treasury.gov/system/files/136/2024-National-Terrorist-Financing-Risk-Assessment.pdf
[83] AUSTRAC - *Money Laundering in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Money%20Laundering%20NRA.pdf

- The increased speed of financial transactions in recent years has made it harder for reporting entities to identify and freeze suspicious transfers before funds leave an account. This is further complicated when individuals open and transact through multiple products across multiple financial institutions.
- Opaque legal structures can be created in Australia and used by criminals to help conceal their identity and illicit activity. These structures can limit or obscure visibility of the ultimate beneficial owners of corporate entities, assets and financial infrastructure. They create a significant money laundering vulnerability for Australian authorities and industry.
- The use of professional service providers, either witting or unwitting, to establish, advise on or operate corporate and financial infrastructure also reduces visibility of ultimate beneficial ownership and creates money laundering vulnerabilities for Australian authorities and industry.

The *Terrorism Financing in Australia National Risk Assessment*[84] assessed the risk associated with the methods and channels used to finance and support terrorism activity. It also examines the international and domestic drivers that influence the Australian environment and considers how Australia mitigates and combats terrorism financing activity and where improvements could be made. The NRA noted the following:

- The number of violent extremists who have both the intention and capability to undertake terrorist attacks in Australia has decreased in recent years. However, violent extremists across the ideological and religious spectrums continue to connect and radicalise. Any terrorist attack is most likely to be conducted by a lone actor or a small group.
- Australia's terrorism financing environment is small scale and low value. Domestic terrorist attacks are infrequent and are usually committed by individuals, known as lone actors, who self-fund their activities and often lack a detectable financial element. When financing is evident, it usually involves the direct provision of a weapon or small amounts of cash by known associates of the offender.
- Australia is primarily an exporter of small-scale terrorism financing funds flows to offshore terrorist organisations and affiliated groups. Organisations assessed as most likely to receive funds or support from Australians include Islamic State, al-Qa'ida and both their respective affiliates, and Hamas and Hezbollah to a lesser extent. The scale of funds to support foreign fighter travel has decreased, in line with fewer individuals participating in offshore conflicts.
- Terrorists and their financiers largely continue to use the same established methods for raising funds. The use of personal funds and contributions from individual supporters, often under the guise of charitable giving, provide a viable revenue stream for both domestic and offshore funding. For violent extremists across the ideological and religious spectrums, the use of social media, communication, and crowdfunding platforms have become integral to recruitment and fundraising activities. Terrorist financiers also continue to prefer readily available and proven methods to move funds, such as banking, remittance and exchange of cash, over complex schemes. An uptick in the use of digital currencies has been observed, but there is no evidence to suggest it will overtake more simple methods over the next three years.
- TF can be difficult to detect. Transactions conducted through regulated financial channels often mirror legitimate financial activity and do not raise suspicion. The increased speed of financial products in recent years has also made it harder for reporting entities to identify and freeze suspicious transfers before funds leave an account. Funds can also be raised or moved via less visible channels such as cash or unregistered remittance dealers.
- Australia's CTF regime, operational capabilities and investigative outcomes nationally and in the Southeast Asia region have evolved substantially in recent years. Operational CTF working groups collaborate across government agencies and national boundaries to share intelligence and coordinate activities and provide a significant toolkit for disrupting terrorism and terrorism financing actors.
- Financial intelligence efforts continue to evolve from a largely reactive role in monitoring suspected violent extremists and supporting investigations, towards a proactive role in countering violent extremism. Public private partnerships have enabled national security agencies and members of Australia's largest FIs to share classified information in near-real time. This is a critical element in

[84] AUSTRAC - *Terrorism Financing in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2024-07/2024%20AUSTRAC%20Terrorism%20Financing%20NRA.pdf

preventing and countering violent extremism given the sometimes rapid and unexpected escalation to acts of violence.

3.1.2 Hong Kong, China

Hong Kong, China (HKC) is currently conducting its 3rd ML and TF Risk Assessment (3rd HRA). Based on the latest quantitative and qualitative data, key findings of risks include:

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

3.1.3 Indonesia

Indonesia conducted a *Risk Assessment of Money Laundering and Terrorism Financing from Human Trafficking and Migrant Smuggling 2023* (data period: January 2018-June 2023). Key findings:

- Trends, modus operandi and structure of organisations and networks, and flow of funds indicative of ML crimes originating from human trafficking, migrant smuggling and labour smuggling
- Currently, the trend of indications of ML crimes originating from criminal acts of human trafficking, migrant and labour smuggling in Indonesia is increasing, based on the PPATK financial intelligence database during the 2017 to 2023 period, it has reached 159 financial intelligence products. PPATK financial intelligence data shows that there are various categories of forms of exploitation from human trafficking and migrant smuggling, including: child and sexual exploitation, ship crew, migrant workers/domestic workers, child adoption without going through procedures, organ and forced labour (forced to participate in online scamming).
- Based on the flow of funds, PPATK has identified based on the suspicious financial transaction reports during the 2019 to 2019 period. Semester I of 2023 which has been reported by 79 (seventy-nine) reporting parties amounting to USD 5.3 million. According to the PPATK database of the migrant worker distribution companies' population (licensed and unlicensed) there were 59 suspicious financial transactions involving 8 Indonesian migrant worker placement company (P3MI) with active status and 5 migrant worker distribution companies with inactive status with a total nominal value of suspicious financial transactions reaching USD 2.5 million. The indications of predicate criminal acts identified include criminal acts of human trafficking, fraud/embezzlement, and narcotics for the reason of reporting suspicious financial transactions, including requests from PPATK and/or law enforcement, negative reporting in media news regarding indications of human trafficking, and financial transactions involving deviated from the profile.
- Based on the PPATK database and the results of data searches from reporting parties who are respondents, it has been identified that there are very massive and significant financial transaction activities among unlicensed migrant workers, both domestic transactions and funds coming in from/out of the jurisdiction carried out by 37 migrant worker distribution companies. which has inactive status and there are several migrant worker distribution companies that have been reported as having suspicious financial transactions, including 37 migrant worker distribution company entities with total incoming funds of IDR 1.96 trillion (~ USD 129 million). Based on the results of the analysis and in-depth study, there are various maps of human trafficking and migrant smuggling networks according to regional distribution, where the majority occur in the Asia Pacific and Middle East regions, either through conventional approaches, social media propaganda or job vacancy websites, under the guise of job training institute propaganda, and non-procedural placement by licensed and unlicensed migrant workers.
- The high risk on ML by types of exploitation, forms of sexual exploitation; use of physical, sexual, reproductive organs; and Indonesian migrant workers have a high level of risk. There is an increasing trend in cases of human trafficking and reporting of various forms of exploitation, especially the phenomenon of online scamming which has become an emerging trend by utilising information technology, such as websites and social media.

- The trend in human trafficking and forms of exploitation, especially the phenomenon of online scamming, investment fraud (such as: pig butchering) with domestic and overseas targets, and also there are emerging trend by utilizing information technology, such as websites and social media.

Red flag Indicators on Human Trafficking:

- Entity (actor or party):
  - Transaction actors from unlicensed recruitment and job placement entities.
  - The perpetrator of the transaction is a suspect in a human trafficking case.
  - Perpetrators carry out social engineering to recruit through social media, websites or job search platforms that are fake or do not have credibility.
- Transaction:
  - Use of transaction news with the words: fees for Indonesian workers, labor, pompom, passport, immoral or pornographic sentences, handling TKW, tickets, gurda, nier, sinjang, workforce, workers.
  - Receipt of incoming funds from labor agencies in jurisdictions that do not have cooperation agreements between jurisdictions and do not have regulations on labor protection.
  - Receipts of funds go to several high-risk areas as a source and transit for sending and placing workers, as well as jurisdictions that have not implemented ratification of international provisions, such as not implementing regulations regarding the protection of migrant workers, social security regulations for migrant workers, jurisdictions that still have dual power (Libya, Iran, Syria), jurisdictions in conflict or war (Russia, Ukraine, Lebanon), jurisdictions that do not welcome foreign workers (Lebanon).
  - Use of the banking sector, money remittances and money changers as funds transfer and foreign exchange services.
  - Transaction patterns are pass-by, transactions do not match the profile and business field.
  - Using the co-mingling transaction method by mixing crime proceeds with the proceeds of legitimate business ventures or investment products.
  - Use of cash deposits and withdrawals via ATM machines with a structuring pattern (a number of transactions carried out on the same date).
  - Placement of funds in the form of a safe deposit box.
- Activity:
  - Purchase of travel tickets in significant quantities and repeatedly.
  - Negative reporting in the mass media.
  - Transaction actors from employment training institutions impersonate themselves as labor distributors.
  - Financial transaction activities do not match the characteristics or customary transaction patterns, namely involving law enforcement officers who have authority on land, sea and air.
  - Use of employee accounts from Indonesian migrant worker placement companies.
  - Significant cash withdrawals in international border areas.
  - High frequency financial transactions via the internet to avoid financial service officers.

3.1.4 Japan

Japan published its *National Risk Assessment-Follow up Report* on 7 December 2023, (and will publish an English translation version in late 2024).

3.1.5 Lao PDR

Lao PDR conducted its second Money Laundering and Terrorist Financing NRA (NRA) to assess threats, vulnerabilities, gaps, methods, and trends related to all predicate offenses stipulated in the AML/CFT Law in 2023. It will be completed and made public in late 2024. Lao PDR has also conducted a sectoral ML/TF risk assessment, focusing on high-risk sectors such as banking, casinos, real estate, VASPs, NPOs and legal persons.

3.1.6 Malaysia

Malaysia noted fraud, corruption, illicit drug trafficking, organised crime, and smuggling remain the prevailing crimes domestically as identified in its 2020 NRA.

Malaysia is in the process of completing its NRA 2023 due for completion by the latter half of 2024. The primary objective of the NRA is to identify, assess, and understand the ML/TF risks within the jurisdiction, encompassing threats, inherent risks within various sectors, control measures, pertinent emerging trends, and the interconnection between sectoral and threat evaluations. The NRA also covers emerging trends and patterns since the last iteration of the NRA.

3.1.7 Philippines

AMLC conducted and published the following studies on ML/TF in 2023:

- *Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*[85] (May 2023).
- *Typologies Brief: Money Mules*[86] (January 2023).
- *Analysis of Suspicious Transactions Associated with Casino Junkets*[87] (January 2023).

3.1.8 Singapore

The key risks for Singapore continue to relate to misuse of legal persons, corruption, trade and tax-based ML, as well as syndicated ML, including cyber-enabled fraud. As a financial centre, Singapore remains vigilant to the potential ML risk arising from the wealth management sector.

Case Study # 95: Strengthening Singapore's AML/CFT regime through whole-of-government coordination

Organised criminal group; fraud; self-laundering; financial institutions

The Singapore Police Force (SPF) launched a comprehensive, coordinated intelligence probe after receiving information on suspicious activities, including suspicious transaction reports on the use of suspected forged documents to substantiate sources of funds in bank accounts in Singapore. This led to one of Singapore's largest AML law enforcement operations to-date. In August 2023, the SPF charged ten persons for offences including laundering proceeds from overseas criminal activities and their assets in Singapore were seized/prohibited. As of June 2024, all ten persons have been convicted and sentenced to imprisonment terms ranging from 13 to 17 months for offences including ML and fraudulently using forged documents. About SGD 944 million (~ USD 734 million) of assets linked to them, which is more than 90% of their seized/prohibited assets, have been forfeited to the State.

This case is a reminder that Singapore's AML/CFT regime will need to keep pace with evolving ML risks and typologies and that these efforts are a constant endeavour. Learning from the case, an Inter-Ministerial Committee (IMC), comprising of officials across multiple government ministries and agencies in Singapore, has been set up to look into further measures to strengthen Singapore's AML/CFT regime. Broadly, the review by the IMC focuses on the following three areas:

- To prevent the misuse of corporate structures from being misused by money launderers.
- To enhance FIs' controls and collaboration, and the effectiveness of DNFBPs in safeguarding Singapore's financial system.
- To strengthen monitoring and sense-making capabilities across government agencies to facilitate early detection of suspicious activities and subsequent intelligence sharing.

The IMC's work is ongoing.

[85] Anti-Money Laundering Council - *Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*: http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf
[86] Anti-Money Laundering Council - *Typologies Brief: Money Mules*: http://www.amlc.gov.ph/images/PDFs/PR2023/2022%20DEC%20TYPOLOGIES%20BRIEF%20MONEY%20MULES_For%20Publication.pdf
[87] Anti-Money Laundering Council - *Analysis of Suspicious Transactions Associated with Casino Junkets*: http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATED%20WITH%20CASINO%20JUNKETS_FINAL.pdf

Source - Singapore

In March 2023, the Monetary Authority of Singapore (MAS) issued a circular on *Money Laundering and Terrorism Financing Risks in the Wealth Management Sector*[88]. This circular reminds all financial institutions (FIs) to stay vigilant to the ML/TF risks in wealth management sector and sets out MAS' expectations for FIs to review its existing controls to ensure that they remain adequate to mitigate the ML/TF risks from high growth areas. MAS also conducted an industry-wide survey of CFT controls and followed-up with a series of thematic reviews to assess the FIs' TF risk understanding and examine the effectiveness of their CFT-related controls.

In May 2023, MAS published a guidance paper *Strengthening Financial Institutions' (FIs) Countering the Financing of Terrorism (CFT) Controls*[89]. This paper was based on the MAS observations from an industry-wide survey of CFT-related controls and a series of thematic reviews conducted in this area. It sets out MAS' key observations, and highlights MAS' supervisory expectations that FIs should review against their own controls. Following the publication of the guidance paper, MAS advised FIs to benchmark themselves against the practices and supervisory expectations set out in the guidance paper in a risk-based and proportionate manner, and to conduct an analysis of their gaps.

To ensure that FIs remain vigilant to the change sanctions risks landscape, MAS had also issued a circular in August 2023 on *Ensuring Effective Detection of Sanctions-Related Risks*[90]. In particular, the circular encouraged FIs to continue to ensure strong board and senior management oversight on sanctions-related risks, and strengthen its sanction-risk detection capabilities, including through the use of data analytics.

Furthermore, the sectoral regulators and LEAs in Singapore actively partner with the industry partners to collaboratively identify, assess, and mitigate ML/TF risks. The AML/CFT Industry Partnership (ACIP) is one such public-private partnership initiative, co-chaired by the Commercial Affairs Department (CAD) of the Singapore Police Force and the Monetary Authority of Singapore (MAS). ACIP has published best practices papers for combating ML/TF, including the *Industry Perspectives on Best Practices - Management of Money Laundering, Terrorism Financing and Sanctions Risk from Customer Relationships with a Nexus to Digital Assets*[91] in July 2023, and the *Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risk Associated with Receiving Referrals from Corporate Service Providers*[92] in February 2024.

3.1.9 Vietnam

Vietnam has completed its ML/TF NRAs in 2024 and developed action plans for mitigating high and medium risks. According to the results of the ML/TF Risk Assessment for legal persons.

Vietnam is not considered an attractive jurisdiction for foreign jurisdictions to establish a company due to legal regulations, including strict regulations for foreign investment and taxes. Vietnam is reviewing the criminal liability of its domestic legal persons and is proposing amendments to its Enterprise law to include beneficial ownership obligations.

[88] Monetary Authority of Singapore - *Money Laundering and Terrorism Financing Risks in the Wealth Management Sector*: https://www.mas.gov.sg/-/media/mas/regulations-and-financial-stability/regulatory-and-supervisory-framework/anti_money-laundering_countering-the-financing-of-terrorism/circular--mltf-risks-in-the-wealth-management-sector-3-mar-2023.pdf
[89] Monetary Authority of Singapore - *Strengthening Financial Institutions' (FIs) Countering the Financing of Terrorism (CFT) Controls*: https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidance/amld/strengthening-fi-cft-controls/strengthening-fi-cft-controls.pdf
[90] Monetary Authority of Singapore - *Ensuring Effective Detection of Sanctions-Related Risks:* https://www.mas.gov.sg/-/media/mas-media-library/regulation/circulars/amld/circular---ensuring-effective-detection-of-sanctions-related-risks.pdf
[91] The AML/CFT Industry Partnership - *Industry Perspectives on Best Practices - Management of Money Laundering, Terrorism Financing and Sanctions Risk from Customer Relationships with a Nexus to Digital Assets:* https://abs.org.sg/docs/library/acip-best-practices-for-the-management-of-ml-tf-and-pf-risks-from-customer-relationships-with-a-nexus-to-digital-assets_100723-(publish).pdf
[92] The AML/CFT Industry Partnership - *Best Practices for Financial Institutions to Manage Money Laundering, Terrorism Financing and Proliferation Financing (ML/TF/PF) Risk Associated with Receiving Referrals from Corporate Service Providers:* https://abs.org.sg/docs/library/acip-best-practices-for-banks-to-manage-ml-tf-pf-risks-associated-with-receiving-referrals-from-corporate-service-providers.pdf

3.2 Observations on emerging trends; declining trends; continuing trends

UNODC - *Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat*.

Southeast Asia faces unprecedented challenges posed by transnational organised crime and illicit economies, and in recent years has become a testing ground for new technologies. Fundamentally, the expansion of the illicit economy has necessitated a revolution in the underground banking systems of the region.

Southeast Asia's booming casino industry, followed by connected junkets, then online casinos, e-junkets and increasingly illegal and underregulated cryptocurrency exchanges have become foundational pieces of the banking architecture organised crime are using. Casinos and related businesses have proven both capable and efficient in moving and laundering massive volumes of state-backed fiat as well as cryptocurrencies undetected; creating channels for effectively integrating billions of dollars in criminal proceeds into the formal financial system.

At the same time, the development of scalable and digitized solutions has supercharged the criminal business environment across Southeast Asia, particularly in the Mekong region, creating opportunities for those who have made the region their base of operations. In turn, this has attracted criminal networks, innovators, and service providers to circle around, support, and benefit from the various illicit markets in the region while simultaneously driving the need for underground banking.

The UNODC developed this report through extensive examination and analysis of criminal indictments, case records, financial intelligence, court filings, and related public disclosure, as well as consultation with both international and regional law enforcement and criminal intelligence partners over more than a year. It represents a unique attempt to understand the mechanics, intricacies, and drivers of underground banking in the region. The report makes a number of broad recommendations intended to help jurisdictions in the region address the identified findings and vulnerabilities, and ultimately to strengthen the awareness, understanding, and capacity of governments, oversight authorities, and law enforcement in Southeast Asia, and particularly those in the Mekong region.

The Financial Action Task Force - *Crowdfunding for Terrorism Financing*

Crowdfunding activity has grown in recent years and experts expect that it will continue to rise. Some estimates have valued the global crowdfunding market at USD 17.2 billion in 2020 and note that it is expected to reach USD 34.6 billion by 2026.[93] Previous FATF research has shown that soliciting donation through online crowdfunding is a known method of TF.

This report[94] builds deeper knowledge of the methods and techniques used by individual terrorists, terrorist organisations and violent extremists, through crowdfunding, to finance all types of terrorist activity. This report also builds a common understanding of the different types of crowdfunding activities, placing focus on the ones that pose the highest TF risk.

Experts from Canada and Spain co-led the project team with support from the FATF Secretariat. The project team consisted of experts drawn from 12 members of the FATF Global Network and one observer: Canada, the European Commission, France, Greece, India, Italy, Japan, Philippines, Spain, Türkiye, the United Nations (CTED), and the United States.

The findings in this report are based on: A review of existing literature and open-source material on this topic, including reports by the FATF, FSRBs, and FATF members and observers; Responses to a questionnaire sent to the FATF's Global Network. Forty delegations provided information on a variety of topics including risk indicators and case studies of crowdfunding for TF; Discussions and insights shared by FATF members and observers, academia, think tanks and the private sector at the FATF's Joint Experts Meeting in India (April 2023) and the Seminar on Countering Terrorist Financing hosted by Spain (September 2023); and Written input from the private sector and NPO Global Coalition on FATF.

Key findings, recommendations

The report notes four main ways in which crowdfunding platforms can be misused for TF purposes, and in practice, terrorists and violent extremists rely on multiple methods to raise funds and may combine various

[93] Market Data Forecast - *Global Crowdfunding Market Research Report*: www.marketdataforecast.com/market-reports/crowdfunding-market
[94] FATF *Best Practices and Guidelines on the Fight against Proliferation Financing - Strengthening Authorities for Action* - https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Speech-psi-political-meeting-may-2018.html

techniques. While certain jurisdictions and industry participants proactively implement measures to mitigate these risks, AML and counter-terrorist financing (AML/CFT) regulation is not consistent across the globe. Donations-based crowdfunding, noted by jurisdictions across the Global Network to be the most vulnerable to TF misuse given its characteristics, often falls outside of AML/CFT regulations. One reason for this is that many jurisdictions do not systematically assess the risks related to crowdfunding activity and therefore comprehensive data about its misuse is still generally lacking. The diverse nature of the crowdfunding industry, the multiple crowdfunding models that are used, and the rapidly evolving nature of the payment technologies also help explain the different regulatory approaches that exist to date in different jurisdictions.

The report highlights the challenges that government authorities and stakeholders in the crowdfunding ecosystem encounter in detecting and deterring TF. Law enforcement agencies investigating suspected cases of TF linked to crowdfunding face challenges in proving the funds were used for terrorism-related offences. The complexity of crowdfunding operations, lack of data, and the use of anonymizing techniques also complicate tracing efforts for law enforcement, reporting entities and supervisors. Intermediary platforms that offer crowdfunding services can have difficulty identifying TF activity on their sites because of limited training and TF expertise among their staff, and often lack reporting mechanisms to flag potential TF to the authorities. Efforts to take action to remove illegal content varies by company.

Jurisdictions reported examples of best practices to address these challenges, for example by improving understanding of the nature and scope of the domestic crowdfunding industry and including crowdfunding in their NRA. Conducting outreach in the crowdfunding sector has also proved effective in improving identification and reporting of potential TF activity. Strong domestic and international information sharing mechanisms as well as public-private sector engagement is also at the basis of effective counterterrorism and AML/CFT efforts.

This report recommends that jurisdictions and all stakeholders involved in the crowdfunding industry identify and understand TF risks associated with this activity and have proportionate risk-based measures in place to mitigate potential misuses, in line with United Nations Security Council Resolution 2462. Due to the global reach of crowdfunding, jurisdictions should be aware of the cross-border nature of fundraising activity and guard against their jurisdiction being used to finance terrorism abroad. Jurisdictions should also take into account that the sector is evolving and therefore TF risks may change over time.

Public-private information sharing should also be a priority for jurisdictions, and they should engage in continuous outreach and awareness raising to private sector stakeholders. This practice improves detection of potential TF activity, fosters better mutual understanding of the industry and control mechanisms, and helps ensure that legitimate crowdfunding activity is not restricted. Given the link between crowdfunding and other financial and non-financial sectors, jurisdictions should fully implement the FATF Standards relevant to VA, NPOs and money or value transfer services, and avoid treating crowdfunding as a siloed sector. Finally, jurisdictions should ensure a multi-stakeholder approach that includes competent authorities, private sector, civil society and academia when developing risk mitigation strategies related to crowdfunding, to ensure human rights due diligence and avoid hindering legitimate fundraising activity.

The report also includes a list of risk indicators to help public and private sector entities, and the general public identify suspicious activities related to crowdfunding.

3.2.1 Canada

Emerging: In Canada, the legalisation of cannabis has created opportunities for organised crime to exploit a grey market for illicit cannabis sales through online cannabis dispensaries. These companies exploited electronic funds transfer systems to obfuscate the source of funds through multiple shell companies owned by professional money launderers (PMLs), thus shielding the PMLs from knowledge of the source of funds; and also effectively layering the funds to prevent the loss of all funds to forfeiture.

Continuing: Canada continues to see trafficking of illicit narcotics including methamphetamine, fentanyl, and cocaine as a major predicate offence associated to ML, associated with ML techniques such as the use of numbered corporations to place proceeds of crime (POC) in the legitimate economy through purchases of real property, the use of structuring and cuckoo smurfing to integrate POC into financial institutions, and the use of (Informal Value Transfer System) IVTS to convert or move bulk cash.

Transnational serious and organised crime groups continue to use cryptocurrency both to purchase wholesale supplies of illicit narcotics for resale, as well as to receive payment from customers. Tied into this is the emerging use of AI and/or deepfake technology to counterfeit identification documents and subvert know your client efforts of certain VASPs.

3.2.2 Cook Islands

The Cook Islands noted continuing trends for predicate offences involving drug trafficking, fraud and corruption.

3.2.3 Hong Kong, China

Emerging trends: Over the past few years, the VA market has been developing rapidly, and VAs have been used in the course of laundering proceeds of crime. Sometimes, arrestees who had received proceeds of crime claimed that the transactions in their accounts were related to their genuine cryptocurrency trading and denied knowledge of the proceeds of crime.

In some cases, ML syndicates / money mules used fake identity documents or deepfake technology for authentication. While case numbers remained low at the moment, attention is being paid to these sorts of activities.

Also, the introduction of new cross border payment mechanism fosters the financial transactions between HKC and other jurisdictions but on other hand, exposes HKC to potential transnational ML risks, for example, cross-border layering. By transferring crime proceeds between HKC and other jurisdictions, syndicates can create layers of cross-border payments, causing substantial delay to law enforcement agencies in tracing the flow of funds.

Continuing trends: Fraud-related crime continued to be the most common predicate, followed by drug-related offences. Other predicate offences in HKC, including foreign tax evasion and foreign corruption, remained stable. The banking sector continued to be the most popular conduit for ML activities.

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

- ML syndicates recruited non-residents, students and low-paid stooges to open bank accounts for a small monetary reward.
- In some cases, the recruitment of stooges was also identified as an employment fraud. Some criminals were alleged to be employing staff on behalf of companies with different kinds of business (where the company may not even exist) and instructed the jobseekers to open a bank account (usually personal account in their own name). These accounts were used to handle transactions and funds, alleged to be related to business operations however, it was later revealed that the funds were the proceeds of crime from victims of fraud cases.
- In recent cases, domestic helpers were recruited as stooges.

The increase in bank's using remote onboarding processes has continued to lead to a high level of involvement of bank accounts (both traditional and virtual banks) in criminal activities:

- Criminals also recruited money mules to set up virtual bank accounts.

Over the past years, predicate offences involving the use of the internet, email, and social media are increasingly common due to the advancement of technology and the prevalence of electronic financial services.

The misuse of stored value facilities (SVFs) remains popular:

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

Declining trends: The use of offshore companies to facilitate ML activities has become less popular as reporting entities have enhanced their CDD requirements to identify beneficial owners of all types of companies.

3.2.4 Indonesia

Indonesia has carried out ongoing ML and TF risk assessments. Risks and emerging trends have been identified, including:

- Legal Persons:
  - The emerging trend of ML and legal persons is the use of vulnerable apostille documents for investment purposes from jurisdictions that have not complied with the apostille convention and the use of virtual corporations or virtual offices.
  - The use of fictitious entities, companies having unclear legality, such as not having a business license or institutional permit or both, as well as the use of nominees or front men or straw men such as registered close associates and family members. in legal structures to hide the identity of the true beneficial owner and the mingling of funds.
- Financial Technology (FinTech):
  - Fraud is the type of predicate crime that is high risk for ML in financial technology, Embezzlement, gambling and corruption have medium risks.
    - Industrial sectors that have high risk for ML include commodity futures trading, crypto assets, money remittance, banks and e-money and e-wallet providers.

Financial technology for Investments and Remittances and Payments face high risks and an emerging trend for ML/TF, as set out in the table below:

Payment and Remittances	Lending	Crowdfunding	Investment	Others
Transactions with complex layering schemes, for example: deposit and disbursement transactions that do not directly use a bank account but through several transaction services (including: digital wallets, currency conversion websites). Misuse of electronic wallets for storing and transferring online gambling proceeds. Cash withdrawal and cash deposit features are used as a means to cut	The funders and recipients of funds in online loans are conspiring. ii. Virtual account payments for online loan transactions do not use the account recorded on the online loan account.	For crowdfunding activities, we did not obtain examples of new ML/TF threats from respondents, but in the election context we identified the potential for collecting election funds through social crowdfunding mechanisms. Crowdfunding can obscure the origins of funds because the source of funds comes from the community and can also potentially exceed the limits on individual donations.	Crypto transactions outside the market (transactions on private block chains, transactions between individuals directly/Person-to-Person/P2P). Crypto asset transactions using exchangers abroad. Investment via e-commerce. Examples are online mutual fund investment, gold investment in collaboration with e-commerce platforms. Digital wallet/digital money transaction agreements via social media (usually for buying	Creation of fictitious corporate (merchant) accounts used for ML activities. ii. Abuse of buy now, pay later by criminals to purchase goods.

off the flow of funds. iv. Cross-border QR payments.			and selling crypto assets). Non-fungible tokens. Investment payments by third parties.	

3.2.5 Japan

Japan provided the following tables:

(Numbers and Ratios of Cleared ML cases under the act on Punishment of Organized Crimes and the Anti-Drugs Special Provisions Law, Categorized by Predicate Offences)

Misused transactions / Year	Domestic exchange transactions	Cash transactions	Deposit transactions	Credit Card	Prepaid payment	Crypto-assets	Legal persons	International transactions	Funds transfer services	Precious metals and stones	Legal/accounting professionals	Foreign Currency Exchanges	Financial instruments	Total
2020	110	120	96	20	11	32	14	16	1	2	1	1	0	424
2021	208	72	40	40	21	9	16	9	9	2	1	1	2	430
2022	266	105	24	55	39	16	6	7	10	1	1	0	0	530
Total	584	297	160	115	71	57	36	32	20	5	3	2	2	1,384

(Major transactions, etc. misused for ML)

Predicate Offences	Theft	Fraud	Computer Fraud	Violating of the Investment Act/ Money Lending Business Act	Habitual gambling/running a gambling venue for profit	Violating of the Immigration Control and Refugee Recognition Act	Drug-related offences	Violation of the Amusement Business Act	Violation of the Trademark Act	Document forgery offences	Extortion	Distribution of obscene materials, etc.	Violation of the Anti-Prostitution Act	Embezzlement	Armed robbery	Unauthorized creation of private electromagnetic records	Others	Total
Number of cases	701	691	220	67	38	34	33	26	26	24	20	20	18	17	13	12	61	2,021
Ratio	34.7	34.2	10.9	3.3	1.9	1.7	1.6	1.3	1.3	1.2	1.0	1.0	0.9	0.8	0.6	0.6	3.0	100

Japan analysed the cases of arrested ML offenders and information reported as suspicious transactions, and noted the following;

- Domestic exchange transactions accounted for 584 transactions (~ 42.2%), followed by cash transactions with 297 transactions (~ 21.4%) and deposit transactions with 160 transactions (~ 11.6%), accounting for the majority of transactions in which goods and services handled by depository financial institutions were misused for ML.
- There are many cases in which persons who intend to launder money have their criminal proceeds transferred to fictitious accounts in the name of others through domestic exchange transactions that enable quick and reliable transfer of funds. Ultimately, the proceeds of crime deposited into accounts through domestic exchange transactions or deposit transactions are converted into cash, which often makes it very difficult to track the funds thereafter.
- As credit card fraud has increased, so has the number of credit cards misused for ML.
- The diversification of payment methods, such as the increase in the misuse of credit cards, prepaid payment instruments, crypto assets, and fund transfer services, has led to a spread of major transactions that are being misused

3.2.6 Lao PDR

Lao PDR noted the continuing trends (indicators) identified from suspicious transaction reports in 2023, as:

- Use of personal accounts to conduct business. This is an indicator of tax minimisation/tax evasion. Instead of using the business bank account to conduct transactions, the customer uses her/his own personal bank to conduct transactions.
- Conduct of high value transactions without sufficient reason and/or inconsistent with the customer's profile.
- Frauds: the majority of suspected fraud cases identified from suspicious transaction reports are related to social media scams, call centres, and cybercrime, involving person-to-person fraud.

3.2.7 Macao, China

Common ML methods detected from STRs and ML and TF trends in 2023 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.
- Chip conversion / marker redemption / gambling on behalf of third parties.
- Use of automatic teller machines, phone banking, cash deposit machines.
- Use of cheques/account transfer etc. to transfer funds.
- Suspicious wire transfers.
- Use of online banking/ internet.
- Possible match with screening system watch-list or other blacklists.

Throughout the period from January to December 2023, GIF received 4,614 STRs, with 3,431 STRs from the gaming sector, 887 STRs from the financial sector (including banking, insurance and financial intermediaries) and 296 STRs from other sectors. During the same period, GIF disseminated 116 STRs to the Public Prosecutions Office for further investigation by law enforcement agencies. These cases were mainly related to crime syndicates and fraud.

Money laundering trends. Even while the majority of crimes, including drugs, gambling-related crimes, and theft, increased year over year, they were still lower than the 2019 level. In 2023, cybercrimes and telecommunications fraud continued to rise and were at a level higher than prior to the COVID-19 pandemic. The Judiciary Police (PJ) are guided by three concepts they are using to adapt to changes in the criminal environment. These concepts focus on strengthening the crackdown on gambling-related crimes, deepening the anti-fraud work, and enhancing law enforcement agencies deployment to respond to the increased risk of cross-border crimes. PJ also conducts numerous prevention and anti-crime measures that have proven effective in protecting social security and the public's legitimate rights and interests.

Terrorism financing trends. In recent years, Macao, China observed that NPOs within Southeast Asia have been misused for TF which has raised concerns. PJ has stayed vigilant to the situation and has continuously implemented a threat analysis. To date, PJ has found no relevant connection to Macao, China. Further, PJ have not identified any domestic terrorist organisation in Macao, China, and no foreign terrorist has travelled to Macao, China. Further, apart from the risk-based approach for CFT and the continuous observation on suspicious funds flows implemented by financial institutions, PJ launched the specialized Counter-terrorism investigation division in Oct 2020. This division actively analyses and investigates funds that had been remitted out to those high-risk jurisdictions. PJ found none of the investigations were related to TF so far, and the overall trend remains stable.

3.2.8 Malaysia

Based on cases reported to Malaysia's National Scam Response Centre, scams involving fake jobs, investment, telecommunication, and e-commerce remain the prevalent tactics employed by criminals:

- Fake job scams: the fraudsters commonly attract the victim with lucrative offers to gain quick and easy money such as subscribing to YouTube channels, providing feedback, or purchasing products.
- Investment scams: victims were offered to join non-existing investment schemes that promised high and quick returns with little or no risk.
- Telecommunication scams: a common tactic employed by telecommunication scam syndicates involves impersonating authorities to lend legitimacy to their schemes, playing on the victim's fear of legal authorities, leveraging the victim's personal information to gain the victim's trust.
- E-commerce scams: a noticeable increase in e-commerce scams related to festivities products during festival seasons. This surge in scams includes various deceptive practices such as counterfeit goods, fake promotions, and phishing schemes targeting buyers who are actively seeking festive-related goods.

3.2.9 Maldives

In 2023, the FIU conducted a strategic analysis of the threshold transactions (cash and electronic fund transactions above MVR 200,000 (~ USD 12,970)) for the period of January 2022 to March 2023. The FIU identified an increasing trend of trade-based money laundering (TBML) related transactions conducted by customers through the banks. This trend is consistent with the STR analysis findings of 2023.

The FIUs shared their observations with banks, law enforcement agencies and regulatory authorities, and instructed the banks to strengthen their KYC and CDD efforts to prevent TBML activities. The FIU's strategic analysis and their instructions to banks that followed resulted in a decline in TBML-related STRs during the last quarter of 2023.

Maldives noted the other trends observed from 2023 STRs include:

- Predicate offences: tax crimes, fraud and scam, embezzlement, corruption and misuse of authority, illegal foreign exchange, document forgery, drug offences, and organised criminal activities.
- Proceeds of crime involving real estate (apartments).
- Misuse of legal entities.

3.2.10 Philippines

Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines[95] (May 2023)

The number of OSAEC-related STR submissions by CPs has generally increased, reaching 92,200 by the end of 2022, up from 204 in 2015. Likewise, STRs were filed for: child pornography (94.47%), human trafficking & people smuggling (0.69%), photo & video abuse (0.75%), and other circumstances Identified (4.05%). Notably, 73% of OSAEC-related STRs were proactively disclosed as a result of the CPs' internal screening and/or investigations on clients' transactions which were determined to be consistent with OSAEC typologies. Meanwhile, the remaining 27% were reactively reported by CPs, the majority of which were triggered by AMLC referrals.

Analysis of Suspicious Transactions Associated with Casino Junkets[96] (January 2023)

The study underscored the junket system's inherent vulnerability to ML/TF risks due to the associated substantial volume and value of suspicious transactions.

Analysis of STRs in Dataset 1[97] indicated a rising trend in volume from 2021 onwards. Oddly, the volume of STRs was highest in 2023, notwithstanding the fact that Dataset 1 only captured the first 18 days of the year. Upon closer inspection, it was found that these STRs were filed by four CPs on 17 individuals (11 of which are Filipinos, four from Jurisdiction B, and two from Jurisdiction C). The reporting CPs disclosed that these individuals (1) were allegedly involved in a criminal syndicate being investigated for a Ponzi or pyramiding scam; (2) had cash-in and chips redemption transactions but did not participate in any gaming activities; (3) performed bank transactions that were not commensurate with their profile; or (4) lacked documents to support the legitimacy of their transactions.

Meanwhile, the annual value of junket-related STRs seems to have spiked every three years, starting in 2016. The largest spike was seen in 2022, where the aggregate amount of junket-related STRs reached PHP9.68 billion (or 54.42% of the total value of STRs in Dataset 1) (~ USD 168 million). This sudden increase in the value of STRs in 2022 can be attributed to 13 STRs, pertaining to junket players who deposit their casino chips with the Casino Treasury Division for safekeeping, valued between PHP100 million and PHP300 million.

[95] Anti-Money Laundering Council - *Online Sexual Abuse and Exploitation of Children (OSAEC) in the Philippines*: http://www.amlc.gov.ph/images/PDFs/Main/Online%20Sexual%20Abuse%20and%20Exploitation%20of%20Children%20in%20the%20Philippines.pdf

[96] Anti-Money Laundering Council - *Analysis of Suspicious Transactions Associated with Casino Junkets:* http://www.amlc.gov.ph/images/PDFs/PR2023/2023%20JAN%20ANALYSIS%20OF%20SUSPICIOUS%20TRANSACTIONS%20ASSOCIATE D%20WITH%20CASINO%20JUNKETS_FINAL.pdf

[97] The study utilised two sets of STRs that were mined separately from the AMLC database. Dataset 1 consisted of 3,308 STRs that were generated by pooling all STRs containing the keyword "junket" in the narrative field. Dataset 2 consisted of STRs 4,110 filed by four integrated resorts that were identified by an Appropriate Government Agency for Casinos to have the highest risk to ML/TF in their updated individual risk matrix covering the period December 2021 - September 2022.

In terms of both volume and value, the majority of the junket-related STRs in Dataset 1 were filed on the basis of suspicious circumstances enumerated under Republic Act No. 9160, as amended. The suspicious circumstance: "There is no underlying legal or trade obligation, purpose, or economic justification" (SI1) alone accounted for more than half of the sample, with a 58.71% share in the total STR volume and a 54.04% share in the total STR value. These STRs refer primarily to cases where the identified subjects failed to establish the legitimacy of account transactions due to lack of supporting documents.

Among the predicate crimes cited in the sample STRs, "Fraudulent practices and other violations under the Securities Regulation Code of 2000" comes in with the highest volume, which is equivalent to 2.24% of total STR count. In terms of value, the predicate crime "Swindling" ranks first with a corresponding value of PHP15.84 million (or 0.09% of the total STR value).

Similar to Dataset 1, the majority of the STRs pooled for Dataset 2 were filed on the basis of suspicious circumstances, particularly suspicious indicator 1: 'there is no underlying legal or trade obligation, purpose, or economic justification'. While the overall share of predicate crimes remains trivial in Dataset 2, 16 other predicate crimes that were not found in STRs submitted by CPs outside the casino sector, were reported by the high-risk integrated resorts.

3.2.11 Singapore

The key risks for Singapore continue to relate to misuse of legal persons, trade-based money laundering, as well as syndicated ML, including cyber-enabled fraud. As a financial centre, Singapore remains vigilant to the potential ML risk arising from the wealth management sector.

As set out in circular on *Money Laundering and Terrorism Financing Risks in the Wealth Management Sector*[98], FIs should stay vigilant towards higher risk customers and transactions. In particular, be cognizant of the added ML/TF risk when dealing with legal structures/arrangements used for the purpose of wealth management (such as trust arrangements) established for the benefit of the beneficial owners, take note of prospective customers that withdraw their applications due to an inability or unwillingness to provide requisite CDD information and as part of their ongoing monitoring, remain watchful of anomalous transaction spikes and unexpected fund flows with third parties or purportedly for business purposes, especially to or from higher risk jurisdictions.

Further, as set out in Singapore's *Terrorist Financing National Risk Assessment Report*, Singapore is vulnerable to the TF threat of raising and moving of funds in support of terrorists/terrorist organisations/terrorist activities overseas. Radicalised individuals continue to pose a salient TF threat to Singapore. FIs are also reminded of new and emerging international typologies in which TF can be financed, including through ransomware, arts and antiquities, and online crowd-funding mechanisms.

Singapore observed crowdfunding as an emerging TF typology, with its ability to reach a large international audience to raise funds for causes. Of note, terrorist actors may pretend to raise funds for charitable or humanitarian causes and attract unwitting victims to inadvertently donate funds to a TF cause. In this regard, Singapore has championed FATF projects pertaining to TF risks arising from crowdfunding under our FATF Presidency (2022 to 2024), which culminated in the *Crowdfunding for Terrorism Financing* report published by FATF in October 2023.

3.2.12 Chinese Taipei

Third-party payment. In recent years, third-party payment providers have been broadly used, with the payment providers acting as intermediaries between buyers and sellers of online transactions. Apart from enhancing the security, fairness, and reliability of transactions between buyers and sellers, third-party payment providers also provide convenient credit card and virtual account payment services for small-scale e-commerce sellers, thus achieving the goals of financial inclusion and e-commerce development. However, third-party payment providers have also been exploited as channels for ML recently. Criminals use money mules or shell companies to apply for financial services from third-party payment providers, then enticing victims to transfer funds to virtual accounts provided by the third-party payment provider for the purpose of collecting payments for online transactions. Once the funds are transferred to the accounts controlled by the criminals, they are then transferred multiple times through multiple accounts, or withdrawn by couriers,

[98] Monetary Authority of Singapore - *Money Laundering and Terrorism Financing Risks in the Wealth Management Sector*: https://www.mas.gov.sg/regulation/circulars/circular-on-money-laundering-and-terrorism-financing-risks-in-the-wealth-management-sector

creating breakpoints in the flow of funds to increase the difficulty of tracing the funds in investigation. Since 2019, the number of STRs related to third-party payment service providers has been gradually increasing. (2019: 462 STRs, 2020: 504 STRs, 2021: 496 STRs, 2022: 702 STRs, 2023: 1,186 STRs).

Indicators of suspicious activity include:

- Violation of regulations: Third-party payment providers violating the *Regulations Governing Anti-Money Laundering and Countering the Financing of Terrorism for the Third-Party Payment Enterprises* by entering into contracts with other third-party payment providers as payers or payees.
- Rapid cash withdrawal or fund transfer: After the third-party payment provider transferred funds to the sellers, the sellers quickly withdraw cash or transfers funds, and the withdrawals are often conducted by a group of individuals who are suspected to be money mules.
- Small capital and identical business addresses: Third-party payment providers involved in abnormal transactions often have excessively small capital and share the same business address as other similar businesses, raising concerns of the use of shell companies.
- Lack of genuine online transactions: Clients claim to operate online stores, but the website addresses provided often have invalid links, fake websites, websites lacking a shopping system for placing orders, or they are reluctant to provide online store URLs.

Online gaming platform. Online gaming platforms utilizing tradable in-game currency, have opened up a new path for ML, allowing criminals to exploit the in-game economic systems to purchase and sell virtual goods or currency for the purpose of laundering money.

Drug crime. Drug related transactions primarily involve cash payments. If there is a need for cross-border or international transactions, criminals use alternative remittance systems such as underground banking and dummy accounts. Criminals and professional money launderers also use bulk cash smuggling techniques, employing methods such as having travellers couriering cash internationally for delivery. To ensure security, mitigate risks of internal conflicts within criminal syndicates, and to evade law enforcement scrutiny, the criminal syndicates commonly separate the movements of people, drugs, and money.

The predominance of cash is also seen in the domestic drug trade, aside from a few cases involving drugs exchanged for other drugs. Commonly, cash is seized at drug bust sites however, few instances of evidence is found that indicates violation of the Money Laundering Control Act. Only when a law enforcement agency can identify related funds as proceeds of drug crimes and the flow of funds into into dummy accounts, are the elements of the crime of concealing the origin of criminal proceeds made out, and the suspects can be prosecuted for ML offenses. However, if suspects do not transfer or alter the proceeds of their drug crimes, or if their actions do not effectively conceal the source of criminal proceeds, it is difficult to prosecute as ML charges.

Law enforcement officers will seize funds found to be proceeds of drug crimes during enforcement operations. In 2020, MJIB has seized TWD 1,969,350 (~ USD 61,542) and MYR 45,673 (~ USD 9,718). In 2021, the MJIB seized TWD 17,553,856 (~ USD 548,558) and two automobiles. In 2022, the MJIB sized TWD 6,098,520 (~ USD 190,579) and one yacht. In 2023, MJIB seized TWD 6,321,400 (about USD 197,544), USD 402, six cars and one yacht.

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

3.3.1 Canada

In 2023, Canada made it an explicit offence in the Proceeds of Crime (Money Laundering) and Terrorist Financing Act to structure transactions in a manner designed to deceive a reporting entity such that the entity will not report a financial transaction to Canada's FIU. This has led to the development of new investigations into ML.

3.3.2 Cook Islands

In 2022, a drug investigation identified multiple individuals acting as money mules to deposit funds into three separate accounts. The deposits were under the cash transaction reporting threshold of NZD10,000. The transactions identified a gap in the reporting requirement, prompting discussion with the banking industry to address and reduce the reporting threshold. A proposal to reduce the reporting cash threshold was endorsed by the banking industry, Western Union, and Vodafone - Mobile Banking.

3.3.3 Hong Kong, China

In mid-2023, HKC established a licensing system and regulatory requirements for VASP. Currently, two licensed VA trading platforms, through licence upgrades, are able to offer Bitcoin (BTC) and Ethereum (ETH) trading services to retail investors. Licensed platforms are subject to rigorous regulation by the Securities and Futures Commission (SFC) to provide substantial protection for investors. The SFC also maintains a list of “Suspicious virtual asset trading platforms” which is a list of entities which have come to the SFC’s attention because they are unlicensed in HKC and are believed to be, or to have been, targeting local investors or claim to have an association with HKC. It serves as an early warning service to investors and increases the public’s general awareness.

Considering that fraud syndicates had been using a large number of stooge accounts to collect fraudulent payments and launder money, the Hong Kong Police Force (HKPF) collaborated with the Department of Justice (DOJ) to streamline the procedures for evidence gathering and prosecution to expedite prosecutions. Also, HKPF and DOJ established a protocol for applying enhanced sentencing. Since the implementation of this protocol, HKPF has succeeded in enhancing the sentences received by stooge account holders, on average by 20%.

3.3.4 Indonesia

Indonesia has identified areas where its countermeasures require improvement in its legal review "Optimizing the Implementation of the Obligation to Report Suspicious Financial Transaction Reports by Professional Reporting Parties to the Financial Transaction Reporting and Analysis Center."

Key findings

The legal review identified: Obstacles in Reporting Suspicious Financial Transactions by the Reporting Party; Factors that Influence Optimizing the Implementation of Reporting Obligations; and Required Policy Directions.

Obstacles for Professional Reporting Parties in registering GOAML applications include (i) PPATK cannot impose sanctions in the form of revoking the permit of the Professional Reporting Party; (ii) for the Advocate Reporting Party, several advocate organisations have the authority to appoint advocates; (iii) for Financial Planning Reporting Parties, there are no regulations governing the procedures for appointing financial planners as well as the agencies that have the authority to grant permits or appoint financial planners; and (iv) for Financial Planning Reporting Parties, there are financial planners in the form of financial services information technology.

Factors influencing the optimization of the implementation of the STR reporting obligations of Professional Reporting Parties to PPATK including internal factors and external factors. Internal factors are related to the limited authority of PPATK as a regulator to provide sanctions for several Professional Reporting Parties, namely Advocate Reporting Parties and Notary Reporting Parties. The sanctions that can be given by PPATK are limited to warning sanctions, that cannot have a direct deterrent effect on professional reporting parties. Therefore, it is necessary to have stronger sanctions against professional reporting parties within PPATK’s authority, such as sanctions for revoking business permits.

The policy directions needed to optimize the implementation of the STR reporting obligations of Professional Reporting Parties to PPATK include (i) implementation of training and socialization to equalize perceptions among Professional Reporting Parties; (ii) collaboration between PPATK and Supervisory and Regulatory

Institutions or Associations that have the authority to appoint Professional Reporting Parties for the imposition of sanctions; (iii) the need for a legal basis that provides regulations regarding financial planning; (iv) expansion of provisions regarding the scope of KYC that can be carried out by professional reporting parties to service users; and (v) possibility of a Trustee Concept Regulation in Service Provision Activities by Professional Reporting Parties.

3.3.5 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 2020 - 2022

Number of cleared-money laundering cases

Year / Category	2020		2021		2022	
	Number of Cases	Ratio	Number of Cases	Ratio	Number of Cases	Ratio
Number of Cleared-ML Cases	600	—	632	—	726	—
Act on Punishment of Organised Crimes	597	99.5	623	98.6	709	97.7
Anti-Drug Special Provisions Law	3	0.5	9	1.4	17	2.3

Japan noted that it had an increase in the number of suspicious transaction reports reported by regulated entities over the years 2020-2022.

Number of STRs by business type reported by competent authorities

Year / Category	2020	2021	2022
	Number of Reports	Number of Reports	Number of Reports
Financial Institutions, etc.	402,868	495,029	542,003
Deposit-taking institutions	342,226	411,683	435,728
Banks, etc.	319,812	390,381	414,651
Shinkin Banks, Credit Cooperative	19,793	18,461	18,520
Labour Banks	300	318	316
Norinchukin Banks, etc.	2,321	2,523	2,241
Insurance Companies	2,635	3,458	3,939
Financial Instruments Business Operators	17,933	19,718	19,032
Money Lenders	25,255	35,442	45,684
Fund Transfer Service Providers	6,040	10,499	20,271
Crypto-assets Exchange Service Providers	8,023	13,540	16,550
Commodity Derivatives Business Operators	320	388	318
Currency Exchange Operators	252	201	430

	Electronic Monetary Claim Recording Institutions	5	7	0
	Others	179	93	51
Financial Leasing Operators		123	163	71
Credit Card Operators		29,138	34,904	41,106
Real Estate Brokers		7	4	11
Dealers in Precious metals and Stones		63	48	124
Postal Receiving Service Providers		2	0	1
Telephone Receiving Service Providers		0	0	0
Telephone Forwarding Service Providers		1	2	1
Total		432,202	530,150	583,317

3.3.6 Macao, China

AML/CFT legislative or regulatory developments in 2023:

The *Financial System Act* (FSA) was reformulated and came into effect on 1 November 2023, to support the development of the financial sector alongside the alignment with the international regulatory and supervisory standards. From an AML/CFT perspective, the reformulation reinforces the prevention of ML/TF risks of the financial sector. It includes enhancements of licensing requirements and fit-and-proper assessments on board members, supervisory board members and the persons who effectively manage the business by specifying the AML/CFT-related prerequisites. In addition, the penalties for administrative offences including AML/CFT related violations are strengthened to enhance their dissuasive effect. Unauthorised acceptance of deposits or other repayable funds from the public is a criminal offence with increased penalty, with the aim to further combat illegal financial activities.

Revision of the Gaming Credit Law. To further promote a safe and healthy environment for the gaming sector in the new round of gaming concessions, in 2023, the Government of Macao, China strengthened the gaming legal framework through the enactment of the Law no. 7/2024 in April 2024. This law revised the gaming credit framework of casinos and at the same time revoked the previous Law no. 5/2004. The revision includes refining the principles of providing gaming credits in the gaming sector, affirming the legal obligations for record-keeping and risk management mechanisms, and providing clear rules for administrative sanctions of non-compliance, namely fine penalties and restrictive measures (e.g. prohibiting concessionaires from providing gaming credit for a period at maximum of one year). The new Law will be effective from 1 August 2024.

Revision of the Law Against Illegal Gambling (legislation in process). In December 2023, the Government of Macao, China submitted the draft bill of the Law Against Illegal Gambling to the legislative assembly, which is still under discussion and consideration by lawmakers. It is expected to be approved during 2024. The draft legislation is intended to strengthen the healthy development of gaming through enhancement in criminal procedures and consider the significant criminal threats arising from gaming. The major changes include a clearer definition for criminalisation for illegal gaming relying on Macao, China gaming results (covering side-table betting, proxy betting and online casinos), extending the criminalisation of illegal online gaming operations (even where the infrastructures are not physically present in Macao, China), and expanding the investigation power and capacity of law enforcement agencies in combating these crimes. The ultimate objective of the revision is to align with the changes in the criminal environment of Macao, China, and providing more dissuasive criminal penalties for these criminal activities, particularly increasing the years of imprisonment.

3.3.7 Malaysia

Issuance of *Revised Anti-Money Laundering (AML) /Countering Financing of Terrorism (CFT) /Countering Proliferation Financing (CPF) Policy* document.

Bank Negara Malaysia (Central Bank of Malaysia) has recently revised its AML/CFT/CPF Policy Documents for financial institutions, designated non-financial businesses and professions (DNFBPs), and non-bank financial institutions (NBFIs) which came into effect in February 2024.

The revisions are intended to align with the FATF Standards and provide clarity on the requirements imposed on reporting institutions (RIs). The major revisions are as follows:

- Imposing requirements for RIs to identify, assess, and mitigate PF risks in response to the growing threat of weapons of mass destruction and PF observed globally and ensuring that RIs do not unwittingly support designated persons.;
- Expanding the definition of financial groups, introducing the definition of DNFBP groups and other DNFBP structures, as well as the application of group-wide programs on DNFBP groups in identifying and managing its ML/TF/PF risks.
- Enhancing the requirement on non-face-to-face business relationships for corporate customers of money services business to ensure effective identification and verification of corporate customers.

As part of Malaysia's initiative to rapidly address online financial scams effectively, it established the National Scam Response Centre (NSRC) in October 2022.

As of December 2023, the NSRC identified more than 60,000 suspected mule accounts to allow financial institutions (FIs) to take immediate action to prevent further layering and dissipation of stolen funds. Collaborative efforts with FIs have resulted in the opening of 8,754 investigation papers on online financial scams by the Royal Malaysia Police (RMP) for cheating offences and frozen suspected collection accounts amounting to RM69 million (~ USD 14.6 million).

Building on the efforts of the NSRC, the National Fraud Portal (NFP) in collaboration with banks and Payments Network Malaysia Sdn Bhd (Paynet) will operate as a shared payment infrastructure in Malaysia to elevate the capability of the NSRC. The NFP will be equipped with enhanced functionalities to quickly trace stolen funds and maintain a comprehensive database of mule accounts. With access to a wider set of higher-quality information, this feature within the NFP is expected to improve how financial institutions analyse and spot mule accounts and decide on appropriate actions in response.

3.3.8 Singapore

From 2023, Singapore has enhanced our AML/CFT legislative levers to ensure that they remain effective against the evolving crime landscape.

Amendments to the Corruption, Drug Trafficking and Other Serious Crimes (Confiscation of Benefits) Act (CDSA) and *Computer Misuse Act* (CMA) in 2023. These amendments introduced new provisions to enhance LEAs' ability to combat ML. These changes empower authorities to take action against individuals acting as money mules in ML schemes and those assisting others in retaining proceeds from criminal activities and drug offences. These amendments seek to deter individuals from enabling or facilitating the commission of criminal activities by others.

Case Study # 96: Strengthening Singapore's AML/CFT regime against scams-related money mule offences

Cyber-enabled fraud

In September 2024, 40 persons were charged in court for new offences connected to scams-related money mule activities, which were introduced through the amendments to the CDSA and CMA in 2023. These new offences were introduced to curb the facilitation of scams and the movement of criminal proceeds as well as the abuse of 'Singpass' (Singapore's digital identity service). These offences came into force in February 2024 and target persons who hand over control of their bank accounts or disclose their Singpass credentials to others, who are then able to use these accounts and credentials to commit scams and launder scam

proceeds.

The Sentencing Advisory Panel has also published Guidelines that recommend significant imprisonment sentences as the norm for scams-related offences involving the handing over of bank accounts or the disclosure of Singpass credentials.

Source - Singapore

Online Criminal Harms Act in 2023. This Act granted Singapore Police Force (SPF) the authority to disrupt the recruitment of money mules by criminals for ML activities. The SPF is empowered to direct online service providers to prevent suspected scam accounts or content from interacting with or reaching users in Singapore.

Anti-Money Laundering and Other Matters Act in 2024 – This Act further enhances cross-agency data sharing to better detect ML, TF and PF; to enable LEAs to launch ML investigations into foreign serious environmental crimes; enhance ability of LEAs to pursue and prosecute ML offences; and to allow the Court to order the sale of seized or restrained properties linked to suspected criminal activities, where either of the three criteria are met:

- Parties consent to the sale.
- The value of the property is likely to depreciate, or undue costs are involved in maintaining the property.
- The sale would be in the interest of justice.

Protection from Scams Bill in 2024 This Bill empowers the SPF to issue Restriction Orders (RO) to banks to temporarily restrict the banking transactions of targets of ongoing scams who refuse to believe that they are being scammed. ROs will cover the following banking facilities. ROs will be issued for a period of 28 days in the first instance. This gives the SPF time to take further measures (e.g., continue engaging the individual and the next-of-kin, gather additional evidence to convince the individual, convince the individual to adopt the necessary banking safeguards) to stop the ongoing scam. At the end of the 28-day period, if the SPF assess that the individual is still at risk of being scammed, they will renew the RO for up to 28 days at a time. Money transfers (including online banking, mobile banking, and in person over-the-counter) out of the victim's bank accounts and into other accounts, will be suspended. Singapore will introduce a mechanism for these individuals to apply to the SPF to have access to their monies for legitimate purposes (e.g. sustain daily living, pay bills).

4 - PROLIFERATION FINANCING METHODS AND TRENDS

This section of the typologies report provides a brief overview of United Nations Interregional Crime and Justice Research Institute's PF-related work, including overviews of the *1540 Compass* reports and its report on the Southeast Asian perspective on PF. It also includes information from APG members about the PF risk assessments they have undertaken, and the publications and guidance they have issued to mitigate these risks.

Proliferation financing

Financing is an essential part of proliferation activity. Criminals often exploit weaknesses in legal and operational systems across different jurisdictions to allow them raise and move funds and carry out financial transactions. PF actors use these same means. Financial measures are one of the most effective tools jurisdictions can use to counter proliferation activity:

- Preventive measures make it difficult for criminals to raise and move funds, reducing the capacity of proliferation networks.
- Financial intelligence provides advance warning of attempts to illegally transfer sensitive goods and materials. Shipments can be discovered and interdicted on the basis of suspicious transaction reports by financial institutions.
- Every movement of goods has an associated financial transaction: financial investigation can follow the money trails to look behind declarations, analyse proliferation networks, and identify facilitators.

The *FATF Recommendations* on countering PF operationalise the financial provisions of UN Security Council Resolutions by setting specific requirements for jurisdictions to implement. They require jurisdictions to establish the necessary legal authority and identify competent authorities responsible for implementing and enforcing targeted financial sanctions (TFS) in a timely manner[99].

The *FATF Recommendations* require jurisdictions to customise their PF risk assessments and mitigation strategies to address the specific threats they encounter. These threats arise from both the jurisdiction context of their own jurisdictions and their exposure to high-risk jurisdictions. A thorough understanding of these dynamics enables jurisdictions to identify potential PF typologies they may be exposed to. This, in turn, helps pinpoint sectors or channels at greater risk, where controls need to be strengthened.

TFS are applicable to persons and entities that:

- Act on behalf of or under the direction of designated persons or entities.
- Are owned or controlled by designated persons or entities.
- Assist designated persons or entities in evading sanctions or violating resolution provisions.

With TFS in place, those intent on evasion may attempt to conceal their involvement by exploiting financial and trade services. This includes the use of trade finance products, clean payment services, and money remittance services to facilitate the procurement and payment for proliferation-sensitive goods.

4.1 Observer's initiatives

Royal United Services Institute - *Challenges for Counter-Proliferation Finance and Sanctions Control in Banking***
The Royal United Services Institute's *Challenges for Counter-Proliferation Finance and Sanctions Control in Banking* report[100] addresses the growing complexities in the global financial system due to sanctions and

[99] FATF Remarks by the FATF Executive Secretary David Lewis on *Best Practices and Guidelines on the Fight against Proliferation Financing - Strengthening Authorities for Action:* https://www.fatf-gafi.org/en/publications/Fatfgeneral/Speech-psi-political-meeting-may-2018.html#:~:text=Financial%20intelligence%20provides%20advance%20warning,transaction%20reports%20by%20financial%20institutions.

[100] Royal United Services Institute - *Challenges for Counter-Proliferation Finance and Sanctions Control in Banking*: https://www.rusi.org/explore-our-research/publications/special-resources/challenges-counter-proliferation-finance-and-sanctions-control-banking

PF challenges. As governments set regulatory landscapes to combat PF and maintain the integrity of the financial system, the responsibility largely falls on FIs to implement these regulations effectively. However, several key challenges hinder FIs in their efforts:

- Disconnect between regulatory expectations and practical implementation - FIs struggle to align regulatory expectations with practical, on-the-ground implementation. There is often a gap in understanding how to apply international and national sanctions effectively within their operational limits.
- Limited data quality and access - FIs face challenges due to limited access to high-quality data. This hampers their ability to detect and prevent PF and sanctions evasion effectively. There is a need for better data sharing and adoption of advanced technologies like distributed ledger technology (DLT) to enhance transparency.
- Limited subject matter expertise - the banking sector often lacks the necessary expertise to manage the complex and evolving sanctions landscape. The rapid changes in regulations demand continuous education and guidance from authorities to help FIs stay compliant.
- Disparity across the banking sector in PF and Sanctions Risk Assessments - there is inconsistency in how different banks assess and manage risks related to PF and sanctions. This disparity can lead to vulnerabilities within the global financial system, making it harder to enforce effective sanctions.

Recommendations:

To address these challenges, the report offers several recommendations:

- Regulatory guidance and support - competent authorities should provide clear, practical guidance for FIs on interpreting and implementing sanctions. This includes sharing best practices, step-by-step instructions, and sector-specific advice to help banks navigate complex regulations.
- Data sharing and technological adoption - the report encourages the adoption of DLT and other advanced technologies to improve data quality and access. Authorities should also consider mandating the use of Harmonised System codes for dual-use goods to facilitate detection of suspicious activities.
- Expertise development - competent authorities should invest in training and resources to help FIs develop the necessary expertise. This includes offering sector-specific guidance and supporting the calibration of transaction monitoring tools.
- Harmonisation of risk assessments - there is a need for standardised guidance on PF and sanctions risk assessments across the banking sector. Authorities should conduct reviews to identify gaps and ensure a more consistent approach to managing these risks.

Conclusion:

The report places emphasis on the importance of collaboration between governments and the financial sector to enhance the effectiveness of counter-proliferation finance and sanctions control. By addressing the identified challenges and implementing the recommended measures, FIs can better protect the global financial system from the risks associated with PF and sanctions evasion.

The United Nations Interregional Crime and Justice Research Institute - *1540 Compass*

Adopted unanimously on 28 April 2004, UNSCR 1540 stands as a cornerstone in global efforts to safeguard international peace and security. However, the challenges inherent in comprehending, implementing, and adapting to its provisions persist. Recognizing this knowledge gap, the United Nations Interregional Crime and Justice Research Institute (UNICRI) re-launched the *1540 Compass*.[101]

The *1540 Compass* is an e-journal dedicated to advancing the objectives, awareness and implementation of United Nations Security Council resolution 1540 (2004) (UNSCR 1540) and its successor resolutions. The journal aims to be a trusted source of knowledge, analysis, and dialogue for countering the proliferation of weapons of mass destruction (WMDs) and fosters a space for robust knowledge exchange, insightful analysis, and meaningful dialogue among Member States, academic experts, policymakers, practitioners and followers of everything resolution 1540 related.

The *1540 Compass* serves as a valuable resource for policymakers, practitioners, and academics involved in non-proliferation efforts. By providing a platform for knowledge exchange and dialogue, it aims to support the continued implementation of UNSCR 1540 and contribute to global security.

April 2024 edition

The April 2024 edition of the *1540 Compass* marks the 20th anniversary of United Nations Security Council Resolution 1540 (UNSCR 1540). This resolution is a significant component of global efforts to

[101] United Nations Interregional Crime and Justice Research Institute - *1540 Compass*: https://unicri.it/Publications/Magazine-1540%20Compass

prevent the proliferation of weapons of mass destruction (WMDs) and their means of delivery by non-State actors. The journal, relaunched by the United Nations Interregional Crime and Justice Research Institute (UNICRI), aims to foster dialogue and share best practices related to the resolution's implementation.

Key themes and content:

- The issue features a series of articles, interviews, and timelines that reflect on the past 20 years of UNSCR 1540. The topics range from the resolution's impact on non-proliferation efforts to the challenges faced in its implementation.
- Interviews with prominent figures, including Ambassador Mihnea Motoc, the first Chair of the 1540 Committee, and Ambassador José Javier De La Gasca, the current Chair, provide insights into the resolution's history and future direction. They also discuss the geopolitical context at the time of the resolution's adoption, its implementation challenges, and strategies for enhancing its effectiveness in the face of evolving global threats.
- The issue also explores the relationship between UNSCR 1540 and other non-proliferation initiatives, highlighting synergies and potential areas for improvement. There is also an examination of the role of the 1540 Committee in supporting Member jurisdictions, promoting transparency, and facilitating technical assistance.

Challenges and recommendations:

- Several challenges to the effective implementation of UNSCR 1540 are identified, including the need for better coordination among Member States, the complexities of managing dual-use technologies, and the ongoing threat of WMD proliferation by non-State actors.
- Recommendations for strengthening the resolution's impact include improving data sharing, enhancing international cooperation, and developing more robust legal frameworks at the national level. The importance of technical assistance and capacity-building, particularly in developing jurisdictions, is also emphasised.

September 2024 edition

The September issue of the *1540 Compass* includes three articles on PF:

- Resolution 1540 (2004) and Proliferation Finance

  Resolution 1540 (2004) and successor resolutions set out the Security Council's baseline requirements regarding WMD PF. CPF is important to combating WMD proliferation, but the Report of the 2022 Comprehensive Review did not identify a significantly higher level of implementation by States than compared to 2016. Although the 1540 Committee offered no direction in this respect, the Security Council acknowledges FATF guidance in several 1540 successor resolutions, suggesting FATF is well-placed to do so. Publishing 1540 proliferation financing implementation guidance would be a good start.

- Understanding Proliferation Financing Risk Assessments

  The renewed interest in assessing the risks associated with the financial support to WMD proliferation activities, spurred by the amendment to FATF Recommendation 1, represents a pivotal moment to accelerate the paradigm shift from a rule-based to a risk-based approach. The article argues that, despite the challenges posed by the complexity of the matter and the production of the risk assessment, it is critical that national authorities and the private sector do not miss the opportunity of assessing the risk of proliferation finance more broadly, by not only focusing on compliance with the FATF standard. Although FATF Recommendation 1 focuses on UN targeted financial sanctions related to WMD proliferation, other risks of financing WMD programmes, including the violation of resolution 1540 (2004), should not be overlooked.

- UNSCR 1540 and Indirect Proliferation Financing

  UNSCR 1540 has played a significant role over the past two decades in curbing the proliferation of WMD by non-State actors. However, its effectiveness is hampered by a lack of clarity and specificity in addressing the financing of WMD proliferation, particularly indirect financing through, for example, the trade of luxury goods. To enhance the resolution's impact, it is crucial to address these ambiguities, expand the scope of proliferation finance in the context of UNSCR 1540, and strengthen international cooperation and capacity-building initiatives.

Further, recognising the critical role that civil society plays in preventing weapons of mass destruction proliferation, the issue features two articles on how stakeholders such as industry and academia can collaborate with governments and international organisations to ensure compliance with the resolution.

The United Nations Interregional Crime and Justice Research Institute - *CBRN Proliferation Financing: A Perspective from Southeast Asia*

The United Nations Interregional Crime and Justice Research Institute's (UNICRI) - *CBRN Proliferation Financing: A Perspective from Southeast Asia* report[102] is the result of a project by UNICRI that sought to improve understanding of chemical, biological, radiological and nuclear weapon proliferation financing risks, enhance awareness of and compliance with relevant international norms, and identify priority actions at the national and regional levels to increase jurisdictions' capacities to effectively tackle PF risks. This report consolidates findings from UNICRI's research and consultations.

The report is structured in two parts. The first presents an overview of the threats in Southeast Asia associated with the risk of exposure to proliferation financing, particularly regarding weapons of mass destruction (WMD) procurement schemes, WMD proliferation networks, and revenue raising activities that evade non-proliferation sanctions programmes. The second part illustrates the proposed measures to mitigate the PF risk.

The report found that Southeast Asia is uniquely exposed to the DPRK's WMD proliferation ambitions. Geographically located in proximity to the DPRK, and characterised by extensive maritime borders, Southeast Asian jurisdictions are easily accessible to DPRK proliferation networks. Further, the expanding trade and financial hubs in growing Southeast Asian economies, coupled with the interest in developing nuclear energy programmes and chemical and biotech industries, attract WMD proliferators, who seek to misuse the services and technical assistance provided to business operators to pursue criminal purposes. PF actors exploit the lack of advanced counter-proliferation financing regimes in some jurisdictions to operate undetected in the region.

The report also gives an overview of PF in the maritime sector. Satellite imagery and information provided by Member States show that the DPRK has been violating trade restrictions imposed by the UN Security Council mainly by breaching the cap on the import of refined petroleum products and the export of sanctioned commodities, such as coal or sand. Maritime import-export operations are carried out through sophisticated tactics involving vessels - e.g. ship-to-ship transfers, misuse of automatic identification systems, false documentation - and corporate structures aiming to obfuscate the management or ownership of the vessels.

The report highlights that when, featuring as director or shareholder of the company owning or operating a vessel engaged in sanctions violation, exposes jurisdictions to PF risk. Further, providing the services required to operate a vessel: from insurance services to crew services, to vessel classification or certification, also exposes jurisdictions to PF risk Ship registration is a requirement under international law and the country of registration, or flag state, determines the nationality of the vessel, which is then allowed to sail internationally. Ship registries certify the compliance of vessels with specific standards for navigation. The provision of these forms of technical assistance to designated vessels or to vessels linked to designated entities or individuals becomes instrumental to the illicit trade and therefore to the DPRK revenue-raising.

Louis de Koker - *The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges*

Louis de Koker is a Professor of Law at La Trobe Law School and coordinator of the La Trobe LawTech research group at the Law School.

This study[103] considers the challenges faced by regulated institutions to comply with the 2020 amendments to the FATF's standards aimed at combating the financing of the proliferation of mass destruction. The amended PF standards require jurisdictions and reporting entities to undertake risk assessments and to enhance their risk control measures where risks were assessed as higher.

This study identified four broad groups of challenges:

- Navigating different definitions of PF.
- Assessing and mitigating PF risk with limited information about PF threats and with a limited geopolitical and geo-economic capacity to identify and mitigate threats.
- Monitoring trade-related transactions effectively to prevent PF-TFS while having limited or no information about the goods involved.

[102] The United Nations Interregional Crime and Justice Research Institute - *CBRN Proliferation Financing: A Perspective From Southeast Asia*: https://unicri.it/sites/default/files/2023-10/CBRN%20Proliferation%20Financing.%20A%20Perspective%20from%20Southeast%20Asia.pdf
[103] Louis de Koker - *The FATF's Combating of Financing of Proliferation Standards: Private Sector Implementation Challenges*: https://link.springer.com/chapter/10.1007/978-3-031-59543-1_6

- Efficiently and effectively combating PF-TFS without being allowed to simplify compliance measures where risks are lower.

However, the study notes an overarching challenge is a lack of considered policy about the purpose and strategic objectives of the new measures to be implemented.

The study proposes the following as elements of a national PF-TFS strategy:

- Adopting a meaningful definition of PF that fits with the country's general proliferation policy.
- Implementing a phased approach that first focuses on a select group of higher risk institutions with capacity.
- Embracing a collaborative approach bringing that select group together with the range of government authorities that address aspects of PF-TFS to explore best practice approaches to supporting effective and efficient compliance.
- Making appropriate use of the FATF's low risk exemption to exclude low risk institutions from PF-TFS risk management obligations.
- Facilitating PF-TFS compliance by supporting sectoral risk assessments and the development of appropriate compliance technologies.
- Tailoring compliance expectations given the limited information that institutions may have.
- Monitoring implementation for intended and unintended consequences and reporting on impact and progress.

The task of CFP is complex, with the focus now on assisting jurisdictions to implement the *FATF Recommendations* and undertake PF risk assessments. Limited attention is being given to the dilemmas the private sector will face to implement effective and efficient compliance measures, as reporting entities will play a key role in risk-informed PF-TFS. Therefore, regulators should do more now to understand the constraints faced by the private sector and what they would require to perform these functions effectively and efficiently, without undue disruption of business, or undue imposition of increased costs on customers and society.

The *FATF Recommendations* are minimum standards. Jurisdictions and regulated institutions may therefore elect to go beyond the standards and adopt policies, regulations and compliance practices that serve broader non-proliferation and disarmament objectives. Given the current increase in WMD risks globally that approach deserves serious consideration.

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

4.2.1 Australia

In 2022, AUSTRALIA published a *National Risk Assessment on Proliferation Financing in Australia*. The most significant PF threats facing Australia include:

- Use of Australian financial services and infrastructure to procure dual-use goods and evade sanctions.
- Use of Australia-based corporate structures to facilitate PF and evade sanctions.
- Use of Australian or third-jurisdiction nationals to facilitate PF and evade sanctions.
- Exploitation of Australian citizens to source and export sensitive technologies and knowledge for actors of proliferation concern.
- Use of designated non-financial businesses and professions (DNFBPs) to facilitate PF and evade sanctions.

4.2.2 Japan

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:

- Japan acknowledges its potential exposure to various threats:
  - Actors that seek to steal funds via trade, service, and cyberattacks.
  - Actors that seek to steal technologies and goods through trading dual-use items, illegal ship-

to-ship transfers.
    - Actors that 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.

4.2.3 Malaysia

In 2021, Malaysia's completed its first *Proliferation Financing Risk Assessment* (PFRA) and presently, Malaysia is finalising the revised/refreshed PFRA 2023 at the National Coordination Committee to Counter ML. The PFRA intends to provide an up-to-date assessment of Malaysia's PF-risk exposure through identifying key vulnerabilities in the financial and DNFBP sectors that may be exploited to finance proliferation-related activities or to evade UNSC sanctions. The assessment also intends to address key vulnerabilities by developing appropriate strategies and recommended measures in mitigating the identified risks and vulnerabilities to strengthen Malaysia's overall countering PF framework.

4.2.4 Philippines

The Philippines is currently finalizing its first PF National Risk Assessment (NRA) document led by the Department of Trade and Industry - Strategic Trade Management Office (DTI-STMO) and AMLC, in collaboration with other Philippine government and law enforcement agencies. The PF NRA seeks to evaluate the overall domestic PF risks by looking at threats arising from predicate crimes to ML and sector-specific threats, along with sector-specific vulnerabilities. It covers four main sectors – government, exporters of strategic goods, financial institutions (FIs), and designated non-financial businesses and professionals (DNFBPs).

4.2.5 Singapore

PF (PF) risks remain a priority risk concern for Singapore, with the misuse of shell and front companies being a key risk focus area. Other risk areas relate to the use of false documentation and vulnerabilities associate with Singapore's status as transport and transshipment hub.

Singapore consistently reviews its risks via the Risks and Typologies Interagency Group (RTIG) to identify and review Singapore's ML/TF and PF risks. Relevant authorities would also communicate key PF risks to industry through industry engagement and guidance produced by the authorities.

Singapore is also in the process of updating our PF risk understanding via a national PF risk assessment (PF NRA) which is targeted to be published in 2024. To ensure that the PF NRA is comprehensive and considers the elements recommended by the FATF, the assessment involves relevant law enforcement agencies (including the financial intelligence unit) and supervisory agencies. In addition, we have set up a Work Group under the auspice of Singapore's AML/CFT Industry Partnership to seek industry feedback from FIs and DNFBPs for the purpose of the PF NRA. The Work Group is also looking to publish in 2024 a PF best practice paper to enhance the industry's PF risk understanding and mitigation.

4.2.6 Chinese Taipei

Among Chinese Taipei's existing DPRK-related PF cases, the most common typology is to transfer oil to North Korean ships on the high seas with third-jurisdiction ships that are controlled by Chinese Taipei oil companies, or to sell oil to ships owned by other jurisdictions who resell it to North Korean sanctioned ships, but there is also a case of Chinese Taipei nationals buying anthracite from DPRK and reselling it to other jurisdictions for PF.

Petroleum products are still the most common commodity traded by Chinese Taipei nationals who committed PF. They are often the representative, or the beneficial owners of the shipping company involved.

While filing the export declaration, they commonly provide false export information, such as a false destination port. The oil products are traded on the high seas or carried to the high seas and then moved to DPRK-related ships via ship-to-ship transfers.

After the Polaris case, the Customs Administration created "ZZZ99" as the customs declaration code for high seas transactions. Many vessels departing from the Taichung Free Trade Zone export oil to high seas. Therefore, starting from 1 July 2023, Chinese Taipei implemented new regulations regarding customs declaration for the exportation of oil products from Free Trade Zone to the high seas. In instances where a business engages in oil transactions on the high seas and cannot confirm the final destination jurisdiction of the vessel, if the trading partner is known at the time of completing the export declaration, the relevant information about the oil transaction must be provided, including the time and location (latitude and longitude) of the oil delivery, along with the vessel's name and IMO ship identification number. In cases where the trading partner remains unidentified at the time of export, information regarding the transaction must be reported upon returning to port for further verification by relevant authorities.

Analysis of relevant cases of PF reveals that vessels under control of Chinese Taipei oil companies engaging in oil transfer activities near Chinese Taipei, North Korea, or on the high seas, mainly trade with non-DPRK vessels, these vessels are not subject to sanctions, and many seafarers are not Chinese Taipei nationals. The masterminds usually have international trade experience and use offshore companies to cover up these transactions. Thus, commonly their business structures have a high degree of complexity. In addition, criminals will use legal trade to cover up their illegal trade activities. Most of those caught had successfully conducted more than one trade with DPRK and had used offshore accounts to transfer the payment for goods, in order to prevent the funds from being tracked by law enforcement agencies. One challenge facing Chinese Taipei authorities is Article 9, Paragraph 1, Subparagraph1 of the *Counter-Terrorism Financing Act* has a subjective element, which requires the suspect to "knowingly" trade with the sanctioned target, and the use of intermediaries has made this difficult to prove.

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

4.3.1 Cook Islands

Guidance materials provided to FIs and DNFBPs, VASPs or other sectors (e.g. shipping) on identifying, assessing, and mitigating sanctions evasion / PF risks.

FIU provides UN Sanction listing of individuals and entities through the CIs Ministry of Foreign Affairs and Immigration to FIs and DNFBPs.

4.3.2 Hong Kong, China

The Joint Financial Intelligence Unit (JFIU) issued Suspicious Transaction Reports (STR) Quarterly Analysis and Alert Messages to STR reporting entities, with topical strategic analysis reports promoting intelligence exchange on PF, triggering law enforcement actions and providing insights into formulation of PF regulations/policy.

4.3.3 Japan

Japan noted that it published its first report of the *National Risk Assessment of Proliferation Financing*[104] in March 2024. In summary, relevant sectors covered under the legislation, including banks and funds transfer service providers, are required to conduct a risk assessment of their exposure to PF risk, taking into account

[104] Japan Ministry of Finance - *National Risk Assessment of Proliferation Financing in Japan (Provisional Translation)*: https://www.mof.go.jp/policy/international_policy/councils/aml_cft_policy/20240312.html

Japan's national risk assessment of PF report. Further, other private sectors including DNFBPs are expected to recognize such risks and take actions to mitigate them.

4.3.4 Philippines

In terms of trade controls, the Department of Trade and Industry - Strategic Trade Management Office (DTI-STMO) published the following:

- Publication of the *National Strategic Goods List Annex 3*[105]: Nationally Controlled Goods, under unilateral controls for reasons of national security, foreign policy, anti-terrorism, crime control, and public safety. Annex 3 contains goods and items listed in UNSCR 1718 (2006), 2231 (2015) and their subsequent resolutions which are the prohibited goods going to and coming from the DPRK and Iran.
- Issuance of DTI *Memorandum Circular 20-13*[106] to adopt the United Nations Security Council (UNSC) Consolidated List of Individuals and Entities as the STMO's own List of Prohibited Users, effectively prohibiting any persons from engaging in any trade of strategic goods with those included in the List of Prohibited Users.
- Issuance of DTI *Memorandum Circular 21-06*[107] to provide guidelines in the implementation of brokering and financing to satisfy requirements of UNSCR 1718 (2006), 2231 (2015) and their subsequent resolutions.
- DTI-STMO assistance in granting authorization to access frozen assets for purposes of making payments due under prior contracts under AMLC *Regulatory Issuance No. 5 - Guidance for De-Listing and Unfreezing Procedures*[108]. This is possible when the DTI-STMO has determined that the contract is not related to any of the prohibited items, financial assistance, brokering or services, and the payment is not directly or indirectly received by a person or entity subject to the measures, both referred to in UNSCR 2231 (2015) and its subsequent resolutions.

In terms of outreach activities and enhancing due diligence, the DTI-STMO published the following:

- Conducted several outreach activities to inform its covered stakeholders of possible repercussions when transacting business with sanctioned individuals and entities. These awareness activities can be in the form of one-on-one sessions with DTI-STMO, targeted outreach with specific sectors, and town hall sessions attended by both government and industry stakeholders.
- In addition, the DTI-STMO provides end-user business advice to ensure compliance with applicable requirements of sanctioning states. To date (2023), the DTI-STMO has accommodated more than 10 transactions relevant to business advice on future business activities/contracts with new foreign business partners.
- Some of the announcements and notices that are published on the DTI website:
    - *Advisory October 2023 - "Export enforcement five" release joint guidance on countering Russia evasion*[109].
    - *Advisory 08 March 2022 - On unilateral sanctions imposed by certain states*[110].
    - *Advisory to all persons who might be transacting business with sanctioned individuals and entities*[111].

[105] Department of Trade and Industry - *Philippine National Strategic Goods List Annex 3:*
: https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/STMO/Policies/Annex+III.pdf
[106] Department of Trade and Industry - *Memorandum Circular 20-13:* https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/e-library/Laws+and+Policies/140420_MC20_13.pdf
[107]Department of Trade and Industry - *Memorandum Circular 21-06:* https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/Laws+and+Policies/Memorandum+Circular+No.+21-06+Implementation+of+FInancing+and+Brokering+Under+Republic+Act+No.+10697.pdf
[108] Anit-Money Laundering Council - *Regulatory Issuance No. 5 - Guidance for De-Listing and Unfreezing Procedures:*
https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/Advisories/Guidance+for+Delisting+and+Unfreezing+-+PF+TFS.pdf
[109] Department of Trade and Industry - *Advisory October 2023 - "Export enforcement five" release joint guidance on countering Russia evasion*: https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/STMO/Announcements/October+2023+-+Sanctions+Advisory.pdf
[110] Department of Trade and Industry - *Advisory 08 March 2022 - On unilateral sanctions imposed by certain states:*
https://dtiwebfiles.s3.ap-southeast-1.amazonaws.com/STMO/Announcements/SanctionsMarch2022.pdf
[111] Department of Trade and Industry - *Advisory to all persons who might be transacting business with sanctioned individuals and entities:*
https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Announcements/STMO+Advisory_Sanctioned+Individual+and+Entities.pdf

- *A guide on common red flags to help companies examine transactions and comply with the Strategic Trade Management Act*[112].
- *Restricted party screening. Supplementary guideline to DTI-STMO Memorandum Circular 20-13 s. 2020 List of Prohibited End-Users*[113].

In terms of strengthening capacities of persons and offices involved in the TFS on PF implementation, the following were conducted:

- Counter-Proliferation Investigative Methods and Enforcing Philippine Strategic Trade Management Act Workshop
- TFS Implementation Workshop
- Counterproliferation Finance for Financial Intelligence Units: Addressing Evasion of Sanctions Against Russia
- Forum on Countering Democratic People's Republic of Korea (DPRK) Proliferation and Sanctions Evasion
- Tabletop exercise of DPRK-related sanctions implementation • series of consultative meetings on the data gathering, assessing and finalizing the PFNRA document

The AMLC likewise released the *2021 Sanctions Guidelines*[114], focusing on TFS Related to Terrorism, TF, and PF. This publication discusses the various sanctions and legal provisions applicable to TF and PF.

Moreover, the AMLC issued *Targeted Financial Sanctions related to Proliferation of Weapons of Mass Destruction and Proliferation Financing*[115], effective 1 February 2021. These consist of United Nations Security Council Resolutions (UNSCR) lists 1718 and 2231.

4.3.5 Singapore

Over the years, the Monetary Authority of Singapore (MAS) has issued various guidance to FIs to assist them in their countering of PF risks, including the following:

- Following a series of counter-PF supervisory visits to banks, MAS published a guidance paper *Sound Practices to Counter Proliferation Financing* [116], which covered key findings noted and sound practices observed that FIs could use as benchmarks to enhance their existing controls. MAS also published guidance papers: *Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons*[117] and *Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures*[118] which cover sound practices to address the risk of misuse of legal persons which is a known PF typology.
- In addition, MAS provided guidance on countering PF, which included potential indicators of PF, in its AML/CFT Guidelines for FIs.
- In August 2023, MAS issued a circular, *Circular on ensuring effective detection of sanctions-related risks*[119] to all FIs to set out additional guidance that FIs should consider incorporating in their processes to better detect and manage sanctions-related risks.

[112] Department of Trade and Industry - *A guide on common red flags to help companies examine transactions and comply with the Strategic Trade Management Act:* https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/red+flags.pdf
[113] Department of Trade and Industry - *Restricted party screening. Supplementary guideline to DTI-STMO Memorandum Circular 20-13 s. 2020 List of Prohibited End-Users:* https://dtiwebfiles.s3-ap-southeast-1.amazonaws.com/STMO/Publications/restricted-party-screening-2.pdf
[114] Anit-Money Laundering Council - *2021 Sanctions Guidelines:* http://www.amlc.gov.ph/images/PDFs/2021%20SANCTIONS%20GUIDELINES.pdf
[115] Anit-Money Laundering Council - *Targeted Financial Sanctions related to Proliferation of Weapons of Mass Destruction and Proliferation Financing:* http://www.amlc.gov.ph/un-sanctions-list/notice-on-tfs-obligations-on-proliferation-financing-of-wmd
[116] Monetary Authority of Singapore - *Sound Practices to Counter Proliferation Financing:* https://www.mas.gov.sg/regulation/guidance/sound-practices-to-counter-proliferation-financing
[117] Monetary Authority of Singapore - *Effective Practices to Detect and Mitigate the Risk from Misuse of Legal Persons:* https://www.mas.gov.sg/regulation/guidance/effective-practices-to-detect-and-mitigate-the-risk-from-misuse-of-legal-persons
[118] Monetary Authority of Singapore - *Strengthening AML/CFT controls on risks of misuse of legal persons/arrangements and complex structures:* https://www.mas.gov.sg/regulation/guidance/amlcft-controls-on-risks-of-misuse-of-legal-persons-arrangements-and-complex-structures
[119] Monetary Authority of Singapore - *Circular on ensuring effective detection of sanctions-related risks:* https://www.mas.gov.sg/regulation/circulars/circular-on-ensuring-effective-detection-of-sanctions-related-risks

Also, MAS (working in conjunction with the Association of Banks in Singapore (ABS)) has made counter-PF a standing agenda item at the ABS' annual Financial Crime Seminar (FCS). The ABS FCS is one of Singapore's key AML/CFT industry outreach events and is regularly attended by over 500 practitioners from Singapore and the region. Both experts from Singapore and overseas (e.g. the United States) have spoken at the ABS FCS over the years to raise the industry's awareness of PF risks and PF risk mitigation measures. During this time, MAS has also conducted outreach to raise other sectors' (e.g. MVTS and VASPs) PF risk awareness.

4.3.6 Chinese Taipei

Chinese Taipei noted that it had provided the following guidance materials to FIs and DNFBPs, VASPs or other sectors on identifying, assessing and mitigating sanctions evasion/PF risks.

On January 20, 2022, the Ministry of Finance published the *Operation Guide on Anti-Money Laundering and Counter-Terrorist Financing for Certified Public Bookkeepers and Bookkeeping and Tax Return Filing Agents*[120] (Chinese version only) on its official website.

The Administration for Digital Industries, Ministry of Digital Affairs has published the *Guidelines for Anti-Money Laundering and Countering the Financing of Terrorism for the Third-Party Payment Enterprises* to prevent ML/TF/PF. The guidelines include how third-party payment enterprises in our jurisdiction should identify and assess ML/TF/PF risks in various business aspects, as well as formulate AM/CFT and proliferation plans. Third-party payment enterprises are required to assess risks based on a risk-based approach, formulate prevention measures and mitigation measures against ML, terrorist financing and PF risks, and allocate resources, establish internal control systems, and formulate and implement policies, procedures, and control measures for AML/CFT and proliferation plans. Due to differences in the size and scale of third-party payment enterprises, the guidelines have established a risk assessment form for third-party payment enterprises, subdividing customer risks, product, service, and transaction risks, payment channel and business practice risks, and regional risks into four dimensions, and providing implementation recommendations for control measures, providing third-party payment enterprises with a basis for complying with laws and regulations.

In August 2021, the Administration of Commerce and the Ministry of Economic Affairs published the *Anti-Money Laundering and Countering the Financing of Terrorism Guidance for Jewellery Businesses*[121] on the Commerce Industrial Services Portal (Chinese version only).

The financial industry associations have formulated the following guidelines for assessing ML, TF, and PF risks:

- *Guidelines for Assessing Money Laundering and Terrorism Financing Risks and Formulating Relevant Prevention Plans for Banks*.
- *Guidelines for Assessing Money Laundering and Terrorism Financing Risks and Formulating Relevant Prevention Plans for Electronic Payment Institutions*.
- *Guidelines for Assessing Money Laundering and Terrorism Financing Risks and Formulating Relevant Prevention Plans for Securities Firms*.
- *Guidelines for Assessing Money Laundering and Terrorism Financing Risks and Formulating Relevant Prevention Plans for Credit Card Issuers*.

These guidelines provide reference practices for financial institutions on how to identify and assess ML, TF, and PF risks in various business areas, as well as how to formulate AML/CFT and PF plans.

The Bankers Association established the *Suggested Best Practices for Banks to Combat Trade Based Money Laundering* to provide practical insights for banks in identifying, assessing the ML/TF/PF risks associated with trade finance, and formulating relevant control measures.

In 2021, the Department of Land Administration, M.O.I. formulated *The Guidance and Supervision Manual of AML/CFT/CPF for Land Administration Agents and Real Estate Brokerages* which was provided to The Land Administration Agent Association and placed on the official website for the agents to follow and understand their supervision methods (Chinese version only). The manual contains information on the ML/TF/PF threats, vulnerabilities, and sectorial risks identified in Chinese Taipei's national risk assessment.

[120] Ministry of Finance - *Operation Guide on Anti-Money Laundering and Counter-Terrorist Financing for Certified Public Bookkeepers and Bookkeeping and Tax Return Filing Agents:* https://www.mof.gov.tw/download/6c9319f86c0b41079f47bf13fb2f0085
[121] Administration of Commerce and the Ministry of Economic Affairs - *Anti-Money Laundering and Countering the Financing of Terrorism Guidance for Jewellery Businesses:* https://gcis.nat.gov.tw/mainNew/subclassNAction.do?method=getFile&pk=252

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

In these case studies, APG members noted the trends towards online efforts to avoid TFS, as well as existing physical efforts such as the smuggling of petroleum through ship-to-ship transfers. Of note is some of these recent efforts involve the misuse of legal persons.

4.4.1 Japan

Case Study # 97: North Korean IT workers proliferation financing

Use of the internet (encryption, access to IDs)

Japan noted that it suspected North Korean IT workers were presenting themselves as Japanese nationals and generating income through receiving work on online work platforms provided by Japanese companies. The reports of the Panel of Experts established pursuant to resolution 1874(2009) indicated that the income earned by North Korean IT workers contributes to North Korea's nuclear and missile programmes and therefore, contributes to PF.

In response, the Government of Japan published an advisory illustrating how North Korean IT workers operate, to raise awareness and encourage platform companies to take measures such as closely scrutinizing identity verification documents, to mitigate this.

Source - Japan

4.4.2 Macao, China

In 2023, GIF coordinated the member agencies of the Interdepartmental AML/CFT Working Group to consolidate the information from various sector review reports and threat analysis reports (including the analysis on PF, the overall PF risk and the individual risk level for various sectors) to prepare "Macao Special Administrative Region Risk Assessment Report on Money Laundering/Terrorist Financing/Financing of Proliferation of Weapons of Mass Destruction (2022)" for stakeholders. The NRA Report was released to stakeholders in the first quarter of 2024. Overall, the risk of PF in Macao, China is low as the inherent PF risk exposure is pretty low while there are sufficient mitigating control measures in place.

Since the establishment of the Asset Freezing Regime (Law no. 6/2016) in 2016, Macao, China has not implemented any PF-related freezing actions on any natural person, legal person or entity in Macao, China, according to the requirement of UNSCR. Further, Macao, China has not prosecuted any PF-related cases, and has not identified or detected any breaches, non-implementation or evasion of the TFS obligations referred to in FATF Recommendation 7.

Under the requirement of the Asset Freezing Regime, FIs and DNFBPs are obliged to apply control measures to freeze the assets of individuals and legal persons included in the UNSCR PF sanction lists. Macao, China's supervisors have also established an effective communication mechanism with the financial and gaming sectors for asset freezing.

In order to continuously raise the awareness of risk assessment of the sector, the Monetary Authority of Macao (AMCM) sent out sector questionnaires to understand the financial sector's PF-risk and the financial institutions' relevant controls measures.

4.4.3 Singapore

Case Study # 98: Prohibited supply of gasoil to the DPRK

Proliferation financing

Between September and November 2019, Person A allegedly conspired with five other individuals abroad to supply approximately 12,260 metric tons of gasoil to the DPRK on seven occasions. The supply was facilitated through ship-to-ship transfers on the first six occasions and at a port in the DPRK on the last occasion. This constituted a violation of the United Nations (Sanctions – DPRK) Regulations 2010.

In order to facilitate the payment transactions for the purchase and supply of gasoil to the DPRK, Person A allegedly utilised the bank account of Company X, a company of which he was a director, on four occasions. Person A also allegedly falsified documents belonging to Company X on two occasions. In addition, Person A also allegedly utilised the bank account of Company Y, another company under his control, to receive payment for the prohibited supply of gasoil to the DPRK on five occasions. The Suspicious Transaction Reporting Office (STRO) shared its analysis with the Commercial Affairs Department (CAD) of the Singapore Police Force, particularly on transactions with a possible nexus to the sanctioned activities.

During CAD's investigations, Person A allegedly lied to the investigation officer and disposed of evidence pertaining to his involvement in the prohibited supply of gasoil to the DPRK. Person A also allegedly failed to inform the CAD about the prohibited supply of gasoil to the DPRK by another vessel in February 2019.

In December 2023, authorities charged Person A with various offences under the *United Nations (Sanctions - DPRK) Regulations 2010*, *Penal Code 1871* and the CDSA. Additionally, as separate legal entities, Company X was charged with four counts of transferring financial assets that may contribute to a prohibited activity under Regulation 12(1)(b) read with Regulation 16(1) of the United Nations (Sanctions – DPRK) Regulations 2010 while Company Y faces five counts of acquiring benefits from criminal conduct under Section 47(3) of the CDSA.

Source - Singapore

4.4.4 Chinese Taipei

Case Study # 99: Illicit Transfer of oil to DPRK's ships

Proliferation financing

Persons A and B jointly invested with Persons C, D and others to operate a maritime bunkering business. They used multiple foreign-flagged oil tankers and falsely declared the destination ports for exports, then conducted bunkering operations near the port of DPRK for sanctioned DPRK vessel "SAEBYO". Chinese Taipei's authorities prosecuted Persons A, B, C, and D for violating *Counter-Terrorism Financing Act* on December 2022 and are now on trial.

Source - Chinese Taipei

Case Study # 100: Violation of the *Foreign Trade Act*

Proliferation financing

Item S is on the list of strategic high-tech commodities regulated by Chinese Taipei's Ministry of Economic Affairs (MOEA). Exporters shall apply for an export permit (license) with the International Trade Administration, MOEA or the appointed or entrusted government authority, prior to export. With the intension of evading this provision, Company A falsely reported the tariff number and declared that Item S is not a strategic high-tech commodity and also to avoid custom inspection and transport the goods to Jurisdiction B, a restricted region.

In June 2023, Company A and its representative Person A were referred to the prosecutor for violating the *Foreign Trade Act*. They were granted deferred prosecution by the prosecutor and paid TWD 100,000 (~ USD 3,138) to the public treasury.

Source - Chinese Taipei

4.5 Proliferation financing - the misuse of legal persons and professional enablers

As demonstrated by various typologies, evasion often involves the misuse of front companies and correspondent banking relationships to transfer funds internationally while obscuring the identity of the ultimate beneficial owners. This is particularly prevalent in banks with foreign branches located in high-risk jurisdictions, which are susceptible to high-risk diversion activities.

4.5.1 Case studies

The following case study illustrates the nexus between the misuse of legal persons, and use of third parties to hide beneficial ownership information to avoid sanctions.

Case Study # 101: Sanction evasion by using shell companies and an art advisor

Sanctions; use of legal persons and arrangements

Two individuals who were sanctioned by the US Treasury's Office of Foreign Assets Control (OFAC)[122] were still able to access the US financial system and the art market after their OFAC designation, by using shell companies and a third-party art advisor to hide the beneficial ownership.

In 2014, after being designated by OFAC, the sanctioned individuals purchased tens of millions of dollars' worth of art from major auction houses and other art market participants. They used a third-party art advisor to represent their interests at auction, and reports suggest that at least some professional staff within an auction house were aware of the identities of the persons who ultimately purchased the art[123].

Source – FATF: *Money Laundering and Terrorist Financing in the Art and Antiquities Market*

Case Study # 102: Proliferation actors exploiting DNFBPs

Sanctions; use of legal persons and arrangements

A[124] Hong Kong-based accounting firm known for specialising in offshore company registration and providing secretarial services is believed to have helped an Australian resident establish front and shell companies (Company X and Company Y) for the purpose of facilitating high-risk financial transactions to beneficiaries in Russia, including to an entity subject to US financial sanctions.

In 2018, a foreign bank submitted a suspicious matter report (SMR) to AUSTRAC regarding Company X. The report noted Company X had a declared principal place of business in the Dalian province in China (near the border of the DPRK and considered a high-risk region for sanctions evasion and PF activity). Company X received a number of incoming transfers from shipping companies located in Hong Kong and China, and then attempted to remit these funds to an unknown beneficiary in Vladivostok, Russia.

In 2018, another major bank submitted an SMR regarding Company Y, which was an Australian-registered company with limited public details available. The report noted Company Y attempted to remit funds to a US-sanctioned beneficiary in Russia.

Source - *Proliferation Financing in Australia National Risk Assessment*

Members provided the following case studies.

Case Study # 103: Contravening sanctions laws

Sanctions; use of legal persons and arrangements

In 2021 the New South Wales Supreme Court sentenced a foreign-born Australian citizen to three years and six months imprisonment for contravening Australian sanctions law relating to the DPRK. The

[122] Please note: although the sanctions mention are jurisdiction sanctions, the methods used for evading the sanctions highlight typologies of commonly used sanction evasion techniques for PF.

[123] FATF - *Money Laundering and Terrorist Financing in the Art and Antiquities Market*: https://www.fatf-gafi.org/en/publications/Methodsandtrends/Money-Laundering-Terrorist-Financing-Art-Antiquities-Market.html

[124] AUSTRAC - *Proliferation Financing in Australia National Risk Assessment*: https://www.austrac.gov.au/sites/default/files/2022-12/AUSTRAC_Proliferation_Financing_in_Australia-National_Risk_%20Assessment_Web.pdf

individual used offshore bank accounts and a series of Australia-based front companies to broker trade with the DPRK in a variety of goods, including coal, graphite, copper ore, gold, crude oil (including purchasing Iranian petrol on behalf of the DPRK), missiles and missile-related technology. This was the first-time charges were laid in Australia for breaches of sanctions in relation to the DPRK.

Source - Australia

4.6 Shipping registries

Proliferation networks exploit the entire global commercial supply chain to evade detection and finance the acquisition of controlled material. Shipping companies and vessels feature prominently in sanctions evasion and export control violation activities, and this use of the maritime sector is abetted by the use of front and shell companies. As documented in the March 2020 global maritime advisory[125], Iran, Syria, and the DPRK falsify documents, reflag vessels, and switch of automatic identification systems to avoid being discovered in the process of illicitly transferring goods[126].

In Recommendation 7 and Immediate Outcome 11 of the FATF Methodology, there is a particular emphasis on TFS under UN Security Council Resolutions. This includes obligations that require jurisdictions to freeze property owned or controlled by designated persons and entities and any persons or entities under their ownership or control. These obligations apply to persons or entities that offer services related to registration and flagging of vessels, as vessels, licences and flag rights constitute property and/or assets.

In conducting mutual evaluations, the APG considers the vulnerabilities posed by shipping registries with respect to the FATF Recommendations on PF and where relevant, to TF. When assessing effectiveness, assessors need to understand what role a registry may have with a freezing action in case of a match. This particularly related to actions that can be taken to prevent dealing in any way with a designated vessel, including transacting a change of title or registration. More broadly, the APG has also noted the possible risk of transnational crime and related ML posed by vessels using flags of convenience that may be misused to facilitate movement of prohibited goods.

Further, the following four examples of APG members' shipping registries shows additional vulnerabilities arise when a jurisdiction outsources the management of the registry to a commercial entity. While there is nothing inherently wrong with this, vulnerabilities arise where there is insufficient accountability communication and understanding between the commercial entity and the jurisdictions' competent authorities.

4.6.1 Republic of the Marshall Islands

The Republic of the Marshall Islands (Marshall Islands) operates a large, well-regulated open shipping registry. It is the legal domicile of many of the world's largest shipping companies, with the third-largest fleet of ships in the world (over 5,600 vessels as of 31 January 2024). Revenue from the ship registry and non-resident domestic entities (NRDEs) (41,000 entities) is the Marshall Islands' third largest source of income.

The Marshall Islands' NRA identified the registration of ships and NRDEs as presenting a medium risk for PF. The NRA noted that the vulnerabilities for PF linked to Marshall Islands-flagged ships or NRDEs providing assets or financial services which are used for the purpose of transport, transfer, transhipment or the delivery of materials or related materials that may be used in or for nuclear, chemical or biological weapons. Although the NRA identified legal entities, shipping, registry and beneficial ownership as one of five functional vulnerabilities, the risks associated with NRDEs was understated given the ease with which legal persons can be created and challenges with transparency of their beneficial ownership and control.

The Trust Company of the Marshall Islands Inc. (TCMI) serves as the Marshall Islands' Registrar for NRDEs and its Maritime Administrator. As, the Marshall Islands' shipping related NRDEs increase the vulnerability to PF related activities, TCMI implemented a range of measures in its shipping registration processes to

[125] U.S. Department of State, U.S. Department of the Treasury's Office of Foreign Assets Control and U.S. Coast Guard - *Guidance to Address Illicit Shipping and Sanctions Evasion Practices*: https://ofac.treasury.gov/media/37751/download?inline
[126] The U.S. Department of the Treasury - *National Proliferation Financing Risk Assessment*: https://home.treasury.gov/system/files/136/2022-National-Proliferation-Financing-Risk-Assessment.pdf

respond to and mitigate PF and TFS evasion risks. TCMI has a well-developed understanding of these risk, especially for shipping companies, due to its coordination with international organisations and foreign governments, including the UN Panel of Experts.

The Maritime Administrator part of TCMI vets all known parties to any NRDEs or maritime transaction through a commercial database, which combines the UN, US, EU, and other domestic and international sanctions lists and lists of persons publicly accused, investigated, arrested, charged, indicted, detained, questioned, or put on trial related to any criminal activity. Further, it screens all parties to a vessel registration (including all owners, beneficial owners, and operators), all vessel identifiers, and all seafarers serving onboard a vessel against all UNSCR lists and a variety of other domestic and international sanctions and criminal lists using a commercial screening database. It also automatically checks all known parties every 12-24 hours and clears any false positives according to detailed methodology, with escalating approval requirements. It collects identification documents, proof of residence, police clearance certificates, and other documentation as needed, to rule out potential matches. The technology it uses continuously screens these parties, vessel identifiers, and seafarers and automatically notifies compliance personnel if any is subsequently added to a sanctions list. or is publicly accused, investigated, arrested, charged, indicted, detained, questioned, or put on trial related to any criminal activity, including any related to PF.

The Maritime Administrator also proactively monitors vessels for potential sanctions evasion with a location monitoring solution and issues guidance and notices related to illicit shipping and sanctions evasion practices. All vessels registered in the Marshall Islands are subject to ongoing inspections requirements, including an annual inspection by a dedicated Marshall Islands nautical inspector.

In the event TCMI was required to freeze or seize entities based on a UN sanction, it could strike a ship from the registry or revoke permission to navigate or annul a company. One Marshall Islands entity that was listed on a UN sanctions list (Kingly Won International Co., Ltd.,) was detected and forcibly dissolved by TCMI, before it was listed by the UN Security Council.

Marshall Islands Maritime Registry information sharing on sanctions violations
The Marshall Islands Shipping Registry was a founding member of the Registry Information Sharing Compact (“RISC”) in 2019, which creates a system for flag States to notify each other when a vessel is denied registration or is de-registered for suspected sanction-related activity. RISC gives the Marshall Islands access to information on vessels not in its fleet and allows the Marshall Islands to apply its sanctions screening practices to assist smaller flag States, which are often more vulnerable to sanctions evasion. The RISC includes over 40% of the world’s merchant shipping tonnage.

4.6.2 Cook Islands

In its 2015 NRA, the Cook Islands assessed its exposure to PF as low, its links with DPRK and Iran are negligible, and it had not identified or frozen any funds or assets of designated persons. The Cook Islands financial sector does not have any direct trade links with DPRK or Iran and is prohibited from conducting business with DPRK but must apply enhanced due diligence and monitoring (including filing STRs) to business with Iran. Since 2010 competent authorities had been alerted to some interactions with DPRK and Iran - *all related to shipping activities*.

In 2015 a bank lodged an STR due to funds received from Iran, linked to the registration of a ship with the Cook Islands Shipping registry. In 2016, during the license application process of an insurance company, the Financial Supervisory Commission (FSC) discovered that the applicant had previously provided insurance to DPRK vessels in 2005. The issue was raised with the applicant and the FSC was satisfied that this business line had long since discontinued.

The Cook Islands *2017 Review of Risk* identified the potential for exposure to PF through its shipping registry. The Ministry of Transport (MoT) outsources most administrative functions to a private contractor: the Maritime Cook Islands (MCI). The MoT is unfamiliar with TFS obligations and considers its role to be limited to overseeing the shipping registry contractor to ensure its delegated powers are used in compliance with the International Maritime Organisation standards. MCI advised it understands that its contractual obligations include conducting sanctions screening on behalf of MoT and taking appropriate action in relation to sanctioned vessels in coordination with the Cook Islands Government agencies.

As of November 2017 there were 566 vessels registered on the Ships Register, approximately half of which are privately owned yachts. The owners of vessels registered are generally corporations and come from 65 different jurisdictions, most commonly the Marshall Islands, Cook Islands, Singapore, British Virgin Islands, Russia and the United States.

In December 2016 MCI commenced a subscription to a commercial sanctions screening provider that is specifically designed to provide sanctions screening and vessel tracking for organisations exposed to shipping and cargoes. MCI screens the "controlling principal" of a vessel (the ship manager, bareboat charterer, or other person operating the vessel, or, if these are not applicable, the owner) at the time of registration or re-registration using this software and are further subject to daily sanctions screening of entities associated with a vessel and vessel tracking for high-risk movements. MCI also examines the movement history of a vessel based on vessel tracking signals before registration, looking for travel to high-risk areas which, amongst other things, may indicate a breach of UNSCRs. However, MCI does not appear to screen entities with beneficial ownership or control of a vessel other than the controlling principal (for example a beneficial owner of a vessel who is not the controlling principle but is directly or indirectly associated with the vessel) for sanctions matches. Further, there is no evidence the Cook Islands' shipping registry was screened for TFS pursuant to UNSCRs 1373 or 1267 and its successor resolutions prior to December 2016.

In response to the Cook Islands identification of potential for exposure to PF through its shipping registry, the National AML/CFT Strategy included measures to strengthen the Cook Islands' TFS against PF regime. One of these measures was the creation of Regulations which require MCI to conduct due diligence on its registered vessels to detect any links to sanctioned entities. In November 2017, the Cook Islands issued the *Financial Transaction Reporting (Maritime Cook Islands) Regulations 2017* (MCI Regulations). The MCI Regulations designate MCI as a reporting institution (RI) with a limited scope of obligations, including the requirement to conduct customer due diligence (including sanctions screening) on the controlling principal of certain vessels prior to registration, and STR obligations. However, the MCI Regulations do not require MCI to conduct sanctions screening on persons other than the controlling principal. The MCI Regulations also assign the FIU as the supervisor of MCI in relation to these obligations. Further, there is high-level commitment across government to implement the provisions, with the National Anti-Money Laundering Coordination Committee adopting a PF action plan in 2016. There have been no sanctioned entities identified as operating in or moving funds or assets through the Cook Islands.

Case Study # 104: Sanctioned shipping vessels on registry captured

Sanctions

In May 2024, FIU received two suspicious activity reports regarding four flagged registered vessels with Cook Islands shipping registry Maritime Cook Islands. The vessels were captured under the OFAC sanctions[127] for breach of transporting Iranian drones to Russia.

The four registered vessels have been deregistered and investigation for non-compliance is ongoing.

Source - Cook Islands

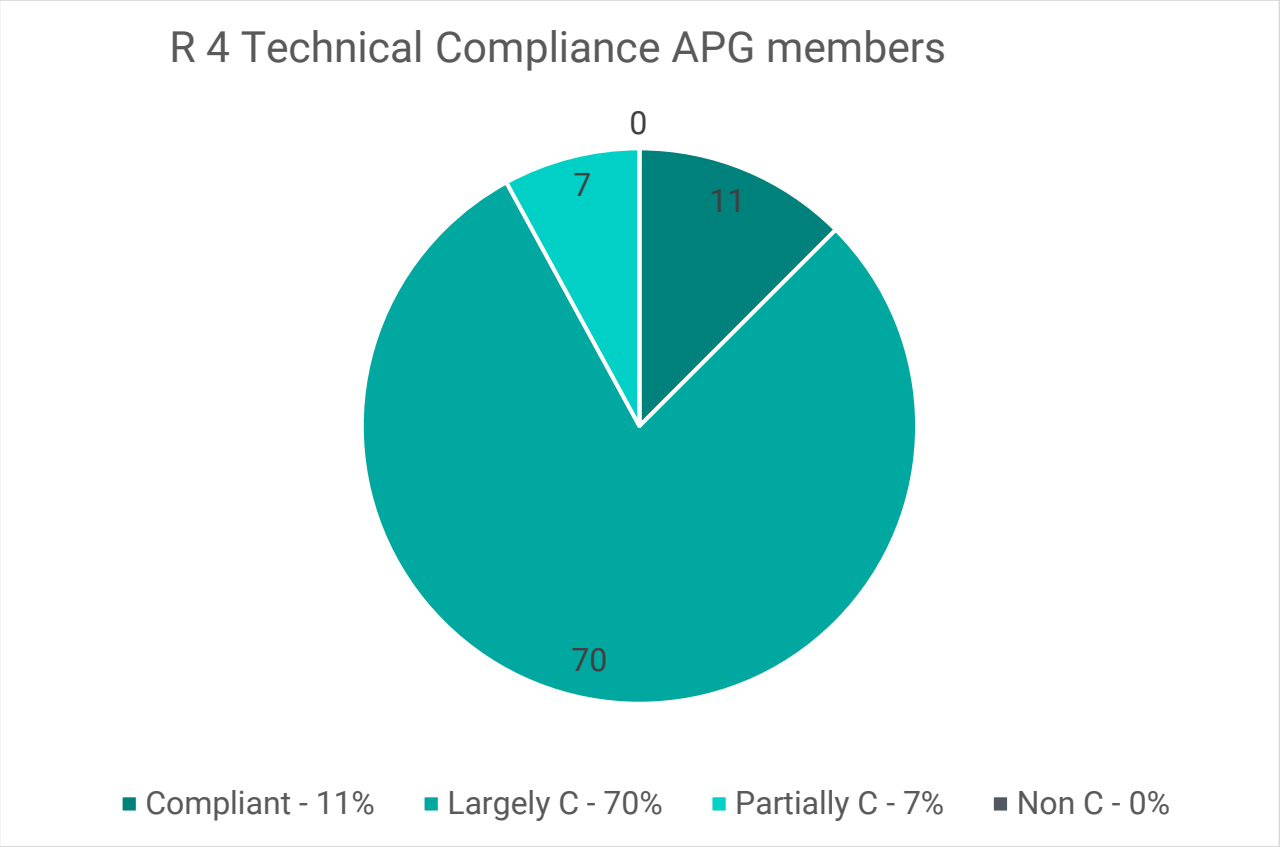
[127] Please note: although the sanctions mention are jurisdiction sanctions, the methods used for evading the sanctions highlight typologies of commonly used sanction evasion techniques for PF.

5 - ASSET RECOVERY METHODS AND TRENDS

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

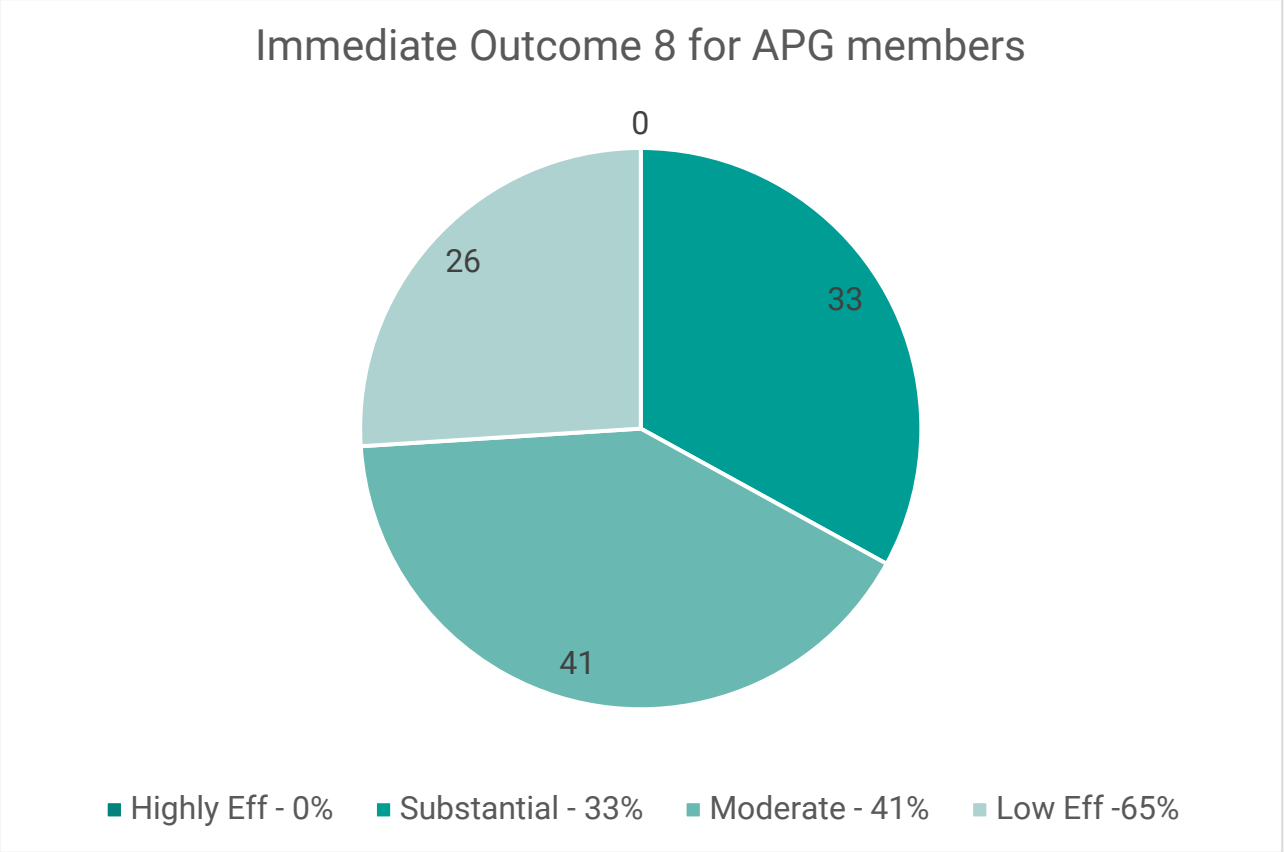
As the APG moves to finalise its 3rd round of mutual evaluations (only three jurisdictions within APG's remit remain to be evaluated)[128], it is possible to extract some statistical data in relation to compliance and effectiveness with the FATF Standards in relation to confiscation and provisional measure (Recommendation 4 and Immediate Outcome 8), and international cooperation in relation to mutual legal assistance for freezing and confiscation (Recommendation 38 and Immediate Outcome 2).

FATF Recommendation 4: Confiscation and provisional measures.



FATF Immediate Outcome 8: Proceeds and instrumentalities of crime are confiscated.

[128] Afghanistan, Niue and Tuvalu



As these charts demonstrate, while members are largely technically compliant with *FATF Recommendations*[129], they are generally have a lower level of effectiveness, when it comes to achieving the outcome intended by implementation of the recommendations.

Similarly, whilst most APG members have legal frameworks for international cooperation on asset tracing, freezing, confiscation and sharing proceeds, operational results are only moderately effective.

In anticipation of the APG's 4th round of mutual evaluations which commenced in 2024 and will be finalised in 2032, members should be aware of the amendments to *FATF Recommendations* in relation to Recommendations 4 and 38) and the increased focus upon channels for informal cooperation between jurisdictions and streamlined formal processes.

Jurisdictions are encouraged to participate in and make use of channels such as Interpol, Egmont, ARIN-AP, PFIC and PILON, amongst others.

The Stolen Asset Recovery Initiative Asset - *Recovery Watch Database*
The Stolen Asset Recovery Initiative (StAR) Asset Recovery Watch[130] is a public database that tracks efforts by prosecution authorities worldwide to go after assets that stem from corruption. The objective of StAR Asset Recovery Watch is to collect and systematize information about completed and ongoing recovery efforts of proceeds of corruption that have an international dimension.

[129] FATF - *The FATF Recommendations*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/Fatf-recommendations.html
[130] The Stolen Asset Recovery Initiative (StAR) - *Asset Recovery Watch*: https://star.worldbank.org/asset-recovery-watch-database

The Stolen Asset Recovery Initiative Asset - *Managing Seized and Confiscated Assets: A Guide for Practitioners*

This guide[131] aims to provide guidance to practitioners on asset management, from pre-seizure planning to preserving value during custody to maximizing value at disposal. It is intended to provide practitioners with the foundations to build an effective asset management function and to grow the asset portfolio to manage complex assets. Accordingly, the Guide includes recommendations and good practices derived from international studies, experience from interviews with asset management experts, and case examples. In addition, practitioners may benefit from discussions of different approaches among jurisdictions, the case examples, and the detail on managing specific asset types.

The Stolen Asset Recovery Initiative Asset - *Victims of Corruption: Back for Payback*

This publication[132] aims to provide an overview of the existing international legal framework, and to start the debate on important questions, such as what are the avenues for reparation, who are victims, how to define their legal standing and how to establish damages. In doing so, the publication has identified a number of measures to explore in order to properly promote the reparation of victims of corruption.

5.1 Asset tracing, including restraining actions - targeting and investigating proceeds and instrumentalities of crimes (both domestic and foreign) or of property of an equivalent value.

5.1.1 Australia

Case Study # 105: Joint international operation confiscates more than $2.25 million in illicit funds and property

Purchase of real estate; proceeds of crime; international cooperation

Operation Bassing saw domestic, international and industry partners cooperate to locate and confiscate proceeds of crime in Australia and offshore. Approximately $3 million worth of assets were forfeited as a result of this international ML and tax fraud investigation.

Operation Bassing commenced with Australia's FIU (AUSTRAC) identifying suspicious account activity and large international funds transfers between bank accounts located in Western Australia and Jurisdiction X. Each of the identified bank accounts were allegedly linked to an individual based in Western Australia, although the bank accounts were held in the names of companies or other individuals.

AUSTRAC referred this financial intelligence to the Australian Federal Police (AFP). In 2020, the AFP-led Criminal Assets Confiscation Taskforce (CACT) then used AUSTRAC's financial intelligence to commence an international investigation with Jurisdiction X's police service. The investigation identified that the balances in the accounts appeared grossly disproportionate to the individual's personal and business income declared to the Australian Taxation Office.

AUSTRAC provided further financial intelligence reports to the CACT to support the investigation, and also exercised its information gathering powers to obtain further information from reporting entities.

After an extensive investigation and civil court proceedings, in 2022 the Supreme Court of Western Australia ordered more than AUD 2.45 million (~ USD 1.69 million) in illicit funds, and a Perth apartment valued at approximately AUD 585,000 (~ USD 404,533) be forfeited to the Commonwealth of Australia under the Proceeds of Crime Act 2002. Further, AUD 1 million (~ USD 691,569) of funds located in Jurisdiction X, were also restrained with the assistance of Jurisdiction X's police service and FIU.

Source - Australia

[131] The Stolen Asset Recovery Initiative Asset - *Managing Seized and Confiscated Assets: A Guide for Practitioners:* https://star.worldbank.org/publications/managing-seized-and-confiscated-assets-guide-practitioners

[132] The Stolen Asset Recovery Initiative Asset - *Victims of Corruption: Back for Payback*: https://star.worldbank.org/publications/victims-corruption-back-payback

5.1.2 Canada

The Royal Canadian Mounted Police (RCMP) has been working to develop capacity with respect to tracing illicit virtual assets, including cryptocurrencies. The RCMP has procured licenses from private sector vendors to obtain the ability to scan and search blockchains to trace the flow of illicit virtual assets. The RCMP is working with these companies to understand the tools on a technical level to strengthen knowledge of how companies identify transactions and collect this information and ensure these processes meet standards required by courts.

To best use these tools the RCMP has designed a training course that teaches investigators how to trace illicit virtual assets in support of criminal investigations, and prepare virtual asset tracing affidavits for use in court

5.1.3. Cook Islands

Case Study # 106: United States - Securities and Exchange Commission fraud

Fraudulent offences (wire transfer, fraud scheme)

On 24 June 2021, the Cook Islands' FIU received a suspicious activity report from a financial institution. The report identified an individual who was the director and controller of corporate entities in the Cook Islands with a value of USD 1.3 million in the corporate bank accounts. The subject, a United States (U.S.) citizen, was allegedly involved in a fraudulent investment scheme on the U.S Securities and Exchange Commission (US-SEC).

The FIU received confirmation of the subject's arrest in the US by the US Department of Justice and received a request to prepare an application for an emergency asset freeze order. The head of the FIU is empowered to apply for freeze orders under the FIU Act 2015.

On 25 June 2021, the High Court of the Cook Islands issued a Freeze Instruction order pursuant to section 35 of the FIU Act 2015 over the USD 1.3 million held with the financial institution. The order was valid for 60 days with the expiration dated 24 August 2021. The Freeze Instruction order was made urgently to prevent dissipation, noting the subject's request, through his counsel, for USD 1.25 million to be transferred to the U.S. for payment of his bail and release from custody.

The FIU's preliminary investigation revealed the subject's corporate entities accounts were opened on 27 January 2021. The nature and purpose of the accounts were stated to be for business activities such as international payments and financial investments, convertible debt investment and paying and receiving payments for services. The FIU prepared a dissemination report for appropriate foreign counterparts and the lead investigation authority – the U.S-SEC.

On 16 November 2023, the Chief Justice of the High Court of the Cook Islands issued a sealed judgment order granting the repatriation of the frozen funds to the U.S., and the repatriation commenced in December 2023. The process for obtaining the final order in the High Court was undertaken pursuant to a Mutual Assistance Request from the U.S and three previous successful extension orders made pursuant to the *Financial Intelligence Unit Act 2015*. The FIU used their power under the FIU Act provision to instruct the reporting institution to extend the Freeze Instruction order. The court submissions were made by the Crown Law Office on behalf of the FIU.

Source - Cook Islands

5.1.4 Hong Kong, China

In late 2023, the Hong Kong Police Force (HKPF) launched a platform, the Anti-Deception Alliance (ADA), where representatives from 10 major banks will be assigned to work alongside officers of the Anti-Deception Coordination Centre (ADCC) under the purview of the Commercial Crime Bureau of HKPF. The ADA is an initiative to provide real-time assistance to HKPF in addressing fraudulent activities, for instance, expediting the processing of handling stop-payment requests to improve the efficacy of the mechanism.

Case Study # 107: Successful stop payment in a business email compromise involving company bank account

Fraud; financial institutions; foreign predicate offence

In early 2023, a manager of a company in Jurisdiction A remitted USD 11 million from the company's bank account to another company bank account in Hong Kong, China upon the receipt of an instruction in an email sent from the company director's email account, which had been hacked. The scam was soon unveiled as the manager learnt that the director's email account was hacked. The case was reported to the Hong Kong Police and a total of USD 8.3 million in the fraudster's account was suspended from further dissipation. Restitution of the defrauded money is ongoing.

Source - Hong Kong, China

Case Study # 108: Successful stop payment in a business email compromise involving company bank account

Fraud; financial institutions

In 2023, an accountant of a local trading company received a bogus email from a scammer who purported to be the company's business partner via spoofing, and then remitted USD 6.8 million from the company's bank account to a company bank account in Jurisdiction A. The scam was soon unveiled when the accountant contacted the real business partner. The case was reported to the Hong Kong Police and the full sum in the fraudster's account was suspended from further dissipation. Restitution of the defrauded money is ongoing.

Source - Hong Kong, China

5.1.5 India

Case Study # 109: Proceeds of crime laundered from multiple frauds

Fraud including forgery; theft; financial institutions; use of legal persons & arrangements

In 2015 and 2016, Indian authorities filed several reports against Person A and others, where it was alleged that a criminal conspiracy existed to commit fraud against a bank-led consortium in relation to fraudulently obtained loans. Some of these allegedly improperly obtained loans were siphoned off within India and overseas through shell companies and converted into real estate and other assets.

The Enforcement Directorate (ED) identified proceeds of crime to the value of INR 112.910 billion (~ USD 1.3 billion) of which INR 50.427 billion (~ USD 601 million) was seized through two provisional attachment orders in 2016. That same year, Person A was declared a proclaimed offender due to having absconded from India. Properties owned by Person A to the value of INR 16.942 billion) (~ USD 202.million) were also attached under S.83 of CrPC without requiring a proven link to predicate offending.

Between 2016 and 2020, the ED issued 21 Egmont requests and Letters Rogatory to eight jurisdictions to identify property and other assets belonging to Person A. These have resulted in a number of seizures, including a French property worth EUR 1.6 million (~ USD 1.8 million), and other assets located in India and abroad.

Person A has yet to face trial in India and in 2019, was declared a Fugitive Economic Offender. Also in 2019, Indian authorities approved his extradition from the United Kingdom (UK) but he is yet to be extradited to India, due to a number of ongoing UK court processes.

The consortium of banks which had lost money as a result of the fraudulent loans filed an application under the *Prevention of Money Laundering Act 2022* for restoration of the properties attached by ED. In 2021, the Special Court ordered INR 141.313 billion (~ USD 1.8 billion) of moveable and immoveable property be restituted to the consortium prior to the completion of the criminal case. This property was 25 per cent higher than the value of proceeds of crime identified and included interest earned while the property was under the control of the Indian Central Government. This was returned to the consortium and not into Indian government revenue.

Source - India

5.1.6 Indonesia

Case Study # 110: Misuse of community funds collected by cooperatives

Fraud

From 2007 to 2014, Cooperative C collected funds of approximately IDR 4.7 trillion (~ USD 308 million), from a total of approximately 23,193 partners. All partner funds (participation capital) were not used to increase the Cooperatives' business activities but paid out as interest and partner capital to 8,414 people/partners, whose membership had reached maturity (from 2007 to 2014) amounting to IDR 1.5 trillion (~ USD 98 million) and also used for the personal interests of the defendant (Chairperson in the Cooperative Management) and several companies. The actions of the defendants caused losses to the entire collection of community funds, amounting to around IDR 3,264,688,621,100. (~ USD 213,661,206) - which is the total savings or investment from 14,779 partners. The defendant was sentenced to 2 years imprisonment, a fine of IDR 5 billion (~ USD 327,237), and confiscation of assets in the form of land scattered in various places to be auctioned off to pay creditors and the remainder handed over proportionally to the victims through an association.

Source - Indonesia

5.1.7 Malaysia

Case Study # 111: Tax evasion - under-reported income

Tax evasion

Person A was the former executive director of a sovereign wealth fund company that was formed to promote economic development (Wealth Fund A). Person A also acted as an arranger to execute syndicated loans, which involved foreign banks and tax havens jurisdictions.

During the investigation, the investigator found that Person A received a significant amount of funds in her bank account from Wealth Fund A and it matched with an indicator that was reported in a suspicious transaction report (STR). Further, the Inland Revenue Board of Malaysia (IRBM) used the net worth method on Person A to determine her under-reported income. and the IRBM found that Person A was involved in tax offences and concealed the amount that she received to evade tax.

Furthermore, the IRBM issued a freezing order on Person A's bank account and subsequently, the court issued a forfeiture order on Person A's two cars and MYR 26,000 (~ USD 5.400) cash in her bank account.

Source - Malaysia

Case Study # 112: Cannabis products

Drug related crime

In June 2022, after a proactive disclosure by FIU Malaysia to the Royal Malaysian Customs Department (RMCD) the RMCD conducted a controlled delivery (following the parcel) operation against a syndicate for suspected selling of cannabis products online.

The syndicate would purchase compressed cannabis from an overseas supplier valued at MYR 3,500 (~ USD 700) per kilogram and then process the cannabis into cannabis flowers and cannabis biscuits. They then actively marketed and received orders for their cannabis flowers and cannabis biscuits via Telegram.

During the operation, the RMCD arrested three suspects and issued freezing order for the freezing of a total of 19 bank accounts amounting to MYR 500,000 (~ USD 104,000). Other items the RMCD seized included a car, and utensils and equipment used in manufacturing the cannabis flowers and cannabis biscuits. All three suspects are connected and have family ties. The RMCD charged all three suspects in court under Section 39B of the *Dangerous Drugs Act 1956*. The case remains ongoing.

Source - Malaysia

Case Study # 113: Disruption of contraband smuggling syndicate involved in drug related crimes

Smuggling (Contraband liquor); drug related crime; self-laundering

As part of an operation to combat contraband smuggling in Malaysia, the Royal Malaysian Police (RMP) seized over 7,000 boxes of contraband liquor, in which the RMP also found (Methylenedioxymethamphetamine (MDMA)) drugs, machinery, and lab equipment that were believed to be used onsite as a small-scale drug processing laboratory.

Person A and Person B were allegedly running this contraband smuggling operation and also used the site to process drugs before distributing them to the local market. Subsequent RMP investigations and asset tracing, which included the use of financial intelligence, resulted in the seizure of assets, including luxury vehicles, bank accounts, jewellery, and cash amounting to approximately MYR 3 million (~ USD 625,000) in value. The RMP also identified that Person A used several companies to launder illicit proceeds through its accounts.

The RMP charged five persons under the *Dangerous Drugs Act 1952* for drug trafficking. The confiscation proceedings for all seized assets under the *Dangerous Drugs (Forfeiture of Property) Act 1988* remain ongoing.

Source - Malaysia

5.1.8 Singapore

Case Study # 114: Confiscation of unexplained wealth from a remote gambling syndicate operator

Organised criminal group; racketeering

In an operation against a criminal syndicate that operated remote gambling services facilitating lottery, soccer, and horse betting since 2014, Person A was arrested along with nine others for their involvement in the syndicate. The Singapore Police Force (SPF) investigation revealed that Person A was an upstream agent in-charge of creating and issuing online betting accounts for six co-offenders on various illegal remote gambling websites. He also facilitated the collection and payment of illegal bets. On 12 July 2018, he was sentenced to a term of imprisonment of 26 months and a fine of SGD 160,000 (~ USD 124,395) for providing Singapore-based remote gambling service and receiving illegal bets under the *Remote Gambling Act 2014*.

Financial investigations revealed that Person A was found to have accumulated unexplained wealth through his illegal activities over the years that was disproportionate to his known sources of income. Following his conviction, the SPF sought a confiscation order against Person A to confiscate the benefits derived from criminal conduct, pursuant to Section 7(1) of the CDSA. On 13 March 2023, the confiscation order was granted by the High Court against Person A to recover a total sum of approximately SGD 110,332.67 (~ USD 85,768).

Source - Singapore

Case Study # 115: Seizure of assets believed to be proceeds of crime obtained from unlicensed money lending and money laundering offences

Unlicensed Moneylending offences

Investigations revealed that between June and October 2020, Person A had allegedly carried on a moneylending business in Singapore without license by issuing illegal loans at the premises of his company, using the business of buying and leasing preowned mobile phones as a front. During the course of investigation, authorities froze five bank accounts connected to the man's criminal activities and seized more than SGD 700,000 (~ USD 544,186). On 22 January 2024, Person A was charged in court for carrying on a moneylending business without license under the Moneylenders Act 2008 and acquiring property which represents the benefits from criminal conduct under the CDSA. Court proceedings against Person A are ongoing.

Source - Singapore

Case Study # 116: Confiscation of proceeds of crime relating to drug trafficking

Drug-related crime

On 18 March 2015, Person A was arrested for trafficking in a controlled drug under the *Misuse of Drugs Act (MDA) 1973.* On 14 December 2017, he was sentenced to the mandatory death penalty for his drug predicate offence.

During his arrest, authorities seized cash amounting to SGD 25,218.30 (~ USD 19,614). During investigations, two bank accounts with a balance of SGD 18.45 (~ USD 14.35) were also put on hold. Person A claimed that out of the monies seized, only SGD 1,000.00 (~ USD 778) was drug proceeds while the rest was from legitimate sources.

To ascertain the magnitude of the benefits Person A had received from his drug trafficking activities, a concealed income analysis was computed. It showed that Person A had a concealed income of SGD 46,199.81 (~ USD 35,872) with realizable assets of SGD 25,236.75 (~ USD 19,629). This was the amount which Person A could not satisfactorily account for as his accumulated wealth, that was disproportionate to his known sources of income.

On 20 February 2023, a Confiscation Order for SGD 25,236.75 (~ USD 19,629) was granted, being the value of the benefits derived from Person A's drug trafficking, in accordance with Section 6 of the CDSA.

Source - Singapore

Case Study # 117: Confiscation of proceeds of crime relating to drug trafficking

Drug-related crime

On 14 March 2012, Person A was first arrested for trafficking in a controlled drug under the *Misuse of Drugs Act (MDA) 1973.* On 6 August 2014, he was sentenced to 11 years of imprisonment for the drug trafficking offence.

During his first arrest, cash amounting to SGD 26,974.10 (~ USD 20,978) and BND 10.00 (~ USD 7.78) was seized. During investigations, one bank account with a total balance of SGD 228.20 (~ USD 177) was also restrained. During financial investigations, Person A claimed that the monies seized were of legitimate source.

During his second arrest on 30 April 2013, authorities seized cash amounting to SGD 5,899.20 (~ USD 4,588). During financial investigations, Person A claimed that only SGD 1,749.20 (~ USD 1,360) was from drug proceeds.

To ascertain the magnitude of the benefits Person A had received from his drug trafficking activities, a concealed income analysis was computed. It showed that Person A had a concealed income of SGD 365,514.32 (~ USD 284,264) with realizable assets of SGD 35,347.66 (~ USD 27,491). This was the amount which Person A could not satisfactorily account for as his accumulated wealth was disproportionate to his known sources of income.

On 7 August 2023, a Confiscation Order for SGD 35,347.66 (~ USD 27,490)[133], being the value of the benefits derived from Person A's drug trafficking, in accordance with Section 6 of the CDSA was granted.

Source - Singapore

Case Study # 118: Cash couriering by money service bureaus through cash smuggling

Smuggling; currency exchange/cash conversion; cash

Singapore's cross-border cash movement reporting regime requires all travellers arriving and departing Singapore to submit a full and accurate cash movement report of any physical currency and bearer negotiable instruments exceeding SGD 20,000 (~ USD 15,554) into or out of Singapore.

In June 2023, Person A had only declared a sum equivalent to SGD 505,500 (~ USD 393,143) upon arrival in Singapore but was found to be physically carrying cash equivalent to about SGD 1.98 million (~ USD 1,539,906). This was detected by Singapore law enforcement officers during an enforcement check at Singapore Changi Airport. Through investigations by the Commercial Affairs Department of the Singapore Police Force, Person A was found to be employed by a money-service business in Jurisdiction A and had couriered cash into Singapore for foreign currency exchange purposes. Investigations also revealed that Person A had previously submitted another false declaration on arrival in Singapore in June 2023, where

[133] The final forfeiture amount is not finalized yet, as it is pending auction

he had only declared a sum equivalent to SGD 458,000 (~ USD 356,200), when he was in fact carrying the equivalent of SGD 1 million (~ USD 777,706).

For the above two instances, in November 2023 Person A was convicted of two offences under Section 60 of the CDSA read with Section 108B of the *Penal Code 1871* and sentenced to a total fine of SGD 30,000 (~ USD 23,329). These are charges for engaging in a conspiracy to move cash into Singapore which exceeded the prescribed amount of SGD 20,000 (~ USD 15,554) without giving a full and accurate report to an authorised officer on the movement of that cash. On the Public Prosecutor's application, the Court granted a Confiscation Order under Section 64 of the CDSA for the sum of SGD 400,000 (~ USD 311,051) to be paid to the State.

Source - Singapore

Case Study # 119: Confiscation of benefits derived from man who dealt with uncustomed cigarettes

Smuggling; self-laundering; cash

Investigations by the Singapore Customs saw the arrest of Person A for dealing with over 800kg of duty-unpaid cigarettes, thereby evading over SGD 400,000 (~ USD 311,051) in excise duties and taxes. He was convicted and sentenced to 37 months' imprisonment for offences including Section 128I(1)(b) of the *Customs Act 1960*.

As the suspect was arrested with over SGD 160,000 (~ USD 124,412) in cash which he could not satisfactorily account for, the Customs authority referred the case to the Commercial Affairs Department of the Singapore Police Force to conduct financial investigations. A sum of about SGD 110,000 (~ USD 85,531) deemed to be the benefits from his criminal conduct, was eventually confiscated from Person A in August 2023 pursuant to Section 5 of the CDSA.

Source - Singapore

5.1.9 Chinese Taipei

Case Study # 120: The Lafayette Frigate case

Corruption and bribery

The Lafayette Frigate case that attracted attention in Chinese Taipei involved the illicit kickbacks received by the arms broker Person A, and in 2001, European media revealed that Person A's family had an abnormally large amount of money flowing into European jurisdictions. With assistance from the Ministry of Justice, the Supreme Prosecutors Office sought mutual legal assistance from various jurisdictions to freeze their overseas assets. From 2001 to 2003, Jurisdiction A successively froze as many as 27 bank accounts controlled by Person A's family. During 2006, Jurisdiction B agreed to provide assistance and to freeze the family's overseas bank accounts. The co-defendant Person B and others were indicted for receiving kickbacks together, and Person A's family members were indicted for helping to receive kickbacks, in accordance with the Anti-Corruption Act. Person A and his family members fled abroad for a long period of time. Although the court issued a wanting warrant, the trial still could not be carried out substantively. Person A's family possesses a huge amount of illicit proceeds, and their accounts and assets were located in multiple jurisdictions, so the cross-jurisdiction pursuit of the proceeds of crime became extremely difficult.

After the amendment of the confiscation system of the Criminal Code implemented on July 1, 2016, the Supreme Prosecutors Office immediately filed a petition for declaration of confiscation. The Supreme Court ruled in 2019 and 2021 respectively, that the principal amount of the criminal proceeds to be confiscated in this case totalled more than USD 487,190,000, which provided the legal basis for the Ministry of Justice to request the confiscation of Person A's family's overseas illicit proceeds of crime in other jurisdictions. Then the Ministry of Justice liaised and actively assisted the Taipei District Prosecutors Office in requesting Jurisdiction B and Jurisdiction C to return the frozen assets of Person A's family. With the support and assistance of the two jurisdictions, Jurisdiction B has transferred more than USD 11.03 million in February 2023, and Jurisdiction C has transferred USD 138.04 million to Chinese Taipei in July 2023. Under dedicated efforts and with the help of the Ministry of Foreign Affairs and Délégation culturelle et économique de Taipei in Jurisdiction C, the mutual legal assistance, which has lasted for more than 20 years, has finally come to fruition. To properly respond to public's expectations, the Ministry of Justice will continue working on international cooperation, to recover all the proceeds of crime hidden overseas, to completely deprive the illegal benefits obtained, and ensure that social justice prevails.

Source - Chinese Taipei

Case Study # 121: Recovery of Jurisdiction A' assets

Fraud

In 2019, Chinese Taipei received a mutual legal assistance request from Jurisdiction A to retrieve proceeds of crime from a fraud against its citizens, that was transferred to Chinese Taipei, who had subsequently seized it. The investigations lasted years in both jurisdictions, with the relevant competent authorities holding numerous discussions, and Chinese Taipei eventually requested Jurisdiction A to provide the relevant evidence. With the assistance and arrangement of Chinese Taipei's competent authority, Jurisdiction A's Ministry of Justice sent its investigator and assistant to Chinese Taipei to retrieve the proceeds of crime held in Chinese Taipei's Prosecutor's Office, which was physical currency of approximately USD 34,000. This is the first successful case between Jurisdictions A and Chinese Taipei in cross-border asset recovery in recent years.

Source - Chinese Taipei

5.1.10 Vietnam

Case Study # 122: Fraud and misappropriation of funds using computer networks, telecommunications networks, and electronic media

Fraud including social media

The case of eight defendants who defrauded and appropriated a total amount of VND 657,353,973,788 (~ USD 27,115,207).

The defendants committed the crime of using computer networks, telecommunications networks, and electronic media to commit acts of property appropriation. The defendant's company built software to develop company websites, applications, and e-commerce exchanges to call on investors to buy "decentralised" shares under a type of multi-level marketing. By mobilizing high interest payments in the form of multi-levelling, taking money from newer investors to pay commissions and bonuses to previous investors, which appropriated the newer investors' money.

During the investigation, the Investigation Agency froze and confiscated VND 179,686,704,902 (~ USD 7,411,900) in the accounts of Company A and the defendants as the proceeds of crime. Further, the Investigation Agency seized 12 houses and plots of land that were the headquarters of Company A's representative offices and seized five cars that belonged to Company A, used by a number of heads of the representative offices, as the proceeds of crime.

Source - Vietnam

Case Study # 123: Property appropriation fraud that occurred at joint stock company

Theft; use of capital markets

The case related to property appropriation fraud that occurred at joint stock company and its related companies.

The defendant, Person A brokered and cooperated with Person B, a foreign investment broker, to carry out transactions of buying and selling shares of different companies. Person A directly received money from Person B and his partners, signed a contract with Person B to buy and sell shares of Company C in order to appropriate Person B's money of approximately VND 77,577,600,000 (~ USD 3,2000,000).

Person A's family paid VND 20,000,000,000 (~ USD 824,980) in cash to overcome the consequences, and the prosecution agency seized three real estate properties.

Source - Vietnam

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

5.2.1 Japan

Japan noted the National Police Agency managed seized assets based on the *Rules of the National Public Safety Commission* and their *guideline for the storage and management of material evidence*.

5.2.2 Macao, China

The asset seizure mechanism and procedures of Macao, China are mainly regulated by the Criminal Procedural Code. According to the law, judicial authorities may approve or order seizing assets 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 assets that may be regarded as evidence. The seized assets shall be attached to the case file, and where not possible to do so, they are entrusted to the custody of the judicial employee responsible for that proceeding or of the depositaries. If the seized assets could 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 handle the seized assets (which are lawfully managed by the Public Prosecutions Office (MP)) during the course of proceeding, more systematically and efficiently, MP built the "seized assets management system" with a user manual available. MP also planned to gradually develop a structured format for the transmission of information on seized assets with the police departments, and it will continue to discuss and promote the systematic exchange of data.

5.2.3 Philippines

The AMLC is mandated to preserve, manage, or dispose of assets pursuant to a Freeze Order, Asset Preservation Order, and Judgment of Forfeiture pursuant to Section 7(16) of the AMLA, as amended.

In line with this undertaking, the AMLC, through its Asset Management Group, ensures that all frozen, preserved, and forfeited assets subject of freeze orders, preservation orders and judgments for forfeiture are monitored, maintained, and preserved, disposed of, if necessary, and transferred to the National Government.

Assets subject of pending civil forfeiture (CF) cases (2003-2023)

As of 31 December 2023, there are total of 119 pending civil forfeiture cases with a total of preserved assets amounting to PHP 9,143,220,299.09 (~USD159 million), consisting of bank assets, insurances, other stock investments and real properties with valuation. Details of which are as follows:

Table 9. Assets Subject of Pending CF Cases per Asset Type (2003 – 2023)

Cases	119
Bank Assets[134]	~~PHP~~ 3,900,448,592.34
Other Monetary Instruments[135]	~~PHP~~ 277,568,924.03
Insurance[136]	~~PHP~~ 236,517,787.22
Real Properties (RP) with valuation (Stillin the Name of the Respondents)	~~PHP~~ 4,630,036,333.00
Motor Vehicles with valuation	~~PHP~~ 98,648,662.50

[134] FX converted to PHP
[135] FX converted to PHP
[136] FX converted to PHP

Total	**PHP 9,143,220,299.09**

Moreover, the following shows the distribution of assets subject of pending CF cases per unlawful activity.

Assets Subject of Pending CF Case per Unlawful Activity (2003 to 2023)			
Rank	**Unlawful Activity**	**Amount**	**Percentage (%) to Total**
1	Corruption	~~PHP~~ 3,925,751,560.30	42.94%
2	Illegal Drugs	~~PHP~~ 3,013,789,505.13	32.96%
3	Other Crimes*	~~PHP~~ 904,378,702.96	9.89%
4	Fraud	~~PHP~~ 815,870,084.83	8.92%
5	Terrorism Financing	~~PHP~~ 483,430,445.86	5.29%
	Total Assets Preserved	~~PHP~~ 9,143,220,299.09	100%

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

5.3.1 Hong Kong, China

The most common restrained and confiscated assets in HKC were funds in bank accounts, insurance and securities held with licensed corporations or banks. Other assets included precious metals, stones, jewellery, wristwatches and physical cash.

Case Study # 124: Laundering of proceeds of crime from email scam

Fraud; foreign predicate offence

In 2011, several victimized companies in several jurisdictions fell prey to email scam with their business partners and were deceived to remit over HKD 500,000 (~ USD 69,570) to a bank account set up in Hong Kong, China by a stooge. Subsequent enquiries revealed that the stooge had immediately left Hong Kong, China after setting up the stooge bank account. In 2023, the Hong Kong Police successfully prevented the dissipation of the proceeds of crime and eventually obtained a local confiscation order to confiscate the tainted funds remaining in the stooge's account.

Source - Hong Kong, China

Case Study # 125: Money laundering via bank accounts

Drug related crime

Intelligence suggested that a couple had laundered the proceeds of crime in relation to drugs. Financial investigation revealed that between 2014 and 2016, they had laundered proceeds amounting to HKD 14 million (~ USD 1.948 million) through five personal bank accounts. The ML hallmarks observed, were for instance, frequent and significant turnover which was not commensurate with their income. The couple were subsequently charged and convicted for ML and after trial at Court in 2023, assets of HKD 150,125 (~ USD 19,311) were confiscated.

Source - Hong Kong, China

Case Study # 126: Money laundering syndicate exploiting foreign domestic helpers as stooges

Fraud; transnational organised crime group; foreign predicate offence

In April 2021, intelligence exchange between the Joint Financial Intelligence Unit (JFIU) and Jurisdiction A suggested that a bank account in Hong Kong, China held by a foreign domestic helper was involved in an attempted romance scam that occurred in Jurisdiction A. Further investigation revealed that over 20 foreign domestic helpers had sold their bank accounts to a money laundering syndicate. The syndicate used the bank accounts to receive money originated from various online scams and then immediately withdrew the money in cash through ATMs. The Hong Kong Police arrested two core syndicate members who were responsible for withdrawing cash and 24 foreign domestic helpers who sold their bank accounts to the syndicate. The two core syndicate members and six stooges were convicted for ML and sentenced to between eight to 30 months' imprisonment. The court approved a Confiscation Order to confiscate a total of HKD 204,598.42 (~ USD 26,319), USD 200 and PHP 20 (~ USD 0.35). Prosecutions against other stooges are ongoing.

Source - Hong Kong, China

5.3.2 Macao, China

With respect to confiscating instruments and proceeds of crime, the Penal Code of Macao, China has set aside specific chapters with stipulations regarding the loss of assets or rights related to criminal activities. It also has provisions for the handling of assets 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 the criminal activities. In cases where certain proceeds of crime cannot be seized in a material manner, the criminal will have to pay a certain amount of money to Macao, China as compensation.

5.3.3 Malaysia

Malaysia observed the following general challenges in implementing confiscation or forfeiture of criminals' assets:

- Difficult to establish the money/asset trail or link.
- Defendant could not be located, contacted or absconded.
- Difficulty in repatriating assets if it was moved overseas (e.g., differing legal framework, involving multiple jurisdictions.
- Loss of value of the asset/depreciation.

5.3.4 Chinese Taipei

The confiscation provisions of Chinese Taipei's Criminal Code took effect on 1 July 2016. As of February 2024, the total confiscation amount ordered by the court has reached more than TWD 169.5 billion (approximately USD 5.3 billion).

On 17 November 2023, the Constitutional Court held a debate on the provisions of Article 19, Paragraph 3 of the Narcotics Hazard Prevention Act which concluded on 26 January 2024. The Constitutional Court declared that the extended confiscation of gains serves the same purpose as general confiscation, which is to revert unlawfully acquired property to its legal state, rather than imposing punishment. This does not violate the principles of nulla poena sine lege, culpability, presumption of innocence, and the intelligible principle. The judgment also acknowledges that the provision for extended confiscation of gains is based on public interest, which is reasonably related to the objective of preventing drug crimes and is in accordance with the principle of proportionality.

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

5.4.1 China

Case Study # 127: Cross-border asset recovery

International cooperation

In October 2015, the public security agencies in Hunan Province, China launched an investigation into a criminal syndicate. The criminal syndicate had more than ten members and cheated participants by eliciting payment of Chinese yuan to purchase foreign products and stocks online. Participants could receive a commission if they recruited more members or bought more products. This pyramid scheme spread across 18 provinces and involved nearly 50,000 participants.

In December 2015, the leaders of the criminal syndicate were arrested and later convicted of the crime of organising or leading the pyramid selling activities. Meanwhile, the public security agencies in Hunan Province, under the guidance and deployment of the Office for the "Fox Hunt Operation" at the Ministry of Public Security, cooperated with foreign police for asset recovery procedures. Proceeds of the criminal activity were laundered through an underground banking network (illegal cross-border money transmitter). After negotiations, in 2023 an in-principle asset sharing agreement was reached between both jurisdictions to enable each to recover from forfeited assets. The foreign counterpart shared and returned assets with a total value of 166 million yuan (~USD 22.8 million).

Source - China

5.4.2 Japan

Case Study # 128: Proceeds from a case of fraud on fund investment performance

Fraud; money laundering; confiscation; collection of a sum of equivalent value

Three people (Persons A, B and C) collaborated to defraud a pension fund through presenting falsified investment performance data on a fund managed by Company A, where Person A served as CEO. This resulted in the trio fraudulently obtaining approximately JPY 24.8 billion (~ USD 158 million) Upon prosecution, the court found all three guilty and ordered the confiscation and collection of a sum of equivalent value to deprive them of the proceeds of crime.

Following the court decision, the Japanese authority sent a mutual legal assistance request to Jurisdiction B, requesting to confiscate money held in bank accounts in Jurisdiction B. In May 2023, Jurisdiction B transferred the funds valued at approximately JPY 717 million (~ USD 4.59 million) to Japan. Japan is currently distributing these funds to the victims.

Source - Japan

Case Study # 129: Proceeds from a case of fraud on foreign exchange transaction

Fraud; money laundering; collection of a sum of equivalent value

Persons A and B worked together to defraud people conducting foreign exchange transactions through an investment school. They fraudulently obtained approximately JPY 1.9 billion (~ USD 12 million) from the victims. The court found Persons A and B guilty and ordered the confiscation and collection of a sum of equivalent value to deprive them of the proceeds of crime.

Following the court decision, Japan sent a mutual legal assistance request to Jurisdiction A to confiscate approximately JPY 120 million (~ USD 769,000) sitting in a bank account held by Person B. After receiving the funds from Jurisdiction A, Japan distributed these to the victims.

The remaining funds of JPY 1.78 billion (~ USD 11.2 million) were remitted to bank accounts in other jurisdictions.

Source - Japan

Case Study # 130: Investment fraud and money laundering

Fraud, Standalone money laundering

The Malaysian FIU received a suspicious activity report (SAR) information from a foreign FIU regarding a large amount of virtual assets belonging to two Malaysian individuals stored in accounts with a VASP.

According to investigations conducted by the Royal Malaysian Police (RMP), the RMP determined the virtual assets reported by the foreign FIU can be linked to fraudulent activities associated with a previously operating ponzi scheme in Malaysia. The ponzi scheme cantered around a Bitcoin investment program that targeted investors through social media, offering a daily return on their investments. In addition, investors were enticed with a referral commission for bringing in new participants to join the investment.

Malaysian authorities took immediate action by submitting a MLA request which led to the seizure of VAs amounting to approximately USD 34.5 million, stored in VA accounts with assistance from the foreign jurisdiction. Investigations are ongoing.

Source - Malaysia

5.4.3 Singapore

Case Study # 131: Successful repatriation of funds to Jurisdiction L

Corruption; international cooperation; self-laundering; third party laundering; purchase of real estate; asset recovery

In 2015, Singapore's Corrupt Practices Investigation Bureau (CPIB) received information that Company U, an Aircraft manufacturer from Jurisdiction X, had engaged an 'adviser' in Jurisdiction L to pay bribes to officials from the National Airlines of that jurisdiction to secure contracts for the provision of aircrafts and aftermarket service of the aircraft engines. Investigations identified the adviser to be Person A and the officials from the airlines who had allegedly received bribes to be Person B, President and Chief Executive Officer, Person C, Executive Vice-President of Maintenance and Fleet Management, and Person D, Vice-President of Asset Management.

CPIB also received information that all the subjects mentioned above have banking presence in Singapore and that bribes might have been paid and laundered through the Singapore banking system. Fund tracing by CPIB revealed that Person A had transferred monies to Persons B, C and D by layering through accounts belonging to him or companies beneficially owned by him.

A joint investigation was carried out by authorities in Jurisdiction X, Jurisdiction L, and CPIB on the corruption as well as ML offences.

Seizure of Accounts and Property

On 16 January 2017, CPIB exercised its powers under *Criminal Procedure Code* and seized 32 relevant bank accounts and a private (real) property registered under the name of Person B. The purchase price of the property was SGD 2,626,140 (~ USD 1,944,000)

Other Information

On 17 January 2017, authorities in Jurisdiction X reached a Deferred Prosecution Agreement (DPA) with Company U. The indictment, which was suspended for the term of the DPA, covered 12 counts of conspiracy to corrupt, false accounting, and failure to prevent bribery. In the DPA, it was stated that the corrupt conduct spanned three decades and involved several jurisdictions including Jurisdiction L.

In late 2019, authorities in Jurisdiction L obtained the cooperation of Person D to surrender the funds he had remaining in a Singapore bank account to the authorities.

On 3 September 2020, CPIB coordinated with AGC and the authorities in Jurisdiction L and successfully transferred USD 1,402,125.49 from Person D's Singapore bank accounts to Jurisdiction L by way of voluntary repatriation of funds.

On 8th May 2020, Persons B and A were convicted on corruption and ML charges in Jurisdiction L.

In April 2021, Singapore received a foreign confiscation order from the authorities of Jurisdiction L against the private property. Singaporean authorities are currently working towards obtaining a confiscation order from the High Court and will thereafter proceed with realisation of the private (real) property and repatriation to Jurisdiction L.

Source - Singapore

Case Study # 132: Successful confiscation of assets

Corruption; suspicious transaction reporting; international cooperation; self-laundering; asset recovery

In 2017, Singapore's Corrupt Practices Investigation Bureau (CPIB) received information that Person A, the former President of a State-owned Railway Company of Jurisdiction S, was under investigation by the authorities of Jurisdiction S for receiving approximately USD 34 million in bribes. Person A and his wife fled Jurisdiction S before the authorities were able to arrest them. They were believed to have laundered the bribery money to various destinations such as United States, Australia, Cyprus, St. Kitts & Nevis, Hong Kong, China and Singapore.

Singapore's Suspicious Transaction Reporting Office (STRO)'s analysis revealed that in March 2017, suspected criminal proceeds were transferred to an Investment Platform account in Singapore registered in the name of Person A's wife, and the SRO disseminated this information to the CPIB.

Based on the information received, CPIB commenced investigation into possible CDSA offences against the investment platform. CPIB seized USD 500,028 under CPC powers. Investigations revealed that the investment platform was not complicit in any offences.

From March 2018 to January 2020, CPIB worked closely with the authorities in Jurisdiction S to defend the seizure of USD 500,028. The authorities in Jurisdiction S provided sufficient evidence to show that the funds stemmed from corrupt proceeds.

In January 2020, the Court of Jurisdiction S granted an order for the confiscation of the assets in Singapore. Singaporean authorities are currently working towards realization of the assets with the aim to repatriate funds to Jurisdiction S in 2024.

Source - Singapore

Case Study # 133: Close collaboration with foreign counterpart leads to successful conviction and confiscation of assets

Corruption; international cooperation; self-laundering; third party laundering; purchase of real estate; asset recovery

In 2016, Singapore's Corrupt Practices Investigation Bureau (CPIB) investigated two Singaporeans, Persons A and B (siblings), who had assisted two trucking companies in Jurisdiction S, to win the trucking contracts for a major hard disk manufacturer, Company X. Person A was a Senior Director of Company X. Person A leaked confidential information to Person B, who then helped the two trucking companies win the contracts. In return for winning the contracts, the two trucking companies paid bribes disguised as 'commissions' to company Y, in Jurisdiction T, owned by a boyfriend of Person B. The total amount of bribes received was about USD 1.6 million. The 'commissions' were deposited by the trucking company into the boyfriend's personal bank accounts in Jurisdiction S. Person B would withdraw the monies from the account and deposit them into her own bank account in Jurisdiction S. Person A then withdrew the money in Singapore, using Person B's ATM card. Person A had used the money to purchase a property under Person B's name in Singapore.

Singaporean authorities sent an MLA request to Jurisdiction S to retrieve bank accounts details and transaction details of the deposits within the account. Authorities in Jurisdiction S also assisted to interview two representatives from the trucking companies. The evidence obtained from Jurisdiction S was critical to the case. It was established that Person A had withdrawn SGD 703,480 (~ USD 547,082) to pay for the property and legal fees incurred. The purchase price of the property was SGD 1.12 million (~ USD 871,005) and CPIB lodged a caveat against the property.

Persons A and B were convicted of corruption as well as CDSA offences and in 2023, Singapore successfully confiscated approximately SGD 2.2 million (~ USD 1.7 million) from them.

Source - Singapore

5.4.4 Chinese Taipei

Case Study # 134: The Lafayette Frigate case

International cooperation

Since Jurisdiction A and B have assisted the aforementioned Lafayette Frigate Case for more than 20 years, and by considering the spirit of the *United Nations Convention against Corruption* and international practices, Chinese Taipei has shared the assets with Jurisdiction A and B to facilitate long-term international collaboration and cooperation.

Source - Chinese Taipei

6 - 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 2023/2024.

6.1 Financial Action Task Force

The FATF developed the following reports that outline some of the latest AMLCFT methods and trends.

Illicit Financial Flows from Cyber-enabled Fraud[137]

Online fraud and scams have dominated the cyber-enabled crime landscape. Left unchecked, they will only grow in sophistication and pose a greater threat and risk as more organised crime groups engage in this illicit activity and take advantage of opportunities presented by new technologies, such as generative artificial intelligence.

This report focuses on illicit financing arising from cyber-enabled fraud (CEF) that is enabled through or conducted in the cyber environment and that:

- Involves transnational criminality such as transnational actors and funds flows.
- Involves deceptive social engineering techniques (i.e., manipulating victims to obtain access to confidential or personal information).

This report aims to enhance competent authorities' risk understanding of the threat posed by CEF. The report builds upon existing work already done by the FATF and other international bodies (including the Egmont Group, Europol, and INTERPOL), and looks to identify significant and emerging developments which are relevant for enhanced risk understanding.

Experts from Singapore (on behalf of the FATF), FIU Hong Kong China (on behalf of the Egmont Group) and INTERPOL, co-led this project. In addition, the following jurisdictions and entities contributed to the work as part of the project team: Azerbaijan, Brazil, Belgium, Canada, China, the Council of Europe, the European Commission, Europol, Germany, the Inter-Governmental Action Group against Money Laundering in West Africa (GIABA), India, Italy, Israel, Japan, Malaysia, Mexico, the Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism (MONEYVAL), Pakistan, Portugal, Saudi Arabia, Togo, the United Kingdom, and the United States.

The findings in the report are based on: A review of existing literature and open-source material on this topic. This includes data and research done by the Egmont Group and INTERPOL; a request to the FATF's Global Network and the Egmont Group of over 200 jurisdictions and 170 FIUs respectively, for information on risks, enforcement frameworks and strategies, as well as domestic and international cooperation and co-ordination mechanisms. In total, the project team received inputs from more than 80 delegations; and discussions and insights shared at the FATF's Joint Experts Meeting (April 2023) and the Private Sector Consultative Forum (May 2023), including a targeted engagement with the private sector.

<u>Key findings, recommendations</u>

CEF is a growing transnational organised crime, and CEF criminal syndicates are often well structured into distinct sub-groups with specialised areas of criminal expertise, including ML. These sub-groups may also be loosely organised and de-centralised across different jurisdictions, which further complicate efforts to investigate CEF activity. CEF syndicates are also found to be linked to other types of criminality, notably human trafficking and forced labour in CEF call centres as well as PF-linked to illicit cyber activities from the DPRK.

ML groups and professional enablers are involved in the CEF-ML process. The ML network of accounts typically involves money mules but can also include shell companies or legitimate businesses. ML networks also feature different types of FIs, including banks, payment and remittance providers, and VASPs. To further conceal the financial trail of their ill-gotten gains, criminals use a combination of various ML techniques, such as the use of cash, TBML and unlicensed services.

Aided by digitalisation, technology has allowed CEF criminals to develop and increase the scale, scope, and speed of their illicit activities. They use various tools and techniques to deceive victims or prey on their

[137] FATF - *Illicit Financial Flows from Cyber-enabled Fraud*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Methodsandtrends/illicit-financial-flows-cyber-enabled-fraud.html

psychological state and emotions to extract as much funds as possible. CEF syndicates are exploiting technological developments to make it easier and faster to launder the proceeds of their crimes. Virtual services, such as remote online account opening, also allow criminals to easily set up foreign accounts and launder proceeds abroad, with financial transactions being executed at near-instantaneous speeds. Criminals are taking advantage of social media and messaging platforms to recruit money mules across borders at scale. Criminals are also quick to exploit vulnerabilities that emerge through new digital financial institutions and products, as well as non-traditional sectors such as e-commerce and social media and streaming platforms.

Jurisdictions need to respond more effectively to tackle CEF. They need to: employ initiatives to increase victim reporting and enhance suspicious transaction reporting; effectively analyse voluminous information inflows; and given the cross-cutting nature of CEF, strong domestic co-ordination mechanisms are required to holistically combat and prevent CEF and related ML.

The location where CEF predicate offences occur tends to be different from where the ML process occurs. Proceeds of crime can be laundered quickly through a network of accounts, which often span across multiple jurisdictions and financial institutions. Jurisdictions must collaborate multi-laterally to effectively and expeditiously intercept CEF proceeds that are laundered across borders. To do so, they should leverage and support existing (and any future) multi-lateral mechanisms (such as INTERPOL's IGRIP and the Egmont Group BEC Project) for rapid international cooperation and information exchange to more effectively combat CEF.

Lastly, the report includes a list of risk indicators, as well as useful anti-fraud requirements and controls, that are useful for public and private sector entities to detect and prevent CEF and related ML.

Misuse of Citizenship and Residency by Investment Programmes[138]

Each year, tens of thousands of people around the world become new citizens or permanent residents of jurisdictions in which they were not born by virtue of investing in those jurisdictions. Citizenship and residency by investment (CBI/RBI) programmes are government-administered programmes that can benefit both host jurisdictions (by spurring economic growth, such as through expanding foreign investment channels) and wealthy individuals (by allowing them to gain citizenship or residency and the associated additional rights by expediting or bypassing the normal, more lengthy migration processes). These programmes attract an array of clients, many of whom have gained their assets legitimately and have benign intentions. However, they can also be misused by criminals who seek to launder and conceal proceeds of crime or commit new offences, including financial crimes, undermining these programmes' intended objectives.

This joint report of the FATF and the Organisation for Economic Co-operation and Development (OECD) holistically examines ML and financial crime risks associated with investment migration programmes, including risks related to foreign bribery, fraud and corruption, alongside other policy considerations related to public integrity, tax and migration.

Experts from the United States and United Kingdom co-led this project team alongside experts from the OECD, and with support from the FATF Secretariat. The project team consisted of experts drawn from 19 members of the FATF Global Network and three FATF Observers: Antigua and Barbuda, Bahamas, Canada, China, Dominica, European Commission, Greece, Grenada, India, Ireland, Malta, Mexico, Nigeria, Portugal, Saint Lucia, Trinidad and Tobago, Türkiye, United Kingdom, United States, Caribbean Financial Action Task Force Secretariat, International Monetary Fund IMF and the OECD.

The project relied on information, case studies, and jurisdiction examples provided in questionnaire responses returned by 36 jurisdictions within the FATF Global Network, as well as discussions held in a session of the FATF Joint Experts' Meeting in April 2023. Inputs also included responses to a questionnaire circulated to delegates to the OECD Working Party of Senior Public Integrity Officials (SPIO), and insights from private sector investment migration practitioners and the financial sector through a session at the FATF's Private Sector Consultation Forum in May 2023. The project team also engaged with academics and noted available published academic literature, government reports and NPO research papers published in this field.

Key findings, recommendations

Criminals have exploited a range of vulnerabilities in CBI/RBI programmes to perpetrate massive frauds and launder proceeds of crime and corruption reaching into the billions of dollars (USD), while also hiding assets in less compliant or effective jurisdictions, facilitating organised crime and evading law enforcement. CBI programmes are particularly vulnerable because they allow illicit actors more global mobility, the ability to open

[138] FATF - *Misuse of Citizenship and Residency by Investment Programmes*: https://www.fatf-gafi.org/en/publications/Methodsandtrends/misuse-CBI-RBI-programmes.html

bank accounts and establish shell companies in other jurisdictions, and to disguise their identity or conceal where they may owe taxes or other liabilities from financial institutions by using new identification documents.

Both CBI and RBI programmes can provide the criminally wealthy with a range of opportunities, such as the ability to place assets and family members overseas to prevent or hinder asset recovery efforts, explain suspicious high-value transactions, and enable the movement of significant sums of illicit funds across borders. These programmes can act as a gateway for their recipients to the financial systems of both small and large jurisdictions, as well as regional markets. The provide the new citizens or residents with access they might not have enjoyed by virtue of their original citizenship or jurisdiction of origin, and the likely lesser scrutiny that comes with being a domestic (as opposed to foreign) actor within their new financial system.

Investment migration programmes are complex and international – the high level of involvement by intermediaries in their design and development, and the necessary involvement of multiple agencies across a government, can provide challenges in coordination, implementation and regulation. These programmes are also vulnerable to misuse by professional enablers and fraudsters targeting opportunities to service or exploit the users of these programmes. Criminal, negligent, or complicit property agents, wealth managers immigration agents, marketing agents and concierge firms can assist in the misuse of these programmes. They often do this by failing to carry out their due diligence and financial crime reporting functions properly or by creating fraudulent/misleading evidence for clients to present in their applications to a competent authority.

Opportunities for misuse tend to arise especially when governments struggle to govern their programmes effectively. Malign interests can infiltrate programmes when there is a lack of clarity around the roles of public and private actors involved, where conflicts of interest are not adequately managed, and where resources are lacking to ensure proper oversight. These challenges are compounded where there is a lack of internal control and audit measures to ensure that programmes are operating as intended, as well as the difficulties government agencies face in coordinating across public authorities and borders to manage risks. Programmes appearing vulnerable to criminal misuse may lead to suspension of visa-free travel to third jurisdictions and undermine business and international relations.

To help policy makers and programme operators strengthen the governance of programmes and address ML and financial crime risks, this report proposes a series of mitigation measures. Conducting sound analysis of ML and corruption risks, setting clear objectives and building integrity measures into the design and implementation can help set programmes on a solid footing. Domestic co-ordination across law enforcement authorities, immigration authorities, and financial intelligence units is important to effectively monitor and mitigate ongoing risks. As risks extend beyond the jurisdiction operating the programme, there is also a need for multilateral cooperation to ensure that information is swiftly exchanged and enforcement mechanisms are mutually supportive.

Jurisdictions operating programmes that permit private sector investments have increasingly grappled with fraud risks and the need to control not just where funds come from, but also to where funds subsequently flow.

Ultimately, policymakers, programme operators, financial institutions and law enforcement should be particularly alert to the elevated risks of ML and financial crime not just in relation to applicants but also from professional enablers and intermediaries who are engaged in investment migration-related transactions. Ensuring clarity around the respective roles and responsibilities of public and private sector actors is a key step to prevent undue infiltration of private interests in the execution of citizenship and residency by investment programmes.

Recovering the International Proceeds of Crime through Inter-Agency Networks [139]

This report on Asset Recovery Inter-Agency Networks (ARINs) is specifically designed for policymakers and law enforcement agencies across the globe. ARINs help LEAs across different jurisdictions work together to track money gained from crimes like ML and other related offenses. This report is aimed at provides a broad review of ARINs. It covers their global impact, roles, management, challenges, and cooperation with other international groups.

This report equips policymakers with a deeper understanding of the role of ARINs and identifies areas with potential for improving practices, developing enhanced performance monitoring, and strengthening collaboration with international organisations. It underscores the importance of robust data collection and reporting to demonstrate the invaluable role of ARINs in the global fight against financial crime.

This study is based on a project by the FATF, aiming to improve collaboration with ARINs, their secretariats,

[139] FATF - *Recovering the International Proceeds of Crime through Inter-Agency Networks*: https://www.fatf-gafi.org/en/publications/Methodsandtrends/recovering-international-proceeds-crime-inter-agency-networks.html

and other global organisations focusing on asset recovery.

Key findings, recommendations

ARINs facilitate informal assistance during the asset recovery process, including asset identification, tracing, seizing, freezing, confiscation and repatriation efforts. Despite the ARINs' important role, there is often a lack of clarity among policymakers regarding the nature of ARINs and their contributions to the global landscape of criminal asset recovery. The use of ARINs is also not wide-spread or systematic, with only a handful of investigations facilitated by these networks globally

ARINs play a vital role in building trust among law enforcement practitioners. They also collaborate with various international organisations in this domain and can act as intermediaries with other regional networks. Nevertheless, co-ordination between ARINs and other international organisations often falls short, limiting opportunities to bolster member jurisdiction capacities.

While the coverage of ARINs has expanded, regional gaps persist, notably in the Middle East, North Africa, and Central Africa regions. Currently, there are 178 Member jurisdictions within ARIN networks, including 159 members of the FATF's Global Network of 205 jurisdictions.

ARINs operate independently, each with its own governance structure, mandate and guiding principles. While participation in ARINs is not compulsory, they are proven to build stronger ties between investigators and asset recovery offices. This leads to greater trust and more open lines of communication across borders. As a result, jurisdictions have successfully provided important and sometimes crucial details on assets like the existence of bank accounts, businesses, real estate and registered possessions of suspected criminals and money launderers in other jurisdictions.

ARINs facilitate many cases, but they are also facing resource challenges. Estimates and qualitative feedback suggest some leading ARINs can oversee hundreds, if not thousands of tracing requests from members yearly. While this is not the case in all ARINs, these figures show the important role that can play in international investigations. Nevertheless, in most of these networks Secretariats, staffing can be a limiting factor. The resourcing from one ARIN to the next varies greatly, but in general they experience difficulties in assisting jurisdictions and following-up on requests, which can affect overall effectiveness on asset recovery. Ensuring the long-term financial sustainability of secretariat functions is a common challenge for ARINs. Other obstacles to the effectiveness of ARINs include language and cultural barriers.

The relationship between ARINs and the FSRBs varies considerably from one region to another. In some cases, there is close co-ordination with the FSRBs, while in others, there is none.

Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs[140]

In 2019, the Financial Action Task Force (FATF) extended its global standards on AML/CFT to apply to VAs and VASPs. To strengthen implementation of Recommendation 15 (R.15), the FATF adopted a Roadmap in February 2023. As part of the Roadmap, the FATF published a table that sets out the status of implementation of R.15 by FATF members and other jurisdictions with materially important VASP activity. The FATF and its Virtual Assets Contact Group (VACG) will continue to conduct outreach and provide assistance to support global compliance with R.15 and update the table in 2025.

This report provides a fifth targeted review of implementation of the FATF's Standards on VAs and VASPs including the Travel Rule, and an update on emerging risks and market developments in this area. This work was led by the VACG, co-chaired by Japan and the United States. The report also drew on input from the private sector, via ongoing discussions through the VACG.

Key findings, recommendations

Compared to the 2023 survey results, jurisdictions, including some with materially important VASP activity, have made progress in putting AML/CFT regulation in place or are in the process of doing so. However, a continued lack of implementation of the relevant FATF Standards globally means that VAs and VASPs remain vulnerable to misuse and overall implementation of the Standards remains behind that of other financial sectors. In that context, this report sets out key areas for improvement and recommendations for both public and private sectors.

VAs continue to be used to support the proliferation of weapons of mass destruction as well as by scammers, terrorist groups, and other illicit actors. The DPRK continues to steal or extort virtual assets from victims and

[140] FATF - *Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html

increasingly uses sophisticated methods to launder illicit proceeds. VAs are increasingly used by terrorist groups, in particular by ISIL in Asia and groups in Syria, and terrorist groups that are using virtual assets often use stablecoins and experiment with anonymity-enhancing cryptocurrencies.

During VACG engagements, private sector stakeholders reported on market developments, including the increasing use of stablecoins for ML/TF/PF purposes and continued hacks of decentralised finance (DeFi) arrangements. Certain progress in risk mitigation measures that leverage smart contracts was also noted. Several jurisdictions reported progress in regulation, supervision, and enforcement, such as introducing AML/CFT/CPF, including Travel Rule requirements, for stablecoin service providers, taking regulatory and enforcement actions against DeFi arrangements, and conducting risk assessments on DeFi and unhosted wallets including peer-to-peer transactions.

Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption[141]

Corruption and ML are inextricably linked. Corrupt actors must launder bribes and misappropriated funds to enjoy their criminal profits. Through their role as gatekeepers to the financial system, non-financial professionals can facilitate, unwittingly or wittingly, high-level corruption.

To minimise such risks, the FATF took action over 20 years ago by requiring jurisdictions around the globe to apply AML/CFT measures to gatekeepers: lawyers, accountants, TCSP, and real estate agents. These measures aim to address the vulnerability of the sectors to ML and corruption threats, by equipping professionals with the necessary knowledge to detect indications of possible crimes. When these professionals are not regulated in accordance with the FATF Standards, they remain exposed to significant criminal risks and lack those measures that would allow them to see the red flags of ML.

The FATF has undertaken this Horizontal Review to assess the current state of play and identify areas that FATF members must prioritise for further improvement. This is a deep dive into the actions that FATF members have taken to apply important aspects of the FATF Recommendations to gatekeepers.

This is a FATF Horizontal Review that was scoped to conduct a review of FATF members' compliance with Recommendation 22 (criteria 1 to 3), Recommendation 23 (criteria 1, 2 and 4) and Recommendation 28 (criteria 2 to 5) as it relates to the following non-financial professions who as gatekeepers play a role in preventing and detecting ML and predicate offences including corruption and who could knowingly enable corruption and related ML: real estate agents, lawyers, notaries, other independent legal professionals and accountants, and TCSP.

Key findings, recommendations

On the surface, the Horizontal Review shows positive results - over half of FATF members have scores over 80%. However, these results are less promising when one considers the context and materiality of the seven FATF members falling below the score of 50%. These jurisdictions represent more than half of the world's GDP.

Although it is a common perception that the legal profession is subject to fewer AML/CFT rules than other gatekeeper sectors, the Horizontal Review found little difference in coverage scores of the four gatekeeper sectors under the scope of the review - lawyers, accountants, TCSP, and real estate agents.

Finally, this review found that some cornerstone obligations of the FATF Recommendations fall behind the compliance levels of other obligations. These requirements - conducting customer due diligence, implementing internal controls, and providing a supervisor with adequate powers to conduct risk-based supervision - are essential requirements to address the vulnerability of gatekeepers to ML and corruption threats.

It is urgent that those FATF members still lagging behind ensure that gatekeepers are adequately covered in line with the FATF's longstanding Recommendations in this area. In no way should this project, its analysis or conclusions pre-empt or prejudice the results of any upcoming Mutual Evaluation Report.

[141] FATF - *Horizontal Review of Gatekeepers' Technical Compliance Related to Corruption*: https://www.fatf-gafi.org/content/fatf-gafi/en/publications/Fatfgeneral/Gatekeeper-TC-Corruption.html

FATF-style regional bodies

6.2 Caribbean Financial Action Task Force

The Caribbean Financial Action Task Force (CFATF) has published the following two research project reports.

CFATF Cannabis Project Report[142]

This project addressed the implications of AML/CFT on cannabis legalisation. The objective was to assist member jurisdictions in comprehending the AML/CFT risks associated with decriminalisation, legalisation, or hybrid approaches to cannabis use. The project focused on comprehending the various approaches jurisdictions took on this matter, identifying associated risks, and proposing strategies for risk mitigation.

CFATF De-Risking Update 2023[143]

This initiative updated the 2018-2019 assessment of de-risking within CFATF member jurisdictions, concentrating on measures implemented by central banks and financial institutions to alleviate its impact. The report also outlined the adverse effects of de-risking on the region and the responsive measures taken. It detailed de-risking practices observed from 2019 to 2022.

6.3 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.

EAG AML/CFT Financial Investigation Guidance

Under the decision of the 34th EAG Plenary Meeting the project team of the working group on typologies and combating terrorist financing and crime (WGTYP) prepared the document *EAG Methodological Recommendations on Organising and Conducting Financial Investigations in the AML/CFT Sphere*[144]. The following jurisdictions and organisations took part in the project team: the EAG Member States (Belarus, India, Kazakhstan, China, Kyrgyzstan, Russia, Tajikistan, Turkmenistan and Uzbekistan), the EAG Secretariat, the EAG Observers (FATF Secretariat, APG, CIS ATC, BKBOP, EEC, CSTO, SCO RATS, CARICC).

The following issues are considered: legal provisions governing AML/CFT financial investigations, grounds for conducting financial investigations, types of obtained information and use of financial investigation findings, specific features of certain types of financial investigations, private sector involvement in financial investigations, domestic and international cooperation, group (integrated) financial investigations, problems and recommended actions. The document was approved by the 39th EAG Plenary Meeting.

Key findings and recommendations:

- As financial investigations are themselves an effective tool for ensuring financial transparency of money flows and property circulation in the State, it is necessary to strive for the widest possible coverage of financial investigations in areas and tasks within the fundamental framework of the legal system.
- Financial investigation mechanisms should be improved and their effectiveness enhanced by defining, based on specific tasks, the competent authorities that will conduct such investigations and the limits of their powers.

[142] Caribbean Financial Action Task Force - *CFATF Cannabis Project Report*: https://www.cfatf-gafic.org/documents/resources/22443-cfatf-cannabis-project-report/file
[143] Caribbean Financial Action Task Force - *CFATF De-Risking Update 2023*: https://www.cfatf-gafic.org/documents/resources/22442-cfatf-de-risking-update-2023/file
[144] Eurasian Group on Combating Money Laundering and Financing of Terrorism - *EAG AML/CFT Financial Investigation Guidance*: https://eurasiangroup.org/files/uploads/files/Public_typology_reports/FI_Guidence_eng.pdf

- To improve the efficiency of financial investigations, progressive and purposeful work on the digitalisation of financial and other information, as well as providing direct and unhindered access to it to the bodies carrying out financial investigations is necessary.
- Provide ongoing targeted and specialised training for financial investigators. Improve the selection and organisation of financial investigators.

Laundering of the proceeds from corruption offences and crimes against the interests of public service[145]

The typology project was aimed at analysing the menace of corruption in order to better understand corruption, its mechanisms and vulnerabilities, through an AML lens, identifying various tools and methods used for ML in these cases, identifying current trends, new threats, vulnerabilities and typologies that have been observed in corruption cases and subsequent ML, thus increasing awareness and opportunities for early detection. The results of this study are intended to be used by LEAs, FIUs, authorities engaged in anti-ML, anti-corruption enforcement, banking and financial sector and the private sector in their work. The project was led by the Republic of India. All the EAG members took part in it. The document was approved by the 39th EAG Plenary Meeting.

Key findings and recommendations:

- In Member States where the agencies investigating the offences of corruption and ML are different, while investigating offence of corruption, efforts should be made to conduct parallel financial investigation to explore / investigate the ML offence.
- Enhanced customer due diligence PEPs.
- Adoption of beneficial ownership registries can be promoted and may be made mandatory for legal persons and legal arrangements to disclose their ultimate beneficial owners.
- Promoting International Cooperation. Sending clear and concise requests; providing sufficient supporting information in the MLA request itself; informal channels of communication should be explored more frequently and efficiently before submission of formal request to ensure that request placed through formal channels of communication gets timely and effectively executed; providing regular training and assistance to personnel / investigators who are involved in drafting and submitting requests; and development and implementation of electronic platform for the exchange of MLA requests.
- Strengthen investigative and enforcement capabilities: adequate resources, training, and technical assistance to LEAs and financial intelligence units responsible for investigating and combating ML should be provided so that their skill sets do not lag behind with the technological advancements in financial sector. Also, business establishments need to be encouraged to implement robust internal controls, risk management systems, and employee training programs for better identification of ML risks / attempts.
- Strengthen asset recovery: specialised units or agencies dedicated for the recovery of illicit assets may be established so that they have single point agenda / goal towards recovery of proceeds of crime / stolen assets.
- Digitalisation and technological solutions: the COVID-19 pandemic accelerated digitalisation across various sectors, including finance. This shift towards digital platforms and online transactions may provide an opportunity for the implementation of technological solutions to detect and prevent ML and corruption. Advanced data analytics, artificial intelligence, and machine learning algorithms can be employed to identify suspicious patterns and transactions more effectively.

Laundering of the proceeds from illicit trade of narcotics and precursors[146]

The project aims to identify typologies, methods and tools used for laundering proceeds of illicit trafficking of narcotic drugs and their precursors and to develop better understanding of this issue by LEAs, FIs and other stakeholders for more effective fight against this type of criminal activity. The project team considered different aspects of ML, including methods and techniques used by criminals, legislative and financial frameworks in place and international and domestic laws and regulations adopted for combating this illegal activity in a more effective way. The project was led by the Republic of India. All the EAG Members took part

[145] Eurasian Group on Combating Money Laundering and Financing of Terrorism - *Laundering of the proceeds from corruption offences and crimes against the interests of public service*: https://eurasiangroup.org/files/uploads/files/Public_typology_reports/WGTYP_(2023)_7_rev_1_eng.pdf
[146] The document is publicly unavailable and published on the secure part of the EAG website for the use of Members and Observers: https://eurasiangroup.org/d.php?doc=69e98753d860c28af3bda71f1eff93ea

in it. The document was approved by the 39th EAG Plenary Meeting.

Key findings and recommendations:

- Improve information sharing and cooperation among jurisdictions and international organisations to better detect and disrupt transnational drug ML schemes.
- Consider ways to prevent the use of bank cards and wallets by front persons, with the possibility of legal liability for citizens who contribute to their distribution (intentionally acting as 'lessors' of their banking instruments).
- Improve the skills of LEA officers, financial institutions and other organisations in detecting indicators of drug proceeds laundering.
- Develop and implement mechanisms to monitor transactions involving cryptocurrencies that could be used to launder drug proceeds.
- Revise the requirements for entities' internal control rules.
- Strengthen risk management programs.

Criteria for identifying suspicious money recovery lawsuits for the purpose of money laundering[147]

The first-round EAG regional risk assessment report[148] identify a regional risk that requires standard measures to be taken in order to mitigate it. This risk is using schemes to offshore funds through enforcement means. It is often manifested in practice in the use of court judgements rendered on fictitious grounds. There are serious challenges and risks that criminal proceeds may be lost when it comes to identifying suspicious actions at the stage of enforcement of a judicial or other act. To mitigate the identified regional ML/TF risks the EAG Secretariat has developed the criteria to identify suspicious claims for the recovery of funds for ML purposes. The project was led by the EAG Secretariat, and all the EAG Members took part. The document was approved by the 40th EAG Plenary Meeting.

Key findings and recommendations:

- There are serious challenges and risks that criminal proceeds may be lost when it comes to identifying suspicious actions at the stage of enforcement of a judicial or other act.
- It is extremely difficult to identify an ML scheme at the stage of enforcement since this stage of proceedings does not involve any examination of evidence, meaning that suspicious features may be identified only in clear-cut cases. More or less covert schemes, which are prevalent in such ML cases, are highly unlikely to be identified during enforcement proceedings.
- Judicial or other acts delivered in cases involving a covert ML scheme are usually enforced in the shortest possible time because the criminals want to legalise the funds as fast as possible and, to avoid being exposed, to take them out of reach of the competent bodies or to conceal their next location.
- It is critical for relevant officers of judicial, law enforcement, and enforcement bodies become suspicious about ML schemes as early as possible.

The EAG expects to adopt the following typology projects in November 2024.

Guidelines for the EAG Member States on the procedure for identifying suspicious money recovery lawsuits for the purpose of money laundering

- This project is conducted under the proposals of the EAG Members as a follow-up of the development of the criteria for identifying suspicious money recovery lawsuits for the purpose of ML to establish an example procedure to identify claims for the recovery of funds for ML purposes, to enable cooperation among the competent bodies on this matter, as well as to envisage actions that may be made during judicial proceedings and on the merits of such claims.
- The project is led by the EAG Secretariat with the involvement of the EAG Member States delegations and based under the analysis of the EAG Members legislation.

[147] 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

[148] 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/Summary_RRA.pdf

- It's expected that the document of the project will be adopted by the 41st EAG Plenary Meeting in November 2024.

Report on the monitoring the operational environment in the Member States in terms of new risks

- At the 37th Plenary Meeting, the Member States approved the stages of development of the Mechanism to monitor the operational environment in the EAG Member States in terms of new risks. This document is the pilot version of summarised information under the monitoring mechanisms based on input and information provided by the Member States before the 41th Plenary Meeting.
- The project is led by the EAG Secretariat and based under the analysis of the EAG Members information.
- It's expected that the document of the project will be adopted by the 41st EAG Plenary Meeting in November 2024.

Monitoring the risks of use of virtual assets for criminal purposes

- The project aims to identify the risks, threats and vulnerabilities associated with the use of virtual assets in the EAG Member States and the ways to minimise them.
- The project is led by the delegation of the Russian Federation and based under the analysis of the EAG Members information.
- It's expected that the document of the project will be adopted by the 41st EAG Plenary Meeting in November 2024.

6.4 Eastern and Southern Africa Anti-Money Laundering Group

The Eastern and Southern Africa Anti-Money Laundering Group (ESAAMLG) published the following two reports.

Illicit Dealings in Gold, Diamond and Rubies and related Money Laundering and Terrorist Financing[149].

This report aims to depict the financial flows that fuel crimes such as Illicit Dealings in Gold, Diamond and Rubies and related ML/TF in the ESAAMLG Region. The report includes a list of risk indicators and case studies that can help the concerned institutions in the region to identify and investigate illicit activities in the precious stones and metals (PMS) markets, and also highlights the importance of rapidly identifying and tracing PMS involved in ML/TF.

The lucrative returns associated with illicit dealing in PMS have made the criminal activity an attractive vehicle for laundering money and financing terrorists. Illicit dealing in PMS provides a mechanism for organised crime groups to convert illicit cash into a stable, anonymous and easily exchangeable asset to realise or invest the profits from their criminal activities. Precious metals and stones have been used as an alternative currency to purchase prohibited or restricted goods, such as gold for cocaine, and diamonds for weapons, or as a means to store wealth generated by illegal activity which is not easily traceable for criminal processes such as seizures and confiscations.

PMS have been smuggled from source to consumer jurisdictions, including to finance armed conflicts. Additionally, the high value of PMS may lead officials from relevant competent authorities to demand or accept bribes at every stage of the extraction and trade process. If the use of PMS in illegal activities remains unabated in the ESAAMLG region it can pose serious threats to the economies and political stability of the region.

This has led to jurisdictions undertaking intensive efforts to protect the sector from the risk of being abused by criminals. In the quest to have effective responses, it is imperative for the region to better understand the nature of these crimes as they relate to the region's specific characteristics.

[149] Eastern and Southern Africa Anti-Money Laundering Group - *Illicit Dealings in Gold, Diamond and Rubies and related Money Laundering and Terrorist Financing*: https://www.esaamlg.org/index.php/methods_trends/readmore_methods_trends/15

The report includes some good practices that ESAAMLG jurisdictions have taken to address the challenges they face, including the establishment of specialised units and access to relevant databases and cooperation with experts to help identify, trace, and investigate illicit financial activities involving PMS.

ESAAMLG At 25: Celebrating a Legacy of Fighting Financial Crimes and Progress (1999-2024)[150]

This report commemorates and critically assesses 25 years of ESAAMLG's operations, highlighting the organisation's achievements, challenges, and impact on the Eastern and Southern African region.

6.5 El Grupo de Acción Financiera de Latinoamérica

The El Grupo de Acción Financiera de Latinoamérica (GAFILAT) (The Latin American Financial Action Group) published the following products.

2021-2022 Regional Typologies Report[151] (published in Spanish)

The GAFILAT prepared its 2021-2022 Regional Typologies Report as a product of the GAFILAT 2023 Biennial Regional Typologies Exercise. The objective was to identify new modalities of ML/TF, the amounts involved, the changes or variations that are noted in relation to previous typology reports, the consistency between analysed typologies and the present and emerging threats identified in the region in the last update of regional threats and the impact of these crimes in GAFILAT member jurisdictions.

6.6 The Middle East and North Africa Financial Action Task Force

Money Laundering and Terrorist Financing through Legal Persons and Legal Arrangements in the Middle East and North Africa Region

The MENAFATF members expressed their willingness to implement a typology report project on ML/TF through legal persons and legal arrangements. This implementation was based on the results of preliminary research and related studies, which highlighted the continued challenge of exploiting legal entities in illicit financial activities globally. The FATF MERs have revealed inadequacies in combating such misuse and emphasize the urgency for jurisdictions to fully and effectively implement FATF standards.

The Middle East and North Africa region's MERs indicated a significant gap in compliance with standards related to preventing the misuse of legal entities in ML/TF operations. A considerable proportion of evaluated jurisdictions in the region require substantial or fundamental improvements in preventing the misuse of legal persons and legal arrangements.

To address these issues, the FATF has amended Recommendation 24 and Recommendation 25 to enhance ownership transparency and mitigate risks associated with legal entities' misuse. FATF developed a comprehensive guideline to assist jurisdictions in implementing these standards effectively. The Typology project aims to assess risks associated with the misuse of legal entities in financial crimes and provide recommendations to enhance compliance with international standards.

The main objectives of the project include understanding risks associated with legal entities in illicit financial activities, identifying threat indicators, analysing case studies, and proposing measures to increase effectiveness in implementing international standards. Recommendations will focus on sharing best practices, urging jurisdictions to expedite the application of FATF amendments, and addressing challenges in detecting and preventing the misuse of legal entities.

While not published yet, this comprehensive report considers literature from the FATF, the International Monetary Fund, the World Bank, the Organisation for Economic Co-operation and Development, and the Tax Justice Network among others.

[150] Eastern and Southern Africa Anti-Money Laundering Group - *ESAAMLG At 25: Celebrating a Legacy of Fighting Financial Crimes and Progress (1999-2024)*: https://www.esaamlg.org/index.php/all_news/readmore_news/476
[151] El Grupo de Acción Financiera de Latinoamérica - *2021-2022 Regional Typologies Report*: https://biblioteca.gafilat.org/?p=6966

6.7 Committee of Experts on the Evaluation of Anti-Money Laundering Measures

The Committee of Experts on the Evaluation of Anti-Money Laundering Measures (MONEYVAL) published the following products.

Typologies report on money laundering and terrorist financing risks in the world of virtual assets[152]

The report aims to present in an integrated manner an overview of the ML/TF risks in the world of virtual assets and their service providers in MONEYVAL members. It includes an overview of the measures taken to regulate and supervise the VASPs, as well as some features of the identified risks that criminals VASPs and VAs to launder the proceeds of crime. MONEYVAL members continue to struggle with implementation of the FATF R.15, with around 80% of the assessed members are only partially, or not compliant with it.

The report also considers whether law enforcement agencies have adequate powers and tools to investigate, locate and impose interim measures in respect of VAs, and includes examples of types of virtual assets platforms used for financial support of criminal activity and of cases investigated by the relevant authorities. It also highlights good practices and challenges in applying risk-based supervision of the sector.

Observer organisations

6.8 Asian Development Bank

The Asian Development Bank (ADB) published the following products.

Key Aspects of UNIDROIT Principles on Digital Assets and Private Law[153]

Designed as part of ADB's efforts to bolster financial market infrastructure in ASEAN+3 jurisdictions, this brief sets out ways to improve understanding of digital assets and strengthen global legal certainty over cross-border transactions. The brief centres on the International Institute for the Unification of Private Law's (UNIDROIT) Principles on Digital Assets and Private Law. It sets out 19 International Institute for the Unification of Private Law (UNIDROIT) principles covering private law issues around digital assets, explains they are jurisdiction and organisationally neutral, and shows why national laws could be tweaked to accommodate digital asset transactions.

An Introduction to Digital Assets[154]

In the absence of universal digital asset definitions, the brief shows how various jurisdictions and national standard-setting organizations are drawing up their own guidelines to define and regulate digital and crypto-assets. It highlights the comprehensive and tech-agnostic principles devised by the UNIDROIT, explains how they treat existing and emerging digital assets, and why they could make transactions safer and more efficient.

[152] Committee of Experts on the Evaluation of Anti-Money Laundering Measures - *Typologies report on money laundering and terrorist financing risks in the world of virtual assets*: https://rm.coe.int/moneyval-2023-12-vasp-typologies-report/1680abdec4
[153] Asian Development Bank - Key Aspects of UNIDROIT Principles on Digital Assets and Private Law: https://www.adb.org/publications/unidroit-principles-digital-assets
[154] Asian Development Bank - An Introduction to Digital Assets: https://www.adb.org/publications/introduction-digital-assets

Imagining an Inclusive Economy: The Role of SMEs and Digital Payment in Elevating Economic Equality[155]

This study focusses on small and medium-sized enterprises (SMEs) and mainstreaming digital features that transform access to finance in imagining an inclusive economy. Underlining the advancement in technology, especially in the context of a digital payment system, perpetuates the financial-economic rationale as a means of financial inclusion. Nevertheless, the implementation remains a long-standing challenge, most notably in developing economies. This study examines the relationship between SMEs' contribution to gross domestic product, digital payments, and the existing inequality proxied by the Gini coefficient. The study concludes with two core findings:

- SMEs significantly help reduce inequality within the economy.
- Digital payment, as a digital transformation, narrows the inequality gap within Southeast Asian jurisdictions.

The study also presents concluding remarks, recommendations, and suggestions for future research.

The Rule of Law Approach for More Resilient Institutions: Judicial Accountability and Independence, and Global Economic Activities[156]

This paper underscores the importance of impartial judicial institutions, focusing on independence, accountability, and their role in stabilising global supply chains and financial systems. In the first part, we derive three key policy implications from two research papers. First, it stresses the significance of independent judicial appointments to enhance decision-making and economic integrity. Appointments based on merit, rather than political favouritism, bolster public trust and guard against judicial compromise. Second, it advocates for understanding the interplay between cultural norms and political institutions. The paper proposes measures to separate religious and political power, including affirmative action in religious education regions and secularization of bureaucracies. Last, it calls for the creation of judicial selection procedures to insulate judges from political influence, promoting an independent and accountable judiciary.

Rule of Law Approach for More Resilient Global Supply Chains and Financial Architecture[157]

This paper examines how the application of the rule of law principles and a rule-based approach can significantly contribute to strengthening global supply chains and the global financial architecture. Key points:

- Ensuring the stability of global supply chains and financial systems is fundamental for our economies and societies.
- There is a conceptual difference between the "rule of law" and a "rule-based approach."
- The rule of law is a foundational principle in governance, ensuring accountability, fairness, and transparency and extends to international trade and global finance.
- A rule-based approach highlights the importance of predictability, transparency, consistency and accountability in building resilience and promoting sustainable economic growth.
- The application of the rule of law principles and a rule-based approach can significantly contribute to strengthening global supply chains and the global financial architecture.

Managing Fintech Risks: Policy and Regulatory Implications[158]

Using examples of how economies are handling the fintech boom, this paper outlines why regulators urgently to adapt and adopt flexible policies that improve oversight of emerging products and providers. It sketches out the fintech landscape and explains how economies can encourage innovation while increasing

[155] Asian Development Bank - *Imagining an Inclusive Economy: The Role of SMEs and Digital Payment in Elevating Economic Equality*: https://www.adb.org/publications/imagining-an-inclusive-economy-the-role-of-sm-es-and-digital-payment-in-elevating-economic-equality
[156] Asian Development Bank - *The Rule of Law Approach for More Resilient Institutions: Judicial Accountability and Independence, and Global Economic Activities*: https://www.adb.org/publications/the-rule-of-law-approach-for-more-resilient-institutions-judicial-accountability-and-independence-and-global-economic-activities
[157] Asian Development Bank - *Rule of Law Approach for More Resilient Global Supply Chains and Financial Architecture*: https://www.adb.org/publications/rule-of-law-approach-for-more-resilient-global-supply-chains-and-financial-architecture
[158] Asian Development Bank - *Managing Fintech Risks: Policy and Regulatory Implications*: https://www.adb.org/publications/managing-fintech-risks-policy-regulatory-implications

international cooperation to insulate against the growing financial, operational, and cybersecurity risks the new technology brings.

Recent Central Bank Digital Currency Developments in Asia and Their Implications[159]

This report outlines global developments and emerging trends, it shows why a robust digital infrastructure, strong public-private collaboration, and fintech literacy are central to ensuring central bank digital currencies (CBDCs) help drive the transition to a digital economy.

The Role of Central Bank Digital Currencies in Financial Inclusion: Asia–Pacific Financial Inclusion Forum 2022[160]

This report considers how CBDCs could leverage digital finance technologies and enhance the reach and value of formal financial products and services among the unbanked. It also looks at the challenges involved and how these could be addressed. The report provides recommendations for policy makers and regulators on designing CBDCs, establishing preconditions, and managing risk. It shares insights from the Asia-Pacific Financial Inclusion Forum, a policy initiative of the Asia-Pacific Economic Cooperation Finance Ministers' Process.

6.9 International Monetary Fund

The International Monetary Fund (IMF) published the following products.

Central Bank Digital Currency Data Use and Privacy Protection[161]

This note offers a framework to help jurisdictions navigate, as well as tools to help them manage, the trade-offs between CBDC data use and privacy protection. It addresses retail CBDC, as data access and privacy-preserving considerations in a wholesale environment are similar to those of the traditional real time gross settlements systems. It emphasizes the role of institutional arrangements, data collection, access and storage policies, design choices, and technological solutions. At a given level of preference for privacy, central banks can facilitate better use of CBDC data through robust transparency and accountability arrangements, sound policies, and judicious adoption of privacy-by-design approaches including the use of privacy-enhancing technologies.

2023 Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy[162]

This paper reviews the IMF's efforts to safeguard financial integrity and proposes the way forward for the IMF's AML/CFT Strategy. For over 20 years, the IMF has recognised that effective AML/CFT frameworks, and financial integrity more broadly, are key to the soundness and stability of the financial sector and to prevent the negative macroeconomic implications of financial crimes on the broader economy of members, progressively integrating this work across all its core functions and in a broad set of IMF policies. The paper takes stock of the implementation of the IMF's AML/CFT strategy since 2018. It also proposes deepening the integration of financial integrity issues and an enhanced focus on the macroeconomic impact of AML/CFT issues for the way forward.

[159] Asian Development Bank - *Recent Central Bank Digital Currency Developments in Asia and Their Implications*: https://www.adb.org/publications/central-bank-digital-currency-developments-asia-implications
[160] Asian Development Bank - *The Role of Central Bank Digital Currencies in Financial Inclusion: Asia–Pacific Financial Inclusion Forum* 2022: https://www.adb.org/publications/asia-pacific-financial-inclusion-forum-2022
[161] International Monetary Fund - *Central Bank Digital Currency Data Use and Privacy Protection*: https://www.imf.org/en/Publications/fintech-notes/Issues/2024/08/30/Central-Bank-Digital-Currency-Data-Use-and-Privacy-Protection-554103
[162] International Monetary Fund - *2023 Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy*: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Funds-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542015

2023 Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy - Background Papers[163]

These background papers support the stocktaking analysis and the proposed way forward for the 2023 review of the IMF's AML/CFT Strategy. The five background papers provide in-depth discussions on the following key topics:

- Illicit financial flows.
- The impact of money laundering in financial stability.
- Synergies between financial integrity issues and other IMF policies and work.
- The IMF's collaboration with key partners in the AML/CFT global policy architecture.
- Stakeholders' views of the effectiveness of the IMF's AML/CFT engagement.

Central Bank Digital Currency - Initial Considerations[164]

The paper briefs the IMF's Executive Board on the initial considerations on CBDCs. These cover a framework to guide jurisdictions' CBDC exploration, as well as implications for monetary policy transmission, capital flow management measures, and financial inclusion.

IMF Approach to Central Bank Digital Currency Capacity Development[165]

The global central banking community is actively exploring CBDCs, which may have a fundamental impact on both domestic and international economic and financial stability. Current IMF CBDC efforts have focused on facilitating peer learning and developing analytical underpinnings for staff advice to member jurisdictions. This paper sketches a multi-year strategy to address frequently asked questions related to CBDC and outlines the process for developing a CBDC Handbook which will document emerging lessons, analytical findings, and policy views.

Elements of Effective Policies for Crypto Assets[166]

This paper outlines how to respond to the rise of crypto assets and the associated risks. It defines and classifies crypto assets based on their underlying features and describes their purported benefits and potential risks. The paper presents a policy framework for crypto assets that aims to achieve key policy objectives such as macroeconomic stability, financial stability, consumer protection, and market and financial integrity. The framework outlines key elements that are necessary to ensure that these objectives are met. However, such a framework will not fix any underlying crypto design flaws.

The Rise of Payment and Contracting Platforms[167]

This note explores the design and governance of platforms to enhance cross-border payments in line with public policy goals. While much innovation in recent years has more narrowly targeted end-user frictions, the vision in this paper is based on the mandate of the IMF, governed by the central banks and finance ministries of 190 member jurisdictions. Cross-border payments present the foundation for the global financial system, and its functioning is overseen by the IMF.

[163] International Monetary Fund - *2023 Review of The Fund's Anti-Money Laundering and Combating The Financing of Terrorism Strategy - Background Papers*: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/12/05/2023-Review-of-The-Fund-s-Anti-Money-Laundering-and-Combating-The-Financing-of-Terrorism-542020
[164] International Monetary Fund - *Central Bank Digital Currency - Initial Considerations*: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/11/14/Central-Bank-Digital-Currency-Initial-Considerations-541466
[165] International Monetary Fund - *IMF Approach to Central Bank Digital Currency Capacity Development*: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/04/12/IMF-Approach-to-Central-Bank-Digital-Currency-Capacity-Development-532177
[166] International Monetary Fund - *Elements of Effective Policies for Crypto Assets*: https://www.imf.org/en/Publications/Policy-Papers/Issues/2023/02/23/Elements-of-Effective-Policies-for-Crypto-Assets-530092
[167] International Monetary Fund - *The Rise of Payment and Contracting Platforms*: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/06/16/The-Rise-of-Payment-and-Contracting-Platforms-534794

Central Bank Digital Currency's Role in Promoting Financial Inclusion[168]

Financial inclusion is a key policy objective that central banks, especially those in emerging and low-income jurisdictions, are considering for retail CBDCs. If properly designed to address the barriers to financial inclusion, CBDCs have the opportunity to gain acceptance by the financially excluded for digital payments. CBDC can then serve as an entry point to the broader formal financial system. CBDC has special aspects that may benefit financial inclusion, such as being a risk-free and widely acceptable form of digital money, availability for offline payments, and potentially lower costs and greater accessibility. However, CBDC is not a panacea to financial inclusion, and additional experience is needed to fully understand its potential impact.

How Should Central Banks Explore Central Bank Digital Currency?[169]

Digitalisation of the economy provides both challenges and opportunities. Central banks should ensure that they have the capacity to continue to meet their policy objectives in the digital age. It is in this context that CBDCs should be evaluated. If designed appropriately, CBDCs could allow central banks to modernize payment systems and future-proof central bank money as the pace and shape of digitalisation continues to evolve. However, the decision to proceed with CBDC exploration and an eventual launch would need to be jurisdiction specific, depending on the degree of digitalisation of the economy, the legal and regulatory frameworks, and the central bank's internal capacity. This paper proposes a dynamic decision-making framework under which the central bank can make decisions under uncertainty. A phased and iterative approach could allow central banks to adjust the pace, scale, and scope of their CBDC projects as the domestic and international environment changes.

Macro-Financial Implications of Foreign Crypto Assets for Small Developing Economies[170]

To explore risks associated with digital money, this note simulates the hypothetical large-scale adoption of crypto assets in a model of a small open economy. The model highlights that a foreign-currency denominated stablecoin can amplify currency substitution and capital outflows in response to negative shocks. Monetary policy transmission is also weakened, forcing the central bank to adjust interest rates more aggressively in response to shocks. Capital flow management measures - if they do not constrain crypto flows - further incentivize households to hold foreign stablecoins for circumvention purposes, exacerbating the negative effects of crypto adoption on the macroeconomy. This underscores that widespread crypto adoption can weaken policymakers' available options for mitigating external shocks and potentially increase cross-country spillovers.

Capital Flow Management Measures in the Digital Age (2): Design Choices for Central Bank Digital Currency[171]

This fintech note looks at how capital flow measures (CFMs) could be implemented with CBDCs, and what benefits, risks and complexities could arise. There are several implications of the analysis. First, CBDC ecosystems should generally be designed such that they can accommodate the introduction of CFMs. Second, thanks to the programmability of the payment infrastructure given by the new digital technologies, certain CFMs could likely be implemented more efficiently and effectively with CBDC compared to the traditional system. Third, implementing CFMs requires central banks to collaborate on practices and standards. Finally, CFMs on CBDC need to operate alongside traditional CFMs.

[168] International Monetary Fund - *Central Bank Digital Currency's Role in Promoting Financial Inclusion*: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/22/Central-Bank-Digital-Currency-s-Role-in-Promoting-Financial-Inclusion-538728
[169] International Monetary Fund - *How Should Central Banks Explore Central Bank Digital Currency?*: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/08/How-Should-Central-Banks-Explore-Central-Bank-Digital-Currency-538504
[170] International Monetary Fund - *Macro-Financial Implications of Foreign Crypto Assets for Small Developing Economies*: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/12/05/Macro-Financial-Implications-of-Foreign-Crypto-Assets-for-Small-Developing-Economies-541440
[171] International Monetary Fund - *Capital Flow Management Measures in the Digital Age (2): Design Choices for Central Bank Digital Currency*: https://www.imf.org/en/Publications/fintech-notes/Issues/2023/09/15/Capital-Flow-Management-Measures-in-the-Digital-Age-2-Design-Choices-for-Central-Bank-538509

6.10 United Nations Office on Drugs and Crime

The United Nations Office on Drugs and Crime published the following.

Liability of Legal Persons: Implementation under the United Nations Convention against Corruption with a focus on Malaysia[172]

The United Nations Convention against Corruption (UNCAC), came into force in 2005 and commits to combating corruption through a holistic approach, involving the public and private sectors engaging in preventive measures, law enforcement, and international cooperation.

The liability of legal persons for corruption offences is a well-established international standard. This means that legal persons, as distinct from natural persons, can be held accountable for corrupt acts. Providing for such liability is important as serious and sophisticated crime can be committed by, through or under the cover of legal persons, such as companies, corporations or charitable organizations. The actions of individuals within a legal entity may be difficult to identify due to complex corporate structures and multiple layers of decision-making, particularly if such individuals reside abroad. Article 26 of the UNCAC requires States parties to adopt measures to establish the liability of legal persons for participation in offences criminalised in accordance with the Convention.

Implementation of UNCAC Chapter III: Criminalization and Law Enforcement in ASEAN States Parties and Timor-Leste[173]

The *Implementation of UNCAC Chapter III: Criminalization and Law Enforcement in ASEAN States Parties and Timor-Leste* report offers a comprehensive analysis of how the UNCAC provisions are implemented by these parties, all of whom are also APG members. It presents an overview of the challenges and good practices by ASEAN States parties and Timor-Leste in implementing provisions under chapter III of UNCAC.

Challenges

Challenges to implementation of the Chapter III provisions are legislative and operational. Many jurisdictions lack comprehensive legal frameworks or have fragmented legislation that fails to fully align with the UNCAC provisions. In some cases, domestic laws have higher thresholds than UNCAC requirements, complicating the identification, investigation, and prosecution of corruption. Existing sanctions are often insufficient, incomplete, or inconsistent, undermining enforcement efforts. Operationally, a significant challenge for many jurisdictions is the lack of resources, including technology, training, and capacity, including the lack of regional offices, which impacts the effectiveness of anti-corruption measures. Limited resources also impede inter-agency coordination and the collection of statistical data on corruption offences.

Best practices

Despite the challenges, the report highlights several best practices that have been adopted in implementing the Chapter III provisions. Some jurisdictions have successfully drafted comprehensive legislation that closely aligns with UNCAC requirements, facilitating effective identification, investigation, and prosecution of corruption. Recommendations have been made for balanced discretionary powers and concrete procedures for suspending public officials involved in corruption. Effective and transparent asset declaration systems for illicit enrichment have been established in some jurisdictions, enhancing accountability. Strengthening the administration of frozen, seized, or confiscated property has been identified as a good practice to improve the effectiveness of anti-corruption measures.

[172] United Nations Office on Drugs and Crime - *Liability of Legal Persons: Implementation under the United Nations Convention against Corruption with a focus on Malaysia*:
https://www.unodc.org/roseap/uploads/documents/Publications/2024/Liability_of_Legal_Persons_-_Implementation_under_UNCAC_with_a_focus_on_Malaysia_Sep_2024.pdf

[173] United Nations Office on Drugs and Crime - *Implementation of UNCAC Chapter III: Criminalization and Law Enforcement in ASEAN States Parties and Timor-Leste:*
https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_UNCAC_Chapter_III_-_ASEAN_States_parties_and_Timor-Leste_March_2024.pdf

Technical assistance needs

The report identifies significant technical assistance needs including:

- Summaries of Good Practices and Lessons Learned: Over 40 requests were made for summaries of good practices and lessons learned to enhance understanding and implementation of anti-corruption measures.
- Model legislation: More than 20 requests were made for model legislation to guide legislative drafting and align domestic laws with UNCAC requirements.
- Legal advice and capacity-building: Around 20 requests for legal advice and capacity-building highlights the need for expert guidance and training to strengthen anti-corruption efforts.
- Legislative drafting: Close to 20 requests for assistance in legislative drafting indicate a need for technical support in developing comprehensive legal frameworks.
- IT/data systems: Assistance in developing IT and data systems was frequently requested to improve the management and analysis of corruption-related data.

Overall, the report found that gaps remained for the criminalization of corrupt acts in the private sector, including bribery and the embezzlement of property in the private sector. The liability of legal persons was also not uniformly established across the region and was highlighted as a priority area through the UNCAC Implementation Review Mechanism for some States parties.

Regional Roadmap to Reinvigorate the Regional Platform to Fast-Track the Implementation of UNCAC in Southeast Asia (2024-2027)[174]

The UNODC has been supporting the establishment of regional platforms to fast-track UNCAC implementation. The regional platform approach is catalytic, as it seeks to identify gaps in existing anti-corruption efforts, and to coordinate and leverage the work of technical assistance providers while promoting better regional coordination and collaboration. In February 2024, delegates from Brunei Darussalam, Cambodia, Indonesia, Lao PDR, Malaysia, Mongolia, the Philippines, Thailand, Timor-Leste and Viet Nam gathered in Bangkok, Thailand for the Conference to Reinvigorate the Regional Platform to Fast-Track the Implementation of UNCAC in Southeast Asia. Jurisdictions assessed their implementation of UNCAC, including the identification of successes and challenges, as well as reform needs to progress implementation. The report articulates thematic areas identified that serve as a guiding framework to advance anti-corruption action including: developing/strengthening legal frameworks on beneficial ownership transparency, and liability of legal persons, etc.

Implementation of UNCAC chapter III: Criminalization and law enforcement in ASEAN States parties and Timor-Leste[175]

Article 26 requires States parties to take the necessary steps, in accordance with their fundamental legal principles, to provide for the liability of legal persons. This liability can be criminal, civil or administrative. At the same time, article 26(4) requires that the sanctions introduced must be effective, proportionate and dissuasive. This report that also focuses on ASEAN implementation of UNCAC article 26.

Right to Information in ASEAN Member States, Mongolia and Timor-Leste[176]

This paper provides an overview on right to information under international law and examples of right to information frameworks and practices in these States, including good practices, recommendations, and suggestions for enhancing right to information legislation and mechanisms.

[174] United Nations Office on Drugs and Crime - *Regional Roadmap to Reinvigorate the Regional Platform to Fast-Track the Implementation of UNCAC in Southeast Asia (2024-2027):* https://www.unodc.org/roseap/uploads/documents/Publications/2024/2024-2027_UNCAC_Implementation_Roadmap_in_Southeast_Asia.pdf
[175] United Nations Office on Drugs and Crime - *Implementation of UNCAC chapter III: Criminalization and law enforcement in ASEAN States parties and Timor-Leste:* https://www.unodc.org/roseap/uploads/documents/Publications/2024/Implementation_of_UNCAC_Chapter_III_-_ASEAN_States_parties_and_Timor-Leste_March_2024.pdf
[176] United Nations Office on Drugs and Crime - *Right to Information in ASEAN Member States, Mongolia and Timor-Leste:* https://www.unodc.org/roseap/uploads/documents/Publications/2024/Right_to_Information_in_ASEAN_Member_States_Mongolia_and_Timor-Leste_Sep_2024.pdf

Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape[177]

The report identifies that the transnational organized crime threat landscape in Southeast Asia is evolving faster than in any previous point in history. This change has been marked by growth in the production and trafficking of synthetic drugs and cyber-enabled fraud, driven by highly sophisticated syndicates and complex networks of money launderers, human traffickers, and a growing number of other service providers and facilitators. Despite mounting enforcement efforts, cyberenabled fraud has continued to intensify, resulting in estimated financial losses between US $18 billion and $37 billion from scams targeting victims in East and Southeast Asia in 2023.

6.11 World Bank Group

The World Bank Group (WBG) published the following.

Beneficial Ownership Registers: Implementation Insights and Emerging Frontiers[178]

This Insight distils critical insights from the implementation of Beneficial Ownership Registers in Nigeria, North Macedonia, Kenya, and the United Kingdom. The experiences of these jurisdictions offer valuable lessons for similar reform efforts worldwide aimed at enhancing beneficial ownership transparency.

The Impact of Corruption on Sustainable Development[179]

Corruption fuels a vicious cycle: climate change leads to food insecurity, population and resource stress which in tun can spark more corruption. This think piece by the G20 Anti-corruption Working Group investigates ways to break this cycle.

6.12 World Customs Organisation

World Customs Organisation (WCO) AML-CTF Programme

Project TENTACLE

Project TENTACLE, launched in 2019, is a cornerstone initiative of the WCO in the fight against ML and TF. This WCO-led, joint effort with the Egmont Group of FIUs and INTERPOL, is dedicated to combat bulk cash smuggling and the illicit trade of gems and precious metals. An important additional component of this effort is the targeting of TBML. This initiative has effectively expanded its reach and influence, deploying comprehensive operational and educational programs across the globe, specifically encompassing the regions of the Asia Pacific, Latin America, Africa, the Middle East, and Eastern Europe.

Capacity building remains at the core of Project TENTACLE's mandate. Throughout the 2023-2024 period, the project has supported and enhanced the professional competencies of relevant authorities through the training of 630 frontline officers, investigators, and analysts. The workshops and hands-on training focuses on suspicious activity/transaction reporting, operational and strategic analysis, TBML investigations, and TF. These trainings both sharpen the practical skill-sets of participants and foster inter-agency cooperation, through insights in current trends and methodologies utilised by organised crime groups. These efforts extend across the regions of Asia/Pacific, Eastern Europe, Latin America, and the Mediterranean.

Operation TENTACLE Asia/Pacific (AP) II surpassed previous benchmarks through the interdiction/seizure of more than $20 million (US) in the form of different currencies and precious metals. The operation uncovered a complex web of criminal activities, exposing multiple Middle East-based hawala networks that

[177] United Nations Office on Drugs and Crime - *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape:* https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

[178] World Bank Group - *Beneficial Ownership Registers: Implementation Insights and Emerging Frontiers*: https://openknowledge.worldbank.org/entities/publication/43aa154d-eb9c-49ea-b952-6811755b94da

[179] World Bank Group - *The Impact of Corruption on Sustainable Development*: https://www.unodc.org/corruption/uploads/documents/Corruption_sustainable_development_C.pdf

were linked with methamphetamine smuggling organisations in Myanmar. These findings unveiled an innovative exchange modality whereby gold was traded for illicit drugs, deviating from traditional regional monetary transactions associated with narcotics trafficking.

$20 Million (US) in Gold and Currency Seized: Operation TENTACLE AP II

- 116 gold seizures – 266.3 kilograms of gold bars, 153 gold coins, and 122 pieces of jewellery
- 153 currency seizures – 3.36 million USD in currency
- 1 wildlife seizure: 69 toucans and macaws
- 1 TBML case connected to high-duty consumer goods and alcohol
- 29 watches (4 Rolex watches)

The progress achieved in the 2023-2024 period has had a major impact in the global fight against complex ML schemes, from both an operational perspective and an intelligence perspective.

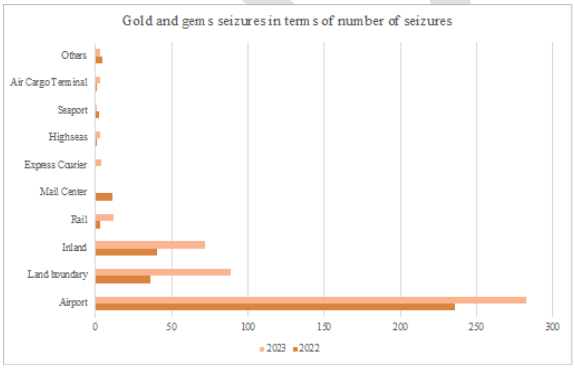
Use of female couriers in the Asia Pacific region: A new trend noted this year was the higher involvement of women from the Asia Pacific region as couriers in the smuggling of gold and currency. This specific demographic targeting necessitates a focused scrutiny and preventative measures to safeguard against exploitation.

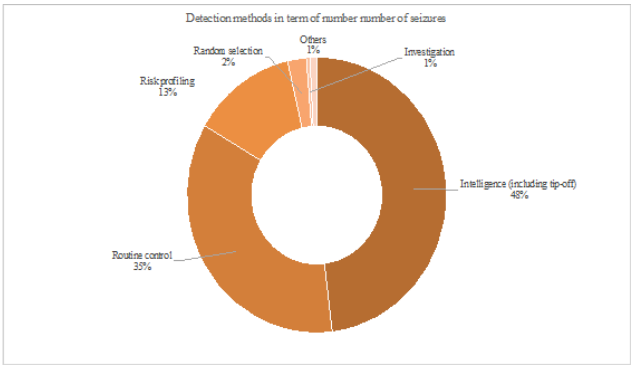
Gemstone seizures: Data gaps and regional enforcement

Data challenges. The report notes a significant deficit in data concerning gemstone seizures, with many regions reporting insufficient cases to form a comprehensive analysis. Gemstones are inherently also a very difficult commodity to identify in counter-smuggling efforts. This lack of data hinders effective strategic planning and international collaboration.

Source and enforcement regions. The seizures that were reported primarily came from the Asia Pacific and Eastern and Central European jurisdictions, with Eastern and Southern Africa noted as significant sources for these gemstones. This points to specific regional routes that may require targeted enforcement strategies.

Tactical insights. Most gold seizures occurred at airports and land borders, confirming the prevalent use of human couriers for smuggling. This trend emphasizes the need for more robust customs enforcement measures and advanced detection technologies at these points of intervention.





Gold seizures: A quantitative and regional perspective

Quantitative increase. Compared to 2022, 2023 saw a dramatic rise in gold seizures, with a 623% increase in seized gold by weight and a 36.8% increase in the number of cases. This suggests not only a rise in smuggling activities but also points to improved detection capabilities and enforcement actions by customs authorities worldwide.

Geographical hotspots. The Asia/Pacific region reported 81% of the total gold seizures by weight, pinpointing this region as a critical area for smuggling activities. The primary source of this gold is from the Middle East and North Africa region, indicating a region with preferred routes used by smugglers. These routes leverage the high demand for illicit gold in Asia/Pacific markets.

Case studies – WCO AML/CTF Programme

Case Study # 135: Directorate of Revenue Intelligence, India

Illicit trafficking in stolen and other goods

During Operation TENTACLE Asia/Pacific II, the Directorate of Revenue Intelligence (DRI) of India, together with the Indian Coast Guard (ICG), intercepted two fishing boats and seized over 32 kilograms of gold in two separate cases in Tamil Nadu. The DRI and ICG personnel intensified coastal surveillance after their intelligence indicated smuggling of foreign-origin gold from Sri Lanka through the Vedhalai coast in Ramnad.

After having identified the suspicious vessel and following a sea chase, the DRI and ICG officers intercepted one of the suspected fishing boats. Despite attempts by the individuals onboard to dispose of the contraband, India Coast Guard divers successfully recovered a package containing 11.6 kilograms of gold of foreign-origin from the seafloor. The DRI and the ICG also seized the smuggling vessel.

DRI officers on board an Indian Customs patrol boat also approached a second fishing boat and witnessed the transfer of a package to two individuals onshore. Upon realising they were being watched, the individuals attempted

Courtesy of the DRI, India (gold bars seized during the operation)

Courtesy of DRI, India (the fishing boat utilised for smuggling gold from Sri Lanka into India, now seized)

Case Study # 136: Moroccan Customs

Illicit trafficking in stolen and other goods

From 15 October to 15 November 2023, the WCO AML-CTF Programme conducted Operation TENTACLE Mediterranea III. The operational effort led to the detection and/or seizure of approximately USD 1.2 million in smuggled currency and approximately USD 686,448 of smuggled gold.

During the operational effort, the Customs administration of Morocco discovered five cases of bulk cash smuggling, amounting to approximately USD 269,467. The majority of the currency seizures were a result of the concealment of the currency in passengers' carry-on luggage. A targeted effort by Moroccan Customs also resulted in the seizure of eight gold bars weighing 10,215kg with a value of approximately USD 686,448. The Moroccan Customs officers at the Guerguarat Border Post seized the gold bars from a passenger vehicle. The gold bars were hidden between the trunk and the fuel tank of the vehicle.

Courtesy of Moroccan Customs

Case Study # 137: Bangladesh Customs

Illicit trafficking in stolen and other goods

During Operation TENTACLE Asia/Pacific II, Bangladesh Customs seized over 36 kilograms of gold bars. These gold bars were smuggled into the jurisdiction from the Middle East by three Bangladeshi males who had arrived at Hazrat Shahjalal International Airport from Dubai, United Arab Emirates. Subsequent interrogations revealed the involvement of a Middle East-based hawala network connected to a Myanmar-based methamphetamine smuggling network. It was discovered that the smuggled gold was used for drug payments and informal trade payment settlements.

Courtesy of Bangladesh Customs

At a separate seaport, Bangladesh Customs exposed the criminal operations of a China-based TBML network during the operation. This network utilised chemical consignments to conceal high-duty consumer goods, including 1,688,000 pieces of primary batteries and 16,824 litres of alcohol, that were used to launder illicit funds through an ongoing misdeclaration scheme. This interdiction and subsequent investigation led to the discovery of a hawaladar and corrupt banker who were involved in the settlement of payments and the laundering of illicit funds.

Courtesy of Bangladesh Customs (photos with alcohol (2) and batteries)

Case Study # 138: Japan Customs

Illicit trafficking in stolen and other goods

During Operation TENTACLE Asia/Pacific II, Japan Customs detected two gold bars concealed in a pair of shoes worn by a female passenger on arrival into Narita Airport. On examination, the inspecting officer noticed the excessively heavy weight of the shoes. The shoe soles were subsequently deconstructed to reveal two gold bars, wrapped in electrical tape, moulded and fitted to the inner lining. This concealment method highlights the ease in which gold can be smuggled and concealed from border agencies by reshaping gold into common objects, as well as the use of gold a ML mechanism.

Courtesy of Japan Customs

Recent academic studies

The WCO also highlighted the following two recent academic articles related to ML.

Factors Influencing the Choice of Technique to Launder Funds: The APPT Framework[180]

This project explores the techniques used by criminals to launder money, developing a new framework called the APPT framework. The framework is named after four factors that influence the choice of ML techniques: the (A) actors involved, the (P) predicate crime, the (P) purpose of laundering, and (T) technological innovations. This study aims to bridge the gap in understanding the motivations and choices behind the techniques launderers use, offering insights that could benefit financial crime investigations and AML efforts.

Key findings

Actors involved. The framework emphasises the role of both criminal and non-criminal actors, highlighting their influence based on their expertise and the complexity of the laundering techniques required.

Predicate crime. The type and severity of the predicate crime significantly affect the choice of laundering techniques, with more complex crimes leading to more sophisticated laundering methods.

Purpose of laundering. The intended use of laundered funds - whether for legitimate integration into the economy or to fund further crimes - shapes the laundering approach.

Technological innovations. Technological advancements have introduced new opportunities for ML, making it necessary to adapt anti-money laundering frameworks continually.

[180] *Factors Influencing the Choice of Technique to Launder Funds: The APPT Framework*. Journal of Economic Criminology, 1, 100006 - https://doi.org/10.1016/j.jeconc.2023.100006

Recommendations. The study suggests adopting a holistic, risk-based approach to AML efforts, moving beyond compliance-based models to more flexible and dynamic frameworks that consider the evolving nature of financial crime.

Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption[181]

This project advocates for the large-scale adoption of graph database platforms to enhance the investigation and detection of ML activities, particularly those involving shell companies. The research highlights how graph databases can be used to uncover hidden relationships within networks of illicit companies, making it easier to identify and combat ML. The study also explores the theoretical underpinnings and practical applications of this technology, proposing it as a robust solution for AML efforts.

Key findings and recommendations

Enhanced detection: The adoption of graph databases can significantly improve the detection of ML by enabling the identification of complex networks and hidden relationships between entities.

Technology adoption. The paper emphasizes the importance of adopting graph databases at a large-scale across various sectors involved in AML efforts, including financial institutions, corporate registries, and investigative bodies.

Practical applications. The use of graph databases has been successfully demonstrated in real-world cases, such as the Panama Papers, indicating its potential to revolutionise how financial crimes are investigated.

Future research. The study suggests further exploration into the application of graph technology for broader AML strategies and encourages the development of more sophisticated detection models.

[181] *Using Graph Database Platforms to Fight Money Laundering: Advocating Large Scale Adoption*. Journal of Money Laundering Control, 26(3), 474-487. https://doi.org/10.1108/JMLC-03-2022-0047

7 - ABBREVIATIONS, ACRONYMS AND CURRENCY EXCHANGE RATES

ABF	Australian Border Force
AFP	Australian Federal Police
AML	Anti-money laundering
AMLC	Anti-Money Laundering Council
APG	Asia/Pacific Group on Money Laundering
ASIC	Australian Securities and Investments Commission
ATM	Automatic teller machine
ATO	Australian Taxation Office
AUSTRAC	Australian Transaction Reports and Analysis Centre
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
FMU	Financial Monitoring Unit (Pakistan)
FSRB	FATF-style regional bodies
GIABA	Inter-Governmental Action Group against Money Laundering in West Africa
GIF	Financial Intelligence Office (Macao, China)
HKD	Hong Kong Dollar
IDR	Indonesian Rupiah
IFTI	International funds transaction instruction
INTERPOL	International Criminal Police Organisation
IPOA-IUU	International Plan of Action to prevent, deter and eliminate IUU fishing
IUU	Illegal, unreported and unregulated fishing
JAFIC	Japan Financial Intelligence Center
JPY	Japanese Yen
KYC	Know your customer
LEA	Law enforcement agency
MENAFATF	Middle East and North Africa Financial Action Task Force
MLA	Mutual legal assistance
ML	Money laundering
MONEYVAL	Committee of Experts on the Evaluation of Anti-Money Laundering Measures and the Financing of Terrorism
MOP	Macao Pataka
MVTS	Money or value transfer services
MYR	Malaysian ringgit
NGO	Non-government organisation
NPO	Non-profit organisation
NRA	National risk assessment
NZD	New Zealand Dollar
OECD	Organisation for Economic Co-operation and Development
PEP	Politically exposed person
PF	Proliferation financing
PHP	Philippine Peso
PKR	Pakistan Rupee
PPATK	Indonesian Financial Transaction Reports and Analysis Center
PPP	Public private partnerships
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
VAT	Value added tax
VND	Vietnamese Dong
WMD	Weapons of mass destruction

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 July and October 2024. These are relatively accurate yet meant to be indicative only.

8 - INDEX

References to numbers against indexed terms relate to case study numbers across this report.

Context: