Asia/Pacific Group
ON MONEY LAUNDERING

Cyber Scam Hubs and Human Trafficking

May 2026

www.apgml.org

SUGGESTED CITATION: 'Cyber Scam Hubs and Human Trafficking,' Asia-Pacific Group on Money Laundering, Sydney, Australia, May 2026.

ACKNOWLEDGEMENTS: This report was made possible by the many APG members who contributed expertise, questionnaire responses and feedback on the report. In particular, the APG gratefully acknowledges the consistent support and leadership from the APG project co-leads, Indonesia and the United Nations Office on Drugs and Crime (UNODC). The APG also gratefully acknowledges the ongoing contributions from the APG project team, which comprised of experts from the governments of Australia; Bangladesh; China; India; Indonesia; Malaysia; Myanmar; Solomon Islands; Singapore: Vietnam; United Arab Emirates and from the Alliance for Financial Inclusion. The lead authors of the report are Tri Andriyanto, Fabrizio Fioroni, Stephen Munro, Melissa Sevil, Melissa Tullis and Aibek Turdukulov.

Cover image: Parker Nate on Unsplash

For more information about the APG, please visit the website: www.apgml.org.

Table of contents

Co-Chair's Foreword

Online scams and cyber-enabled fraud are crimes which affect millions of people around the world, and their negative impacts are keenly felt in the Asia/Pacific region. Across the APG membership, we see the damage caused by cyber scam hubs located within Southeast Asia which often involve forced labour from trafficked individuals from across Asia and beyond, with victims of these scams located across the region and the globe. This is why work such as this APG Typologies Report is critical to improving our understanding of these particular crimes and promoting the importance of regional and international cooperation to bring perpetrators to justice.

During my terms as Co-Chair of the APG I have focused on a number of priorities including strengthening the AML/CFT/CPF regimes in the Asia/Pacific region and enhancing international cooperation, as well as monitoring and responding to evolutions in finance particularly working with the private sector in addressing emerging ML/TF/PF risks including through virtual assets. These two priorities come together in this report and the associated recommendations which I am proud to have supported during my term as the APG Co-Chair.

This work also has a much broader impact and is closely aligned with the FATF Strategic Priorities for 2026 - 2028, including addressing the evolving threats associated with fraud and transnational organised crime. This report demonstrates the need to ensure that fraud committed through cyber scam hubs is appropriately prioritised in order to promote the mobilisation of AML tools, international cooperation and asset recovery to combat fraud and associated money laundering.

Effective mitigation of these crimes requires continued monitoring, enhanced regional cooperation, targeted intelligence sharing and strong AML/CFT/CPF frameworks. These measures are critical to the detection, disruption and prosecution of cyber scam hubs and the protection of victims worldwide. However, these efforts are powerless without strong political commitment and a willingness across the globe to work together to combat these crimes. I take this opportunity to call all of us to action by implementing the recommendations of this report and for us to work together to combat these crimes to deprive transnational organised crime syndicates of the proceeds of scams. Together, we can bring perpetrators to justice and protect our communities from the threat of cyber scams.

Mr Mitsutoshi Kajikawa

Deputy Vice Minister of Finance for International Affairs

Ministry of Finance, Japan

APG Co-Chair, 2024-2026

Executive Summary and Best Practices

Cyber scam hubs are enabled to operate through the exploitation of special economic zones, obfuscation of beneficial ownership (often through the use of gatekeepers) and corruption. These conditions are exploited by organised criminal groups to establish these cyber scam hubs, traffic individuals into forced criminality, and to continue to operate without detection or disruption.

Organised criminal syndicates are utilising forced criminality to staff these scamming operations. Victims may be coerced or forced into working in these cyber scam hubs and are often subject to horrific treatment and conditions.

The human trafficking victims in the cyber scam hubs are typically recruited overseas through fraudulent job advertisements, with criminal syndicates often targeting young adults, with IT skills, social media literacy, and knowledge of cryptocurrency. However, the victim profile is evolving as scams diversify, and the use of AI replaces human interaction to some extent.

Individuals within jurisdictions with higher levels of disposable income and access to the international financial system are often targeted, with cyber scam hubs having victimised people in over 100 jurisdictions around the world. This crime type has a truly global reach, with victims also vary depending on the different scam typologies target different potential victims.

Various estimates suggest cyber scam hubs are generating tens of billions of US dollars annually. The four main sources of this revenue include payment for services associated with human trafficking, as well as ransom payments made by families of human trafficking victims to release them from these cyber scam hubs. Scams also generate large proceeds, depending on type, with the use of fraudulent recovery agents also identified as a mechanism to re-victimise individuals an generate another source of illicit profits.

The laundering of illicit proceeds often follows established methods. These include the use of mule accounts and unlicensed or unregistered financial services providers. There is also an identified use of virtual assets and virtual assets service providers (VA/VASPs) to launder funds, with layering, Peer-to-Peer (P2P) transfers and Over-the-Counter (OTC) brokers, as well as deposits into crypto ATMs identified as emerging typologies.

There have been a number of successful law enforcement investigations and the dismantling of cyber scam hubs across the Asia/Pacific region. However, these efforts have identified a number of challenges related to international cooperation, asset recovery cryptocurrency tracing which impact the successful identification, investigation and prosecution of the organised criminal syndicates operating these cyber scam hubs.

The findings from this project highlight the complexity, adaptability, and transnational nature of cyber scam hubs and human trafficking, particularly in the Asia/Pacific region. While a number of best practices were identified (see below), it is clear that continued monitoring, enhanced regional cooperation, targeted intelligence sharing, and the strengthening of AML/CFT frameworks across jurisdictions is critical to combatting this evolving crime type.

Continued research and enhanced understanding of the evolving methods used to perpetrate these crimes, such as decentralisation, dissipation and the use of artificial intelligence (AI), as well as further engagement with civil society and NGO are needed to support policy decisions and operational responses to protect victims and safeguard the integrity of the international financial system.

Best Practices

Members surveyed identified a number of good practices for detecting and disrupting money laundering / financial crime associated with cyber scam hubs and human trafficking. These practices included:

- Professional, holistic financial analysis expertise and continuous professional development.
- Enhanced, rapid and specific domestic interagency coordination mechanisms or task forces and analytical infrastructure.
- Effective international cooperation which facilitates extremely quick responsiveness from multiple authorities including non-AML/CFT competent authorities such as those which are mandated to address the victims of human trafficking.
- Enhanced public private partnerships.
- Dedicated awareness raising campaigns.
- Enhanced due diligence measures.
- Implement any necessary changes to legislation or national institutional framework to ensure it is suited to respond to the nature of cyber scam hubs.

Methodology

In 2025, the APG membership agreed to a typologies project to investigate the laundering of proceeds of crime stemming from cyber scam hubs and human trafficking. A project team was formed, co-led by Indonesia and the United Nations Office on Drugs and Crime (UNODC) and comprising of 24 individuals from 10 APG members, one observer jurisdiction and one observer organisation[1].

The project and this report seek to build on the growing literature on the topic of cyber scam hubs and human trafficking and highlight the experiences of jurisdictions significantly affected by these crimes. It draws on a number of information sources including:

- A literature review of open-source reports.
- Questionnaire responses from public sector agencies and private sector entities from APG member jurisdictions. These included 17 public sector responses from 17 jurisdictions[2] and 156 private sector responses (predominantly from financial institutions and payment service providers) from 14 jurisdictions[3]. Questionnaire responses were also received from four blockchain analytics companies[4] and one VASP.[5]
- Case studies provided by both public and private sector representatives of APG member jurisdictions. These case studies have been summarised for the purposes of this report.
- Interviews with blockchain analytics companies and a VASP.
- A roundtable discussion held at APG's 2025 Annual Meeting.
- Discussions and presentations with regional experts at the 2025 APG Typologies Workshop, where cyber scam hubs and human trafficking formed one of the workstreams.

[1] Australia; Bangladesh; China; India; Indonesia; Malaysia; Myanmar; Solomon Islands; Singapore: Vietnam; United Arab Emirates and Alliance for Financial Inclusion.
[2] Australia; Bangladesh; Bhutan; Cambodia; China; Hong Kong, China; Indonesia; Japan; Macao, China; Malaysia; Myanmar; New Zealand; Pakistan; Palau; Philippines; Singapore and Chinese Taipei
[3] Australia; Bangladesh; Bhutan; China; Hong Kong China; Indonesia; Japan; Malaysia; Myanmar; Pakistan; Philippines; Singapore; Chinese Taipei and Thailand.
[4] Chainalysis, Crystall Intelligence, Elliptic and TRM Labs
[5] Binance

Cyber Scam Hubs in Operation

Enabling conditions

Exploitation of special economic zones

Cyber scam hubs can operate at scale in regulatory grey zones, where state authority and oversight is weak. Existing literature notes these areas include special economic zones, free-trade areas and border regions, since they do not have clear jurisdictional authorities, limited enforcement and inconsistent regulatory standards.[6] This allows large secure compounds to be established, which are able to be relocated or rebranded when regulatory pressure increases.

Cyber scam hubs are mainly located along border areas between Thailand, Myanmar, Lao PDR and Cambodia, the northern border of Myanmar with China and the Philippines. There are also cyber scam hubs located in special economic zones, such as Dara Sakor special economic zone and Henge Thmorda special economic zone in Cambodia, the Golden Triangle special economic zone in Lao PDR and the Clark Free Port Zone Bamban in Tarlac, and Cebu in the Philippines. There are also reports of cyber scam hubs located in other Southeast Asian, South American, Pacific and West African jurisdictions.

APG members generally noted cyber scam hubs were typically located in urban centres (71% of member responses) or border areas (53% of member responses) which often coincide with the location of special economic zones. These special economic zones are also often subject to low regulatory oversight, limited law enforcement presence and also provide the necessary internet access, availability of space to accommodate the operations, and other facilities to support the number of people involved in these hubs.

When asked which jurisdictions are the primary destination for trafficked individuals for these hubs, members noted these were often special economic zones located in Cambodia, Lao PDR, Myanmar and Thailand.

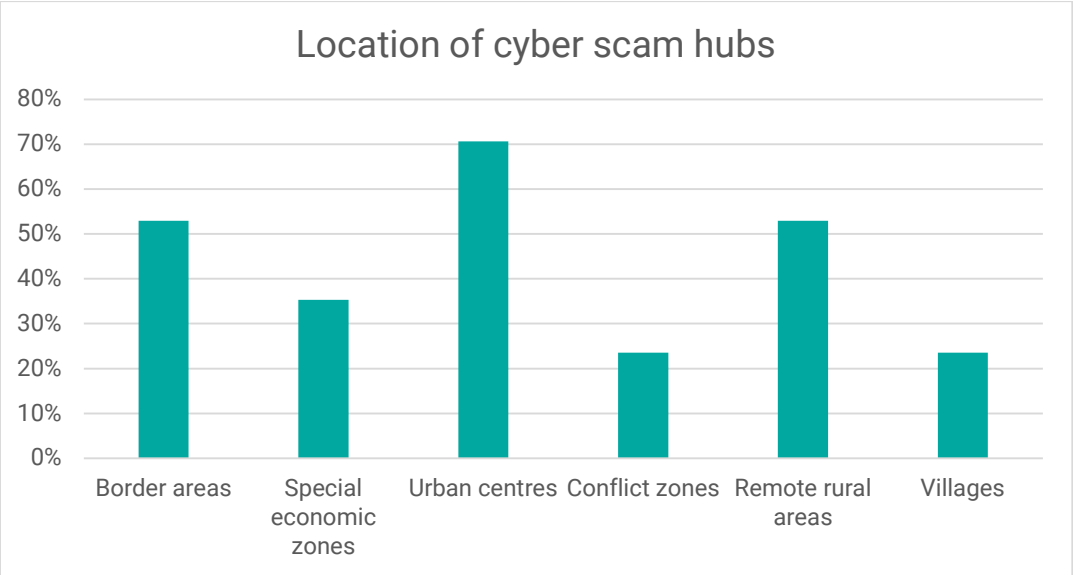


Figure 1: Location of cyber scam hubs, Public Sector Survey

Cyber scam hubs also have their origins in the collapse of Southeast Asia's gambling industry, due to the COVID-19 pandemic, which brought lockdowns and stricter border controls. The casinos and hotels, also often located in special economic zones, could no longer generate the expected proceeds through illegal gambling

[6] United Nations Office on Drugs and Crime, *Casinos, cyber fraud, and trafficking in persons for forced criminality in Southeast Asia* (September 2023) ('UNODC'), p.5.

and other crimes conducted by the organised criminal syndicates. These casinos and hotels were repurposed into cyber scam hubs populated by human trafficking victims to conduct scams. The introduction of legislation in 2025 in the Philippines[7] to ban offshore gaming and related operations had a significant and immediate impact on the prevalence of cyber scam hubs in the Philippines.

Complex corporate structures (including using gatekeepers/DNFBPs) to obfuscate beneficial ownership (BO)

Scam hub operations use opaque corporate structures to conceal beneficial ownership and obscure the scale of operations. Assets are able to be moved across jurisdictions with minimal transparency, through the use of cross-border registration chains, nominee directors and multi-layered shell companies.[8] Vertically integrated criminal ecosystems are difficult to regulate through a single jurisdiction AML framework, since illicit and online marketplaces, white-label online gambling and payment platforms integrate fraud-enablement tools with currency-exchange and settlement functions.[9]

These complex corporate structures are often established as the cyber scam hubs are being developed and operate in a similar way to large scale businesses. 65% of APG members noted the use of complex corporate structures, including shell or front companies, as a primary means of laundering proceeds from cyber scam hubs. Complex corporate structures were also identified in a number of cases submitted by members, including Case Study 1 below.

76% of APG members noted the involvement of gatekeepers in the laundering of proceeds from cyber scam hubs and human trafficking. Of these gatekeepers, 24% were company service providers and 18% believed to be lawyers. The extent to which gatekeepers such as accountants, lawyers and trust and company service providers unknowingly or knowingly facilitate the development of these complex corporate structures was also noted by members as an area which requires further research.

The importance of ensuring these gatekeepers are subject to risk-based AML/CFT supervision was highlighted by members, particularly given the transnational nature of the flow of funds. In some identified cases, the illicit proceeds from the money laundering activities were transferred abroad through complex channels, making it difficult to conclusively identify the gatekeepers involved in handling the criminal gains within the local jurisdiction.

[7] *Republic Act No. 12312*, known as the 'Anti-POGO Act of 2025'
[8] UNODC (2023), p.20.
[9] Ibid, p.15.

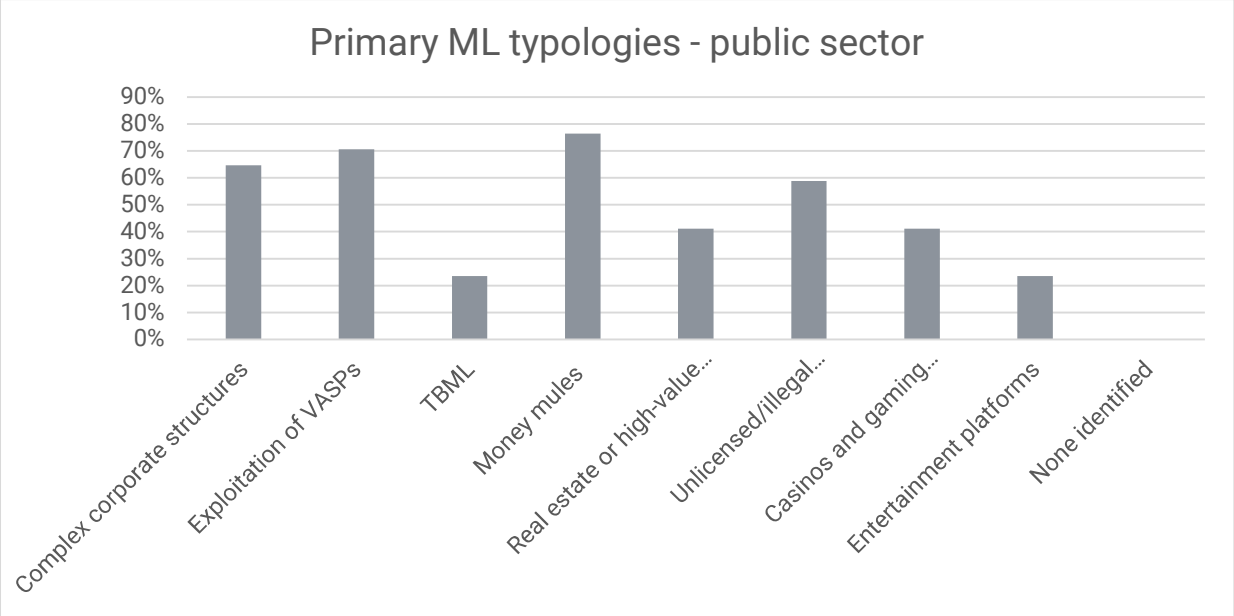


Figure 2: Primary ML typologies, Public Sector Survey

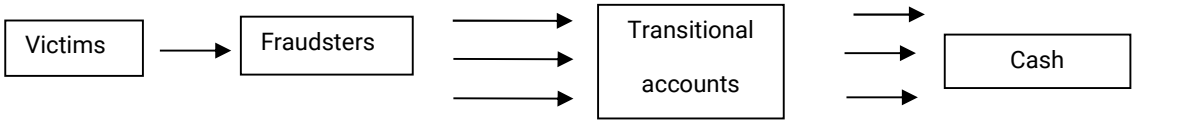
Case Study # 1: Use of shell companies to launder fraud proceeds

Indicators: fraud (phone/SMS/email/social media); third party laundering; structuring/smurfing/refining/mingling; financial institutions; underground banking/alternative remittance services/hawala; cash; wire transfer; suspicious transaction reporting; use of legal persons and arrangements

In 2023, a bank detected suspicious transactions where some accounts first conducted small-amount test transfers before making large-volume batch transfers to multiple counterparts and submitted STRs to the FIU. Based on the STRs the FIU analysed the fund transactions of the suspicious entities and their counterparts through its data analysis system.

Through its analysis, the FIU discovered fraud victims transferred funds into personal accounts controlled by the criminal syndicate. These funds were then immediately transferred to multiple downstream corporate accounts. After being pooled in these company accounts, the money was further dispersed to other personal or corporate accounts. Through multiple layers of transactions, the illicit funds were eventually fragmented across numerous individual accounts.

It was identified that the criminal syndicate pre-established shell companies for fund transit. These companies exhibited frequent transactions shortly after incorporation, followed by abrupt dormancy. In order to evade monitoring, the criminal syndicate used batches of accounts to transfer funds, and after mere days of use, the bath of accounts would be switched to new sets. Prior to bulk transfers, test transactions ranging from tens to hundreds of yuan were conducted to verify account liquidity and absence of freezing orders. Funds were transferred within minutes, demonstrating characteristic high-velocity money laundering patterns. These were then withdrawn as cash or transferred through the underground banking system.



The FIU subsequently forwarding the relevant information to the public security authorities. Acting on this lead, public security authorities dismantled nine telecom fraud 'money laundering rooms' and apprehended over 20 suspects, with CNY1.6 million (~USD230K) case-related funds frozen."

Source - China

Corruption

Systemic corruption of law-enforcement agencies and/or politically exposed persons provides the operational protection for cyber scam hubs to operate at scale. The bribing of local officials, police, border personnel and licencing bodies aid operations with construction permits, land acquisitions, telecommunications access and free cross-border movement of workers.[10] This protection networks allow CSHs to shift easily and quickly to nearby districts or other jurisdictions upon detection.

41% of APG members noted corrupt or complicit local authorities enabling the establishment and continued operation of cyber scam hubs. Organised criminal syndicate leaders have developed alliances with influential figures in government and the private sector. Corrupt bureaucrats and law enforcement officials benefit from the scam hubs and facilitate these operations. It has been alleged that of military, police, and local official corruption and complicity in the scam hubs. The presence of corruption as an enabler for these hubs was also evidence in case studies (see Case Study 2 below).

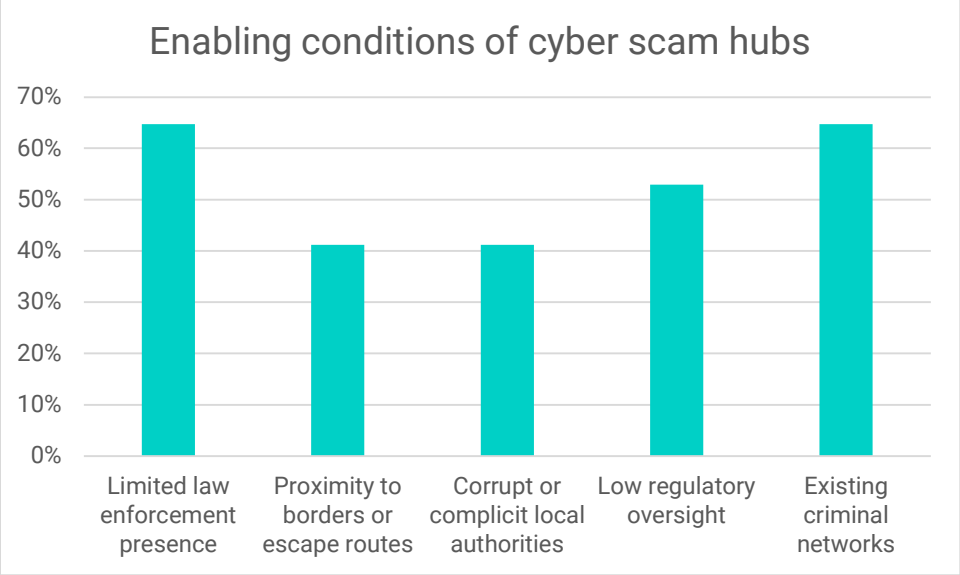


Figure 3: Enabling conditions of cyber scam hubs, Public Sector Survey

Case Study # 2: Bamban Philippine Offshore Gaming Operator (POGO) associated with politically exposed person (PEP)

Indicators: fraud (cyber scam hubs); corruption and bribery; third party laundering; structuring/smurfing/refining/mingling; financial institutions; casinos, gambling houses; real estate agents; dealers in precious metals and/or stones; professional facilitators including lawyers, notaries and accountants; cash; wire transfer; use of virtual assets; politically exposed persons; suspicious transaction reporting; international cooperation; purchase of real estate

The Bamban POGO case was initially detected through inter-agency intelligence sharing and on-ground surveillance, triggered by reports of suspicious foreign worker activity and human trafficking indicators. The Presidential Anti-Organised Crime Commission (PAOCC) and Philippine National Police (PNP) conducted joint operations, supported by intelligence from foreign law enforcement partners and possible reports from financial institutions (e.g., STRs filed with the AMLC).

During the investigation, authorities used search warrants and on-site digital forensic tools to extract data from confiscated devices and trace the financial flows. International cooperation (particularly with Australian and Chinese counterparts) was crucial in tracing transnational fund flows and victim identification.

[10] Global Initiative Against Transnational Organized Crime, *The Business of Exploitation: The Economics of Cyber Scam Operations in Southeast Asia* (August 2025) ('GI-TOC'), p.13.

In the Bamban POGO case, the illegal funds originated from romance and investment scams orchestrated by trafficked workers inside the compound. Victims (mostly foreigners) were lured into sending funds under the pretence of love or high-return crypto investments.

Victim funds were initially funnelled into local bank accounts and e-wallets controlled by the POGO operators and their facilitators. These funds were then layered through multiple transfers across individual and corporate accounts, including those of dummy companies posing as recruitment or outsourcing firms. A portion of the illicit proceeds was converted into cryptocurrency (e.g. USDT) using local and unlicensed over-the-counter (OTC) crypto brokers and peer-to-peer (P2P) platforms, circumventing VASP oversight. Authorities also noted the use of unregistered foreign exchanges and blockchain wallets tied to scam hubs in Cambodia and Myanmar, suggesting transnational flow and obfuscation of funds.

During the financial analysis, it was seen that the amounts involved in the accounts of various POIs, including a PEP of this case reached billions of pesos. Further, the following are the initial findings:

- There was a significant increase in both the transaction volume and the amounts involved in a POI's accounts upon the inception of the POGOs
- A substantial number of foreign exchanges were funded by cash or check deposits made on or near the date of the exchange
- There were cheque payments representing the acquisition of real estate properties totalling PHP409.7 million (~USD7M)
- There was layering of funds from one account to another, multiple deposits in one day, large withdrawals after deposits, creation of transit bank accounts, and misrepresentation of figures on their Audited Financial Statements
- Establishment of potential shell companies related to real estate development and business involved in the retail of high-end second-hand cars
- Incorporation documents of POGOs disclosed information such as same email addresses and contact persons connected to a POI
- There were inconsistencies in a POI's profile and identity based on their declared personal and financial information on KYC documents.

Proceeds were also used to acquire land, build scam compounds, and operate front businesses such as outsourcing and recruitment firms, giving an appearance of legitimacy.

62 counts of money laundering were filed against a PEP and 35 associates, along with charges for qualified human trafficking, serious illegal detention, and related offenses Asset preservation and freeze orders issued via coordination with AMLC and the courts.

Source - Philippines

Trafficking in humans for forced criminality

Cyber scam hubs utilised forced criminality to undertake scamming operations. Victims may be coerced or forced into entering into a contractual arrangement with the cyber scam operators, agreeing under duress to work for a specified period of time. Respondents noted that the cyber scam operators regularly extend these contracts and retain the trafficked individual for longer periods of time.

Case Study # 3: Human trafficking investigation with parallel financial investigation

Indicators: forced criminality, human trafficking and migrant smuggling; fraud; financial institutions; wire transfer; cash; suspicious transaction reporting; international cooperation

Following reports of four foreigners on October 7 2022 coerced into forced criminality, authorities initiated a coordinated operation that included financial investigations alongside traditional investigative techniques. The investigation revealed the use of multiple wire transfer accounts and significant remittances, approximately USD10K per victim sent from Jurisdiction A, facilitated by intermediaries who disguised the funds' origins. Police successfully identified and arrested six suspects, including key figures managing the illicit financial operations, in a collaboration between GCNP, GDI and the National Bank of Cambodia and the Cambodia FIU.

Authorities launched a parallel financial investigation to trace the flow of illicit funds associated with the trafficking activities. This included the money remittance services used by the suspects, examining financial records, wire transfer logs, and bank statements. The investigation revealed that suspects employed intermediaries to disguise the origins of their funds, using legitimate bank accounts to execute

transactions. Police identified seven wire transfer accounts connected to money laundering activities, leading to further investigations into these accounts.

The case was submitted to court with both direct evidence of human trafficking and extensive financial documentation. On November 4, 2022, police secured freeze orders on six wire transfer accounts, totalling approximately USD20K preventing the suspects from accessing these funds.

Source - Cambodia

Case Study # 4: Online scam operation

Indicators: forced criminality, human trafficking and migrant smuggling; fraud (phone/SMS/email/social media); use of the internet; financial institutions; international cooperation

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

The investigation, led by the No. (6) Branch of Anti-Trafficking in Person Police Force (Yangon), revealed that in June 2024, Mr. P and the six persons all residents of Patheingyi Township in the Mandalay Region had sought opportunities to work abroad. During their search, they came into contact with Ms. C, a resident of North Okkalapa Township, Yangon Region, via the Telegram platform. Ms. C informed them that customer service jobs were available in Cambodia, offering a monthly salary of USD800 with free meals, and persuaded them to accept the offer. Ms. H and Mr. S subsequently arranged the necessary travel documents and facilitated their travel.

Upon arrival in Cambodia, the victims were transported to Bavet City, where they were forced to work for an online scam operation. Using Instagram, WhatsApp, and Line accounts, they were made to lure potential victims online. Upon successfully engaging a customer, they were instructed to transfer the contact to a foreign national via WhatsApp or Line. They were compelled to work in these conditions for approximately three months without receiving any salary. The investigation confirmed that Mr. P and the six persons were subjected to forced criminality under coercion, with the traffickers profiting unlawfully from their labour.

As a result, legal action was initiated against Ms. C (arrested), Ms. H (arrested), and Mr. S (under investigation) under applicable laws. On 27th October 2024, an official case was opened in accordance with Sections 35, 36, and 44 of the Anti-Trafficking in Persons Law.

Source - Myanmar

In addition to trafficking across borders, there are also examples of where individuals have been traded between compounds. In an evolution of their business model, the Philippines has identified a criminal syndicate who traded individuals between compounds and criminal syndicates as a form of labour hire[11].

Scams

Cyber scam hubs employ a range of fraud typologies that are tailored to the platform target audience and victim demographics. The most common scam types include:

Investment fraud – This can include includes fake websites, online trading platforms and cryptocurrency-exchanges and is also often referred to as “pig-butchering”. These scams involve sophisticated marketing and social engineering techniques to promote investments which promise attractive returns with little or no risk involved. The scammers often use high-pressure tactics and are very communicative in the initial stages, before disappearing after funds have been transferred. Other investment/pig-butchering scams may also involve initial payments made to investors to enhance the credibility of their scheme, sharing fake diagrams of anticipated future returns and persuading investors to send additional funds to the scammers before disappearing (see Case Study 6 below).

[11] Discussions at the 2025 APG Typologies Workshop

Investment Fraud Case Studies

Case Study # 5 Operation Firestorm - facilitating international cooperation

Indicators: fraud (investment fraud); financial institutions; international cooperation; transnational organised crime group

In August 2024, the Joint Policing Cybercrime Coordination Centre commenced Operation FIRESTORM, as a proactive initiative and a wholistic approach to combatting Cyber Enabled Fraud - specifically scam call centres. Supported by Australian Federal Police (AFP) International Network posts in Southeast Asia, Europe and the Middle East, this operation focuses on delivering accurate, real-time intelligence relating to scam call centres utilised by organised crime groups targeting Australians.

In April 2025, the Australian Federal Police collected intelligence that a scam centre in Bangkok, Thailand was being established to target Australians with investment bonds. The organised criminal syndicate members pitched a well-orchestrated and detailed script involving high-pressure tactics and forged documentation. Members pretended to represent an international financial firm selling fake high-yield fixed-income bonds.

In June 2025, the Royal Thai Police executed search warrants on the identified scam centre, resulting in the arrest of 13 persons, including five Australian nationals, six United Kingdom nationals, one Chinese/Canadian national and one South African national.

13 Australian victims were identified as already invested and had transferred funds in the amount of AUD1.9 million (~USD1.2M) total in just two months, with approximately AUD1.3 million (~USD850K) seized/frozen by Australian banks to be returned to victims. A further 14,868 Australian names had been identified by the syndicated with 1,800 of these at various stages of approval and were pending investing at the time of the raid.

All offenders are currently detained in Thailand prison after charges were upgraded to transnational serious organised crime offences laid by the Royal Thai Police.

This was the first successful off-shore deployment for Operation Firestorm and has triggered increased cooperation from other Thailand law enforcement agencies with new referrals and their request for Australian Federal Police assistance.

Source - Australia

Case Study # 6: Telegram/WhatsApp Investment Scam using "Task-and-Refund" Bait

Indicators: fraud (investment fraud; phone/SMS/email/social media); financial institutions; money value transfer services (MVTS); wire transfer; use of virtual assets (cryptocurrencies or other virtual assets)

Accused/arrests: Four accused (two named in First Information Report, FIR; two found in inquiry); four arrested; three confessional statements under Section 164 of the Code of Criminal Procedure.

Seizure: One mobile phone

Between 27 February and 3 March 2025, a fraud ring posing on Telegram lured the complainant with a "watch ads → profit + refund" scheme, then escalated demands via WhatsApp and bank/mobile-wallet transfers. Funds moved through Dutch-Bangla Bank Limited (DBBL) via NexusPay, BRAC Bank, Islami Bank Bangladesh Limited (IBBL), and Nagad (Mobile Financial Service, MFS). The group extracted about BDT2.1 million (~USD**17**K) and then refused refunds after the victim declined a final "clearance" payment (see identified transactions below).

The ring used Telegram voice calls and in-app messages to pitch micro-investments tied to viewing 75 ads. Early "cashbacks" created credibility, followed by goal-post shifts ("watch more ads," "pay to unlock/clear"), and repeated requests to send money to rotating bank/MFS accounts (likely money-mule controlled). When resistance emerged, the ring withheld all funds and pressed for a final large "clearance" fee.

Identified transactions

- 27 Feb 2025: Trial payment BDT11K (~USD**90**) followed by a quick "return" BDT16K (~USD127) to build trust.
- 3 Mar 2025: Larger transfers: BDT300K (~USD**2**.5K) and BDT610K (~USD**5K)** to accounts controlled by the ring.
- Subsequent "unlock"/"quota" demands triggered additional payments totalling BDT1.2 million (~USD10K) across Bank accounts and Nagad.

- Total outflow BDT2.1 million (~USD17K); a further demand of BDT2.5 million (~USD20K) was refused.

The investigation by the Cyber Police Centre, Criminal Investigation Department, Bangladesh Police led to the arrest of four suspects. Seized and documentary evidence includes the phone used, Telegram/WhatsApp logs, beneficiary account details, transfer proofs, and timestamps consistent with the complaint. Proceedings continue under Penal Code 406/420. Given multi-bank flows and probable mule activity, coordination with AML counterparts and pursuit of restitution/attachment are warranted. Digital forensics and bank responses are ongoing.

Authorities acted quickly to freeze the first account that received the victim's money and rebuild the full money trail. Recipient accounts that share the same identity details, devices, locations, or cash-out times were grouped to find the organizers behind the first recipients. Chats and call logs were exported in a court-ready way with verified screenshots and strict custody records for every seized phone and document. Preservation orders and subscriber information requests were also sent to social-media companies.

Source – Bangladesh

Case Study # 7: Investment fraud

Indicators: fraud (investment fraud); financial institutions; professional facilitators including lawyers, notaries and accountants; corporate vehicles (use of legal persons and arrangements including international business companies, offshore companies or trusts, role of TCSPs)

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 MYR200 million (~USD48.4M) in 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

Romance scams – These often involve building romantic connections using fake online dating application and social media accounts before manipulating victims to send money. Romance scammers then fabricate financial emergencies and ask for victims to send money to help them or share allegedly lucrative investment opportunities with their victims and connect them with investment scams as outlined above.

Romance scam case studies

Case Study # 8: Suspected POGO and scam hub

Indicators: fraud (phone/SMS/email/social media); forced criminality, human trafficking and migrant smuggling; financial institutions; casinos, gambling houses; use of virtual assets (cryptocurrencies or other virtual assets); cash

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

The operation was conducted in the company's compound, which consisted of several buildings inside a 2.6-hectare area in Location X where around 900 workers were rescued. Subsequently thereafter, authorities implemented a court order to open numerous safes where bundles of cash totalling PHP113 million (~USD1.9M) were found.

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

Source - Philippines

Case Study #9: Suspected illegal POGO allegedly involved in human trafficking and scamming activities

Indicators: forced criminality, human trafficking and migrant smuggling; fraud (phone/SMS/email/social media); financial institutions; casinos, gambling houses; use of virtual assets (cryptocurrencies or other virtual assets); cash

In mid-2024, authorities received an information that the businesses in a compound in Location L are allegedly involved in human trafficking and scamming activities. Around 2,724 individuals were rescued purportedly to be victims of human trafficking. The rescued victims were composed of 1,534 Filipinos, and the rest are foreigners from Indonesia, China, Vietnam, Malaysia – and other jurisdictions like Cameroon. The rescued individuals were recruited through Facebook. Filipinos and other foreigners receive PHP24K (~USD409) in compensation each month, with free food and lodging while the Chinese employees receive a PHP40K (~USD682) salary. They were not allowed to leave their workplace and were required to work for 12 hours.

Company X was a subject of several adverse news whereas its operation is suspected to be illegal POGO.

According to reports, Company X is believed to have fostered fugitives and harboured trafficking victims as demonstrated by a raid that targeted seven POGO operations in the compound. Information and pieces of evidence gathered by the authorities linked Company X to possible involvement in human trafficking, cryptocurrency, and love/romance scams among other illegal activities.

Source - Philippines

Impersonation schemes – These scammers falsely claim to be known friend or family associates asking for loans or investment opportunities, or acting as authority figures like police, tax agencies or immigration officials. Scammers may use a variety of techniques to deceive the victim and obtain funds from them.

Phishing – This relates to emails sent on mass and seemingly without a target audience, in order to obtain sensitive information, including log-in credentials. These phishing emails often impersonate trusted companies, such as banks, and use fake websites where victims enter sensitive details which allow scammers to take over their account and access funds. Other phishing scams are used to deceive victims into downloading malware onto their devices which may also be used to steal sensitive information from them and others.

Business-email compromise – This is a subset of phishing which targets employees or executives of a business in order to obtain sensitive business information, fraudulently obtain funds or assets, or obtain access to further targets.

Case Study # 10: Asset recovery made from Business Email Compromise scam through international co-operation

Indicators: fraud (investment fraud; phone/SMS/email/social media); use of the internet; financial institutions; international cooperation

In July 2024, a commodity firm fell victim to a business email compromised (BEC) scam and transferred USD42.3 million to a fake supplier. The funds were transferred to a bank account in Timor-Leste.

The Singapore Police Force swiftly requested assistance from the Timor-Leste authorities through multiple channels, including INTERPOL Global Rapid Intervention of Payments (I-GRIP) mechanism, Asset Recovery Interagency Network - Asia Pacific (ARIN-AP) contact point, Egmont Group's Financial Intelligence Units (FIU) and the Mutual Legal Assistance (MLA) channel.

The Singapore Police Force was quickly alerted that USD39 million was successfully withheld from the fake supplier's bank account in Timor-Leste. Further joint investigations by the Timor-Leste authorities led to the

arrest of seven suspects and the recovery of over USD2.2 million in cash that was purportedly withdrawn by the suspects from the said bank account.

Intelligence exchanged between Singapore, Timor-Leste and Indonesian authorities detected that some of the funds were transferred to bank accounts in Indonesia, held by two of the individuals arrested. This led to the sum of approximately USD120,000 being provisionally frozen by the Indonesian authorities.

Source - Singapore

Employment scams – Scammers may offer jobs with high salaries for minimal work or with limited job experience. Some may pretend to be recruiters form high profile agencies or companies with a goal to obtain identity data or money from victims who are told they need to pay money up-front to be onboarded into the role.

Other employment scams are designed to lure victims to cyber scam hubs where they are forced to perpetrate scams on other victims. As noted in Figure 4, this is the most common recruitment method identified by APG members for victims trafficked to cyber scam hubs.

Fake employment scam case studies

Case Study # 11: International SIM and Account Trafficking

Indicators: fraud (phone/SMS/email/social media); financial institutions; dealers in precious metals and/or stones; money value transfer services (MVTS); wire transfer; use of virtual assets (cryptocurrencies or other virtual assets)

The Cyber Crime Police Station, Patiala, detected an international syndicate involved in the procurement and export of bank accounts and SIM cards from India to handlers operating in the Philippines. The syndicate, led by [Accused #4] and associates, established a supply chain that provided pre-activated bank kits and SIM cards to foreign-based Indian nationals engaged in online cyber-fraud.

The case originated from victim complaints received through the National Cybercrime Reporting Portal. Victims reported fraudulent online job offers wherein small registration fees were demanded through Indian bank accounts.

Initial investigation by the Cyber Crime Police, Patiala, revealed that multiple accounts receiving such deposits were being operated remotely from foreign IP addresses, particularly those geolocated in the Philippines.

Parallel intelligence from a courier interception unit in Ludhiana led to the discovery of consignments containing concealed SIM cards and debit cards, packed inside T-shirt seams and couriered to Manila. The consignments bore fake sender details and used private courier channels.

Subsequent forensic analysis of seized mobile phones and laptops confirmed communication between Indian recruiters and foreign handlers via Telegram, WhatsApp, and Signal. The digital trail included chats referencing “SIM shipments,” “account activation,” and “salary transfers,” indicating systematic coordination.

Network analysis established that the syndicate procured bank accounts by recruiting job-seekers under the guise of remote employment verification. Victims were asked to open new accounts, hand over passbooks, debit cards, and registered SIMs which were later shipped abroad for misuse.

IP and transaction forensics conducted by I4C confirmed multiple logins from the Philippines to Indian bank portals, often through VPN servers located in Singapore and Malaysia. VPN tunnelling was used to disguise geolocation and evade detection by banking systems.

The investigation identified 18 active mule accounts used to channel approximately INR29.9 million (~USD330K) between February and June 2025. The accounts belonged to individuals from Patiala, Bathinda, and Sangrur districts.

Funds were received from victims across India through UPI and IMPS transfers and were quickly transferred to new beneficiary accounts or crypto exchanges. The proceeds were derived primarily from job fraud and fake recruitment scams. The perpetrators impersonated HR executives of reputed companies and promised overseas employment opportunities in exchange for “processing” or “document

verification" fees. Analysis of transaction timestamps showed that 90% of transfers occurred between 21:00 and 02:00 hours, aligning with work hours of overseas handlers.

Bank audit trails confirmed that a portion of the funds was used to purchase prepaid cards and international gift cards on e-commerce platforms, while the remainder was moved to Binance and OKX wallets.

Four principal accused were arrested from Patiala and Sangrur districts and 231 SIM cards, 18 debit cards, multiple passbooks, and courier receipts recovered INR29.9 million (~USD330K) identified as illicit flows, part of which has been frozen by authorities in India.

Source - India

Case Study # 12: Fake employment scam

Indicators: forced criminality, human trafficking and migrant smuggling; fraud (investment fraud; phone/SMS/email/social media); use of the internet; financial institutions; cash

The Criminal Investigation Bureau received intelligence that gang members Person A and Person B, a couple, were suspected of organizing a cyber scam syndicate in Jurisdiction X and cooperating with wanted criminal Person C (Chinese Taipei individual), who was stranded in Jurisdiction X, to lure Chinese Taipei individuals to leave the jurisdiction to engage in cyber scam. The Criminal Investigation Bureau then formed a special task force and reported to the prosecutor's office for command of the investigation.

The investigation found that Person A and Person B have been organizing a cyber scam syndicate since March 2022, recruiting young adults from disadvantaged families in Chinese Taipei to join. At the same time, they set up a cyber scam hub with Person C and a cyber scam syndicate leader Person D (Jurisdiction Y national). Using "well-paid job opportunities abroad" and "monthly salary of TWD100K (~USD3.2K) as attraction, they lured 11 Chinese Taipei individuals to go abroad to engage in cyber scam, and used the method of "pig butchering" to defraud people from other jurisdictions. If the members' performance is not good, they will be beaten and abused with electric batons, and detained.

After the task force obtained key evidence, it was discovered that members of the syndicate frequently entered and exited Jurisdiction X from 2022 to 2024, and had continued to operate an overseas cyber scam syndicate. During the period when the syndicate members returned to Chinese Taipei for the Chinese New Year, a total of 15 people were arrested, 2 people were notified for interview, and 11 criminal bases were raided. Among them, Person A and his wife Person B were both detained incommunicado.

In addition, mobile phones used in the crime, TWD420K (~USD13K) in cash, passbooks, ATM cards, vests, hats, baseball bats and other evidence were seized. The case was referred to the prosecutor's office for violating the Organised Crime Prevention Act, the Human Trafficking Prevention Act, and aggravated fraud and extortion in the Criminal Code.

Source – Chinese Taipei

Hubs are increasingly using tools that allow the scaling of persuasion and payment. They include the use of Artificial Intelligence (AI) for creating deepfakes and multilingual content, encrypting messaging services for the use of automated scripts, and utilising white-label online gambling and payment shells to route funds.[12] Repeatable revenue loops are created by recycling victims through "recovery" or "refund" scams, and using Telegram-based marketplaces to monetise stolen data. It enhances cross-border victim pools, complicates attribution for law-enforcement agencies and financial institutions, while shortening the timeframes between initial contact and withdrawal. Moreover, platforms that enable rapid settlement timeframes (Virtual International Bank Account Numbers, e-money, virtual assets etc.) allow the progression from initial contact to cash-outs within hours.[13] Reducing these recovery windows allows authorities less time to intercept and prevent these transfers, while raising investigative costs across jurisdictions.

Scam call centres have emerged as a significant threat due to their capacity for high-volume, high financial harm to victims, at relatively low risk for the offenders. Various tactics are used to deceive individuals and

[12] UNODC (2023), p.14.
[13] Financial Action Task Force; INTERPOL; Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud* (November 2023) ('FATF'), p.28.

organisations, leveraging a combination of sophisticated technology and psychological manipulation through social engineering.

Case Study # 13: Operation TARGUS HAWK

Indicators: fraud (investment fraud; phone/SMS/email/social media); use of the internet; financial institutions; suspicious transaction reporting; international cooperation

Between January and July 2024, the Singapore Police Force (SPF) received 185 reports pertaining to Technical Support Scams (TSS), resulting in total losses of at least S$17.9 million (~USD14 million).

Victims received screen pop-ups on their laptops or desktops, claiming that their electronic devices had been compromised by malware and instructing them to seek immediate help from Microsoft or Apple technical support. When the victims contacted the number(s) provided, scammers impersonating Microsoft or Apple technical support employees would claim that the victims' devices had been compromised by "hackers" and were used for illegal activities. Following this, the scammers would instruct victims to access websites and/or download software that would grant scammers remote access to their devices.

Scammers then directed victims to log into their internet banking accounts on the pretext of helping to apprehend the "hackers", which allowed the scammers to capture the victim's internet banking IDs and passwords. Thereafter, the scammers used the remote access function to perform unauthorised transactions using the victims' bank accounts. In some cases, the scammers would guide victims to create cryptocurrency accounts or provide One-Time Passwords (OTPs) to authorise internet banking transactions. Victims would only realise that they had been scammed when they discovered unauthorised transfers or deductions from their bank accounts.

In August 2024, following extensive information sharing and joint investigations by the SPF and Hong Kong Police Force (HKPF), officers from the HKPF raided three premises in Hong Kong and arrested one mastermind of the syndicate, three syndicate members and three money mules, aged between 33 and 43. Cash amounting to HK$300,000 (~USD38,000) and over 60 bank cards were recovered and seized as case exhibits.

Through further follow-up investigations, another HK$1.3 million (~USD166,000) in crime proceeds was successfully recovered. Through intelligence sharing from the HKPF, the SPF arrested a 23-year-old male Singaporean for his involvement in money laundering activities. Investigations revealed that he had relinquished his bank account to a criminal syndicate associated with the money-laundering syndicate which was busted by the HKPF. Investigations are ongoing.

Source – Singapore

Victim profiles

Human trafficking victims

Human trafficking enables cyber scam hubs to operate worldwide by providing control over a low-cost and replaceable workforce. Individuals are targeted most in Southeast Asia, Africa, South Asia, Latin America, Eastern Europe and the Middle East.[14] Victims are typically recruited through false job advertisements, third-country brokers and online freelancing platforms. Cyber scam hubs often target students, unemployed youth, skilled professionals and migrant labourers promised employment roles in digital marketing, customer service or information technology.[15] It represents a pattern of organised groups that target regions with limited employment opportunities, norms of labour migration and countries with barriers to legal or safe migration channels (see in-depth analysis conducted by India in Case Study 12 below from repatriated victim debriefings).

Members noted variations in the individuals targeted for trafficking for forced criminality. This reflects the evolving operations of these cyber scam hubs as they require different skills, background and language abilities for the various scams and other criminal activities they engage in. However, achieving continuous online engagement and high-volume outreach, means that digitally literate and multilingual workers are more favoured. This model of forced criminality allows their workforce to have low operating costs, with high productivity and replaceability, while allowing the operations of criminal networks to be sustained even in jurisdictions with mobility controls and weaker labour markets.

False job and business opportunities were the most common recruitment methods identified by members (71% of member responses – see Figure 4 below). The perpetrators run elaborate social media recruitment efforts, where recruiters post professional-looking profile pages on social media sites and approach victims with seemingly credible job offers. They are also increasingly setting up fake company websites and email domains that closely resemble genuine enterprises to facilitate credibility in their fraudulent recruitment activities. The recruitment tactics often specifically target educated individuals with computer skills who are seeking better economic opportunities, with poverty being a driving factor for trafficked victims.

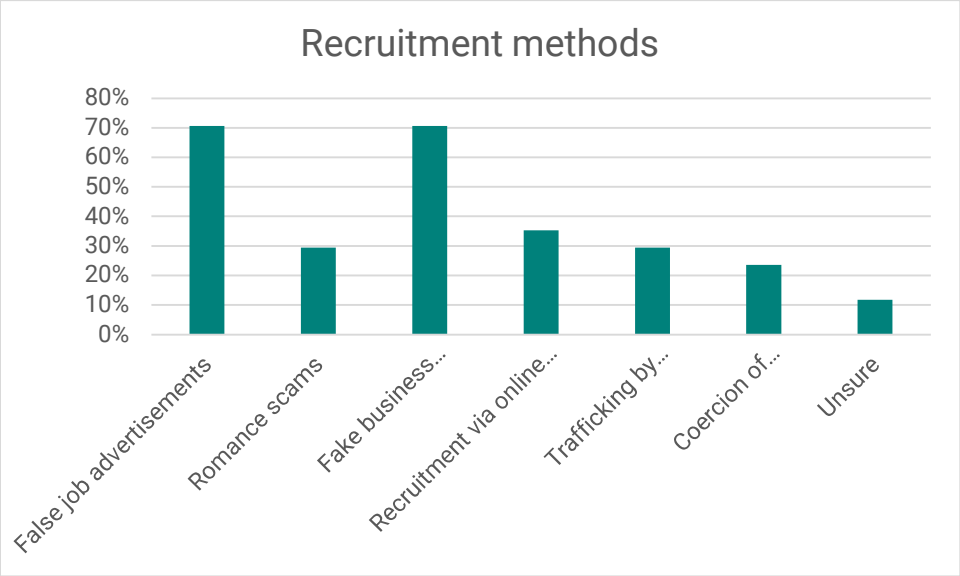


Figure 4: Recruitment methods, Public Sector Survey

[14] UNODC (2023), p.10.
[15] Ibid, p.11.

Case Study # 14: Transnational Cyber Slavery Networks Targeting Indian Nationals in Southeast Asia – An In-Depth Analysis of Repatriated Victim Debriefings

Indicators: forced criminality, human trafficking and migrant smuggling; fraud (investment fraud; phone/SMS/email/social media); use of the internet; financial institutions; international cooperation

This analytical case study examines the emerging nexus between human trafficking and cyber-enabled financial crime, drawing upon the debriefings of 15 Indian nationals repatriated from Myanmar, Lao PDR, and Cambodia between 2023 and 2024. The individuals were recruited under the pretext of high-paying customer-service or IT jobs, transported through Thailand, and then coerced to work in criminal "scam compounds" operated by transnational syndicates. The findings demonstrate a clear pattern of organized trafficking with social-media recruitment, deception, document confiscation, and crypto-based financial systems serving as core enabling mechanisms.

The analysis identifies seven core trends:

(1) balanced geographic distribution of exploitation

The 15 victims were equally dispersed among Cambodia, Lao PDR and Myanmar. This equal distribution emphasizes the Golden Triangle area's function as a central hub for trafficking, with scam compounds often situated in remote border zones that escape effective regulatory control.

Cambodia's policy of visa-on-arrival makes it a favoured entry point, accounting for 60% of the detailed transit paths that pass through Thailand. Cases from Lao PDR often represent extensions of routes originating in Cambodia, featuring sub-agents who manage transfers from airports to inland sites. Myanmar's compounds, located in conflict-affected zones, draw operations relocated from Cambodia following intensified crackdowns, according to accounts of escapes. Approximately 80% of all routes included stopovers in Bangkok. A typical sequence involved local taxi pickups immediately upon arrival, leading to compound seclusion within 1-2 days. The syndicates' strategy of spreading operations across sites has reduced vulnerability to shutdowns.

(2) demographic vulnerabilities

The profiles of the victims show a strong male majority (93%, with only one female represented), an age range of 20-35 (deduced from descriptions of prior employment), and origins across nine Indian states. This aligns with areas of elevated unemployment, where reliance on informal economies and a blend of digital access with economic strain make individuals susceptible to offers of Rs. 50,000-70,000 monthly wages. All victims shared contact details (via phones or WhatsApp), facilitating law enforcement follow-ups but also heightening risks of renewed outreach, which necessitates focused safeguards in these high-risk locales.

(3) digital and network-based recruitment with upfront fees

Every case involved fraudulent recruitment tactics, with 27% occurring through digital means (social media) and 73% via personal connections, invariably involving INR50-70K (~USD560-784) fees paid in cash or online, creating immediate debt bondage. Indian agents form the entry layer, transitioning to foreign sub-agents (taxis in Cambodia; facilitators in Lao PDR), with all individuals using tourist visas masking intent.

(4) Chinese-speaking-dominated compound hierarchies with multi-national workforces

Scam compounds operate as pseudo-legitimate entities with implied ownership largely under control of a Chinese-speaking diaspora and blended oversight teams. Workforces blend Indians with other victims from Africa, South Asia and Southeast Asia. Enclaves like Poipet (Cambodia) or Bokeo (Lao PDR) enforce isolation via passport seizures (100% inferred), with 12-16 hour shifts post 2-3 days of training. The diverse nationalities undermine group cohesion, and secured perimeters prevent breakouts until external interventions.

(5) a spectrum of six cybercrime typologies, led by investment and romance scams

Victims were forced into six categories of cybercrimes, all following a "pig butchering" model of gradual enticement, enforced by daily quotas. These categories of cybercrime included scams related to investment, trading, romance, digital arrest/law enforcement impersonation, social media and gaming. Quotas were mandatory in 100% of cases (non-compliance led to isolation in 20% cases), and the scams often hybridized (e.g., from dating to investment) to boost profitability, starting with social media as the primary hook.

(6) uniform physical and psychological torture methods

Coercion methods were standardized, including electric shock (33%), dark room and isolation room confinement (33%), physical abuse (33%), fines (20%) and mental torture (13%). All had their passports confiscated and were bound by debt from recruitment fees. Tactics advanced from psychological to physical to guarantee adherence, with successful escapes often routed through embassies and local police

(7) repatriation pathways via diplomatic channels, tempered by recidivism risks.

Repatriation occurred via diplomatic channels in the majority of the cases. Signs of recidivism appeared, as one victim contemplated travel to Europe. Law enforcement emphasized intelligence collection over criminal charges. One case involved post-rescue questioning and clearance. A recurring issue is the shortfall in follow-up support, which leaves individuals prone to future exploitation.

Source - India

The perpetrators also frequently recruit within personal networks, where existing victims are paid to refer friends and family members who will trust offers presented to them by other members. They will provide all-inclusive visa and travel facilitation services that position them as international job placement professionals who take care of the logistics that could otherwise make it difficult for victims to accept jobs abroad. As noted by an NGO during the 2025 APG Typologies Workshop, cyber scam hubs are transitioning to more frequently using human recruiters in source countries.

Workers are commonly sold between compounds, where they are subjected to confinement, violence, passport confiscation, and debt bondage. Additionally, victims face dual victimisation, since they are exposed to criminal liability, with authorities often misclassifying trafficked individuals as victims rather than offenders. Interception operations and large-scale rescues have revealed victims from a variety of nationalities and regions, suggesting that recruitment practices have expanded beyond solely regional contexts.[16] Workers are forced to conduct investment fraud, impersonation schemes, romance scams, and illegal online gambling platforms, with performance enforced through physical abuse and threats.[17]

It is clear from the existing literature and the input of members that these trafficked individuals are subject to horrific treatment. In addition to the forced criminality, they are often subject to physical confinement and constant surveillance, psychological and physical violence, sexual exploitation and isolation from support networks.

The methods perpetrator use to keep the participants against their will include confiscating their passports, demands for ransom or repayment of debt if request to leave, violence, torture, threats, handcuffing, 24-hour surveillance (including armed guards monitoring facilities and internet and phone usage strictly monitored) and remote physical location (jungle, desert, etc. which also makes it difficult for victims to raise alarm or seek assistance). Victims also reported include beatings, stress positions, starvation and deprivation of basic necessities including sleep, forced exercise, electric shocks, and 'public punishments' (including being filmed)

[16] Ibid, p.10.
[17] Ibid, p.9.

to intimidate other victims, and specific 'torture rooms' or floors within cyber scam hubs. Further, many victims are coerced into remaining in the hubs through fear of violence or threats to their families.

Scam victims

Scam victims of cyber scam hubs include individuals than span across socioeconomic backgrounds and age, that span across North America, Europe, Asia-Pacific, Latin America and Africa.[18] Adults with retirement funds, savings or access to credit are disproportionately targeted by investment related fraud. They are often manipulated by personalised trust-building communications on messaging apps, networking sites and social media platforms, with many victims reporting they believed they were interacting with a romantic partner, financial advisor or mentor.[19] Some victims are re-targeted through recovery scams, whereby criminals will fraudulently act as asset-recovery or law-enforcement agencies offering assistance.

Individuals within jurisdictions that have higher levels of disposable income and financial access are often targeted. The project team noted that cyber scam hubs have targeted people in over 100 jurisdictions around the world, demonstrating the truly global reach of this crime type. Further, participants target the victims with similar nationalities to the participants and/or perpetrators, likely due to their familiarity. The 'targeting strategy' appears to evolve with the trafficked participants as the bring new language capabilities and cultural awareness that can be exploited to target additional jurisdictions. Further, they target jurisdictions with high levels of cryptocurrency adoption, regardless of geographic location.

Perpetrators' target selection tends to follow the logic of 'risk-reward optimisation': by targeting individuals who are economically vulnerable, emotionally vulnerable, socially isolated, subject to information asymmetry, lacking in legal protection, and exploiting their characteristics of 'desperate needs, information gaps, and weak capacity to defend their rights'. Through this the perpetrators can achieve long-term control and large-scale exploitation at minimal cost. This strategy has the core objective of maximising illegal profits while minimising the risks of being reported and held accountable.

Members also noted that the targeted victims vary depending on the type of scam. As different scam typologies target different potential victims, there is no consistent pattern in the demographics of all scam victims.

[18] FATF (2023), p.9.
[19] Ibid, p.24.

Illicit financial flows

Various estimates suggest cyber scam hubs are generating tens of billions of US dollars annually. Findings from the member questionnaire responses highlight the importance of tracing these financial flows in order to identify the operation of these hubs and undertake the necessary enforcement actions. Unfortunately, most investigations of cyber scam hubs were triggered from reports or complaints by victims (82% of member responses) as opposed to those generated from STRs (59% of member responses). Further review of the STRs received by members indicated that these are more frequently in relation to scams as opposed to cyber scam hubs specifically, with less than 30% of surveyed members having received an STR on cyber scam hubs.

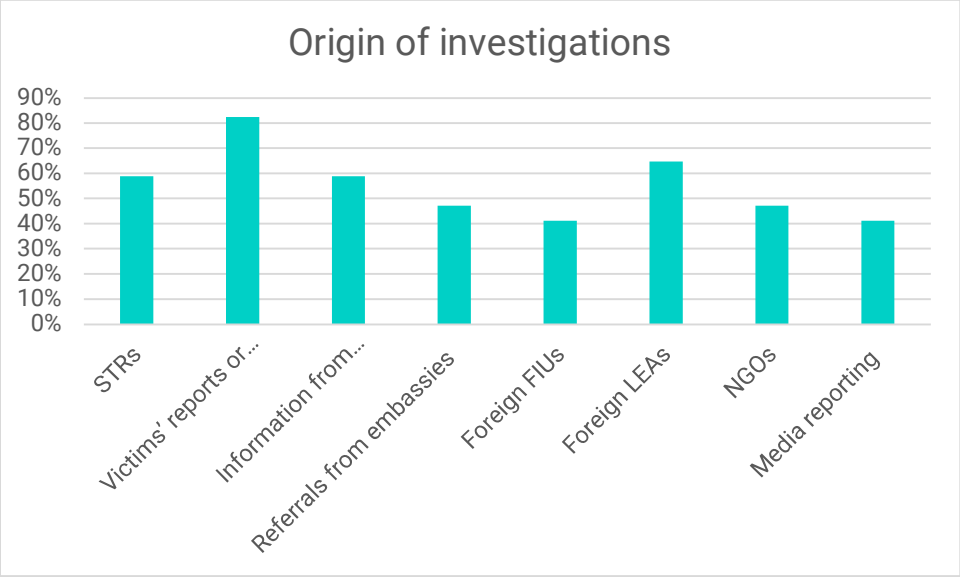


Figure 5: Origin of investigations, public sector survey

Sources of revenue

Associated with the human trafficking element

Revenue is generated by payments linked to human trafficking, through release fees, ransom demands, selling trafficked workers between compounds, and through debt bondage repayments.[20] When the victims arrive at the scam hubs, the criminal syndicates make them bear high debts in the name of various ongoing costs such as accommodation fees and 'on-boarding and training' fees, and these fees are maliciously inflated. Cyber scam operations may keep a record of certain costs that they claim have been borne to bring a participant to the cyber scam hub. These costs may relate to transport or payments to intermediaries ('agents'). This also includes withholding of wages and financial penalties for not meeting quotas and selling victims to other compounds if quotas aren't met. Any ransom amount to free a participant may be calculated in alignment with these recorded costs.

The human trafficking victims may sign contracts under duress stating that they will work for a cyber scam operation for a certain period of time, for example, one year. The victim may not be allowed to leave the cyber scam hub during this time. The duration may also be extended without the genuine consent of the victim, keeping them working for the cyber scam operation.

Members observed a prevalence of cash (53% of member responses) and bank transfers (47% of member responses) to facilitate payments for transportation of trafficked individuals. These costs are largely paid by

[20] UNODC (2023), p.11.

the trafficker or recruitment agent (53% of member responses) or by the third-party sponsor or fake employer (41% of member responses). In other instances, the victim themselves pays these costs (41% of member responses), representing an additional source of illicit revenue for the criminal syndicates.

Case Study # 15: Fake recruitment scheme

Indicators: fraud; forced criminality, human trafficking and migrant smuggling; cash; financial institutions; international cooperation; suspicious transaction reporting; third party laundering; use of legal persons and arrangements (including international business companies, offshore companies or trusts, role of TCSPs)

In 2022, based on leads from law enforcement and media reports, Bank A identified several retail account holders suspected of being perpetrators in fake recruitment schemes that led to the cross-border trafficking of jobseekers. The jobseekers were trafficked from Hong Kong to Cambodia, Lao PDR, Myanmar or Thailand, where they were reportedly held for ransom and often subjected to forced criminality.

Reviews of transactional activities of the perpetrators' accounts identified red flags such as large volumes of cash transactions, unusual transaction flows and unusual overseas ATM activity. Based on open-source reports, Bank A assessed the accountholders may have been involved in operating social media accounts to recruit victims and receiving ransom payments, though these activities were not immediately apparent in their account activities.

Bank A's negative news screening controls, email referral from Hong Kong's Joint FIU, followed by a search warrant from Hong Kong Police Force.

Bank A observed large volumes of cash activity and rapid movement of funds. Bank A observed the movement of funds via self-named accounts and via multiple, unrelated retail bank accounts (including bank accounts that were newly opened) that represented potential money mules.

Arrested individuals were charged in November 2024 with "Conspiracy to defraud" and "Dealing with property known or believed to represent proceeds of an indictable offence".

Source - Hong Kong, China[21]

In some cases, victims or their families are required to significant sums, ranging from an estimated USD3K to USD20K to secure release, further increasing the criminal syndicates' profits. Numerous survivors have also noted organised crime leaders often also accept "headcount" (i.e. require the victim to lure two or more victims to the compound to secure their own freedom) as an alternative and may be more accessible to victims compared to paying ransoms.

Ransom payment case studies

Case Study # 16: Ransom payment in form of cryptocurrency

Indicators: forced criminality, human trafficking and migrant smuggling; fraud; use of virtual assets (cryptocurrencies or other virtual assets); financial institutions

In December 2024, a local resident fell prey to a job scam and told her family members that she would be leaving Hong Kong, China for a few days for a quick cash job in Jurisdiction X. Later, the victim realized the job was actually related to a cyber scam hub in Jurisdiction Y, which is adjacent to Jurisdiction X. She sent screenshots of her GPS location near the border of Jurisdiction X to her family members and told them that she was requested to pay HKD350K (~USD45K) in the form of USDT to several designated cryptocurrency wallets in order to be released back to Hong Kong, China.

Her family eventually agreed to pay the money in exchange for victim's return. The victim's family paid a total of HKD210K (~USD27K) in form of USDT to the designated cryptocurrency wallets on two occasions.

[21] See also Sixth Hong Kong suspect arrested over human-trafficking case involving job scams, with at least 37 victims lured to Southeast Asia and held against will, South China Morning Post, 22 August 2022; 23-year-old student accused of luring Hongkongers to Southeast Asia into forced labour, South China Morning Post, 23 August 2022; HKSAR V. MA CHE HOU, Hong Kong Legal Information Institute, 1 November 2024; HKSAR V. MA CHE HOU AND ANOTHER, Hong Kong Legal Information Institute, 1 November 2024

Two days later, the victim was released and safely returned to Hong Kong, China. The investigation is ongoing.

Source - Hong Kong, China

Case Study # 17: Forced criminality in cyber scam hubs in Southeast Asia

Indicators: forced criminality, human trafficking and migrant smuggling; fraud; use of virtual assets (cryptocurrencies or other virtual assets); financial institutions

In 2022, police received reports from 46 local victims who were recruited to work in Southeast Asian jurisdictions but were confined to work in scam centres upon arrival. The victims were made to stay there and could not leave until they agreed to participate in some scam activities for the culprits there or until the victims' family had paid ransoms for their release.

Ransoms were paid to designated cryptocurrency wallet via crypto transfers. On one occasion, a ransom was paid in form of USDT to a cryptocurrency wallet. Part of the VA was eventually sold via VA trading platform and funds were transferred back to a perpetrator's bank account. Transfers were also detected via a stored value facility.

Upon investigation involving law enforcement agencies from Hong Kong, China and Southeast Asian jurisdictions, a total of 10 persons were arrested and two of which were charged. In November 2024, the two defendants were convicted for Conspiracy to Defraud and sentenced for 36 and 54 months' imprisonment.

Source – Hong Kong, China

Case Study # 18: Use of blockchain analysis to identify ransom payments

Indicators: forced criminality, human trafficking and migrant smuggling; fraud; use of virtual assets (cryptocurrencies or other virtual assets); financial institutions; international cooperation

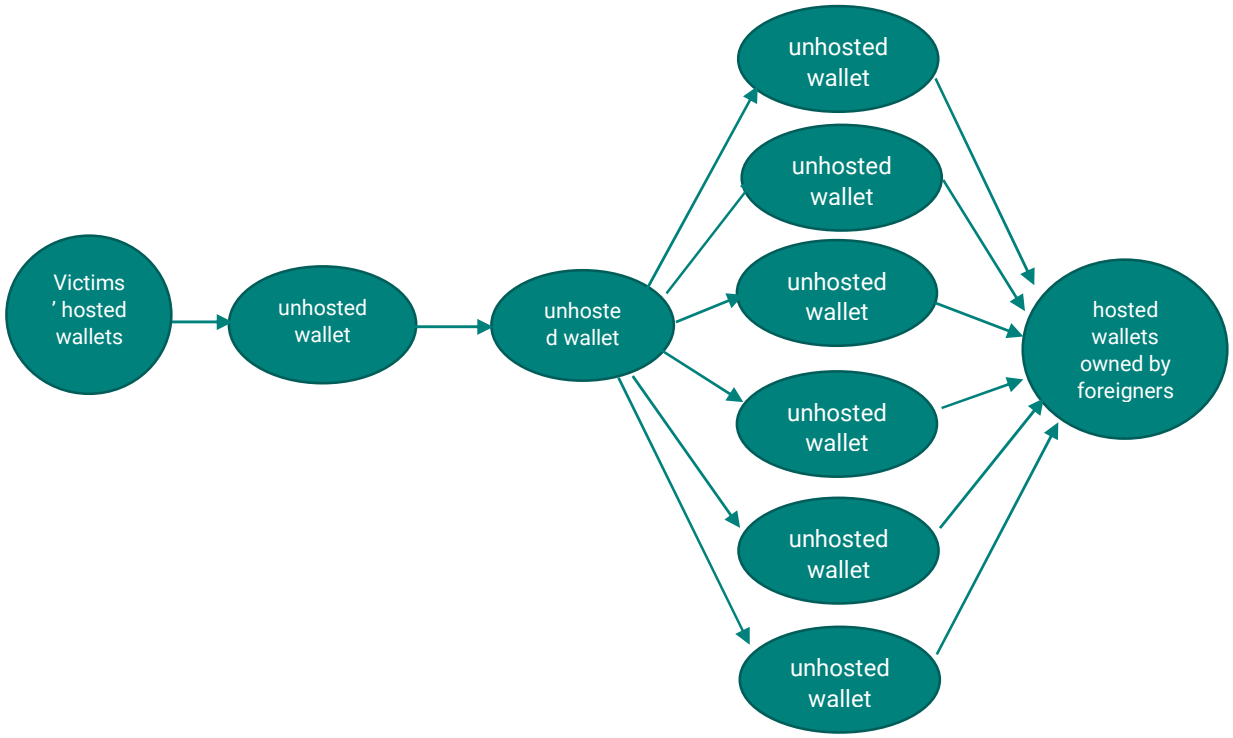
In June 2022, following reports from the victims' families, Person A and B conspired with Jurisdiction X national C and their accomplices to form Scam Group Y. They posted false information on Facebook, such as high-paying job offers and free trips to Thailand to apply for loans in exchange for high commissions, to lure people overseas. Several victims agreed to go abroad. The expenses related to air tickets, passports, transportation, and accommodation were covered by C, who remitted funds in cryptocurrency to A's cryptocurrency wallet. A then transferred the funds to B's cryptocurrency wallet to cover the victims' expenses while still in Chinese Taipei.

Once B confirmed that the victims had successfully departed from Chinese Taipei, B notified A, who arranged for scam syndicates in Thailand to take control of the victims and transport them to the Group Y's base in Myanmar. There, the victims were forced to engage in cyber scam activities.

The scam method used by the group involved communicating with individuals in Jurisdiction Z via messaging applications, persuading them to invest in cryptocurrency, and deceiving them into transferring virtual assets purchased from legitimate exchanges into fake platforms created by Group Y.

For each victim trafficked to Myanmar, B received a commission ranging from USDT 3,000 to 8,000, calculated based on the victim's age—the younger the victim, the higher the commission. C and others would then negotiate ransom payments with the victims or their families. Some victims paid ransom amounts ranging from TWD300K **(~USD9**.6K**)** to TWD710K **(~USD2**3K**)** while others paid USDT 11,000 to 46,000 to an cryptocurrency wallet designated by C in exchange for the opportunity to return home.

Using blockchain analysis tools, it was identified that Group Y used unhosted wallets to receive ransoms, first transferred the cryptocurrencies to various other unhosted wallets, and then transferred the cryptocurrencies to some hosted wallets of certain exchanges, owned by people in foreign jurisdictions in Asia. The cost for the transportation of the victims was paid by cash withdrawal from Person B's bank account.



In December 2022, under the direction of the Prosecutors' Office, the MJIB and the NPA executed arrests and searches. The case was referred for prosecution in March 2023, and the third instance judgement was given by the court in December 2024. The victims were successfully returned back to Chinese Taipei after paying the ransom. The criminal proceeds of A and B was transferred to cryptocurrency wallets owned by foreigners and could not be seized in time. The court ordered the confiscation of their illicit gains.

Source - Chinese Taipei

Facilitators involved in the trafficking of individuals also receive payments in various forms. These include cash and virtual assets as a form of commissions for the number or persons trafficked and/or to cover the transportation costs of trafficking individuals.

Facilitator payment case studies

Case Study # 19: Human trafficking under the guise of overseas employment for cryptocurrency-related work in Cambodia

Indicators: fraud; human trafficking; financial institutions; cash

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

Following this, Person A enlisted the assistance of Person B to identify potential candidates. Person B recommended two individuals, Person C and Person D. Person A received IDR95 million (~USD5.7K) in total from the company in Cambodia—transferred to a BXX bank account after conversion from USD to Indonesian Rupiah. She accompanied Person C and Person D to Hang Nadim Airport, from where they flew to Jakarta and continued to Phnom Penh, Cambodia. Person A received a commission of IDR7.5

million (~USD450) per person. Over the course of 2022, a total of 19 individuals were sent abroad under this arrangement.

Person A collaborated with Person E to facilitate the processing of passports, visas, ferry transportation, and flight tickets. Prospective workers from outside Batam were required to arrange their own lodging prior to departure. Person A informed candidates that they would be employed in Cambodia as Bitcoin telemarketers, working from apartment-based offices. The company would arrange work permits, with employment contracts valid for one year. The offered salary varied according to language proficiency: USD841(~IDR14M) for those with foreign language skills, and USD601 (~IDR10M) for others. Accommodation and travel expenses were to be covered by the company, but if an employee resigned or was terminated before the end of the contract, the company would demand reimbursement of incurred costs.

In total, Person A received USD53.2K (~IDR890M) for sending 19 workers, averaging IDR40M (~USD 2.4K) per individual.

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

Source - Indonesia

Case Study # 20: Analysis of human trafficking victims to cyber scam hubs

Indicators: forced criminality, human trafficking and migrant smuggling; financial institutions; fraud

The Indonesian Financial Transaction Reports and Analysis Center (PPATK) has conducted an analysis in response to public concerns regarding allegations of exploitation and human trafficking involving Indonesian Migrant Workers in Cambodia. These migrant workers were allegedly sent abroad through non-procedural channels by human trafficking syndicates and were subsequently believed to have been exploited and subjected to forced criminality, being compelled to work for online scamming and illegal online gambling operations in Cambodia.

In one case, an NGO reported suspected victims of human trafficking. LSW, an Indonesian citizen who is the wife of a Cambodian national and acts as a trafficker, received funds from various parties abroad. These funds were subsequently transferred to associates in Indonesia who were responsible for purchasing tickets and handling documents, as well as to local recruiters tasked with finding and recruiting victims by luring them with promises of high salaries overseas.

The Indonesian National Police arrested local recruiters, individuals responsible for facilitating departures, and labour placement agents. Indonesian National Police also collaborated with the Ministry of Foreign Affairs to assist in the repatriation process from Cambodia.

Source - Indonesia

Case Study # 21: Recruitments and operational costs for cyber scam hub

Indicators: alternative remittance services/hawala; fraud; financial institutions; cash; forced criminality, human trafficking and migrant smuggling

Based on the account transaction records of customers who were suspects in an alleged human trafficking crime case, it is known that there were incoming fund transfer transactions from other parties with varying nominal amounts, then these funds were transferred out to related parties with the same or almost the same nominal amount.

Based on analysis on account transaction records:

- Trafficker account had active transaction in receiving incoming and outgoing fund transactions with a transaction range of IDR100K (USD6), to IDR10M (USD 601) per transaction.
- Trafficker accounts are often used as transit points, receive frequent incoming transfers from multiple unrelated individuals, Immediate or same-day withdrawals in cash or outbound transfers to other accounts (layering).
- No saving or retention pattern; funds rarely stay longer than 24-48 hours.
- Transactions are deliberately broken into smaller amounts (e.g., under IDR10M (USD601)) to avoid bank reporting thresholds.
- Multiple small transactions from mule accounts (often victims or their associates) Into the trafficker's account.
- Use of multiple bank accounts under different names with similar activity patterns.

- Activity inconsistent with profile (e.g., domestic worker sending/receiving large overseas funds).

These illicit proceeds were typically used to pay processing fees for recruitment and to pay the recruiters and transporters, and to bribe corrupt officials involved in the trafficking chain. Operational costs such as lodging, documentation and transportation of the trafficked individuals were also covered. They were also used for lifestyle spending by syndicate members, such as to purchase luxury goods and real estate.

The identified methods for laundering the proceeds included domestic layering, use of digital payments and fintech, e-wallets and payment apps, use of nominees and mule accounts, and informal remittance systems for overseas payments. Transactions were sometimes described as "family support" or "business remittances".

Source - Indonesia

Scam proceeds

Cyber scam hubs generate revenue through fraud income, forced-labour extraction and parallel illicit services. Investment-related fraud provides high-value transfers from victims, through pig-butchering schemes, fake online trading platforms, and romantic scams. Operators of these hubs typically simulate legitimate trading activities through fabricating dashboards and falsifying profit displays, before preventing victims from withdrawing funds.[22] Hub operators obtain recurrent revenue streams like redirected payments and credential theft, through phishing-enabled account takeovers, impersonation scams and business-email compromises.[23]

Supplementary profit-making activities include operating online gambling services, monetising stolen data, and conducting recovery scams against previous victims.[24] An industrial scale of profitability can be generated through this framework of revenue streams, which allows proceeds to be reinvested into digital tools and recruitment practices to expand across jurisdictions and regions.

Respondents noted scam victims were often tricked into transferring money to a mule account, or other account controlled by the scam operation. Other noted the emergence of payments received through virtual assets. Fast or instant payment systems are also emerging as an attractive method by which to obtain proceeds from scam victims with minimal oversight and limited opportunities to prevent the transfer.

Case Study # 22: Digital payment channels for scam proceeds

Indicators: fraud; financial institutions; money value transfer services (MVTS); use of the internet

Several individual clients were investigated following the creation and submission of Unusual Activity Reports due to customer complaints, which revealed a pattern of account takeovers linked to vishing scams. Victims received fraudulent calls from individuals posing as PNB employees, offering reward point redemption or credit card benefits. Believing the calls were legitimate, victims disclosed sensitive credentials such as OTPs and online activation codes, enabling unauthorized access to their accounts.

The scammer exploits the stolen credentials to initiate unauthorized fund transfers from the victim's deposit accounts, often using digital payment channels such as InstaPay and Pesonet to move money into various accounts

The stolen funds were transferred to various digital bank accounts, such as GoTyme and Maya. It was also observed that the majority of victims targeted by this scheme were senior citizens. The perpetrators remain unidentified, and all incidents were domestic in nature. Suspicious Transaction Reports (STRs) were submitted to the Anti-Money Laundering Council (AMLC), and monitoring continues for further developments and supplementary reports will be filed if warranted.

Source - Philippines

[22] Griffin and Mei (2024), p.9.
[23] FATF (2023), p.25.
[24] UNODC, *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia* (April 2025), pp.22, 36.

There is also an emergence in the use of recovery agents as a version of advanced fee scams. Members of the cyber scam hub will pose as 'recovery agents' and contact the scam victim claiming they have already recovered their stolen funds, asking for a fee in advance to return the funds. Other examples, including Case Study 6 and Case Study 21 below, seek additional funds from victims in order to "release" previously invested funds as an additional source of illicit revenue.

Case Study # 23 Dual income scam

Indicators: use of virtual assets (cryptocurrencies or other virtual assets); transnational organised crime group; financial institutions; money value transfer services (MVTS); fraud

There are allegations of criminal acts involving fraud, embezzlement, and violations of electronic information and transactions laws, committed under the modus operandi of offering part-time or freelance job opportunities. Victims are instructed to complete various online tasks, such as liking social media accounts, and are subsequently asked to top up, deposit, or invest certain amounts of money in order to receive commissions or rewards for these tasks. However, when victims attempt to withdraw their invested funds and the promised rewards or commissions, the administrators become uncontactable, or the victims are asked to make further investments in order to release their previously invested funds.

The financial flows in this case involve several stages and entities. Initially, funds suspected to be derived from victims are transferred into bank accounts held by money mules. These accounts serve as intermediaries to obscure the connection between the victims and the perpetrators. Subsequently, the money is transferred from the money mule accounts into bank accounts controlled by the suspected perpetrators.

From the perpetrators' bank accounts, the funds are then moved into cryptocurrency accounts and used to purchase various cryptocurrencies. Once converted into crypto assets, the funds are transferred between multiple crypto wallets, employing 'pass by' methods, which involve moving funds through a series of wallets to make tracing more difficult. These wallets are often anonymous in nature, posing medium to high risks of being misused for scams or fraud.

A significant portion of the crypto assets eventually ends up in high-risk cryptocurrency exchanges, further complicating tracing and recovery efforts.

In this case, financial institutions such as banks played a role in the initial stages by receiving and transferring the illicit funds. Virtual assets and Virtual Asset Service Providers (VASPs) were then utilized to facilitate the layering process and to obscure the trail of the criminal proceeds. VASPs provided the infrastructure for buying, storing, and transferring cryptocurrencies, which enabled the perpetrators to move assets across borders quickly and anonymously, making it significantly harder for law enforcement to trace and recover the illicit funds

Source - Indonesia

Laundering of proceeds

The laundering of proceeds obtained through fraudulent cyber activities often follows a digitally initiated and high-velocity workflow. Placement of funds will often begin digitally, since most cyber scam hubs generate their revenue through online payments, virtual asset deposits and e-wallet transfers.[25] Unlike physical cash channels, funds will enter the financial system through platform accounts, such as payment service providers, platform accounts and virtual asset gateways.[26]

Operators will then obscure the origin and ownership of funds by employing rapid pass-through chains. These include merchant accounts, cross-border fintech platforms, and sequentially transferring across payment processors, with these processes often timed to exploit financial reporting windows and anti-money laundering thresholds.[27] Funds are often moved between fiat, virtual assets, e-money and stablecoins in conversion cycles, to break transactional linkages and exploit more lightly supervised sectors.[28] These flows

[25] FATF (2023), p.25.
[26] Ibid, p.21.
[27] Ibid, p.21.
[28] Ibid, p.25.

create investigative challenges and limit the opportunity for recovery, since they traverse multiple jurisdictions within minutes.

Integration will occur when these funds are challenged into 'front' companies, real estate, high-value goods or to pay operating expenses for funding new scam infrastructure.[29] Illicit proceeds that seem to support legitimate commercial activities, are often actually reinvestments into digital tooling, recruitment pipelines and expansion into additional jurisdictions. Laundering cyber scam hub proceeds through digital placement, multi-layered cross-border velocity and conversion-driven obfuscation, reduces the traceability of victim funds while allowing scale, resilience and global reach of their operations.[30]

Use of mule accounts

76% of members noted the use of mule accounts and mule networks to launder proceeds from cyber scam hubs (refer Figure 5: Primary ML typologies – public sector). These are attractive to criminal syndicates as they represent a quick and easy way to move and layer funds through the banking system. Weaknesses in CDD and KYC procedures can be readily exploited and different mule accounts can be used when existing accounts have been identified by authorities. Private sector respondents also noted the prevalence of mule accounts in relation to laundering proceeds from cyber scam hubs, with 45% of respondents including this as a primary typology.

Private sector respondents also noted the geographic displacement of these accounts as they seek to move away from heightened enforcement activities to locations in which supervisions and/or enforcement is less robust. Criminal syndicates frequently rotate bank accounts, causing the incapacity to identify transactional accounts that can be reliably traced back to specific suspects.

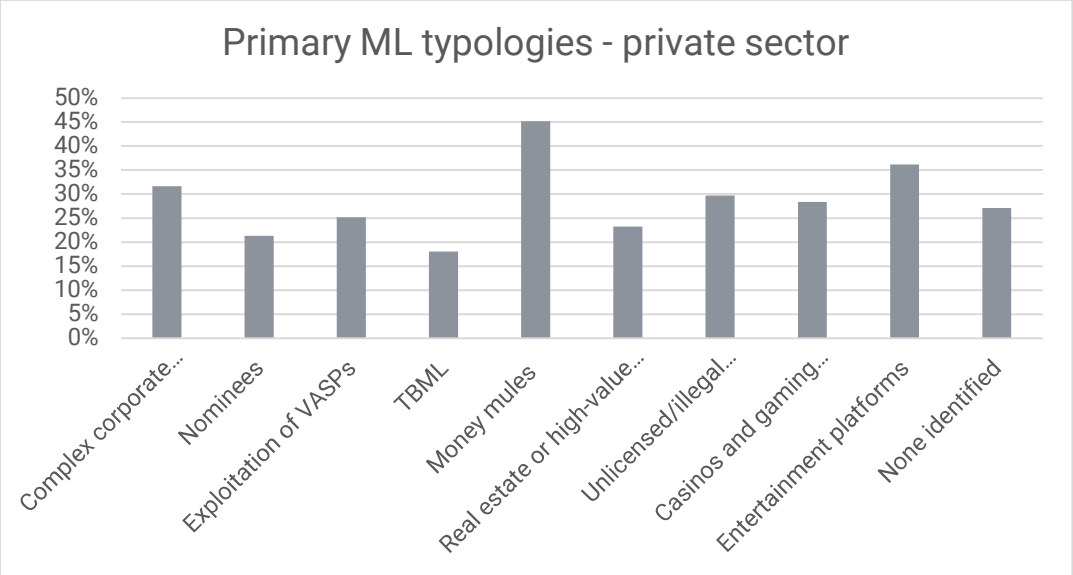


Figure 5: Primary ML typologies, Private Sector Survey

Mule account case studies

[29] GI-TOC (2025), p.29.
[30] UNODC (2025), p.22.

Case Study # 24: Cybercrime-Driven Mule Account Network

Indicators: financial institutions; fraud; money value transfer services (MVTS); use of virtual assets (cryptocurrencies or other virtual assets); wire transfer; cash; transnational organised crime group

The network channelled cyber fraud proceeds from across India into these accounts, later transferring the funds through domestic and international cryptocurrency exchanges such as Binance and DCX. Investigations confirmed that handlers located in Cambodia and other parts of Southeast Asia directed the laundering operations through encrypted messaging platforms like Telegram.

The case originated from Suspicious Transaction Reports (STRs) filed by Punjab Gramin Bank identified unusual transaction volumes in newly opened rural accounts. The reports were shared with FIU-India and subsequently forwarded to the State Cyber Crime Police for investigation.

In parallel, the I4C Financial Intelligence Module detected a cluster of mule accounts showing repetitive IMPS and UPI transactions linked to confirmed cyber fraud complaints from other states. The intersection of the STRs and I4C data confirmed that the same network of accounts was being used to layer proceeds from task-based and investment scams. A special investigation team (SIT) was constituted and raids were conducted simultaneously at Amritsar, Abohar, and Bathinda, leading to the arrest of key intermediaries involved in mule account recruitment.

The illicit funds originated from online “work-from-home” frauds, investment schemes, and digital trading scams, which promised high commissions for completing online “tasks.” Victims across India were induced to transfer small initial sums to demonstrate “earning potential.” Once lured, they were repeatedly asked to top up investment wallets, eventually resulting in complete loss of funds. These frauds were operated from Southeast Asia, with Indian mule account networks providing the domestic placement layer.

Digital forensics of seized mobile phones, passbooks, and routers revealed that the accused coordinated through Telegram groups which communicated instructions for receiving deposits and converting funds to cryptocurrency through these channels. Each Telegram group operated under a three-tier hierarchy — a handler (foreign-based), an intermediary (based in India), and account operators (mule account holders). This structure enabled compartmentalised money movement and prevented direct communication between overseas handlers and account owners.

The Punjab Gramin Bank compliance division provided vital data on account openings and KYC documents, confirming that several account holders were recruited from de-addiction centres and low-income neighbourhoods in the border districts.

Forensic audit of 312 confirmed mule accounts showed cumulative inflows of INR128.2M (~USD1.4M) between January and December 2024. The accounts typically received multiple small-value credits from victims’ accounts across 17 Indian states. Funds were quickly transferred through IMPS, NEFT, and UPI to Binance and DCX exchange wallets. Transfers were executed within 10–20 minutes of receipt, reducing detection likelihood. Each operator handled an average of 8–12 active accounts, cycling funds multiple times per day.

Telegram communications and IP logs traced by I4C established that wallet credentials were accessed from Cambodian IP ranges, confirming offshore control.

Cryptocurrency obtained from Indian mule accounts was used for funding new cyber fraud operations in Southeast Asia, P2P exchange with hawala operators for re-entry into India and limited reinvestment into small-scale real estate and vehicle purchases in border districts.

Four principal accused were arrested, with INR1.1M (~USD12K) recovered in cash and 39 debit cards, 10 SIM cards, 10 passbooks, and 10 Wi-Fi routers seized. 312 bank accounts were also frozen, pending confiscation proceedings. 2,677 victim complaints and 60 FIRs across India linked to the same laundering network.

Source - India

Case Study # 25: Multi-State Cyber Fraud and Mule Account Network

Indicators: financial institutions; fraud; money value transfer services (MVTS); use of virtual assets (cryptocurrencies or other virtual assets); wire transfer; cash; transnational organised crime group

The Cyber Crime Police Station (South), Gurugram exposed a multi-layered cyberfraud and money-laundering syndicate operating across nine Indian states, involving 28 identified individuals. The syndicate

was coordinated by [Accused #5], who maintained operational command via Telegram and WhatsApp channels with handlers located in Cambodia and Sri Lanka.

The group's primary modus operandi involved opening and controlling a large network of mule accounts across different banks to facilitate placement, layering, and withdrawal of fraud proceeds. The cumulative financial impact traced to the network amounted to INR109.8M (~USD1.2M), originating from multiple online investment and job frauds targeting Indian citizens.

The case was initially detected through the National Cybercrime Reporting Portal (NCRP), where multiple investment fraud complaints displayed overlapping beneficiary account details and contact numbers. I4C's financial intelligence fusion system flagged these accounts as part of a larger cross-state laundering network. Subsequent verification by Gurugram Cyber Police confirmed that the same set of accounts had been repeatedly used to receive funds from victims across India and were operated through identical devices and IP addresses.

The illegal funds originated from online investment fraud schemes, primarily "task-based" or "crypto-trading" investment scams promoted via WhatsApp and Telegram. Victims were approached through bulk messaging campaigns and were directed to deposit funds in multiple accounts under the guise of completing "bonus unlocking tasks." These frauds were operated by transnational groups based in Cambodia, using Indian mule networks for domestic placement.

Funds were placed into mule accounts using UPI and IMPS transfers from victims before being layered via successive intra-bank transfers, QR withdrawals, and cash deposits to obscure source trails, within 10-130 minutes of receipt. These funds were then converted to VAs using Binance and OKX wallets and via informal remittance systems (hawala), with cash movements between Gurugram, Delhi, and Jaipur hubs facilitating coordination with hawala operators managing foreign crypto-to-cash settlements in Dubai.

The laundered proceeds were utilized for crypto trading and gambling operations managed from Cambodia and Sri Lanka as well as the purchase of high-value electronic goods, vehicles, and gold within India for local integration. Banking analysis also revealed that several mule account proceeds were reinvested into new scam campaigns, indicating a cyclical reinvestment model typical of organized cyber laundering groups.

The investigation resulted in the identification of 97 FIRs nationwide linked to the same laundering pattern and the detection of 2,922 victim complaints, establishing the national spread of the operation. 28 accused were arrested across nine Indian states, with INR8.5M (~USD95K) seized in cash, along with 38 mobile phones, 91 ATM cards, and 23 passbooks.

Source - India

Case Study # 26: Cyber Crime and use of SIMs

Indicators: fraud (phone/SMS/email/social media); financial institutions; use of virtual assets (cryptocurrencies or other virtual assets); wire transfer

The mule bank accounts originating from state of Punjab used in cyber financial frauds was shared by I4C, MHA, New Delhi. The State Cyber Crime Division, Punjab had analysed the data and shared with districts for verification. During the verifications of the mule accounts, police summoned one of the mule bank account holders, who stated that accused namely MS had promised her a job and asked her to open a new bank account in her name and provide the registered mobile sim and details of bank accounts to them.

Further investigations revealed the gang allegedly supplied bank account details and mobile SIM cards to cyber fraudsters based in Philippines, facilitating online scams amounting to over INR400M (~USD4.5M). The gang exploited unemployed youth by offering them fake jobs. The accused lured victims into opening bank accounts under the pretext of salary deposits. They retained their ATM cards and net banking credentials and sold the complete access to cyber fraudsters in Philippines. These fraudsters identified, reportedly of Punjab origin but currently based in Philippines, used these accounts as mule accounts to move illicit funds derived from victims of cyber frauds across India. One of the accused also operated an unauthorized De-addiction Centre in Patiala, where drug addicts were paid INR500 (~USD6) each to purchase SIM cards in their names. These SIM cards were then hidden in folds of T-shirts and couriered to Philippines, where they were used to target Indian citizens for cyber frauds.

All SIMs were reportedly purchased from a single mobile shop apparently without any verification process. The owner of the shop has also been arrested and a diary containing details of 231 such fake SIM cards has been recovered from him which is being blocked through Samanvaya Portal by State CCPS. Further investigation is in process. The accused used to further share the mule bank account details and SIM

cards with their handlers based in Philippines. As directed by their handlers, the accused used to courier the SIM cards to Manila by hiding the SIM cards in the stitched edges of the shirts.

The commission for providing these mule accounts and SIM cards was transferred to their accounts which was withdrawn from ATMs. Interstate Linkages of the accused to find out involvement in other Cybercrime frauds are being ascertained. The investigation also revealed that eight current accounts were opened by one accused and INR30M (~USD330K) cyber fraudulent money has been transferred in these accounts. All the arrested persons opened 18 accounts in their names and used them actively to deposit the money from cyberfraud. The involvement of bank officials is going to verified in investigation.

Four persons have been arrested.

Source - India

Unlicensed/unregistered financial services providers

59% of members noted the use of illegal/unlicensed remittance systems to launder proceeds from cyber scam hubs. This includes the misuse of informal money transfer systems (hawala/hundi). 30% of private sector respondents also noted the use of unlicensed and illegal remittance systems used to launder proceeds.

Due to their unregulated nature, it was challenging for the project team to obtain detailed information on the size and scale of this sector. Information from open-source reports points towards this are being prominently abused to move funds related to cyber scam hubs and human trafficking.

Case Study # 27: Cross-border cyber laundering via cryptocurrency

Indicators: alternative remittance services/hawala; use of virtual assets (cryptocurrencies or other virtual assets); financial institutions; cash; purchase of high-value items; transnational organised crime group

This 2025 case involved a large-scale, cyber-enabled money-laundering network uncovered in the newly constituted District Didwana–Kuchaman, Rajasthan. The operation exposed a coordinated syndicate engaged in the conversion of fraud proceeds into cryptocurrency and their subsequent movement through informal value-transfer systems to foreign jurisdictions.

Funds originating from online investment and task-based frauds, in which victims were induced to make progressive “investment top-ups” to unlock artificial profits, were channelled through hundreds of mule accounts controlled by local facilitators. Withdrawals and QR based cash extractions were followed by hawala transfers to Dubai, where the amounts were reconverted into USDT.

The case originated from intelligence shared by I4C, which mapped 1,248 bank accounts showing atypical transactional patterns in Maulasar and Nawan blocks. The accounts exhibited repetitive, small-value credits followed by rapid cash withdrawals.

A joint district investigation team was constituted which correlated complaints from multiple states with these bank accounts. Field verification confirmed that deposits from victims of online task and investment scams nationwide were being funnelled into accounts opened locally under false pretexts.

Technical examination of seized mobile devices revealed Telegram and Binance wallet interactions, foreign IP logins, and USDT transactions. CCTV footage from ATMs confirmed multiple individuals conducting sequential withdrawals with different cards. Bank data indicated structured withdrawals between INR40K (~USD448) and INR100K (~USD1.1K) per card per day.

Field intelligence further established the physical collection of cash by local operators, its consolidation at a hub in Kuchaman, and subsequent movement through hawala intermediaries to Dubai. Crypto-wallet tracing confirmed that equivalent value was credited in USDT to wallets controlled by foreign handlers.

Analysis of transaction trails showed direct placement of fraud proceeds from victims into mule accounts at ICICI and PNB branches. The funds were withdrawn in cash and partly through QR transactions. Cash collected was transferred to Dubai through hawala operators, where associates converted the amounts into USDT and remitted the equivalent digital currency to Indian wallets controlled by the syndicate. The cyclical movement between India and Dubai constituted the primary laundering channel. Bank kits and debit cards were also couriered to Colombo, Sri Lanka, for remote operations by foreign handlers.

Illicit proceeds were also converted to cash for domestic purchases of vehicles, gold ornaments, and consumer goods. Evidence also indicated limited investment into real estate and gaming applications.

11 individuals were arrested across four police stations, along with the seizure of 21 ATM cards, 22 SIM cards, 10 mobile phones, cash and one vehicle.

Source - India

VA and VASPs

71% of members identified the exploitation of VASPs and cryptocurrencies as key methods to launder the proceeds of scams and cyber scam hubs. The perceived anonymity or pseudonymity of cryptocurrencies, as well as the quick and relatively inexpensive means to transfer funds across borders appeal to these criminal syndicates. 25% of private sector respondents also noted the exploitation of VASPs.

As discussed during the 2025 APG Typologies Workshop, blockchain analytics companies described how proceeds of crime from scams flow rapidly across jurisdictions, often passing through multiple layers of transactions, mixing fiat currencies and virtual assets before being cashed out, or converted into stable coins. A key observation was criminal syndicates exploit both regulatory gaps and the speed of technological innovation, which requires equally dynamic cooperation among financial authorities, law enforcement agencies and the private sector. The discussions emphasised the need for real-time information sharing, enhanced onboarding and due diligence control and faster mechanisms to freeze and recover assets, as well as the importance of harnessing technology and data analytics to identify red flags and trace layered transactions across traditional and virtual financial systems.

VA and VASP case studies

Case Study # 28: Typology of human trafficking-related financial transactions linked to online scams in Southeast Asia

Indicators: fraud; human trafficking; use of virtual assets (cryptocurrencies or other virtual assets); financial institutions; transnational organised crime group

During 2024, based on reports from the Indonesian Financial Intelligence Unit (PPATK), instances of human trafficking were identified, allegedly perpetrated by individuals suspected to be part of a transnational human trafficking syndicate associated with online scams operating in Cambodia and Lao PDR. These suspicions were based on transaction descriptions or remarks indicating activities such as the recruitment, harbouring, and transportation of human trafficking victims. The transactions involved were valued at approximately IDR141 billion (~USD8.5M).

Funds suspected to be proceeds of human trafficking in Cambodia were identified as being received through Cambodian bank accounts. These funds were subsequently used to purchase the cryptocurrency asset USDT (Tether), amounting to USD295K (~IDR4.9B) through foreign virtual asset service providers.

On the same day, a portion of the USDT was liquidated, and the proceeds in Indonesian Rupiah amounting to IDR2.6B (~USD160K), were transferred to bank accounts in Indonesia belonging to the syndicate. The transfers were conducted using a peer-to-peer method through foreign virtual asset service providers.

Source - Indonesia

Case Study # 29: International cooperation in cyber scam hub investigation involving VASPs

Indicators: fraud; virtual asset service providers (VASPs); use of virtual assets (cryptocurrencies or other virtual assets); suspicious transaction reporting; use of legal persons & arrangements (including international business companies, offshore companies or trusts, role of TCSPs); cash; international cooperation; financial institutions

The case was initially detected through suspicious transaction reports (STRs) filed by financial institutions, which flagged unusual fund flows linked to shell companies and cryptocurrency exchanges. These alerts triggered a parallel financial investigation by the Anti-Money Laundering Council (AMLC), which collaborated with the PNP Anti-Cybercrime Group and international partners such as Interpol and ASEANAPOL.

Illicit funds from cyber scam hubs were funnelled through shell companies and converted into cryptocurrency via Virtual Asset Service Providers (VASPs) often unregulated or offshore. Criminals used mixers, chain-hopping, and peer-to-peer platforms to obscure the money trail. Financial institutions flagged suspicious patterns, triggering investigations that led to asset freezes and crypto wallet tracing.

Authorities used the Anti-Trafficking in Persons Act, Cybercrime Prevention Act, and Revised Penal Code to prosecute trafficking, online fraud, and illegal detention. These laws enabled digital evidence seizure, asset freezing, and criminal charges against both local and foreign perpetrators.

Source - Philippines

Case Study # 30: Organised call centre scams linked to transnational criminal networks

Indicators: fraud (phone/SMS/email/social media); financial institutions; virtual asset service providers (VASPs); use of virtual assets (cryptocurrencies or other virtual assets); suspicious transaction reporting; international cooperation; transnational organised crime group

Between 2024 and 2025, Thailand experienced a surge in organised call-centre scams targeting domestic and international victims, often linked to transnational criminal networks. These scams involved fraudulent phone calls impersonating government agencies, law enforcement, or financial institutions to extort payments in virtual assets (VA). Perpetrators exploited commercial banks and VASPs to 7 launder illicit proceeds, particularly Bitcoin (BTC) and Tether (USDT). The Thai government, led by the Securities and Exchange Commission (SEC), Bank of Thailand (BOT), Anti-Money Laundering Office (AMLO), and Cyber Crime Investigation Bureau (CCIB), launched coordinated operations to disrupt these networks. Key agencies collaborated with international partners to trace cross-border DA flows linked to cybercrime hubs in Southeast Asia.

STRs from compliant VASPs flagged unusual transactions, including rapid BTC/USDT conversions and transfers to high-risk wallets, potentially mule account. The Central Fraud Registry (CFR), a centralized system developed to enable FIs to share and analyse suspicious transaction data, supported the linking of victims to suspects via suspicious transactions and to map connections between suspects. Blockchain analytics were also used to map transaction trails from victim's bank account to mule crypto wallets to consolidation addresses controlled by criminal networks. Joint investigations with Interpol and ASEAN counterparts revealed cross-border links to scam hubs in Cambodia and Myanmar.

Victims were coerced into paying "fines" or "taxes" transfers to bank account/wallets controlled by scammers. Funds were routed through unlicensed VASPs (e.g., offshore exchanges, P2P) to obscure origins. Funds were then split across multiple bank accounts/wallets and mixed with legitimate transactions before being converted to fiat via peer-to-peer (P2P) platforms or offshore VASPs. Non-compliant VASPs acted as intermediaries, bypassing KYC checks, with licensed VASPs inadvertently facilitating transactions due to gaps in real-time monitoring.

The illicit funds have also been used for further funding criminal networks operation e.g. gathering more mule accounts.

Over 50 arrests were made in 2024–2025, including executives of unlicensed VASPs facilitating money laundering. The CCIB recovered USD12M in crypto-assets. Strengthened VASP licensing checks, including of transaction monitoring systems and mule account prevention, have also been implemented to prevent future fraudulent activities.

Source - Thailand

Further analysis of the use of VA/VASPs to launder the proceeds of cyber scams have identified vulnerabilities including VA layering, Peer-to-Peer (P2P) transfers and Over-the-Counter (OTC) brokers[31], as well as deposits into crypto ATMs. These mechanisms are often subject to less supervision and oversight and present challenges to tracing illicit proceeds.

[31] John M Griffin and Kevin Mei, '*How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering*' (SSRN, 29 February 2024), p.19.

OTC case studies

Case Study # 31: 2,700 individuals rescued from cyber scam hub in POGO compound

Indicators: fraud (phone/SMS/email/social media); forced criminality, human trafficking and migrant smuggling; financial institutions; casinos, gambling houses; virtual asset service providers (VASPs); use of virtual assets (cryptocurrencies or other virtual assets); alternative remittance services/hawala; use of legal persons and arrangements; role of TCSPs; cash; purchase of high-value items; transnational organised crime group

Human trafficking complaints filed by survivors and concerned citizens were first routed through the DOJ's hotline, which raised red flags about foreign nationals being forcibly employed within a POGO compound in Las Piñas. Intelligence from migrant workers and embassy channels also supported the case, confirming that several individuals were trafficked from Cambodia, Vietnam, and other ASEAN jurisdictions under false pretences.

Trafficked individuals were coerced into conducting a variety of scams under the direction of syndicates linked to the XC firm and its affiliates. Scammed victims abroad remitted funds via international wire transfers to Philippine-based shell corporations and personal accounts opened using fraudulent or rented identities, or through virtual assets such as USDT and BTC.

Local e-money wallets (e.g., GCash, PayMaya) were used as pass-through accounts for laundering low-value scam receipts from unwitting local or foreign individuals. In addition, VAs were stored in cold wallets, used in peer-to-peer (P2P) transactions, and laundered via exchanges and mixers. Blockchain forensic tools revealed layering techniques such as wallet hopping and splitting into microtransactions. Some funds were also routed through online gaming platforms linked to the POGO license, masking illicit revenues as gambling winnings. These illicit proceeds were often converted to cash with large volumes of cash proceeds were stored in vaults on-site. These were used to pay wages, launder profits through local real estate, or were transported via cash couriers.

STRs submitted to the Anti-Money Laundering Council (AMLC) by financial institutions further validated the existence of unusual inflows and cash withdrawals tied to individuals and shell companies linked to XC. Parallel financial intelligence received through informal exchanges with foreign counterparts (particularly China and Chinese Taipei) helped confirm that the individuals operating the hub had existing red flags or arrest warrants abroad.

Search Warrants and Inspection Orders were obtained by law enforcement and the Anti-Cybercrime Group (PNP-ACG) used digital forensic tools to mirror and recover data from over hundreds of confiscated devices, including computers and cryptocurrency wallets. Asset tracing tools were employed by AMLC to freeze connected accounts and follow the money trail. These included in-house blockchain analytics, bank coordination, and issuance of freeze orders.

In June 2023, over 2,700 individuals—Filipino and foreign—were rescued; operations dismantled at a compound linked to POGO firm XC. PAGCOR's licensing oversight powers were invoked to suspend and order the closure of XC's POGO license, cutting its legal operations link. The Department of Justice recommended human trafficking, cyber fraud, and immigration charges against the operators, while AMLC initiated civil forfeiture proceedings on suspected laundered assets.

Source - Philippines

Case Study # 32: Laundering of proceeds from cyber scam hub and human trafficking using virtual assets

Indicators: fraud (investment fraud; phone/SMS/email/social media); financial institutions; virtual asset service providers (VASPs); use of virtual assets (cryptocurrencies or other virtual assets); purchase of high-value items; transnational organised crime group

In 2022, a large number of victim family members reported to the police, claiming their relatives had been lured abroad and subsequently went missing or requested help. The victims were trafficked to jurisdictions such as Cambodia under the pretence of "high-paying job offers," and then forced to engage in cyber scams, including investment scams and romance scams. These scam hubs not only extorted money from victims but also subjected the trafficked Chinese Taipei individuals to inhumane treatment. These reports served as the initial trigger for the case. This was in addition to extensive media attention and reporting on cyber scam hubs in Cambodia which raised public concern and prompted swift response from the government and law enforcement agencies.

While investigating cases of human trafficking and fraud, law enforcement simultaneously monitored and analysed the bank accounts and virtual asset transactions of suspects, uncovering money laundering activities through financial flow analysis. Law enforcement agencies used blockchain analytics to trace virtual asset transactions, identify wallet addresses linked to criminal proceeds, and uncover the movement of funds across multiple platforms and jurisdictions. This enabled the identification of laundering patterns, the linkage between victims and perpetrators, and the detection of cryptocurrency conversion points.

The syndicate perpetrated a variety of scams, including romance and investment scams, through social media and messaging apps, as well as more traditional phone call and text message techniques Scam victims transferred funds into bank accounts or virtual asset wallets designated by the scam syndicate.

Victims, following the instructions of the scam syndicate, transferred fiat currency into domestic mule bank accounts. The syndicate then swiftly converted fiat in mule accounts into virtual assets through both VASPS and OTCs into USDT or ETH. After acquiring virtual assets, the syndicate moved the assets quickly and frequently through dozens or even hundreds of cryptocurrency wallets, VASPs, and from one blockchain to another, increasing the difficulty of tracing. Some syndicates also used mixers to combine transactions and obscure flows, or converted assets into high-anonymity coins like Monero or Zcash.

Eventually, the laundered virtual assets were converted back to fiat for use by criminal syndicate members through exchange for local fiat through lightly regulated overseas VASPs mad wired to overseas mule accounts for withdrawal. Some funds were repatriated to Chinese Taipei and converted back into local fiat currency through domestic OTC brokers or mules for withdrawal, or to purchase high-value goods—such as real estate, luxury vehicles, and designer goods—to further obscure the source of funds.

The syndicate also used the scam proceeds to cover operational costs (such as server room rentals, transport costs for trafficked individuals and internet infrastructure) and the payment or compensation for the use of mule accounts.

Prosecutors filed charges against dozens of syndicate members involved in human trafficking, fraud, money laundering, and organised crime. Several cases have proceeded to trial or judgment, with multiple defendants convicted and sentenced.

Authorities successfully froze and seized tens of millions of TWD from bank accounts, confiscated physical assets such as vehicles and luxury goods, and some VAs were also frozen with the assistance of VASPs, with the total seized amount still being calculated. Several hundred people were also repatriated to Chinese Taipei and extensive media coverage and government awareness campaigns have significantly raised public awareness in Chinese Taipei regarding overseas scam and human trafficking, thereby reducing victimization rates.

Source - Chinese Taipei

Case Study # 33: Investment scam proceeds moved through crypto ATMs

Indicators: fraud (investment fraud); financial institutions; currency exchange/cash conversion; use of virtual assets (cryptocurrencies or other virtual assets); cash

Australian law enforcement agencies and the FIU (AUSTRAC) have identified investment scam (pig butchering) proceeds which are laundered through cash deposits to crypto ATMs. This is done in order to navigate existing controls in place within banks which are designed to prevent scam proceeds being transferred to VASPs.

A common methodology includes a bank customer being scammed and convinced to invest in cryptocurrency. The scammer convinces the customer to withdraw their personal wealth in the form of cash, which is then deposited into a cryptocurrency account operated by the offender through a crypto ATM. The offender then moves these funds through other cryptocurrency channels.

Source - Australia

Law enforcement responses

There have been a number of successful law enforcement investigations and the dismantling of cyber scam hubs across the Asia/Pacific region. However, these efforts have identified a number of challenges in successfully identifying, investigating and prosecuting those ultimately responsible for these cyber scam hubs.

Challenges with international cooperation

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

Figure 6: Investigation and prosecution challenges, Public Sector Survey

There are particular challenges in sharing information with jurisdictions who may not reciprocate or share details of the outcomes of investigations where international cooperation has been involved. Restrictions on sharing information with jurisdictions who enforce capital punishment may also limit the ability for law enforcement agencies to cooperate internationally. This may lead to separate, smaller investigations within a jurisdiction rather than coordinated efforts internationally to dismantle the entire criminal network involved.

Noting the figures from members that most operations are identified by victim reports, these are often taken as a single report in one jurisdiction. Where there are weak domestic and international cooperation and coordination mechanisms in place, law enforcement agencies may be failing to identify the wider network of offending without piecing all the victim reports together, leaving many more victims without the help and support they need.

Asset recovery

The majority of respondents were unable to provide an estimate of the total value of assets linked to cyber scam hubs and human trafficking laundered in their jurisdictions. This was largely due to the nature of record-keeping and statistics which does not differentiate cyber scam hubs separate to fraud.

Only two jurisdictions (12% of respondents) considered themselves successful in tracing and seizing proceeds laundered from cyber scam hubs in their jurisdiction or from foreign jurisdictions.

Confiscating assets was hampered by the use of virtual assets and challenges with international cooperation. Members also noted the use of foreign nominees and front companies were also challenges to the successful confiscation of laundered proceeds.

The use of various asset tracing, recovery and management tools to deprive criminal syndicates from the proceeds of their crimes requires further development across the Asia/Pacific region and beyond. It is clear that these tools are not being used to their full potential, further fuelling the ongoing growth of these cyber scam hubs and associated criminal activities.

Limited expertise in cryptocurrency investigations/tracing

As noted in Figure 6 above, 71% of members surveyed noted tracing illicit funds through virtual asset service providers and cryptocurrencies was a primary challenge in investigating and prosecuting ML cases linked to cyber scam hubs. A lack of specialised expertise in relation to cyber-enabled fraud and scam was also noted as a key challenges by 65% of member respondents.

Given the identified use of VA/VASPs in the laundering of proceeds from these crimes, the absence of strong regulatory frameworks for VASPs, and insufficient expertise of law enforcement officials or access to blockchain analytics tools are areas of critical concern.

Best practices / lessons learned

Members surveyed identified a number of good practices for detecting and disrupting money laundering / financial crime associated with cyber scam hubs and human trafficking. These practices were closely aligned to and in most cases depend on the identification of the red flags and patterns identified in Appendix A. The most common theme was that the detection and disruption of these crimes and their growing prevalence will benefit from analysts in competent authorities including LEAs who are specifically assigned to these crimes so that skill sets can be developed and evolve over time.

Professional, holistic financial analysis expertise and continuous professional development

Members noted FIUs should conduct expansive network mapping by integrating data from multiple reporting entities, continuously expanding analysis of involved entities and transactions to reconstruct full fund flow pathways and uncover hidden syndicate structures. This network mapping should incorporate device and location-based data, such as IP/MAC addresses, as well as open-source, social media and taxation information.

Continuous professional development of AML compliance staff in the private sector, and the training of FIU and law enforcement staff is crucial. Trained and knowledgeable staff who are informed on emerging techniques and trends will be better placed to identify suspicious activity. FIU and law enforcement staff trained in sophisticated network analysis, blockchain analysis and forensic wallet tracking is essential to keep pace with evolving laundering methods.

Enhanced, rapid and specific domestic interagency coordination mechanisms or task forces and analytical infrastructure

Multi-agency collaboration supporting the investigation of funds transfers, integrating financial intelligence and other information to establish comprehensive evidence chains is also critical. Successful operations against these criminal syndicates have involved information-sharing amount FIUs and government agencies, including cyber intelligence, at the intelligence-gathering stage and resulted in rapid asset tracing to aid seizure and confiscation efforts. Centralised intelligence platforms may also add value by aggregating and analysing fragmented financial and digital data.

Members also noted national policy responses that jointly address cyber scam hubs, money laundering and human trafficking/forced criminality, based on strong victim-centred safeguards are key. This involves integrating anti-human trafficking and victim support services with AML/CFT agencies for a comprehensive prevention and response mechanism. Extending to civil society organisations and academia can also broaden the scope of available information and resources to combat these crimes.

Some members noted the successes of developing “Anti-Scam Centres” as a focal point for coordinating domestic responses to scams and fraud. These centres may also involve representatives from the private sector and support public-private partnerships (PPPs).

Figure 7: Anti-scam centres

Australia coordinates efforts through initiatives such as the National Anti-Scam Centre and multi-agency taskforces such as Operation Firestorm (see Case Study 5) and collaborative frameworks like the Joint Policing Cybercrime Coordination Centre. The National Anti-Scam Centre is a multi-agency initiative involving the Australian Competition and Consumer Commission, the Australian Federal Police, and other partners, whose purpose is to detect, investigate, and disrupt scams, share intelligence and develop proactive measures.

Indonesia's Financial Services Authority (OJK) conducts an Indonesia Anti-Scam Center (IASC) and Satgas PASTI (Task Force for the Eradication of Illegal Financial Activities). These entities integrate data from the banking sector, payment service providers, and e-commerce platforms to trace financial transactions related to scams.

Singapore established the Anti-Scam Centre in June 2019 which serves as a nerve centre to facilitate swift tracing of funds and disruption of illicit flows through the financial system. Through the Anti-Scam Centre, private sector stakeholders such as banks work with the Singapore Police Force to coordinate real time disruption and freezing of funds..

Effective international cooperation which facilitates extremely quick responsiveness from multiple authorities – including non-AML/CFT competent authorities such as those which are mandated to address the victims of human trafficking

Cross-border coordination regional cooperation must evolve alongside domestic frameworks to counter transnational scam networks exploiting jurisdictional gaps. This international cooperation should support timely sharing of information and joint investigative actions. Taking a victim-centred approach and engaging non-traditional partners to combat the human trafficking associated with cyber scam hubs has also been beneficial in minimising future harm and protecting the vulnerable in the community.

Improving and supporting both domestic coordination and international cooperation requires strong political commitment. Raising political awareness of the impact of cyber scam hubs and human trafficking, and harnessing political will is key to giving the members' competent authorities the support, tools and funding they need to effectively address this crime type and work collaboratively across borders.

Enhanced public private partnerships (PPPs)

Leveraging PPPs, and private-private partnerships, can also prompt more timely and targeted suspicious transaction report generation by reporting entity staff. This builds on the effective use of red flag indicator communications across reporting entities both within and across jurisdictions.

These PPPs can also assist reporting entities conduct enhanced transaction pattern monitoring, define "unusual" customer log-in patterns, apply a dynamic and risk-based approach to customer reviews and link behavioural data with transaction data. These activities can flag critical early warning signs to detect anomalies and trigger appropriate actions by FIUs and law enforcement agencies.

Dedicated awareness raising campaigns

National awareness campaigns and outreach to educate the public on recognising scam tactics are another aspect of preventing these crimes from occurring in the first place. This public outreach should be conducted regularly to increase awareness in relation with cyber scams and include real examples of deepfake, social engineering campaigns, and fake cryptocurrency platforms. Key messages can include verifying company registration information with regulatory bodies and checking the legitimacy of website and platforms before sending money. An increase in public awareness will assist in preventing members of the public falling victim to scams and work alongside law enforcement efforts to dismantle cyber scam hubs.

Enhanced due diligence measures

Sharing the red flag indicators (see Appendix A) and emerging trends and typologies related to cyber scam hubs and human trafficking should also direct reporting entities to undertake enhanced due diligence (EDD) measures when red flags are identified. These measures may include:

- Defining "unusual" customer IP login and device ID patterns based on customer due diligence profiles and volume and timeframe of logins from high-risk jurisdiction with scam centres for monitoring.
- Enhanced transaction pattern monitoring, including being tailored for particular transaction patterns associated with cyber scams, such as rapid fund movements across multiple accounts
- Proactive escalation and investigation of high-risk activities even without customer cooperation
- Applying a dynamic, risk-based approach during customer reviews, especially when customer behaviour deviates from expected norms.
- Conducting video calls to confirm identities.
- Incorporating digital footprint data in monitoring and controls

Implement any necessary changes to legislation or national institutional framework to ensure it is suited to respond to the nature of cyber scam hubs.

Jurisdictions with higher levels of 'legislative agility' are able to more effectively amend legislation to address technology-enabled crime, or to implement technology-neutral legislation with a broad application. This is particularly useful in harmonising fiat and virtual assets oversight, implementation of the Travel Rule, and the application of both AML and anti-trafficking laws for a holistic response targeting both financial crimes and human rights violations.

Conclusion and Next Steps

The findings from this project highlight the complexity, adaptability, and transnational nature of cyber scam hubs and human trafficking, particularly in the Asia/Pacific region. These criminal syndicates exploit sophisticated financial channels, opaque legal structures, emerging technologies, regulatory gaps, and corruption to maintain and expand operations. Effective mitigation of these evolving crime type requires continued monitoring, enhanced regional cooperation, targeted intelligence sharing, and the strengthening of AML/CFT frameworks across jurisdictions. These measures are critical to disrupt cyber scam hubs, protect victims, and safeguard the integrity of financial systems against highly organised, technologically enabled criminal syndicates.

The emerging decentralisation and use of AI demonstrate increasing operational sophistication that enables these criminal syndicates to scale activities while minimizing the risk of detection and legal accountability and requires further research. These are issues which have a far greater impact beyond the Asia/Pacific region with the reach of these cyber scam hubs, and their victims of both scams and human trafficking, found all over the world.

Continued research and enhanced understanding of the evolving methods used to perpetrate these crimes

It is clear that the operations of cyber scam hubs and associated human trafficking continue to evolve and adapt. Research should continue on these crimes as well as ongoing sharing of experiences across agencies, jurisdictions and other relevant stakeholders. In particular, enhancing understanding of emerging issues such as dissipation, decentralisation and the use of artificial intelligence (AI) is needed to inform ongoing policy responses and operational outcomes.

The review of existing literature identified the dissipation of scam centre compounds, particularly following law enforcement raids and dismantling of existing cyber scam hubs. As coordinated efforts take place in focus areas of Southeast Asia organised criminal syndicates are relocating their activities two areas where they may be subject to reduced scrutiny. This also includes reducing the scale of operations and decentralising units so as to further avoid detection. There have been observations by members and media reports of these hubs dissipating into smaller operations, using hotel rooms, private residences, vacation rentals, or entire floors of commercial buildings across South Asia and other areas of the world.

Cyber scam hubs are increasingly adopting decentralisation strategies to mitigate detection and disruption by law enforcement and regulatory authorities. In practice, this approach involves fragmenting large-scale operations into smaller, mobile units and relocating them across different areas within cities or regions. By dispersing their activities, criminal syndicates are able to obscure operational footprints, complicate investigative efforts, and minimise the risk of large-scale enforcement actions. 35% of APG member jurisdictions surveyed reported encountering or being aware of instances of decentralisation, highlighting its growing prevalence as a strategic adaptation of cyber scam hubs.

The current operating models of cyber scam hubs already use a high degree of division of labour, with many actors within these hubs kept separate from each other. This model is easily adapted for dissipations as these various units within the enterprise can be relocated and operate in even smaller teams across a number of jurisdictions to avoid detection.

AI plays an increasing role in cyber scams by enabling perpetrators to target victims more efficiently through automated, personalised messaging, using predictive algorithms for potential scam victims, and even deepfake technology to manipulate or deceive individuals. Generative AI is evolving quickly and will likely change how these cyber scam hubs will operate, their scope and scale, and create new opportunities to make illicit proceeds into the future. AI automation also minimises the number of human operators necessary to run

scam operations, potentially altering the human trafficking economics for these operations (and requiring fewer, or different, forced operatives).

Members have already identified a number of ways in which AI is, or could be, used to enhance the operations of cyber scam hubs, and human trafficking, including across the following areas:

- Technical instrumentalization - Deepfakes (for impersonation), voice cloning, chatbots and large language models (LLMs) can be used to increase scale without increasing human labour, and broaden reach to victims, in different languages and across borders. This technology can also be used to perpetrate employment scams to continue to tap into the pipeline of trafficked individuals for forced criminality in these cyber scam hubs. 82% of members have identified the use of deepfakes, and 59% identified the use of voice cloning for these scams (see Figure 8 below).
- Process automation - AI programs can also be programmed to automate repetitive tasks and reduce the level of human intervention to interact rapidly in real time (e.g., chatbots can be programmed to dedicate as much time as possible to build a relationship over an extended period of time to build trust). Chatbots, or AI-generated responses were identified by 65% of members surveyed (see Figure 8 below).
- Large-scale expansion – AI can be used to expand scam operations, improve the efficiency and profits of these scams, as well diversify into other technology-enabled crimes. The increase in "digital-crime-as-a-service" is also being observed, with 24/7 support and even door-to-door services for cyber scam hubs.

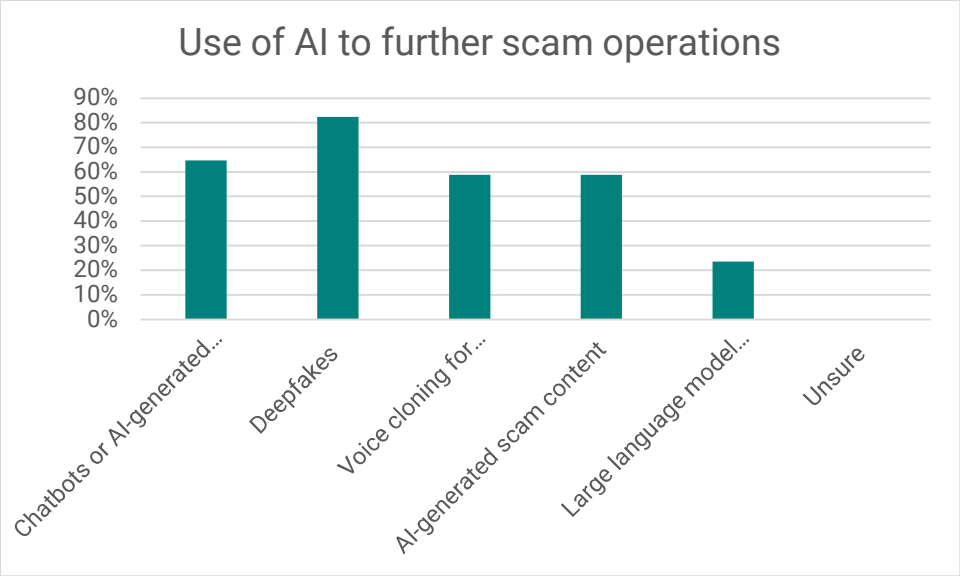


Figure 8: Use of AI to further scam operations, Public Sector Survey

Further engagement with civil society and NGOs

Civil society organisations and NGOs play a pivotal role in identifying and supporting victims of human trafficking and cyber scam hubs. These organisations can assist both in the prevention and detection of these crimes, as well as supporting victim restitution. Further engaging with civil society and NGOs will broaden the understanding of these crimes from a victim perspective and contribute to holistic human rights-based responses. This is already occurring across the APG membership, with 59% of APG members surveyed noting their law enforcement agencies liaise with civil society organisations/academia and their information holdings when addressing this crime type, with a further 12% noting this was under consideration.

References

Financial Action Task Force; INTERPOL; Egmont Group, *Illicit Financial Flows from Cyber-Enabled Fraud* (FATF, November 2023).

Gargi Sarkar and Sandeep K Shukla, 'Bi-Directional Exploitation of Human Trafficking Victims: Both Targets and Perpetrators in Cybercrime' (online first 21 May 2024) *Journal of Human Trafficking* <https://doi.org/10.1080/23322705.2024.2353015>.

INTERPOL, *Crime Trend Update: Human Trafficking-Fueled Scam Centres — Online Scams and Human Trafficking: A Double-Edged Crime Threat with Two Types of Victims* (INTERPOL, June 2025).

John M Griffin and Kevin Mei, 'How Do Crypto Flows Finance Slavery? The Economics of Pig Butchering' (SSRN Working Paper, 29 February 2024) <https://ssrn.com/abstract=4742235>.

Kristina Amerhauser and Audrey Thill, *The Business of Exploitation: The Economics of Cyber Scam Operations in Southeast Asia* (Global Initiative Against Transnational Organized Crime, August 2025).

Michael Schidlow, 'Forced Fraud: The Financial Exploitation of Human Trafficking Victims' (2025) 14 *Social Sciences* 398. *(Published 23 June 2025).*

Mina Chiang and Sharlene Chen, *HRC Briefing: Cyber-Slavery in the Scamming Compounds* (Humanity Research Consultancy, 7 September 2022; rev 12 September 2022).

Nathan Ruser, *Scamland Myanmar: How Conflict and Crime Syndicates Built a Global Fraud Industry* (Australian Strategic Policy Institute, September 2025).

The Mekong Club, *From Fake Job Ads to Human Trafficking: The Horrifying Reality of the Human Trafficking Scam Trade* (The Mekong Club, 2023).

United Nations Office on Drugs and Crime (UNODC), *Casinos, Cyber Fraud, and Trafficking in Persons for Forced Criminality in Southeast Asia — Policy Report* (UNODC Regional Office for Southeast Asia and the Pacific, September 2023).

United Nations Office on Drugs and Crime (UNODC), *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia* (UNODC, April 2025).

United Nations Office on Drugs and Crime (UNODC), *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape — Technical Policy Brief* (UNODC, October 2024).

United States Institute of Peace (USIP), *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security* (United States Institute of Peace, May 2024).

Yen Zhi Yi, 'Safeguarding Singapore: Addressing the Impact of Transnational Scamming Operations in Southeast Asia' (RSIS Commentary No 154, 15 July 2025) (S. Rajaratnam School of International Studies, Nanyang Technological University).

List of Case Studies

List of Figures

List of Indicators

References to numbers against indexed terms relate to **case study numbers** across this report.

Acronyms

AI	Artificial Intelligence
AML	Anti-Money Laundering
ATM	Automatic Teller Machine
BO	Beneficial Ownership
CDD	Customer Due Diligence
DNFBPs	Designated Non-Financial Businesses and Professionals
EDD	Enhanced Due Diligence
FIU	Financial Intelligence Unit
ML	Money Laundering
OTP	One-Time Password
OTC	Over the Counter
P2P	Peer to Peer
POGO	Philippine Offshore Gaming Operator
POI	Person of Interest
PEP	Politically Exposed Person
STR	Suspicious Transaction Report
TBML	Trade-Based Money Laundering
UNODC	United Nations Office on Drugs and Crime
VA	Virtual Asset
VASP	Virtual Asset Service Provider

Appendix A: Red Flag Indicators

Cyber scam hubs and associated human trafficking produce **clear recruitment, social media, financial and geo-spatial patterns**. These patterns can be used as red flag indicators by the public and private sectors. The effectiveness of using red flags to disrupt cyber scam hubs and human trafficking will be greatly increased when all relevant AML/CFT authorities understand cyber scam hubs risk factors and the red flag indicators, which means the government plays a central role in communicating the indicators and how to use them. In some cases – the whole of government approach would go beyond AML/CFT competent authorities to include communications, power, transportation and provincial and municipal authorities.

Effectiveness will increase when there is **close partnership with the private sector** (bank and non bank financial institutions, money service providers and other payment service providers, cellular data service providers and social media providers in accordance with relevant domestic legislation) in the private sector are working in partnership.

Similarly, effectiveness will be increased with close **international cooperation in the sharing of information on risks and red flags.** The survey results showed similar patterns across jurisdictions, indicating that red flags will greatly benefit a robustly coordinated international approach.

The above describes areas where urgent action is need. According to survey resulta **overall, the provision of specific guidance and red flags to both frontline officers and reporting entities was low.**

When surveyed on whether they had issued specific guidance or red flag indicators to frontline officers regarding the human trafficking risks associated with cyber scam hubs, 35% of members had issued comprehensive and updated guidance/indicators, 18% had issued some general guidance that covers these risks exists while 35% of members had not or were unsure (note: not all members answered this question).

Further, when surveyed on whether they had issued specific guidance or red flag indicators to financial institutions and other reporting entities regarding ML/TF risks associated with cyber scam hubs and human trafficking, 18% of members had issued comprehensive and updated guidance/indicators, 41% had issued some general guidance that covers these risks exists, 6% had guidance planned or under development, while 35% had not, were unsure or had only issued general guidance and/or red flag indicators related to scams more broadly.

Largely because cyber scam centres require a large volume of travel and a large amount of equipment and human capital, the use of red flag indicators could make disruption operations highly successful. Members noted several high-level categories of red flag indicators with cyber scam hubs and human trafficking.

(I) Non – Financial Indicators

When surveyed on what the non-financial indicators or patterns that trigger a suspicion of a cyber scam hub, members noted that non – financial red – flag indicators such as internet usage, delivery of food, virtual private networks (VPNs), electricity consumption and the purchase of technical assets were valuable, notably in the establishment of financial, geographic and operational patterns and timelines.

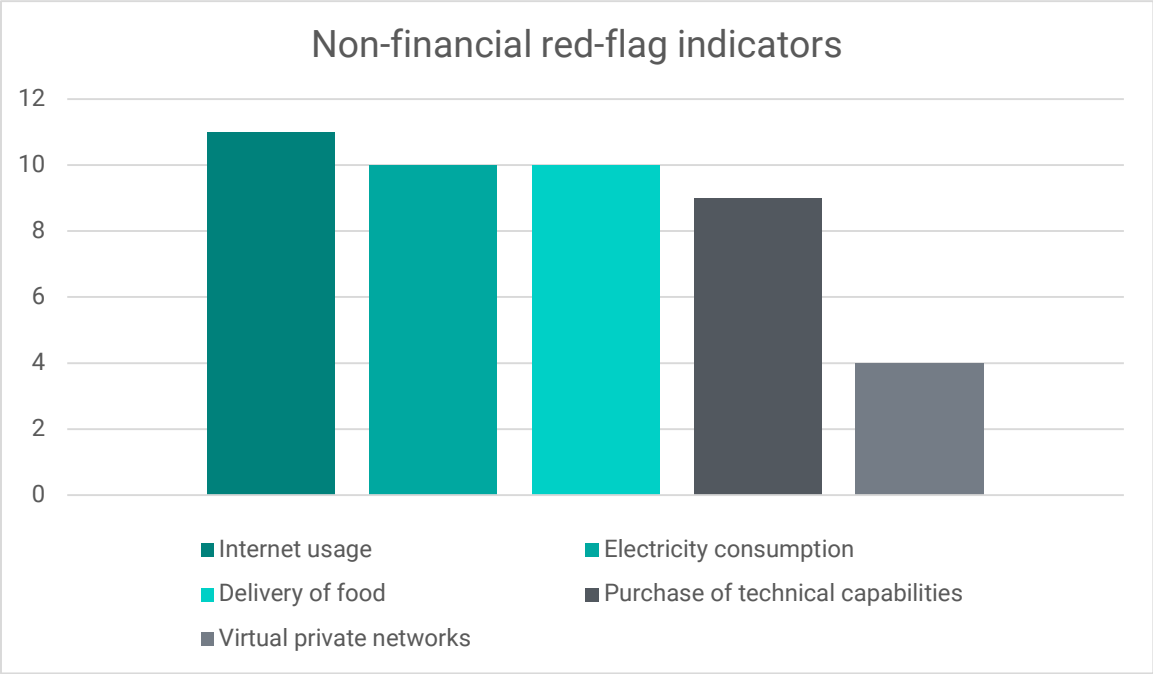


Figure 9: Non-financial red-flag indicators, Public Sector Survey

Recruitment red flags were mentioned often. These included: Unrealistic job offers (promise of unusually high salaries, for minimal qualifications), unrealistic investment schemes (promise of unrealistic high return); requests for passport or ID documents before formal hiring; high levels of recruitment from high-poverty or disaster-affected regions; recruitment of university graduates for low-skill positions; offer/advertisement / recruitment of IT/customer service job functions for high levels of remuneration; an emphasis on or requirement for language skills for non-language focused roles; suspicious online profiles with limited history (when victims search recruiters); recruitment from high-poverty or disaster-affected regions and immediate hiring without proper interviews or verification. Finally, the communication pattern is unusual with perpetrators manipulating the victims through patterns which emphasise the victims need to act quickly. A common pattern is that firstly, victims received unsolicited contact from the perpetrators and the victims are then forced to act quickly to comply with the demand from the perpetrators. Can also be the provision of transportation and air fare and movement of labour from a main airport (international) to transport by road or boat to neighbouring country and the removal of travel documents from new recruits.

Operational and geo-spatial red flags were frequently mentioned: These included: compounds with high security, barbed wire, and armed guards; former hotels or casinos converted to residential facilities; large groups of foreign nationals living in confined spaces; facilities operating 24/7 with unusual power and activity patterns; a high volume of electronic equipment deliveries; unusual internet usage patterns (high bandwidth at odd hours); workers never seen leaving facilities; complete lack of human presence despite large staff and finally, large facilities with these characteristics located in SEZs or border regions. Specifically, increased activity in porous border between countries which takes advantage of the : weak law enforcement (sometimes weak reach of government agencies or authority in general), lack of neighbouring populations,

Red flags associated with places / types of places were: the business is located at a high-risk area for gambling and modern slavery, e.g. the Golden Triangle SEZ, and the Clark Free Port Zone; the business operates in the red flag areas of the city, particularly big warehouses where camps can be located and compounds which have or receive large amounts of technical equipment which does not match the business purpose.

Figure 10: Non-financial indicators noted by members

Hong Kong, China noted that information from management offices and owner's associations could be useful when mapped to other indicators.

New Zealand noted that domain name registration and URLs embedded into scam messages traced back to IP addresses originating from western countries, as well as the use of use of SMS proxy servers provided useful information for the establishment of patterns. In addition, New Zealand noted the tracing of SIM card activations occurring outside of New Zealand and scam messages being sent from New Zealand numbers originating outside of New Zealand (international roaming SIM/e-SIMS) were also used as non-financial indicators, as did international phone numbers sending scam messages to New Zealand based phone numbers.

Pakistan noted high staff movement at odd hours (workers entering/exiting residential apartments at night), unlicensed call centres / IT setups in urban flats, and multiple complaints from victims tied to the same phone numbers, apps, or IP ranges were all used to trace illegal activity.

Philippines also noted that technical equipment, capabilities/assets and volume of foreign IT employees as valuable non-financial indicators. In addition, they noted the prevalence of shuttle vans transporting people (usually of foreign origin) from condominium units/staff houses to office spaces. They note the example of a facilitator in a government one-stop shop that assists foreigners in getting Philippine Statistics Authority birth certificates, Philippine National Police clearance, Taxpayer Identification numbers, etc. found tied to facilitating cyber scam centre associated travel and requirements.

Singapore noted datapoints linked to internet banking accounts used for laundering scam proceeds, including IP addresses (and associated geo-location) as well as device IDs.

(II) Financial Indicators

Financial red flags are prevalent in cyber scam hubs and human trafficking and can be flagged to reporting entities and used most effectively in combination with non-financial red flags – indicating that disrupting cyber scam hubs can most effectively be undertaken with government and the private sector working in partnership. Some of the most prevalent are:

- high volumes of cryptocurrency transactions;
- multiple conversions between different cryptocurrencies;
- structured transactions just below reporting thresholds;
- high-value transactions with no clear business purpose;
- money transfers to/from high-risk jurisdictions;
- unusual patterns of withdrawals following victim payments;
- companies with limited legitimate business activity (denoting front companies); and
- payments to PEPs.

(III) Financial Indicators related to Cryptocurrencies

The prevalent use of cryptocurrencies, and the use of blockchain technologies in these currencies, means that multiple red flag indicators can be identified and used by the public and private sectors. **Blockchain analytics companies** shared the following patterns / red flag indicators:

- High-risk scam flows often involve transactional patterns where multiple unrelated retail wallets send funds to the same small set of intermediary or "aggregator" wallets within short timeframes, whereas legitimate high-volume flows usually originate from a smaller number of known institutional or corporate counterparties.
- Scam-related transactions frequently show immediate conversion from fiat into stablecoins, followed by rapid transfer to offshore or high-risk exchanges, while legitimate high-volume activity often maintains funds on regulated platforms for trading or treasury purposes.

- Accounts linked to scam flows may share device fingerprints, IP geolocation data, or behavioural patterns that suggest operation from centralised call-centre facilities in known scam hub jurisdictions, whereas legitimate users typically exhibit diverse device and location profiles.
- Scam flows often use cross-chain bridges, mixers, or privacy coins within hours of receiving funds, whereas legitimate high-volume trading activity rarely incorporates these obfuscation tools unless tied to specialised privacy-oriented services.
- In scam typologies, there is often a mismatch between the stated business or personal profile of the account holder and the nature or scale of transaction activity, while legitimate high-volume accounts generally have verifiable business operations and transaction histories consistent with their stated purpose.
- Scam flows often involve counterparties or intermediaries flagged on law enforcement or industry watchlists for association with cyber scams, human trafficking, or other illicit activity, whereas legitimate flows more often involve counterparties in regulated markets.
- Scam-linked accounts may show repeated inbound transfers from newly created wallets with little or no transaction history, while legitimate high-volume activity tends to involve counterparties with long and traceable operational histories.
- Scam-related accounts often lack supporting documentation for large transactions, or provide inconsistent or unverifiable KYC/KYB information, whereas legitimate accounts provide complete and verifiable records.
- Transaction velocity in scam flows is often unusually high — with multiple large transactions occurring within short periods and without apparent market-driven justification — whereas legitimate flows tend to be aligned with trading cycles, market events, or predictable business schedules.
- Scam-linked accounts frequently cash out through OTC brokers or unlicensed exchanges in jurisdictions with weak AML/CFT controls, while legitimate high-volume actors generally use licensed exchanges or institutional payment channels.

(IV) Patterns related to cyber scam hubs noted in survey responses

(i) Business size vs budget and other operating discrepancies:

- businesses with a disproportionate budget for wages relative to their size, indicating that employees are being paid low wages;
- for businesses covering living costs or providing dormitories for the employees, the allocated budget for necessities such as medical expenses, food, and other essentials is very low.

(ii) frequency, volume, size and type of financial transactions:

- structured remittances just below reporting thresholds sent to multiple recipients in countries known for cyber scam operations
- use of third-party payment processors to wire funds, especially when the true originator or true beneficiary is being hidden, is a substantial red flag for possible involvement in cyber scam operations.
- use of alternative remittance services/hawala
- frequent and unusual transfers from investment sites, often involving digital currencies
- Using e-money account as an alternative channel of online gambling deposit funds
- Large cash activity
- Purchase of high-value items
- Use of unusual financial instruments (e.g. bank drafts, bank bills, bearer shares etc.)
- Use of mule accounts/use of unwitting third parties
- The customer's credit and debit transaction volumes and values are inconsistent with its CDD profile and deviates from peers.
- There is a sudden increase in the customer's new credit and debit counterparties.
- The customer's account appears to be a temporary repository of funds with rapid movement of matching debits and credits.

- Guaranteed high returns in short timeframes.
- False business declaration (real estate vs crypto/trading).
- Unusual client onboarding without business legitimacy.
- High-volume transfers with no economic rationale.
- Multiple un-related third-party deposits.
- Use of multiple personal accounts for commercial and suspicious activity.

(iii) lifestyle, income and documentation discrepancies:

- transactions that do not align with a person's known occupation or lifestyle, huge purchases or transfers made by individuals with few legitimate income sources, warrant further investigation.
- concealment of beneficial ownership information and use of corporate vehicles
- the use of fake identity cards and the purchase of tickets through e-commerce platforms
- the customer is new-to-bank customer; the retail customer is a non-resident
- travel to and transactions in high-risk jurisdictions for child exploitation (Philippines, Thailand, Indonesia), many-to-one transaction patterns with male senders and female payees, no apparent familial or nationality connections between senders and payees while “familial support” was selected as the pay purpose for many transactions, and lower dollar amounts.
- Impersonating government officials or ‘trusted individuals’ e.g. family members.

(iv) social media /digital footprint discrepancies

- social media accounts with sudden location changes to known cyber scam hubs and then minimal or forceful communications may indicate a trafficking situation.
- the customer shares common Device IDs with multiple former customers exited for financial crime concerns (money laundering, fraud) indicating a network operation.
- the customer records repeated IP logins from scam centre high-risk jurisdictions (Cambodia, Myanmar, Laos, and Sri Lanka) over a sustained period, despite no known rationale in CDD information (nationality, residence, commercial operations and others).
- Use of social media to solicit investments.

Appendix B: Cyber Scam Hubs and Human Trafficking Survey – Public Sector

This survey is part of an information gathering exercise to inform the development of a typology report on the laundering of proceeds of crime from cyber scam hubs and human trafficking.

Members are encouraged to include comments and observations to provide further context to responses.

APG Members and Observers are asked to return their completed survey by 30 June 2025 and mail **to** mail@apgml.org

We encourage APG contact points to share this survey with relevant agencies in your jurisdiction.

Confidentiality of information

The APG will not attribute information to contributing agencies or members unless express permission has been provided. All conclusions and analysis will be anonymised. A copy of the first draft of the report will be sent to all contributors for their review and to collect any comments or concerns prior to publication.

Terminology

For the purposes of this survey:

- ***Cyber scams** represent a structured and transnational form of cyber-enabled fraud,[1] often associated with organised crime groups that systematically exploit digital platforms, human trafficking, and financial infrastructure to defraud victims at scale. Cyber scams employ various fraud techniques, such as pig butchering,[2] romance scams, investment fraud, and impersonation schemes, typically facilitated through messaging apps, social media, and fraudulent platforms.*

- ***Cyber scam hub** refers to a physical or hybrid operational centre often controlled by organised criminal groups, from which large-scale cyber scams are conducted.*

- ***Human trafficking** refers to the trafficking of people to work in cyber scam hubs, who are forced to scam people (often located in other jurisdictions) out of their money.*

Contact details

Jurisdiction	
Organisation	
Contact name	
Contact email	

[1] The Financial Action Task Force (FATF) defines cyber-enabled fraud a fraud that is enabled through or conducted in the cyber environment and that (i) involves transnational criminality such as transnational actors and funds flows and (ii) involves deceptive social engineering techniques (i.e., manipulating victims to obtain access to confidential or personal information) <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf>

[2] Pig butchering refers to a romance-investment hybrid scam wherein criminal actors use social engineering techniques to build trust with victims over time, typically via online messaging platforms, and subsequently induce them to make large-scale financial transfers to fraudulent investment schemes, often involving virtual assets.

Questions

I. Preliminaries and operational methods

1. What year did you first suspect or identify a cyber scam hub operating in your jurisdiction?

   Year: _____ ☐ Not applicable

   If applicable, **in the year you first suspected or identified a cyber scam hub operating** in your jurisdiction,
   How many cyber scam hubs were estimated to be operating? _____
   How many people did you estimate were employed in these hubs (count all employees)? _____
   ☐ Not applicable

   How many cyber scam hubs do you estimate are **currently** operating in your jurisdiction? _____
   What is the estimated number of people **currently** employed in these hubs (count all employees): _____
   ☐ Not applicable

2. What typically triggers investigations linked to cyber scam hubs? (Select all that apply)
   - ☐ Suspicious transaction reports (STRs)/suspicious activity reports (SARs)
   - ☐ Victims' reports or complaints
   - ☐ Information from informants
   - ☐ Referrals from embassies or diplomatic missions
   - ☐ Foreign financial intelligence units
   - ☐ Foreign law enforcement agencies
   - ☐ Non-governmental organisations
   - ☐ Media reporting or investigative journalism
   - ☐ Other (please describe): _____

3. In your understanding of this typology (or from your own research), where are the cyber scam hubs typically located? (Select all that apply)
   - ☐ Border areas
   - ☐ Special economic zones
   - ☐ Urban centers
   - ☐ Conflict zones
   - ☐ Remote rural areas
   - ☐ Villages
   - ☐ Other (please describe): _____

5. What are the main reasons these locations are selected for cyber scam hubs? (Select all that apply)
   - ☐ Limited law enforcement presence
   - ☐ Proximity to borders or escape routes
   - ☐ Corrupt or complicit local authorities
   - ☐ Low regulatory oversight
   - ☐ Existing criminal networks

☐ Other (please describe): _____

6. Have you encountered, or are you aware of any examples of the 'decentralisation' of cyber scam hubs? ('Decentralisation' is where the cyber scam hubs break into smaller components and move to different areas within a city/region, to hide their presence).
   ☐ Yes
   ☐ No
   ☐ Unsure

   If yes, please describe the activity
   Answer: ____

7. How is artificial intelligence (AI) being used to further scam operations? (Select all that apply)
   ☐ Chatbots or AI-generated responses in scams
   ☐ Deepfakes or manipulated videos (including for impersonation)
   ☐ Voice cloning for impersonation
   ☐ AI-generated scam content
   ☐ Large language model (LLM – artificial intelligence that can recognise and generate text)
   ☐ Unsure
   ☐ Other (please describe): _____

8. Are you aware of any domestic or international database or watchlist tracking known or suspected cyber scam operators in your jurisdiction?
   ☐ Yes – actively maintained and used
   ☐ Yes – exists but not regularly updated
   ☐ No – not aware of any
   ☐ Unsure

   If yes, please describe the database or system and who maintains the database (if known):
   Answer: ____

9. What non-financial indicators or patterns trigger a suspicion of a cyber scam hub?
   ☐ Internet usage
   ☐ Electricity consumption
   ☐ Delivery of food
   ☐ Purchase of technical capabilities
   ☐ Virtual private networks
   ☐ Unsure
   ☐ Other (please describe): _____

II. Human trafficking victims

10. Based on evidence (investigations, prosecutions, case studies, requests for assistance, STRs), please complete the table below:
    a) Which jurisdictions are identified as the most common sources for victims of trafficking for cyber scam hubs?
    b) Which jurisdictions serve as common transit points for trafficking victims?
    c) Which jurisdictions are identified as the primary destinations for trafficking victims?

d) Which jurisdictions are destinations for the proceeds of crime from cyber scam hubs and human trafficking?

	(a) Source jurisdictions	(b) Transit jurisdictions	(c) Destination jurisdictions	(d) Destination jurisdictions for the proceeds of crime
1.				
2.				
3.				
4.				
5.				
6.				
7.				
8.				
9.				
10.				

11. Have people from your jurisdiction been trafficked into cyber scam hubs?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

a) If yes, how many people have been trafficked?
Answer: ____

b) Where have they been trafficked to? List as many as applicable in the following table:

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

12. What recruitment methods are commonly used? (Select all that apply)
    - ☐ False job advertisements
    - ☐ Romance scams
    - ☐ Fake business opportunities
    - ☐ Recruitment via online gaming
    - ☐ Trafficking by acquaintances or relatives
    - ☐ Coercion of acquaintances or relatives
    - ☐ Unsure
    - ☐ Other (please describe): _____

13. What types of false information is most provided to recruit victims? (Select all that apply)
    - ☐ Promises of high-paying legitimate jobs
    - ☐ Misrepresentation of job location
    - ☐ Misleading details about working conditions
    - ☐ Assurances of legal travel and documentation
    - ☐ Claims of career advancement or training
    - ☐ Unsure
    - ☐ Other (please describe): _____

14. Where does initial recruitment typically occur? (Select all that apply)
    - ☐ Social media platforms
    - ☐ Dating applications or websites
    - ☐ Job boards or recruitment websites
    - ☐ Physical recruitment centers or agencies
    - ☐ Messaging applications (e.g., WhatsApp, Telegram)
    - ☐ Unsure
    - ☐ Other (please describe): _____

15. How are recruitment advertisements typically presented? (Select all that apply)
    - ☐ Video testimonials on social media
    - ☐ Paid job advertisement platforms
    - ☐ Broadcasts on messaging applications
    - ☐ Word-of-mouth recruitment
    - ☐ Unsure
    - ☐ Other (please describe): _____

16. What demographics are most frequently targeted for trafficking to cyber scam hubs?

    Age group: ☐ Under 18 years; ☐ 18-24 years; ☐ 25-39 years; ☐ 40-54 years; ☐ 55 years and older; ☐ unsure

    Gender: ☐ male; ☐ female

    Educational level: ☐ no formal education; ☐ primary education (7-8 years of education); ☐ secondary education (11-12 years of education); ☐ tertiary education (>12 years of education); ☐ unsure

    Socio-economic status: ☐ low income; ☐ middle income; ☐ high income; ☐ unsure

    Geographic location: ☐ urban area; ☐ rural area; ☐ unsure

    ☐ Other factors (please describe): _____

17. Which sectors or actors have been identified as complicit in recruitment, transport, or exploitation of trafficking victims in cyber scam hubs? (Select all that apply)
    - ☐ Licensed labor recruiters
    - ☐ Unlicensed recruitment agents
    - ☐ Travel agencies
    - ☐ Employers or business operators
    - ☐ Unsure
    - ☐ Other (please describe): _____

18. What transportation routes are most used for trafficking? (Select all that apply)
    - ☐ Air travel
    - ☐ Land border crossings
    - ☐ Sea travel
    - ☐ Irregular routes through conflict zones
    - ☐ Unsure
    - ☐ Other (please describe): _____

19. What methods of payment are used to cover transportation costs? (Select all that apply)
    - ☐ Cash
    - ☐ Debit card
    - ☐ Credit card
    - ☐ Bank transfer
    - ☐ Mobile money
    - ☐ Unsure
    - ☐ Other (please describe): _____

20. Who typically pays for the transportation of trafficked individuals? (Select all that apply)
    - ☐ Victim using own funds or under coercion
    - ☐ Recruitment agent or trafficker
    - ☐ Third-party sponsor (e.g., fake employer or business)
    - ☐ Family or friends (unaware of the trafficking intent)
    - ☐ Unsure
    - ☐ Other (please describe): _____

21. What control mechanisms are used by criminals to retain trafficked individuals? (Select all that apply)
    - ☐ Passport confiscation
    - ☐ Physical confinement
    - ☐ Debt bondage
    - ☐ Threats to family or loved ones
    - ☐ Psychological coercion or manipulation
    - ☐ Unsure
    - ☐ Other (please describe): _____

22. What forms of exploitation are typically associated with trafficked individuals in cyber scam hubs? (Select all that apply)
    - ☐ Forced criminal activity (e.g., online scamming, money laundering)
    - ☐ Sexual exploitation
    - ☐ Extortion or blackmail of the victim's contacts
    - ☐ Unsure

☐ Other (please describe): _____

23. What are the typical working conditions experienced by trafficked individuals in scam hubs? (Select all that apply)
    - ☐ Long working hours with no rest
    - ☐ Threat or violence
    - ☐ Limited or no access to outside communication
    - ☐ Confiscation of phones or restricted internet use
    - ☐ Constant surveillance
    - ☐ Unsure
    - ☐ Other (please describe): _____

24. How are trafficked individuals typically identified and/or rescued in your jurisdiction? (Select all that apply)
    - ☐ Victim self-reporting to authorities or embassies
    - ☐ Reports from non-governmental organisations or civil society organisations
    - ☐ Law enforcement raids on scam compounds
    - ☐ Intelligence from foreign governments
    - ☐ Reporting by local citizens or workers
    - ☐ Unsure
    - ☐ Other (please describe): _____

25. Has your jurisdiction conducted any risk assessments or studies focused on the human trafficking risks associated with cyber scam hubs?
    - ☐ Yes, a comprehensive study has been conducted
    - ☐ Yes, but limited in scope or depth
    - ☐ Assessment is planned or underway
    - ☐ No
    - ☐ Unsure

26. Has your jurisdiction issued specific guidance or red flag indicators to frontline officers (e.g., immigration officers, consular staff, recruitment agencies, airlines, public education campaign) regarding the human trafficking risks associated with cyber scam hubs?
    - ☐ Yes, comprehensive and updated guidance/indicators are provided
    - ☐ Yes, some general guidance that covers these risks exists
    - ☐ Guidance is planned or under development
    - ☐ No specific guidance or red flags issued
    - ☐ Unsure

27. To what extent are the human and social harms caused by human trafficking into cyber scam hubs understood and integrated into your jurisdiction's national policy responses?
    - ☐ Very well understood and reflected in policies and programs
    - ☐ Somewhat understood, with increasing attention
    - ☐ Limited understanding or consideration
    - ☐ Not understood or addressed
    - ☐ Unsure

28. How would you assess the effectiveness of international cooperation mechanisms in identifying and assisting trafficking victims from cyber scam hubs?
    - ☐ Very effective – timely, coordinated, and productive
    - ☐ Moderately effective – some success, but with challenges
    - ☐ Slightly effective – major delays or gaps
    - ☐ Not effective
    - ☐ Unsure

29. What are the main obstacles your jurisdiction faces in securing international cooperation on trafficking cases involving cyber scam hubs?
    - ☐ Lack of communication with countries where cyber scam hubs operate
    - ☐ Delays or lack of responsiveness from foreign authorities
    - ☐ Legal or policy barriers to information sharing
    - ☐ We have faced few international cooperation obstacles for cyber scam hub cases
    - ☐ Unsure
    - ☐ Other (please describe): _____

III. Scam victims

30. What are the prevalent scam typologies targeting **scam victims** in your jurisdiction? (Select all that apply)
    - ☐ Phishing scams (e.g. email, SMS, voice, etc.)
    - ☐ Online shopping scams (e.g. fake e-commerce, auction scams, non-delivery of goods, etc.)
    - ☐ Investment scams (e.g. ponzi schemes, cryptocurrency scams, HYIPs, etc.)
    - ☐ Pig-butchering scams*
    - ☐ Romance scams (e.g. fake profiles on dating sites, emotional manipulation for gain, etc.)
    - ☐ Tech support scams (e.g. fraudulent calls, scams involving fake software, etc.)
    - ☐ Online gambling
    - ☐ Lottery and prize scams
    - ☐ Social media scams (e.g. fake news, etc.)
    - ☐ Job scams
    - ☐ Unsure
    - ☐ Other (please describe): _____

** Pig butchering refers to a romance-investment hybrid scam wherein criminal actors use social engineering techniques to build trust with victims over time, typically via online messaging platforms, and subsequently induce them to make large-scale financial transfers to fraudulent investment schemes, often involving virtual assets.*

31. What demographics are most frequently targeted as scam victims?

    Age group: ☐ Under 18 years; ☐ 18-24 years; ☐ 25-39 years; ☐ 40-54 years; ☐ 55 years and older; ☐ unsure

    Gender: ☐ male; ☐ female

    Educational level: ☐ no formal education; ☐ primary education (7-8 years of education); ☐ secondary education (11-12 years of education); ☐ tertiary education (>12 years of education); ☐ unsure

    Socio-economic status: ☐ low income; ☐ middle income; ☐ high income; ☐ unsure

    Geographic location: ☐ urban area; ☐ rural area; ☐ unsure

☐ Other factors (please describe): _____

32. Has your jurisdiction adopted measures to ensure restitution or compensation for victims of cyber scam hubs and human trafficking?
    ☐ Yes
    ☐ No
    ☐ Unsure

IV. Understanding and awareness of money laundering risks associated with cyber scam hubs and human trafficking

33. Has your jurisdiction assessed the ML/TF risk of cyber scam hubs, and/or scams more broadly?
    ☐ Yes
    ☐ No
    ☐ Unsure

    What was the risk assessment residual risk rating?
    ☐ Low
    ☐ Medium
    ☐ High
    ☐ Other (please provide details): _____

    Please provide a description of the risk assessment findings (*if the risk assessment is publicly available, please attach with your response or provide a hyperlink to the risk assessment*).
    Answer: ____

34. If you have assessed the ML/TF risk of cyber scams, and/or scams more broadly, please describe any mitigation measures you have put in place to address the risk.
    Answer: ____

35. Has your jurisdiction assessed the ML/TF risk of human trafficking and/or human trafficking more broadly? If yes, what was the residual risk rating?
    ☐ Yes
    ☐ No
    ☐ Unsure

    What was the risk assessment residual risk rating?
    ☐ Low
    ☐ Medium
    ☐ High
    ☐ Other (please provide details): _____

    Please provide a description of the risk assessment findings (*if the risk assessment is publicly available, please attach with your response or provide a hyperlink to the risk assessment*).
    Answer: ____

36. Do you have a national policy response to cyber scam hubs and/or human trafficking?
    ☐ Yes
    ☐ No
    ☐ Unsure

If yes, please describe the various elements of your national policy response. If part of a response to scams generally, please describe the policy.
Answer: ____

37. What are the primary money laundering typologies your jurisdiction has identified in connection with the proceeds of crime from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Use of complex corporate structures (shell or front companies)
    - ☐ Exploitation of virtual asset service providers and cryptocurrencies
    - ☐ Trade-Based Money Laundering
    - ☐ Use of money mules and mule networks
    - ☐ Investment in real estate or high-value goods
    - ☐ Use of unlicensed/illegal remittance systems
    - ☐ Use of casinos and gaming platforms
    - ☐ Use of entertainment platforms
    - ☐ No money laundering typologies identified
    - ☐ Other (please describe): _____

38. Please describe the vulnerabilities you have identified in your financial system that are being exploited to launder proceeds from cyber scam hubs and human trafficking.
    Answer: ____

39. Please describe any specific controls implemented to mitigate these identified vulnerabilities (e.g. legislative amendments, issuance of guidance, require/recommend reporting entities to amend/implement procedures, etc.)
    Answer: ____

40. Which gatekeepers are most involved or complicit in the laundering of the proceeds of crime from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Lawyers
    - ☐ Accountants
    - ☐ Notaries
    - ☐ Real estate agents
    - ☐ Company service providers
    - ☐ Unsure
    - ☐ Other (please describe): _____

41. Which sectors are perceived or assessed as most vulnerable to laundering the proceeds of crime from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Banking
    - ☐ Remittance
    - ☐ Real estate
    - ☐ Cryptocurrency platforms
    - ☐ Luxury goods
    - ☐ Informal money service businesses
    - ☐ Online betting and gaming
    - ☐ Unsure
    - ☐ Other (please describe): _____

42. Is the risk of the laundering of proceeds of crime from cyber scam hubs and human trafficking a factor in your risk-based supervision model?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, what is the risk rating?
    - ☐ Low
    - ☐ Medium
    - ☐ High
    - ☐ Other (please provide details): _____

    If yes, please describe how the risk of the laundering of the proceeds of crime from cyber scam hubs and human trafficking influence your risk-based supervision model.
    Answer: ____

V. Financial intelligence, investigations and prosecutions

43. Has your financial intelligence unit (FIU) received STRs on cyber scam hubs?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please complete the table.

Year	2020	2021	2022	2023	2024
Number of STRs					
Total value (if known) Please indicate currency					

44. Has your FIU received any/how many STRs on scams more broadly?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please complete the table.

Year	2020	2021	2022	2023	2024
Number of STRs					
Total value (if known) Please indicate currency					

45. Has your FIU received any/how many STRs on human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

If yes, please complete the table.

Year	2020	2021	2022	2023	2024
Number of STRs					
Total value (if known) Please indicate currency					

46. Has your FIU produced financial intelligence products on cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please describe the intelligence product(s).
    Answer: ____

47. Through your analysis, have you identified connections between human trafficking and cyber scam hubs?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please describe these connections.
    Answer: ____

48. Has your FIU analysed any funds flows related to cyber scam hubs, human trafficking and/or scams more broadly?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please describe your findings/provide an overview.
    Answer: ____

49. Has financial intelligence been used to trigger or inform investigations into cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

50. What do you perceive as the challenges in detecting and preventing money laundering linked to cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Sophistication and speed of money laundering schemes (e.g., rapid movement of funds)
    - ☐ Anonymity-enhancing features of certain virtual assets or platforms
    - ☐ Difficulty in distinguishing legitimate from illicit transactions based on available data
    - ☐ Lack of timely and actionable intelligence on money laundering red flags from authorities
    - ☐ Limitations in cross-border information sharing or jurisdictional issues
    - ☐ Resource constraints for advanced AML/CFT tools or expertise
    - ☐ Unsure

☐ Other (please describe): _____

51. What are the primary challenges your jurisdiction faces when investigating and prosecuting money laundering cases linked to cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Tracing illicit funds through virtual asset service providers and cryptocurrencies
    - ☐ Identifying beneficial ownership of entities used for laundering
    - ☐ Cross-border nature of operations and evidence gathering
    - ☐ Lack of specialised expertise in cyber-enabled money laundering
    - ☐ Difficulty linking laundered assets back to the specific predicate offenses (scams/trafficking)
    - ☐ Insufficient inter-agency cooperation
    - ☐ Legal framework
    - ☐ Unsure
    - ☐ Other (please describe): _____

52. Are there specialised investigative techniques, specialised teams, units or task forces dedicated to tackling the money laundering related to cyber scam hubs and human trafficking?
    - ☐ Yes, both dedicated task forces and specialised investigative techniques are in place
    - ☐ Some specialised techniques are used, but no dedicated task forces
    - ☐ General money laundering investigative techniques are applied
    - ☐ No specific focus or techniques for this type of money laundering
    - ☐ Under consideration
    - ☐ Other (please describe): _____

53. Describe your mechanisms for domestic coordination related to cyber scam hubs and human trafficking.
    Answer: ____

    What are barriers to success when responding to this crime type?
    Answer: ____

54. Have you used any telecommunications interception powers for the investigation of cyber scam hubs and human trafficking? (describe a threshold if necessary)
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please complete the table.

Year	2020	2021	2022	2023	2024
Number of investigations					
Total value (if known) Please indicate currency					

55. How did you use these telecommunications interception powers in operational matters, and how was it effective?
    Answer: ____

56. Do you liaise with telephone/social media companies or use their information holdings as part of your investigative techniques?
    - ☐ Yes
    - ☐ No
    - ☐ Under consideration
    - ☐ Unsure

    If you would like to, please provide further information on your response.
    Answer: ____

57. How do your investigative authorities use telephone/social media information with financial intelligence?
    Answer: ____

58. Do you liaise with/use of any civil society organisations/academia and their information holdings?
    - ☐ Yes,
    - ☐ No
    - ☐ Under consideration
    - ☐ Unsure

    If you would like to, please provide further information on your response.
    Answer: ____

59. To what extent is financial intelligence used to trace recruitment payments, travel arrangements, or other financial patterns related to cyber scam hubs and human trafficking?
    - ☐ High use – routinely analysed and acted upon
    - ☐ Moderate use – occasionally incorporated into investigations
    - ☐ Limited use – rarely used for this purpose
    - ☐ Not used at all
    - ☐ Unsure

VI. Asset seizure, freezing and confiscation

60. Please provide an estimate of the total value of money or assets laundered in your jurisdiction, related to cyber scam hubs and human trafficking.
    Answer: ____
    - ☐ Unable to estimate

61. Please estimate the total value of assets traced and seized in your jurisdiction, related to cyber scam hubs and human trafficking.
    Answer: ____
    - ☐ Unable to quantify

62. To what extent have you been successful in tracing and seizing proceeds laundered from cyber scam hubs located in your jurisdiction?
    - ☐ Highly successful
    - ☐ Moderately successful
    - ☐ Limited success
    - ☐ Rarely successful/significant seizures
    - ☐ Data not available/not applicable

63. To what extent have you been successful in tracing and seizing assets laundered from cyber scam hubs located in foreign jurisdictions?
    - ☐ Highly successful
    - ☐ Moderately successful
    - ☐ Limited success
    - ☐ Rarely successful/significant seizures
    - ☐ Data not available/not applicable

    If successful, please describe the international cooperation mechanisms you used to cyber scam hubs and human trafficking?
    Answer: ____

64. Does your jurisdiction have a dedicated agency or unit responsible for managing seized and confiscated assets?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

65. What types of assets linked to cyber scams hubs and human trafficking are commonly seized in your jurisdiction? (Select all that apply)
    - ☐ Cash
    - ☐ Real estate
    - ☐ Vehicles
    - ☐ Cryptocurrency
    - ☐ Luxury goods
    - ☐ Business assets
    - ☐ No assets linked to cyber scam hubs and human trafficking have been seized
    - ☐ Other (please describe): _____

66. Which challenges most often prevent successful asset confiscation from cyber scam hub operations? (Select all that apply)
    - ☐ Assets held in crypto or hard-to-trace instruments
    - ☐ Use of foreign nominees or front persons
    - ☐ Poor inter-agency coordination
    - ☐ Lengthy judicial processes
    - ☐ Difficulty identifying when crimes are committed
    - ☐ Crimes being investigated by authorities not familiar with asset recovery principles
    - ☐ Lack of staff with financial investigative expertise
    - ☐ Inability to exchange information from domestic authorities in a timely manner
    - ☐ Inability to exchange information from foreign jurisdictions in a timely manner
    - ☐ Insufficient resources (e.g. analytical software, IT equipment)
    - ☐ Cost of asset management
    - ☐ Incomplete, inaccessible or unavailable information regarding beneficial owners of companies (or other legal persons) and trusts (or other legal arrangements)
    - ☐ Legal barriers to exchanging information
    - ☐ Insufficient powers in relation to asset seizure or freezing
    - ☐ Other (please describe): _____

67. Has your jurisdiction implemented measures to ensure restitution or compensation to victims of cyber scams or trafficking for forced criminality?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please explain.
    Answer: ____

VII. International cooperation

68. Has your jurisdiction cooperated internationally in financial investigations aimed at identifying networks involved in human trafficking related to cyber scam hubs?
    - ☐ Yes, please provide details:
    - ☐ No
    - ☐ Unsure

69. How would you assess the effectiveness of international cooperation mechanisms (e.g., mutual legal assistance, informal FIU-to-FIU exchange, etc.) in supporting your jurisdiction's money laundering investigations and asset recovery efforts related to cyber scam hubs and human trafficking, or scams more broadly?
    - ☐ Very effective - timely responses and productive cooperation
    - ☐ Moderately effective - some successes, but also delays or challenges
    - ☐ Slightly effective - significant challenges hinder progress
    - ☐ Not effective, significant obstacles prevent meaningful cooperation
    - ☐ Limited or no experience with international cooperation on this crime type

70. What forms of international cooperation have proven most useful in investigating and prosecuting money laundering from cyber scam hubs and human trafficking? (Select up to two)
    - ☐ Joint/multi-lateral investigative teams
    - ☐ Informal intelligence sharing
    - ☐ Mutual legal assistance treaties
    - ☐ Interpol/ASEANPOL coordination
    - ☐ Other (please describe): _____

71. What are the challenges your jurisdiction faces in securing effective international cooperation on money laundering cases linked to cyber scam hubs and human trafficking? (Select up to three)
    - ☐ Delays in formal MLA processes
    - ☐ Differences in legal requirements for asset seizure/confiscation
    - ☐ Lack of direct counterparts or established communication channels in key jurisdictions
    - ☐ Difficulty enforcing foreign confiscation orders
    - ☐ Legal or institutional barriers to sharing financial intelligence internationally
    - ☐ Other (please describe): _____

VIII. Preventive measures and regulatory framework

72. What preventive measures do you consider the most important in the prevention and detection of cyber scam hubs and human trafficking?
    - ☐ Customer due diligence/Know your customer information
    - ☐ Ongoing customer due diligence – transaction monitoring
    - ☐ STR reporting
    - ☐ Enhanced customer due diligence
    - ☐ Other (please describe): _____

73. Has your jurisdiction issued specific guidance or red flag indicators to financial institutions and other reporting entities regarding ML/TF risks associated with cyber scam hubs and human trafficking?
    - ☐ Yes, comprehensive and updated guidance/indicators provided
    - ☐ Yes, some general guidance that covers these risks exists
    - ☐ Guidance is planned or under development
    - ☐ No specific guidance or red flags issued for this threat
    - ☐ Unsure
    - ☐ Only issued general guidance and/or red flag indicators related to scams more broadly

74. How likely do you consider these sectors to be identifying and reporting suspicious transactions related to the laundering of the proceeds of crime from cyber scam hubs and human trafficking?

Banks	Other FIs	Remitters	Other DNFBPs	VASPs
☐ Very likely	☐ Very likely	☐ Very likely	☐ Very likely	☐ Very likely
☐ Likely	☐ Likely	☐ Likely	☐ Likely	☐ Likely
☐ Unlikely	☐ Unlikely	☐ Unlikely	☐ Unlikely	☐ Unlikely
☐ Very unlikely	☐ Very unlikely	☐ Very unlikely	☐ Very unlikely	☐ Very unlikely
☐ Unsure	☐ Unsure	☐ Unsure	☐ Unsure	☐ Unsure

75. What recommendations would you make regarding implementing preventative measures to detect and effectively address cyber scam hubs and human trafficking?
    Answer: ____

IX. Role of unlicensed/unregistered entities and new technologies in laundering criminal proceeds

76. Has your jurisdiction identified the use of unlicensed/unregistered financial service providers (e.g., payment processors, crypto exchanges, informal money remitters) in laundering the proceeds of crime from cyber scam hubs and human trafficking?
    - ☐ Yes, frequently identified and a major concern
    - ☐ Yes, some instances identified
    - ☐ Suspected, but difficult to confirm or investigate
    - ☐ No significant instances identified
    - ☐ Area not sufficiently monitored

    If yes, please provide further information.
    Answer: ____

77. Has your jurisdiction identified any professional money laundering networks associated with cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

78. Has your jurisdiction identified any new forms of money launderers/money laundering associated with cyber scam hubs and human trafficking (e.g. 'digital gatekeepers')?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure

    If yes, please describe these new forms? (i.e. are they a standalone service, or are they part of the criminal syndicate, etc.)?
    Answer: ____

79. Which unlicensed financial services have been most linked to laundering the proceeds of crime from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Informal remittance systems (hawala, hundi, etc.)
    - ☐ Unregistered crypto exchanges
    - ☐ Unauthorised money changers
    - ☐ Informal payment aggregators
    - ☐ Unsure / not applicable
    - ☐ Other (please describe): _____

80. If any, what new and emerging payment technologies or methods (e.g., specific types of virtual assets, decentralised finance (DeFi) platforms, online gaming currencies) have you observed being used to launder funds from cyber scam hubs and human trafficking in your jurisdiction?
    - ☐ Unsure / not applicable

    Answer: ____

X. Convergence of organised crime / money laundering networks

81. Has your jurisdiction observed any involvement of organised crime elements with cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure / not applicable

82. Has your jurisdiction observed an overlap or convergence between money laundering networks servicing cyber scam hubs and those servicing other major predicate offenses (e.g., drug trafficking, illegal gambling, corruption)?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure / not applicable

    If yes, please describe this convergence.
    Answer: ____

83. Have you observed any use of illegal online gambling platforms used to mix or launder funds from cyber scams hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Unsure / not applicable

    If yes, please describe.
    Answer: ____

XI. Public-private partnerships and capacity building

84. Are there established public-private partnership mechanisms in your jurisdiction for sharing information and typologies related to money laundering from cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ No
    - ☐ Under consideration
    - ☐ Unsure

    If yes, what private sector stakeholders would you recommend including in a public/private partnership to effective address cyber scam hubs and human trafficking?
    Answer: ____

85. What are the most critical capacity-building needs for your jurisdiction's competent authorities (e.g., FIU, law enforcement agencies, prosecutors, AML/CFT regulators) to more effectively combat money laundering from cyber scam hubs and human trafficking? (Select up to two).
    - ☐ Training on investigating cyber-enabled money laundering and virtual assets
    - ☐ Advanced analytical tools and software
    - ☐ Expertise in international asset tracing and recovery
    - ☐ Enhanced inter-agency coordination mechanisms
    - ☐ Resources for specialised personnel
    - ☐ Other (please describe): _____

XII. Intervention and recommendations

86. At which points in the typology do you see the greatest opportunities for effective intervention? (Select all that apply)
    - ☐ Immigration control
    - ☐ Financial transaction monitoring
    - ☐ Border surveillance and customs check
    - ☐ Company registration and beneficial ownership transparency
    - ☐ Internet and digital platform regulation
    - ☐ Labour recruitment and employment agency oversight
    - ☐ Awareness measures for potential human trafficking victims (e.g. targeted awareness at university / technical college media, social media, etc.
    - ☐ Awareness measures for potential scam victims (e.g. broader awareness aimed at the general population)
    - ☐ Victim support and reintegration services
    - ☐ Unsure
    - ☐ Other (please describe): _____

87. Which legal or institutional reforms are most urgently needed to strengthen the response to cyber scams and related money laundering? (Select all that apply)
    - ☐ Stronger cross-border asset recovery frameworks
    - ☐ Enhanced regulation of online platforms and digital financial services
    - ☐ Company registration and beneficial ownership transparency
    - ☐ Increased protection and support for victims and witnesses
    - ☐ Improved inter-agency coordination and data sharing
    - ☐ Unsure
    - ☐ Other (please describe): _____

XIII. Case studies

Please provide notable success stories, case studies, or best practices your jurisdiction has observed regarding illicit proceeds generated from cyber scam hubs and human trafficking.

It is not necessary that an offence of money laundering has been proven. If the case study is demonstrative of how illicit proceeds of cyber scam hubs and human trafficking activity are being laundered, please include it here.

There is no limit on the number of case studies a jurisdiction can submit, however when submitting multiple case studies please note which methodologies are of the highest concern.

It is important that case studies focus on the movement of the proceeds of cyber scam hubs and human trafficking, including movement subsequent to offending. Please provide as much detail as possible in respect of this financial aspect.

Case study template

Overview	Please briefly describe: - Context and narrative of the case (description, ransomware strain used, perpetrators/ransomware actors involved, amount of ransom demanded, agencies involved, timeline, international or domestic case, etc.). - Outcome of the case, including whether ML/TF criminal charges were brought and any asset recovery.
Competent authorities involved	Please describe the competent authorities involved in the case.
Case detection and investigation	Please describe how the case was detected (e.g. STR, parallel financial investigation, international cooperation) and the means and tools employed during the investigation (including any specific tools or powers used).
Financial flows detected	Please describe the financial flows featured in this case. Please explain how financial assets and financial institutions, in particular, virtual assets and virtual asset service providers (VASP), were part of this case.

Source of illegal funds	How and in what form (cash; wire transfer; virtual assets, including any details about specific virtual assets; etc.) was the ransom requested/received?
Movement of funds	Please describe the volume and methods used to move funds, techniques, if any, to conceal the receipt and any subsequent movement of funds.
Use and laundering of funds	Please describe how the funds were used by and/or laundered by the perpetrators?
Link chart or diagram of activity	
Red flag indicators	Were there any particular red flags indicators in this case for competent authorities and/or financial institutions? Was there any particular financial behaviour from the perpetrators themselves that led to detection? **Delete red flags that are not applicable and/or add red flags as necessary.** ☐ Alternate remittance services / hawala ☐ Concealment of beneficial ownership ☐ Corporate vehicles (e.g. trust, shell companies) ☐ Crypto-currencies or other digital assets as a laundering mechanism ☐ False identities ☐ Foreign financial centres ☐ International trade to move value ☐ Large cash activity ☐ Purchase of high-value items ☐ Transnational criminal networks ☐ Unusual financial instruments (e.g. bank drafts, bank bills, bearer shares etc.) (please describe): _____ ☐ Unwitting third parties ☐ Other (please describe): _____
Relevant offences/legislation	Please describe the offences/legislation competent authorities used to achieve a successful outcome.
Outcomes/Results	Please describe outcomes regarding prosecutions, assets confiscation, repatriation of victims, restitution of criminal proceeds, etc.
Challenges and good practices identified, and lessons learned	Please describe any challenges and good practices arising from the case. Please include any methodologies developed as relevant.
Any other relevant information	

Appendix C: Cyber Scam Hubs and Human Trafficking Survey – Private Sector

This survey is part of an information gathering exercise to inform the development of a typology report on the laundering of proceeds of crime from cyber scam hubs and human trafficking.

Members are encouraged to include comments and observations to provide further context to responses.

Target audience

Please share this survey with key **reporting entities** in your jurisdiction: financial institutions, non-financial institutions (e.g. remitters) and virtual asset service providers (crypto currency exchanges), relevant **civil society organisations**, **think tanks** and **academic institutions** to complete.

Confidentiality of information

The APG will not attribute information to contributing agencies or members unless express permission has been provided. All conclusions and analysis will be anonymised. A copy of the first draft of the report will be sent to all contributors for their review and to collect any comments or concerns prior to publication.

Terminology

For the purposes of this survey:

- ***Cyber scams** represent a structured and transnational form of cyber-enabled fraud,[1] often associated with organised crime groups that systematically exploit digital platforms, human trafficking, and financial infrastructure to defraud victims at scale. Cyber scams employ various fraud techniques, such as pig butchering,[2] romance scams, investment fraud, and impersonation schemes, typically facilitated through messaging apps, social media, and fraudulent platforms.*

- ***Cyber scam hub** refers to a physical or hybrid operational centre, often controlled by organised criminal groups from which large-scale cyber scams are conducted.*

- ***Human trafficking** refers to the trafficking of people to work in cyber scam hubs, who are forced to scam people (often located in other jurisdictions) out of their money.*

Contact details

Jurisdiction	
Organisation	
Contact name	
Contact email	

[1] The Financial Action Task Force (FATF) defines cyber-enabled fraud a fraud that is enabled through or conducted in the cyber environment and that (i) involves transnational criminality such as transnational actors and funds flows and (ii) involves deceptive social engineering techniques (i.e., manipulating victims to obtain access to confidential or personal information) <https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Illicit-financial-flows-cyber-enabled-fraud.pdf>

[2] Pig butchering refers to a romance-investment hybrid scam wherein criminal actors use social engineering techniques to build trust with victims over time, typically via online messaging platforms, and subsequently induce them to make large-scale financial transfers to fraudulent investment schemes, often involving virtual assets.

QUESTIONS

I. Organisational role and AML/CFT engagement

1. Which category best describes your organisation's primary role in addressing money laundering risks, particularly those linked to cyber scams and/or human trafficking?
    - ☐ Financial institution and payment service providers - including banks, digital wallets, remittance services, money service businesses, and fintech companies. (e.g., AML/CFT compliance, transaction monitoring)
    - ☐ Virtual asset service provider - such as cryptocurrency exchanges, wallet providers, decentralised finance platforms, and related service operators. (e.g., AML/CFT compliance, blockchain analytics)
    - ☐ Telecommunications and digital communications platforms (detecting/disrupting illicit use, platform integrity)
    - ☐ Cloud services, internet service providers, and IT infrastructure providers – including technology companies offering cloud computing, data hosting, digital storage, and related IT infrastructure
    - ☐ Civil society organisation/non-governmental organisation (e.g., victim advocacy, research on illicit finance impact)
    - ☐ Academia
    - ☐ Think tank (research on ML typologies, policy recommendations or development)
    - ☐ Other (please describe)
    - ☐ Primarily focused on predicate crimes (scams/trafficking) rather than money laundering

2. Is your organisation currently engaged in efforts to detect, prevent, or disrupt money laundering associated with cyber scam hubs and human trafficking
    - ☐ Yes, involved in one or more targeted initiatives
    - ☐ Exploring potential engagement in this area
    - ☐ No, not currently, but see a potential role in AML/CFT
    - ☐ No, not currently

3. If you answered ‘yes’ to Question 2, what is the primary focus of your engagement?
    - ☐ Cyber scam hubs
    - ☐ Human trafficking
    - ☐ Both

4. How would you describe your organisation’s current level of AML/CFT maturity in addressing risks from cyber scam hubs and human trafficking and related money laundering?
    - ☐ Very mature – dedicated units, advanced systems in place
    - ☐ Moderately mature – some systems or units exist, but not yet fully integrated
    - ☐ Basic level of maturity – AML/CFT measures exist but not tailored to this threat
    - ☐ Minimal or no AML/CFT-specific engagement with this threat
    - ☐ Not applicable

5. What motivates your organisation's engagement in addressing cyber scam hubs and human trafficking -related money laundering risks? (Select all that apply)
    - ☐ Regulatory compliance obligations
    - ☐ Reputational risk concerns
    - ☐ Ethical or human rights considerations
    - ☐ Stakeholder pressure (e.g., investors, customers, donors)
    - ☐ Internal risk assessment findings
    - ☐ Other (please describe): _____

II. Observed money laundering trends and detection challenges

6. What are the primary money laundering typologies you have identified in connection with proceeds from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Use of complex corporate structures (shell or front companies)
    - ☐ Use of nominee directors or shareholders
    - ☐ Exploitation of Virtual Asset Service Providers and cryptocurrencies
    - ☐ Trade-Based Money Laundering
    - ☐ Use of money mules and mule networks
    - ☐ Investment in real estate or high-value goods
    - ☐ Use of unlicensed/illegal remittance systems
    - ☐ Use of casinos and gambling platforms
    - ☐ Use of entertainment platforms (e.g. online gaming)
    - ☐ Other (please describe): _____
    - ☐ No money laundering typologies identified

7. From your organisation's perspective, what are current trends in the laundering of proceeds from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Increased use of specific cryptocurrencies/mixers
    - ☐ Use of new digital payment platforms
    - ☐ Sophisticated layering techniques
    - ☐ No trends identified
    - ☐ Other (please describe): _____

8. What does your organisation perceive as the challenges in detecting and preventing money laundering linked to cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Sophistication and speed of money laundering schemes (e.g., rapid movement of funds)
    - ☐ Anonymity-enhancing features of certain virtual assets or platforms
    - ☐ Difficulty in distinguishing legitimate from illicit transactions based on available data
    - ☐ Lack of timely and actionable intelligence on money laundering red flags from authorities
    - ☐ Limitations in cross-border information sharing or jurisdictional issues
    - ☐ Resource constraints for advanced AML/CFT tools or expertise
    - ☐ Unsure
    - ☐ Other (please describe): _____

9. What demographics are most frequently targeted for **victims trafficked** to cyber scam hubs?

   Age group: ☐ Under 18 years; ☐ 18-24 years; ☐ 25-39 years; ☐ 40-54 years; ☐ 55 years and older; ☐ unsure

   Gender: ☐ male; ☐ female

   Educational level: ☐ no formal education; ☐ primary education (7-8 years of education); ☐ secondary education (11-12 years of education); ☐ tertiary education (>12 years of education); ☐ unsure

   Socio-economic status: ☐ low income; ☐ middle income; ☐ high income; ☐ unsure

   Geographic location: ☐ urban area; ☐ rural area; ☐ unsure

   ☐ Other factors (please describe): _____

10. What are the prevalent scam typologies targeting **scam victims** in your jurisdiction? (Select all that apply)

    ☐ Phishing scams (e.g. email, SMS, voice, etc.)
    ☐ Online shopping scams (e.g. fake e-commerce, auction scams, non-delivery of goods, etc.)
    ☐ Investment scams (e.g. ponzi schemes, cryptocurrency scams, HYIPs, etc.)
    ☐ Pig-butchering scams*
    ☐ Romance scams (e.g. fake profiles on dating sites, emotional manipulation for financial gain, etc.)
    ☐ Tech support scams (e.g. fraudulent calls, scams involving fake software, etc.)
    ☐ Online gambling
    ☐ Lottery and prize scams
    ☐ Social media scams (e.g. fake news, etc.)
    ☐ Job scams
    ☐ Other (please describe): _____

** Pig butchering refers to a romance-investment hybrid scam wherein criminal actors use social engineering techniques to build trust with victims over time, typically via online messaging platforms, and subsequently induce them to make large-scale financial transfers to fraudulent investment schemes, often involving virtual assets.*

11. What demographics are most frequently targeted as **scam victims**?

    Age group: ☐ Under 18 years; ☐ 18-24 years; ☐ 25-39 years; ☐ 40-54 years; ☐ 55 years and older; ☐ unsure

    Gender: ☐ male; ☐ female

    Educational level: ☐ no formal education; ☐ primary education (7-8 years of education); ☐ secondary education (11-12 years of education); ☐ tertiary education (>12 years of education); ☐ unsure

    Socio-economic status: ☐ low income; ☐ middle income; ☐ high income; ☐ unsure

    Geographic location: ☐ urban area; ☐ rural area; ☐ unsure

    Other factors (please describe): _____

III. Potential contributions to AML/CFT efforts

12. What key contribution could your organisation realistically make to help combat money laundering originating from cyber scam hubs and human trafficking? (Select all that apply)
    - ☐ Sharing anonymised red flags and typologies
    - ☐ Developing innovative detection algorithms
    - ☐ Strengthening customer due diligence/know your customer measures for at-risk transactions
    - ☐ Providing data for money laundering research
    - ☐ Detect and share suspicious or abnormal usage patterns
    - ☐ None. We would not be able to contribute
    - ☐ Other (please describe): _____

13. Which of the following areas do you believe holds the greatest potential to strengthen AML/CFT responses to money laundering linked to cyber scam hubs and human trafficking?
    - ☐ Enhanced artificial intelligence and machine learning for transaction monitoring and anomaly detection
    - ☐ Greater use of blockchain analytics and virtual asset service providers supervision tools
    - ☐ More effective public-private information sharing partnerships on money laundering threats
    - ☐ Harmonised international AML/CFT standards for new payment methods
    - ☐ Increased focus on identifying and disrupting money mule networks
    - ☐ Greater coordination between law enforcement agencies and the private sector
    - ☐ Unsure
    - ☐ Other (please describe): _____

IV. Collaboration and information sharing for AML/CFT

14. Would your organisation be interested in participating in a secure platform or forum (with public sector involvement) to share anonymised insights, red flags, and typologies specifically related to money laundering from cyber scam hubs and human trafficking?
    - ☐ Yes
    - ☐ Likely / Need more information
    - ☐ Unlikely
    - ☐ No

15. What type of money laundering -related information, if shared responsibly between public and private entities, do you believe would be most impactful for your organisation's AML/CFT efforts against this threat?
    - ☐ Specific, actionable red flag indicators for money laundering from cyber scam hubs and human trafficking
    - ☐ Anonymised typologies of new laundering schemes observed by authorities/peers
    - ☐ De-identified data on common laundering channels/jurisdictions used
    - ☐ Information on emerging risks from new technologies used for ML
    - ☐ Feedback from law enforcement on the quality/utility of submitted suspicious transaction reports related to this
    - ☐ Other (please describe): _____

16. What are the main barriers your organisation faces in sharing information with public authorities? (Select up to three).
    - ☐ Data protection or privacy laws
    - ☐ Lack of legal safe harbors
    - ☐ No formal mechanism for structured sharing
    - ☐ Lack of trust or clarity on use of data shared
    - ☐ Limited resources to prepare/sharing useful data
    - ☐ Other (please describe): _____

V. AML/CFT awareness and capacity building needs

17. For your sector, what areas most need enhanced awareness or capacity to better address money laundering risks from cyber scam hubs and human trafficking?
    - ☐ Understanding evolving money laundering typologies involving virtual assets and new payment methods
    - ☐ Identifying subtle red flags specific to scam-related money laundering within existing systems
    - ☐ Navigating legal/regulatory complexities for cross-border money laundering issues
    - ☐ Effectively utilising data analytics for money laundering detection in this context
    - ☐ Training staff on the nexus between cyber scam hubs, human trafficking, and money laundering
    - ☐ Other (please describe): _____

18. What kind of support or resources would best enable your organisation to strengthen its AML/CFT response to money laundering from cyber scam hubs and human trafficking?
    - ☐ Access to more detailed and timely money laundering threat intelligence from authorities
    - ☐ Sector-specific training on money laundering red flags and investigative techniques for this crime
    - ☐ Funding or grants for developing innovative AML/CFT technologies or research
    - ☐ Clearer guidance from regulators on AML/CFT expectations for this risk area
    - ☐ Platforms for more effective collaboration with law enforcement and other private sector entities
    - ☐ Other (please describe): _____

VI. Role of academia and civil society

19. What roles can academia and civil society play in addressing these crimes?
    - ☐ Conducting research and data analysis on typologies and trends
    - ☐ Monitoring human rights impacts and advocating for victim-centred policies
    - ☐ Delivering public awareness campaigns and education
    - ☐ Providing direct services to victims and survivors
    - ☐ Facilitating policy dialogue and multi-stakeholder engagement
    - ☐ No views
    - ☐ Other (please describe): _____

VII. Case studies

Please provide notable success stories, case studies, or best practices your jurisdiction has observed regarding illicit proceeds generated from cyber scam hubs and human trafficking.

It is not necessary that an offence of money laundering has been proven. If the case study is demonstrative of how illicit proceeds of cyber scam hubs and human trafficking activity are being laundered, please include it here.

There is no limit on the number of case studies a jurisdiction can submit, however when submitting multiple case studies please note which methodologies are of the highest concern.

It is important that case studies focus on the movement of the proceeds of cyber scam hubs and human trafficking, including movement subsequent to offending. Please provide as much detail as possible in respect of this financial aspect.

Case study template

Overview	Please briefly describe: - Context and narrative of the case (description, ransomware strain used, perpetrators/ransomware actors involved, amount of ransom demanded, agencies involved, timeline, international or domestic case, etc.). - Outcome of the case, including whether ML/TF criminal charges were brought and any asset recovery.
Competent authorities involved	Please describe the competent authorities involved in the case.
Case detection and investigation	Please describe how the case was detected (e.g. STR, parallel financial investigation, international cooperation) and the means and tools employed during the investigation (including any specific tools or powers used).
Financial flows detected	Please describe the financial flows featured in this case. Please explain how financial assets and financial institutions, in particular, virtual assets and virtual asset service providers (VASP), were part of this case.
Source of illegal funds	How and in what form (cash; wire transfer; virtual assets, including any details about specific virtual assets; etc.) was the ransom requested/received?
Movement of funds	Please describe the volume and methods used to move funds and the techniques, if any, to conceal the receipt and any subsequent movement of funds.
Use and laundering of funds	Please describe how the funds were used by and/or laundered by the perpetrators?
Link chart or diagram of activity	

Red flag indicators	Were there any particular red flags indicators in this case for competent authorities and/or financial institutions? Was there any particular financial behaviour from the perpetrators themselves that led to detection? **Delete red flags that are not applicable and/or add red flags as necessary.** ☐ Alternative remittance services / hawala ☐ Concealment of beneficial ownership ☐ Corporate vehicles (e.g. trust, shell companies) ☐ Crypto-currencies or other digital assets as a laundering mechanism ☐ False identities ☐ Foreign financial centres ☐ International trade to move value ☐ Large cash activity ☐ Purchase of high-value items ☐ Transnational criminal networks ☐ Unusual financial instruments (e.g. bank drafts, bank bills, bearer shares etc.) (please describe): _____ ☐ Unwitting third parties ☐ Other (please specify): _____
Relevant offences/legislation used	Please describe the offences/legislation competent authorities used to achieve a successful outcome.
Outcomes/Results	Please describe outcomes regarding prosecutions, assets confiscation, repatriation of victims, restitution of criminal proceeds, etc.
Challenges and good practices identified, and lessons learned	Please describe any challenges and good practices arising from the case. Please include any methodologies developed as relevant.
Any other relevant information	