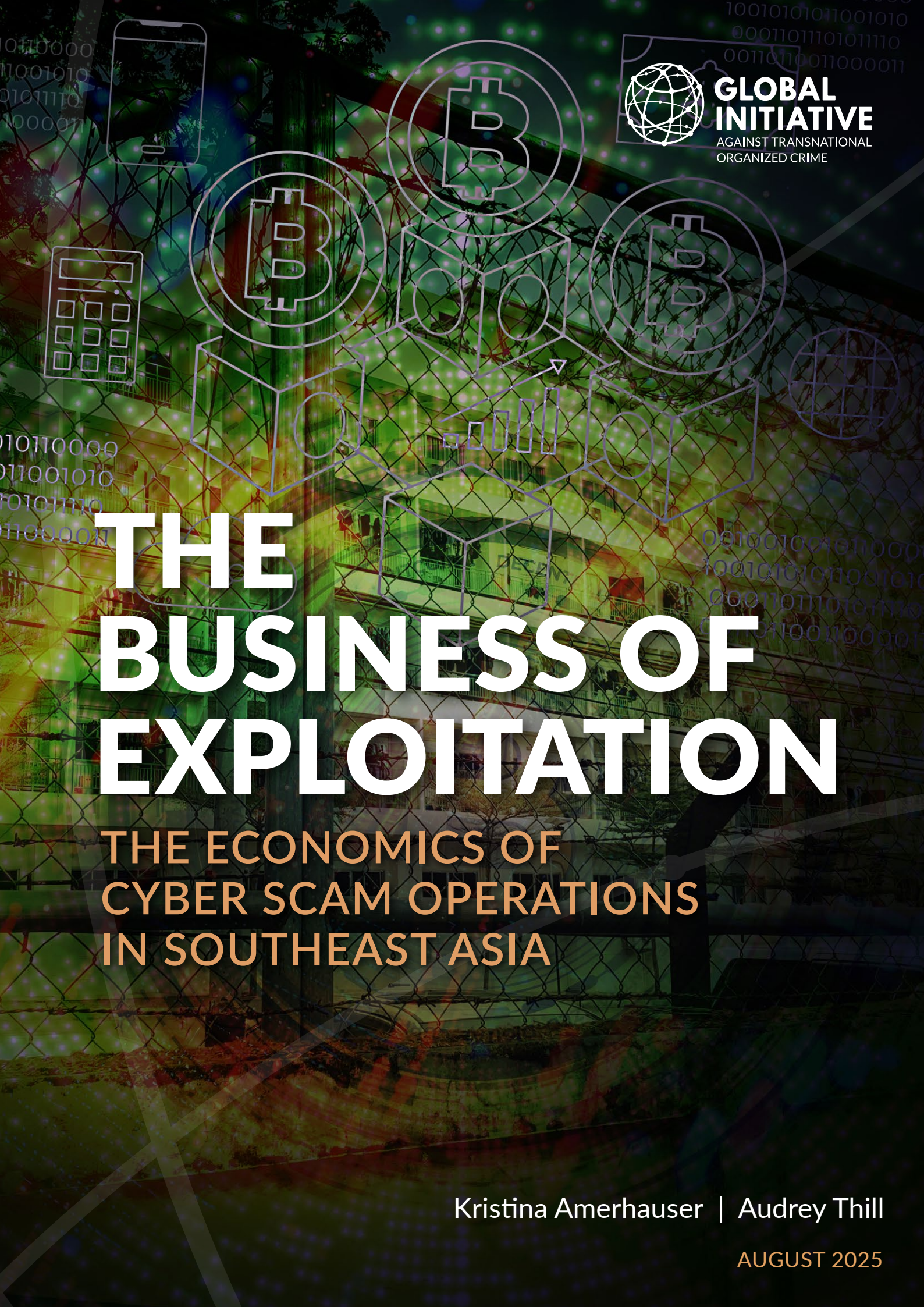


GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

THE BUSINESS OF EXPLOITATION

THE ECONOMICS OF CYBER SCAM OPERATIONS IN SOUTHEAST ASIA

Kristina Amerhauser | Audrey Thill

AUGUST 2025

ACKNOWLEDGEMENTS

This research report was produced by the Global Initiative Against Transnational Organized Crime (GI-TOC)'s Observatory of Illicit Economies in Asia-Pacific in partnership with the Australian-funded ASEAN-Australia Counter Trafficking program and the Regional Support Office of the Bali Process on People Smuggling, Trafficking in Persons and related Transnational Crime. The views expressed in this publication are the authors' alone and are not those of the Australian government.

The brief is based on qualitative and quantitative data and analysis collected by researchers based in and working across Southeast Asia. The authors would like to thank Lindsey Kennedy and Nathan Paul Southern from The Eyewitness Project, Raymond Hantho from Chainbrium, and independent researchers Jan Santiago and Beth Chen for their hard work and dedication to this research. The authors would also like to thank the many interview partners for their open and frank insights and contributions.

Sincere appreciation goes to the external reviewer BC Tan, Managing Director of Investigations, Diligence and Compliance at KROLL, for his comments and feedback.

The authors would also like to thank the GI-TOC's Asia-Pacific team as well as the Editorial and Publications teams for their support.

ABOUT THE AUTHORS

Kristina Amerhauser is a senior analyst conducting research on topics such as illicit financial flows, money laundering and corruption. She works with the GI-TOC's Observatory of Illicit Economies in Asia-Pacific and is responsible for overseeing programming in the Mekong, as well as civil society, government and multilateral engagement in the region.

Audrey Thill is an independent analyst focusing on conflict, illicit economies and environmental crime. Previously, she worked for six years with an international NGO in Cambodia and Myanmar, conducting research and providing technical support to local NGOs in the peace and human rights sector. She collaborated with local researchers in the study of illegal logging and local responses to resource conflicts.

Cover photo: *GI-TOC*

Please direct inquiries to:
The Global Initiative Against Transnational Organized Crime
Avenue de France 23
Geneva, CH-1202
Switzerland
www.globalinitiative.net

CONTENTS

GLOSSARY

Anti-money laundering (AML): set of laws, regulations and procedures designed to prevent, detect and report activities that seek to disguise illicit proceeds as legitimate income.

Association of Southeast Asian Nations (ASEAN): regional grouping of states that aims to promote economic, political, social and security cooperation among its members.

Blockchain: a digital ledger, akin to a series of connected record books, with each 'block' containing cryptocurrency transaction data linked together in a chain. The data stored is unchangeable and publicly available.

Cryptocurrency: form of digital currency that allows people to make payments directly to each other through an online system.

Decentralized finance (DeFi): financial system built primarily on the Ethereum blockchain that operates without traditional intermediaries such as banks.

Escrow account: type of account that is designed to hold funds, securities or other assets pending the fulfilment of certain conditions to release them.

Financial Action Task Force (FATF): the global money laundering and terrorist financing watchdog.

Fiat currency: government-issued currency that is not backed by a commodity such as gold or silver.

Financial intelligence unit (FIU): a national centre for the receipt, analysis and dissemination of suspicious transaction reports and money laundering information, associated predicate offences and terrorist financing.

Gateway companies: intermediaries who facilitate communication and financial transactions between cyber scam operations and money laundering service providers.

Hawala: informal money transfer system that often does not involve the physical transfer of cash. Others include the hundi system, fei qian, etc.

Know your customer (KYC): guidelines and regulations that require professionals to verify the identity, suitability and risks involved with maintaining a business relationship with a customer.

Motorcade: term used to describe a group or network of individuals who specialize in moving cash or digital assets between accounts, platforms and currencies.

Moving bricks term used to describe a money laundering process where funds are moved around to obscure the original source of the funds.

Mule accounts: accounts used to transfer or receive funds as part of the money laundering process.

Non-custodial wallets: cryptocurrency wallet that allows user to maintain control of their private keys and funds rather than the exchange acting as intermediary.

Pankou: (Chinese) term used by gateway companies to refer to their clients who seek money laundering services.

Peer-to-peer (P2P): a decentralized system that facilitates direct connections among individual nodes rather than through a centralized server.

U-merchant: over-the-counter currency dealers who exchange cryptocurrencies and fiat currencies.

United Nations Office on Drugs and Crime (UNODC): UN agency that supports member states to combat organized crime, corruption and terrorism.

SUMMARY

Cyber scam operations in Southeast Asia rely heavily on information and communications technology, financial fraud, trafficking for forced criminality, corruption and elite capture. This creates what can be described as 'compound crimes', reflecting how cyber scam operations are both based in physical compounds and involve multiple criminal markets.[1]

While estimates vary, the scale of funds defrauded from scam victims each year is in the tens of billions of US dollars and trending upward.[2] In addition, illicit proceeds are generated from exploitation of trafficked persons, illegal gambling and corruption. The scale of illicit financial flows represents a clear threat to national economies, governance and international security.

Cyber scam operations and their enabling networks operate at scale across Southeast Asia and beyond. They have reportedly trapped hundreds of thousands of people inside compounds where they are forced to conduct scams.[3] Some operations retain workers through debt bondage, psychological coercion and financial incentives. Significant diversity in operational models – from high-security compounds to thousands of smaller operations located in apartments and other small premises – creates varied patterns of financial flows across jurisdictions.

The money laundering process is part of a sophisticated financial service ecosystem. Most concerning is how networks of actors operate at scale and at the intersection of legitimate and illegitimate economies by using licensed crypto exchanges, registered fintech platforms and traditional banking services. Some are 'crime as a service' providers, explicitly providing money laundering services to cyber scam operations and doing so with corporate efficiency. This means that moving and laundering money has evolved into a marketplace-type structure where actors remain anonymous to others within the network.

Governments, the private sector and civil society actors have sought innovative responses to disrupt the illicit industry. These include initiatives that 'follow the money' and disrupt the money laundering networks used by cyber scam operations.

While some work has begun to explore illicit financial flows stemming from scam operations, notably related to cryptocurrencies, important gaps persist. Less is known about the wider set of financial flows, the mechanisms used to transfer proceeds in and out of the region and the networks involved. This policy brief seeks to help fill this gap by mapping wider related payments and providing insights into how money is moved and where it ultimately ends up. It concludes by providing actionable policy

recommendations for Southeast Asian governments as well as regional and global financial service providers. Crucially, these recommendations identify entry points for disrupting the operations of the transnational organized crime groups that run cyber scam operations. The key findings include:

- Actors involved in cyber scams and trafficking for forced criminality often use cryptocurrency to move illicit money. They also use cash, fintech – such as peer-to-peer (P2P) payment apps – gaming or gambling platforms, bank transfers, shell and front companies, credit cards and pre-paid cards.
- The role of the formal banking sector in these financial flows appears significant, as many scam-related transfers are initiated by the victim from their own bank accounts before being converted into cryptocurrencies at different steps of the laundering process. While most financial institutions likely process these transactions unwittingly, evidence suggests they may be enabled by regulatory loopholes such as weak know-your-customer (KYC) requirements and/or excessively high minimum thresholds for reporting suspicious transactions. After being laundered and converted back into fiat currency[4] from cryptocurrency, illicit funds are also likely to be moved again through the formal financial system.
- Many of the fintech and cryptocurrency platforms that money laundering networks use to convert cryptocurrencies back into fiat are registered companies and hold financial service licences. Some owners of these platforms have close connections to the political and business elites in the countries of registration, suggesting influence over financial regulation and an interest in maintaining a policy environment amenable to the large-scale laundering of criminal proceeds.
- Transnational organized crime groups in Southeast Asia generate highly lucrative profits. This creates a vicious cycle: greater profits enable these groups to expand their influence, including over public officials and the financial sector, which in turn reduces scrutiny of cyber scam compounds and related suspicious financial transactions. With their growing wealth, these criminal networks invest further into other types of crime and crime-as-a-service infrastructure, generating additional profits that allow them to strengthen their influence and market position.

Methodology

This policy brief focuses on cyber scam operations in Cambodia, Laos, Myanmar and the Philippines. While the primary focus is on operations in these countries, evidence is also uncovered of links to the wider Southeast Asian region. This reflects the fact that cyber scam operations and related illicit financial flows are transnational and a global concern.

Multi-method research was conducted in the first six months of 2024 by a team of 14 researchers and civil society partners with significant experience investigating illicit money flows, organized crime and corruption in Southeast Asia. Researchers conducted field visits and semi-structured in-person interviews with representatives of the fintech and banking industry, with people who worked for money laundering companies and scam centres and with investigative journalists and civil society organizations that operate in affected areas. The brief also draws on an extensive literature review, including English and local-language sources.

Input was provided during the 'Technical experts meeting on following the money from trafficking in persons'. This event took place in June 2024 and was co-organized by the Regional Support Office of the Bali Process, ASEAN Australia Counter Trafficking Program and the GI-TOC. Initial results were then tested during the 'Technical workshop on investigating and prosecuting trafficking in persons syndicates involved in cyber scams centre operations across Southeast Asia', which was held in Bali, Indonesia, in October 2024. The latter meeting allowed for input and feedback from member states, law enforcement, anti-money laundering (AML) authorities and financial institutions.

The GI-TOC then triangulated, synthesized and analyzed this information. The policy brief was also reviewed by an external expert working on money laundering and illicit financial flows related to cyber scam operations in Southeast Asia.

GENERATING ILLICIT PROCEEDS FROM CYBER SCAM OPERATIONS

Payments related to cyber scam operations can be broadly grouped into four key areas: online scams and fraud, worker exploitation and trafficking for forced criminality, operational expenses and corruption payments (see Figure 1). While previous research has built crucial understanding of how scammers steal and move scam proceeds,[5] this analysis breaks new ground by mapping the broader ecosystem of financial transfers that sustains these operations. By examining this complex network of payments and beneficiaries, we show how cyber scam operations generate and move illicit funds through multiple interconnected channels. This more comprehensive mapping presents an opportunity to identify an equally wide array of entry points that policymakers, regulators and the private sector can exploit to stem the flow of money to and from cyber scams.

Payment category	Transfer type	From/To	Description	Transfer mechanisms
Scams and fraud	Scams and fraud	**From**: Scam victims **To**: Transnational criminal groups running cyber scams	Money stolen through different types of scams and fraud – the 'core' business of scam compounds.	Bank transfers, cryptocurrencies (including by gaining illegal access to wallets) and cash. Shell companies are used to obscure beneficial ownership of illicit funds.
	Salaries for compound managers and people who conduct the scams	**From:** Transnational criminal groups running cyber scams **To:** Scam compound managers and people who conduct scams	Managers are reported to receive higher pay and a percentage of scam proceeds.	Transfer mechanisms are unclear but are likely to follow similar patterns as payments made to workers, which include payments in cash, digital payments, prepaid cards, cryptocurrencies and more.
Worker exploitation and trafficking for forced criminality	Recruitment fees	**From**: Trafficking victims **To:** Job recruiters, traffickers	Recruitment fees from people seeking work (paid by the victim to the recruiter).	Cash, digital payments and *hawala* (and other informal money transfer systems).[6]
	(Re-)sale of trafficking victims between compounds	**From:** Transnational criminal groups running scams **To:** Traffickers	People who conduct scams are directly recruited by criminal groups or 'bought' from another compound.	Cryptocurrencies or digital payment systems (settled upon delivery of the trafficked person).

Payment category	Transfer type	From/To	Description	Transfer mechanisms
Worker exploitation and trafficking for forced criminality (continued)	Low salaries for people who conduct scams	**From:** Transnational criminal groups running cyber scams **To:** People who conduct scams	Many people who conduct scams[7] receive little or no base pay but some reportedly receive a commission from scam proceeds. People who conduct scams also commonly report that salaries are withheld or that they are overcharged for basic services (for example food, medicine and medical treatment) leading to a situation of debt bondage.	Those wages are reportedly paid in cash, using digital payments or prepaid cards used only in the compound. Sometimes they are also transferred via cryptocurrencies. Some workers report being compensated with consumer goods (e.g., smartphones). Cost incurred at compounds is also directly deducted from workers' pay.
	Payments to in-house entertainment workers	**From:** Transnational criminal groups, military or police officers, and other customers, including people who conduct scams **To:** People who provide 'entertainment' services	Various reports suggest people (often women) work as card-dealers, singers and sex workers at casinos, karaoke TV bars, 'drug bars' and entertainment venues inside or near scam operations. These workers are often victims of trafficking and sexual exploitation.	Payments in cash or through online payment systems are likely but payment mechanisms remain largely unknown.
	Ransom payments	**From:** Family and friends of scam workers **To:** Transnational criminal groups running cyber scams and brokers (who take a cut)	Family members pay to get family members released from compounds.	Cash or digital payments (including cryptocurrencies).
Operational expenses	Rent	**From:** Transnational criminal groups running cyber scams **To:** Businesses and property owners, including high level business and political elites	Most scam operations rent rooms, floors or entire buildings where they house workers and run their scam operations.	Payment mechanisms unknown.
	Utilities, cooking and cleaning services	**From:** Transnational criminal groups running cyber scams **To:** Local companies (utilities) or workers (cooking and cleaning)	Internet, electricity and water are essential services needed at every compound. Cooks and cleaners are typically hired from the surrounding community.	They are likely to be paid in cash or other digital payments common in the country (QR codes, etc).
	Payments to entertainment operators and managers	**From:** People who conduct scams and the transnational criminal gangs running them **To:** Entertainment venue operators and managers, sometimes friends or relatives of the compound owners[8]	Most compound are reported to have karaoke TV bars, massage parlours, bars, restaurants, brothels, etc.	Cash, compound-specific prepaid cards, digital wallets or as rewards.
	Medical services	**From:** People who conduct scams **To:** Public[9] or private clinics and hospitals (some controlled by compound owners)[10]	Some compounds also appear to have medical centres where workers can obtain treatment and notes to skip work, which people who conduct scams can access at inflated cost.	Cash, compound-specific prepaid cards or digital wallets.
	Trafficking victims	**From:** Transnational criminal groups running cyber scams **To:** Job recruiters, traffickers and smugglers	Scam compounds pay the recruiter per person recruited.	Payment mechanisms unknown.
	IT services, technology and software	**From:** Transnational criminal groups running cyber scams **To:** Online merchants, criminal entrepreneurs and companies	Payments made at online marketplaces for scam software, re-brandable websites, phones and phone numbers, money laundering services and numerous other 'crime as a service' offerings. This also includes payments to use certain software or digital services.	Transfers likely made by digital payments, including via cryptocurrency. They may also be made through mediated 'gateway companies' or other guarantors. Money launderers keep a percentage of the funds they launder for scam companies.
	Other scam-related goods and services	**From:** Transnational criminal groups running cyber scams **To:** Telecommunications, utility companies, financial institutions and other companies	Payments are made to utility companies and telecommunications for water, electricity and internet, banking and legal services (including document forgery).	Transfers are likely to be made via digital payment mechanisms and the formal financial system, and resemble 'legitimate' payments to these private sector actors.

Payment category	Transfer type	From/To	Description	Transfer mechanisms
Corruption payments	Protection payments and other bribes	**From:** Transnational criminal groups running cyber scams and traffickers **To:** State-embedded actors, including border guards, police, military and non-state armed actors	Bribes are paid to facilitate the trafficking of people to the scam compounds, for security services and armed escorts, and to avoid intervention from state actors.	Payment mechanisms unclear but believed to be mostly paid in cash.
	Corrupt partnerships	**From:** Criminal groups running cyber scams and traffickers **To:** State-embedded actors	Corruption payments extend beyond operational bribes to include sophisticated arrangements like joint ventures, strategic donations to secure permits or access to land for scam compounds, family business contracts or business licences that create structural protection for compounds even before they begin operating.	Payment mechanisms often remain unknown and are expected to differ widely. Likely include cash, shares in shell companies, payments through consulting fees and in-kind donations.

FIGURE 1 Cyber scam money flows and their value transfer mechanisms.

As detailed below, illicit proceeds stemming from scams and fraud are likely to be the biggest source of income for criminal networks. However, while previous research has attempted to estimate the total amounts of global revenue from 'pig-butchering' (romance investment) scams,[11] there do not appear to be equivalent estimates for other types of cyber-enabled scams, total sums of bribes paid or illicit proceeds generated through trafficking for forced criminality. This is due in large part to challenges with data collection and a close nexus between cyber scam operations and online gambling (much of which is itself fraudulent), making it difficult to disaggregate data. Technology is enabling both cyber scam operations and online gambling, further obscuring the distinction.[12] Unpacking the interconnections between online gambling and cyber scam operations (or estimating illicit proceeds from cyber scam operations and related criminal networks) is beyond the scope of this policy brief; however, doing so would be a valuable contribution to policy engagement and a helpful guide to advocacy going forward.

Scams and fraud

Substantial revenue comes from targeting individuals globally through sophisticated scam operations.[13] Some of the most common scams include, among others, romance investment scams,[14] sexual extortion,[15] crypto Ponzi schemes,[16] liquidity mining scams,[17] job/task scams,[18] impersonation scams[19] and fraudulent gambling or gaming sites.[20] Research on these scams reveals that they are very diverse and involve a wide range of tactics to contact and manipulate victims.[21] More details on and descriptions of common scams can be consulted in the GI-TOC's report 'Compound crime: Cyber scam operations in Southeast Asia'.[22]

Equally diverse are the mechanisms used to gain access to victims' funds. Some transfer money from their accounts directly to mule accounts or shell companies' bank accounts (which are controlled by money laundering networks) believing they are 'investing' in legitimate platforms.[23] Others convert fiat into cryptocurrencies on legitimate exchanges before connecting their digital wallets to fake investment platforms on mobile phone apps and websites. These platforms often contain 'cryptocurrency drainers' (i.e. malware or a malicious smart contract[24]) that gain unauthorized access to victims' wallets. Once a victim has unknowingly given them access, the platforms quickly move the funds out of these digital wallets and into accounts held with a variety of other platforms and financial institutions.[25]

Many of the investment platforms used in scams are designed to appear legitimate, sometimes using mirror websites with randomly generated web addresses[26] and 'spoofed' IP addresses.[27] Some scams use fraudulent sites inserted into legitimate apps that host third-party brokerage services.[28] To further polish the scam, the platforms have interfaces that display the supposed investment growth. Victims often make an initial 'investment,' which appears to go smoothly, tempting them into handing over larger amounts after they trust the process. As their funds appear to yield returns, they invest more.[29] Many victims report that they were initially able to withdraw some funds, but after contributing more, the sites locked them out and demanded payments for 'taxes' or other service fees.[30]

Losses from romance investments scams are reported to be growing, with victims sending larger amounts compared to other types of scams. For instance, the average transfer (often repeated multiple times) for romance scams was nearly US$4 593 in 2023 compared to only US$948 for impersonation scams.[31] Many victims report losing tens of thousands; some have even lost millions of US dollars. For instance, a US citizen targeted by a romance scam on Telegram initially sent US$1 000 in the Ethereum cryptocurrency to a fake investment website and ultimately lost over US$70 000 before the fraudulent platform blocked the victim's access to the funds. Another scammer contacted a victim through LinkedIn, and in subsequent phone conversations convinced them to make fake investments that drained their entire life savings of US$290 000. Yet another victim, initially contacted by text message, was convinced to buy and transfer crypto assets to a fake trading website. In total this victim lost US$1.5 million.[32]

What are cryptocurrencies and why are they attractive in cyber scam operations?

This section outlines key cryptocurrency and digital finance concepts that are essential to understanding how scam and money laundering networks operate financially.

Cryptocurrencies

Cryptocurrencies are a form of digital money that can be sent directly between people online without using traditional banking or wire transfers. These digital assets operate on decentralized blockchain networks. A blockchain is akin to a series of connected record books that are maintained across many computers instead of one central location. Each record book or 'block' contains cryptocurrency transaction data, and these are linked together in a 'chain.' The data stored there is unchangeable and publicly available.[33]

A blockchain typically has two types of assets: native cryptocurrencies or 'coins' (e.g., Bitcoin on the Bitcoin blockchain) and tokens that are hosted on multiple blockchains (e.g. Tether).[34] Bitcoin and Ethereum are the most prominent blockchain networks overall, but TRON appears particularly popular among cyber scam operators and related money laundering groups, in part because of low fees.[35]

Cryptocurrencies can be acquired through traditional brokerage services, much like investing in stocks.[36] Those who wish to use cryptocurrency to make transactions – as opposed to just an

investment – can purchase cryptocurrencies on exchanges. They then store those coins or tokens in digital wallets until they wish to send them to another wallet. All cryptocurrency addresses and transactions are recorded publicly on blockchains, but these addresses do not disclose the owner's identity, making them a pseudo-anonymous form of payment.[37]

Cryptocurrency addresses are meant to be publicly shared, and anyone that knows the address can see its transaction history and current balance. However, only the holder of a 'private key' associated with the address can transfer cryptocurrency out of it. So far, no capability exists to hack or rob a cryptocurrency address. Wallets, which people often use to manage their private keys and facilitate transactions between other wallets, are vulnerable to hacking or malicious smart contracts (i.e. computer programmes that automatically execute transactions when conditions are met).[38] Such methods give criminal actors access to the contents of the wallet.[39]

Decentralized finance

Decentralized finance (DeFi) is a general term that describes a financial system built primarily on the Ethereum blockchain and that operates without traditional intermediaries such as banks. DeFi is not governed by a central authority and is much less regulated than the traditional financial system, making it a highly attractive arena for criminal actors to shift illicit funds.[40] Instead of financial institutions, transactions are facilitated by smart contracts.[41]

The DeFi ecosystem includes a variety of service providers that operate on the basis of smart contracts, such as cryptocurrency 'mixers,' cross-chain bridges and decentralized exchanges. These technologies enable money laundering through automated currency exchanges and chain-hopping, or the practice of deliberately moving cryptocurrency across different blockchain networks. Chain-hopping often uses automated protocols across multiple blockchains.[42] 'Mixers,' for example, combine and scramble assets from multiple sources and redistribute equivalent amounts back randomly, making them particularly effective for obscuring the path between the accounts that receive scam funds and those that cash them out.[43] Cross-chain bridges enable customers to exchange digital assets across different blockchains.[44] Decentralized exchanges are a collection of smart contracts that facilitate crypto-to-crypto transactions; some such exchanges do not require KYC information.[45] Some of these exchanges also provide non-custodial cryptocurrency wallets[46] and chain-hopping services.

To move and launder illicit proceeds, cyber scam operations and affiliated money laundering networks use a variety of DeFi applications and cryptocurrencies, particularly stablecoins,[47] which are digital assets that are pegged to fiat currencies to reduce their volatility.[48] The world's biggest stablecoin by market capitalization is Tether (USDT), which is used on blockchains including TRON. USDT is reportedly the stablecoin of choice for many money laundering networks. According to blockchain analysis firm TRM Labs, 45% of all illicit cryptocurrency transactions worldwide in 2023 were conducted on the TRON blockchain and the majority of these transactions were denominated in USDT.[49] Looking specifically at scam-related transactions in 2023, Chainalysis found 70% involved USDT.[50] Decentralized exchanges are reportedly key enablers of these illicit flows.[51]

Tether has denied it bears any culpability for the use of its token by criminal organizations, stating it condemns 'the illegal use of stablecoins and is fully committed to combating illicit activity'. Tether states that it is working with law enforcement in 48 countries.[52] Tether and the blockchain network TRON also note that they collaborate with blockchain forensic firm TRM Labs to detect and disrupt illicit transactions.[53] ■

Trafficking for forced criminality

Scam compound operations in Southeast Asia rely heavily on forced labour to conduct the scams.[54] People who conduct scams are recruited by false job advertisements on social media, local recruiters, or job recommendations from friends and family with connections to cyber scam operations.[55] This process often appears legitimate and is designed to look professional. In some cases, people pay recruiters hundreds of US dollars to secure what they believe to be jobs at legitimate companies.[56] For instance, an individual in Myawaddy, Myanmar, paid a recruiter THB10 000 (US$304) to secure what he thought was a casino job but what was in reality a scam position.[57]

Payments related to recruitment cover travel cost and 'tea money' (payments) to facilitate recruitment on their behalf. These are reported to be made in cash, digital transfers and *hawala* transfers, depending on who is making or receiving the payment and where they are located.[58] Some smaller payments, such as those to local transporters who take workers across borders, are reportedly primarily in cash.[59] Many of these costs are converted into debt upon arrival.

Scam operators use a variety of techniques to contain and exploit workers, ranging from work contracts and debt bondage (further explained below), confiscating passports, barbed wire fences and armed guards. Some make threats against victims' family members or threaten to turn recruits over to authorities (e.g. for overstaying visas) as a means of control.[60]

Compensation – if paid at all – may include a low base salary, with reported wages falling between US$300 and US$700 per month, which for some people in Southeast Asia is an attractive wage.[61] Others may receive a fixed percentage of scam proceeds to incentivize hard work or they might receive 'commissions' in addition to the base salary. Regardless of pay, people who conduct scams must meet strict quotas – for instance, contacting a certain number of scam targets per day or hitting a monthly minimum value for stolen funds.[62] Non-cooperation or failure to meet the quotas results in restricted wages and other punishments, extending in some cases to torture.[63]

Recruits are sometimes renumerated in cash, compound-specific prepaid cards or cryptocurrency paid into digital wallets.[64] Some reports suggest that workers can still access these wallets even after they leave the compound or escape.[65] Some companies reportedly reward high-performing workers with

Alleged scam centre workers, many reportedly victims of trafficking, sit among dismantled equipment after Myanmar forces raided cybercrime compounds in Myawaddy, February 2025. *© STR/AFP via Getty Images*

access to alcohol, drugs and sex, which is provided by women (who are likely to be victims of sexual exploitation). These activities reportedly take place at entertainment venues or 'drug bars' inside the compounds. Other employees have reported gifts such as phones or watches.[66]

In addition to low wages, some compounds use artificial debt from accommodation, food or missed quotas to prevent people who conduct scams from earning enough to pay for their freedom. As a result, one person reportedly spent their entire US$600 monthly salary on repaying debt to their employer despite working for 70 hours per week.[67] Debt bondage also includes 'work contracts' with exit penalties. These reportedly range from US$1 500 to US$22 000 at some compounds in Myanmar.[68] Scam proceeds are often the only way to repay these 'debts' but one scam boss reportedly told a male worker that he had to pay for his freedom; if he were a woman, he could 'take on sex work.'[69]

Reselling victims across compounds also appears to provide a lucrative additional income for compound operations. People who conduct scams have reportedly been sold between compounds for between US$1 000 and US$15 000 in Cambodia depending on their skills and market conditions (i.e. pressure on scam companies to close and shortages of workers). In Myanmar, where there are added expenses related to travelling through conflict zones, people who conduct scams are reportedly sold for up to US$10 000.[70] There is little information on how these payments are made, but one expert suggested that they may be transferred via third-party payment apps frequently used by scam operators, as well as in cash.[71]

Some workers manage to leave the compounds if their families pay hefty ransoms that sometimes reach tens of thousands of dollars. Families have reported paying ransoms in cash or cryptocurrencies to brokers who negotiate with the scam companies on their behalf,[72] with payments ranging from US$3 000 to US$100 000.[73] In one case, a family paid RMB620 000 (US$85 300) in cash to a broker in China near the Myanmar border, securing the release of their son.[74] Some families have reportedly paid large ransoms but still fail to secure the release of their family member.[75] A blockchain analysis firm found that digital wallets connected to a large scam compound in Myawaddy received hundreds of millions of US dollars, some of which included ransom payments.[76]

Operational expenses

Transnational criminal groups that run cyber scam operations either own facilities or rent them in casinos, hotels, apartments and office buildings in 'hi-tech' industrial parks, which are sometimes owned by local business or political elites.[77] While it remains unclear how rent payments are made, several experts interviewed suggested they are likely paid in cash or through digital payment apps.[78] Scam compounds also require water, electricity and high-speed internet. Utility payments may be bundled with rent or paid separately through common local payment methods.[79] Some operations now use Starlink, a satellite internet service operated by SpaceX, which provides high-speed internet without relying on domestic infrastructure.[80] This US company offers monthly business plans for between US$140 and US$500, which can easily be paid online with a credit or debit card.[81]

Some cyber scam compounds in Southeast Asia hire people from the surrounding community to provide services such as cooking, cleaning and construction. In some communities, cyber scam compounds have become important employers and many of these workers are aware of the operations as they come and go from the compounds daily.[82] Although the amount earned in these roles is not publicly reported, jobs across other sectors in Cambodia typically earn a few hundred dollars per month.[83] The scam compounds may pay these wages in cash, or through electronic deposits if the

A building inside a scam centre in Bamban, Philippines. These operations require high infrastructure investments, including security systems, IT equipment, utilities and staffing to maintain round-the-clock fraudulent activities. *© Jam Sta Rosa/ AFP via Getty Images*

employee has a bank account. While there is less information available on other countries in the region, it is assumed that this pattern can also be observed elsewhere.

Security and political protection are likely significant operational expenses for scam operations, which typically pay for services from multiple providers. This includes security provided by the property owners, private security companies, law enforcement officials, armed groups and the scam operator's own security guards.[84] While there remains little information on these payments, they are likely to vary and include a range of payment methods (e.g. a security guard employed directly by the scam operator is likely to be paid differently from law enforcement officials).

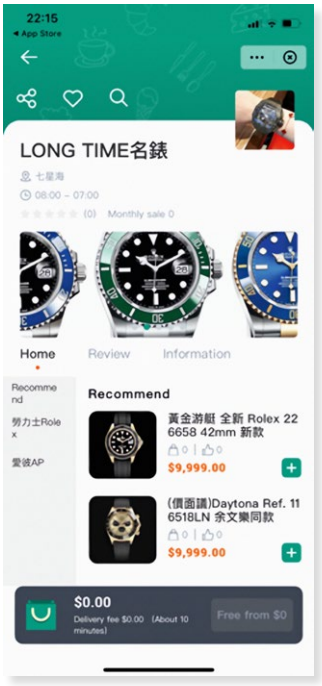
In addition to facilities and security, compounds source many other goods and services through online marketplaces. These marketplaces reportedly use Telegram channels and escrow accounts to facilitate purchases of fake investment platforms, torture devices, SIM boxes, registered Starlink accounts, money laundering services and much more.[85] One of the largest known marketplaces, Huione Guarantee (汇旺担保),[86] reportedly processed US$49 billion in what appears to be mostly illicit payments since 2021, with some of these transactions reportedly linked to scam-related laundering networks and trafficking in persons operations.[87] Huione Guarantee denies these allegations, claiming to be a neutral transaction guarantor.[88]

Financial technology infrastructure is another key expense for compounds and a critical enabler of scam compound operations, facilitating internal payments and the movement of illicit funds through digital criminal marketplaces.

One example that may fit this description is the Fincy app, which was developed for the Yatai New City development in Shwe Kokko, Myanmar, a notorious hotspot for scam operations.[89] The Fincy app and the blockchain technology on which it was based[90] were reportedly funded by GBCI Ventures, a Singapore-based company.[91] With the goal of creating a 'blockchain-enabled smart city,'[92] Fincy offered debit cards, digital wallets and a virtual exchange service offering access to 12 cryptocurrencies and 14 fiat currencies.[93] At the peak of this app's usage, Fincy's CEO claimed that 90% of employers in Shwe Kokko used it to pay their employees, which plausibly included scam workers due to the high

concentration of scam operations based in the development.[94] In 2020, however, Fincy announced it would withdraw from the project in response to allegations that their services were being used for money laundering. In a public letter, Fincy emphasized its 'zero tolerance approach to illegal activity' and said it was cooperating with authorities to investigate the issue.[95]

Another example appears to be LongPay, a blockchain-based app offering digital wallets, QR code payments and P2P transfers.[96] In addition to its payment technology, the LongPay app hosts other services that could front or facilitate laundering operations, such as an investment platform and in-app purchases of luxury watches priced at US$9 999. A hotel casino in Koh Kong, Cambodia, where scam workers were rescued in 2022, is displayed on the digital menu of a café in the app's food delivery service.[97] The app also includes a job listings page for a company owned by one of the directors of ZhengHeng Group, a company that was sanctioned by the United Kingdom for allegedly facilitating cyber-scam operations at its Koh Kong property. The real estate and casino companies connected to the property denied allegations of criminal activity.[98]



The LongPay app lists luxury watches for sale and food delivery by restaurants located inside a reported scam compound. *Source: LongPay*

Current evidence suggests some scam operations use fintech platforms to manage worker payments, facilitate money movement between compounds and external accounts, and convert between crypto and fiat currencies.[99] In some cases, workers are forced to use these platforms in a closed payment ecosystem within compounds, enabling the operators to monitor and control their finances.[100]

Corruption

Paying bribes is part of the cost of doing business for cyber scam operations, as such payments are documented along the entire criminal supply chain.[101] For example, reports indicate widespread bribery, including payments to secure passage at border checkpoints and armed escorts as workers are moved between compounds in Cambodia and Myanmar.[102] Compound managers also pay bribes to local authorities and police; a Vietnamese trafficking victim working at a scam compound in O'Smach,

Cambodia, alleged that the scam operation manager paid the local police US$30 000 per month.[103] Such payments can quickly add up to millions of dollars in areas densely populated by scam operations. Such is the case in Shwe Kokko, where a non-state armed group allegedly pays actors within the military-controlled government between US$19 million and US$96 million annually.[104]

The primarily cash-based and covert nature of these transactions makes them difficult to verify and quantify. Nonetheless, corruption-related payments are believed to be substantial and the gains spread beyond the person who receives them, since patronage networks typically require bribes to be dispersed upward through chains of command, also to secure elite protection from high-level power brokers in return.[105]

In addition, some corruption payments are paid openly as official fees and taxes. Examples were recorded in Myanmar-based cyber scam operations' accounting books as 'soldier fees' and 'river crossing fees.' The latter likely refers to payments made to the Karen National Army, a former Border Guard Force whose leaders profit significantly from the many scam compounds near Myawaddy[106] and tax economic activity in the area, including trade across the river from Thailand to Myanmar.[107] The same armed group also levied a THB8 891 (US$248) 'tax' on all workers in Shwe Kokko in 2024.[108] Similar schemes are likely to be employed elsewhere across the region, as compounds professionalize their structures and relationships with local authorities.[109]

The scam industry is also enabled by high-level political and business elites who profit by renting facilities to scam companies and provide an umbrella of protection to their operations. Some key individuals are alleged to have been active in regional criminal networks for years, including in the illegal and unregulated gambling operations in Southeast and East Asia.[110] Some influential individuals with alleged ties to criminal networks and scam compounds have been charged or sanctioned by the US, the UK and the EU for their suspected involvement in criminal activities, including cyber scam operations. However, there are many more unhindered perpetrators based across Southeast Asia and beyond who appear to be profiting from this form of criminal economy. This high-level protection through property ownership, business and political connections is another crucial way corruption enables the scam industry to flourish, although it remains largely unclear if and how high-level beneficiaries might receive transfers directly.

MONEY LAUNDERING SERVICE PROVIDERS

Money laundering in the cyber scam ecosystem is a professional, complex and multi-layered process that uses a range of diverse financial technologies and transfer mechanisms. While cryptocurrencies have become widely used by these criminal networks, the process is not limited to digital currencies alone. Criminal groups utilize a range of payment methods – including cash, bank transfers (involving accounts belonging to individuals and shell companies), cryptocurrencies and fintech, and gaming and gambling platforms – to deposit, move and launder illicit funds.[111] False invoicing and over-invoicing may also be used to move and hide illicit proceeds.[112]

To match the growing demand stemming from the industrial scale and sophistication of cyber scam operations, money laundering networks have quickly matured and professionalized their operations.[113] At the heart are so-called gateway companies, the trusted intermediaries who facilitate, insure and guarantee the complex financial flows between scam operations and money launderers (commonly referred to as 'motorcades') in return for significant fees.[114] While some gateway companies have been operating for several years, this money laundering ecosystem appears to be growing and is assumed to provide stability to cyber scam operations, allowing operators to budget and forecast effectively.[115]

Despite their primary criminal clientele, many larger gateway companies operate with a facade of legitimacy: they are registered entities that employ specialized departments such as human resources, accounting and marketing teams; they also utilize standard operating procedures.[116] Transnational criminal groups appear to prefer to rely on gateway companies rather than directly laundering money from scam victims. This mitigates risks and enables them to draw on gateway company employees' knowledge of financial and legal systems in scam victims' countries. By offering services such as escrow accounts[117] to facilitate transactions, mediation services to resolve disputes and guarantees for potentially lost funds, they help reduce the risk of losing funds to frozen bank accounts or other scammers.[118]

Money laundering terms

Criminal networks often communicate in public or private social media groups using coded language to make their conversations incomprehensible to outsiders while allowing effective communication among those fluent in money laundering slang. Many of these conversations take place in Chinese and basic terms are sketched out below. This also means that moving and laundering money is not a 'closed loop' anymore, with a specific set of actors, but the industry has evolved into a marketplace structure.

- **Gateway companies**, also referred to as *tongdaos* (通道), are intermediaries who facilitate communication and financial transactions between scam operations and money laundering service providers. They use encrypted messaging apps such as Telegram and digital payment platforms.[119]
- **'Moving bricks'** (*banzhuan*, 搬砖) is a money laundering process by which illicit funds are moved around to create a complex trail that obscures the original source of the funds.[120]
- **'Motorcade'** (*chē duì*, 车队), also referred to as 'trucks', refers to a group or network of individuals who specialize in moving and transferring cash or digital assets between accounts, platforms and currencies to create complex financial trails. 'Motorcades' move funds through mule accounts.
- **Mule accounts** are financial accounts used to transfer or hold illegally obtained money as part of a money laundering scheme.[121] A typical motorcade and its facilitator(s) use a series of mule accounts. To avoid detection, they use accounts affiliated with shell companies or purchase accounts from individuals who sell their account and identity information. In other cases, unsuspecting individuals' accounts are drained and hijacked to serve as a vehicle for channelling illicit funds.[122]
- **'U-merchants'** are over-the-counter currency dealers who often advertise their services in Telegram channels. The 'U' is short for USDT/Tether, the world's most popular stablecoin.[123] They exchange USDT, other cryptocurrencies and fiat currencies for money launderers and other customers.
- ***Pankou*** (盘口) is a term used by gateway company employees to refer to their 'clients' who seek money laundering services, such as the criminal groups running scam operations in Southeast Asia.[124]

According to the United Nations Office on Drugs and Crime (UNODC) and other sources, one of the first companies known to facilitate large scale money laundering services through Telegram chat groups was Fully Light Guarantee, a company associated with the conglomerate Fully Light Group and Myanmar military-affiliated armed groups.[125] This group previously owned and operated numerous casinos in Myanmar's Kokang Special Administrative Zone and it was suspected of playing a significant role in cross-border money laundering.[126] Fully Light Guarantee was believed to have ceased operations when key leaders were arrested and repatriated to China in early 2024, yet UNODC alleged that the group possibly maintained smaller chat groups under new names for the purpose of facilitating money laundering.[127]

Since 2024, Huione Group,[128] whose subsidiaries include Huione Guarantee and Huione Pay (汇旺), has attracted significant attention. It is a gateway service provider based out of Cambodia.[129] As noted above, Huione Guarantee hosts an online marketplace connecting money laundering service providers to clients. Meanwhile, Huione Pay, self-described as 'Alipay in Cambodia,' offers banking, payment

The office of Huione Pay, a gateway service provider under scrutiny for potential money laundering, in Phnom Penh, Cambodia, 2022. *© Google*

and currency exchange services.[130] In July 2024, Huione Pay came under scrutiny when Elliptic, a blockchain analysis firm, revealed it facilitated transfers from numerous illicit actors, including scam companies, armed groups and members of the North Korea-affiliated hacking group Lazarus.[131] In statements after the release of these reports, Huione Group reported that it was cooperating with a blockchain analytics company to 'let them help us with high-risk [cryptocurrency] address identification.'[132] But in March 2025, Radio Free Asia reported Huione Pay had been stripped of its banking licence by the National Bank of Cambodia.[133] Huione then claimed in a Telegram post that its payment operations do not require a licence; it also claimed that media reports linking it to illicit activities were false.[134] In May 2025, the US Department of the Treasury's Financial Crimes Enforcement Network identified Huione Group as a financial institution of primary money laundering concern and a critical node for laundering proceeds from cyber scam operations. It proposed to sever its access to the US financial system.[135] Several days later, Telegram reportedly banned thousands of accounts and usernames used for cyber scam money laundering.[136] Nevertheless, Elliptic reports that Huione continues operations and transaction data appears to show little decline.[137]

While the Huione companies have drawn most public scrutiny, many other gateway companies are reportedly operating in the region.[138] Gateway companies initiate the money laundering process depicted in Figure 2 below by facilitating communication and financial transfers between scam companies and 'motorcades'. This begins when a scam operator reaches out to a gateway company to request money laundering services. To find a suitable motorcade to process the funds, the gateway company posts their 'order' — including the jurisdiction and amount of funds they anticipate receiving from scam victims — in channels hosted on encrypted messaging apps such as Telegram.[139] Some of these channels reportedly boast thousands of subscribers.

After identifying and vetting a motorcade, the gateway company supplies the scam operator with bank account or cryptocurrency wallet details that they will use to receive the funds from scam victims. Scammers then instruct their victims to transfer fiat currency into fake investment platforms that are linked to these accounts or wallets.[140] This means that gateway companies generally do not handle illicit funds directly but instead provide services that connect the cyber scam operations and money launderers.

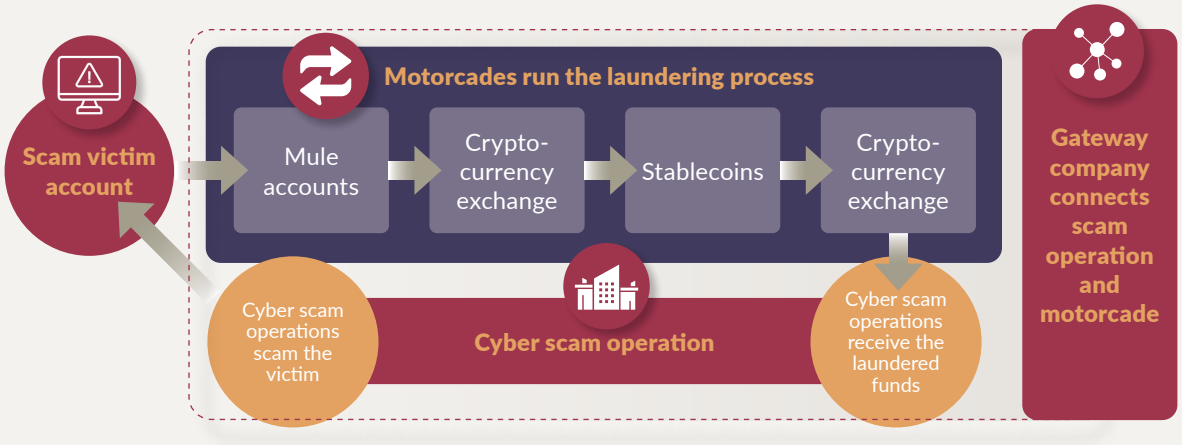


FIGURE 2 Overview of a typical money laundering process facilitated by gateway companies. Motorcades move the funds through various accounts and platforms.

Alternatively, scammers coach their victims on how to convert fiat to cryptocurrency on legitimate centralized exchanges and transfer it to the fraudulent platform, with the latter connecting their wallets to malicious smart contracts that give criminals direct access to their funds.[141] While researchers have observed both of these scenarios, there is no single blueprint for how this process is done. The motorcades, mule accounts and methods used to launder money adapt to avoid detection by law enforcement and banks in diverse jurisdictions.[142]

Once victims' money is placed in the initial account, it then moves through several motorcades or networks of coordinated accounts that receive and quickly send out illicit funds. Motorcades accomplish this by using mule accounts in traditional banks, but also digital fintech platforms and cryptocurrency DeFi applications. Through this process (see Figure 3), the financial trail from victim to the ultimate recipient is obscured by breaking the stolen funds into smaller quantities that are channelled through various platforms and currencies across numerous jurisdictions.

As many researchers have noted, cryptocurrency infrastructure plays a central role in the process. Typically, if the first motorcade receives the funds in fiat currency, they convert it into USDT or another cryptocurrency on a centralized exchange.[143] Next, they pass the funds through decentralized exchanges, fintech payment platforms and DeFi applications, such as cross-chain bridges to swap currencies between blockchains,[144] and 'mixers' to scramble the funds between digital wallets (for more details, see page 8).[145] As funds are redistributed at random to different accounts, the financial trail grows increasingly complex.[146]

Analysis of blockchain transactions has revealed new insights into this highly complex process. By tracing crypto as it passes through suspected money laundering accounts, analysts report seeing motorcades repeating the layering steps described above multiple times. They also believe laundering processes typically involve multiple distinct motorcades, which adds additional complexity to the financial trail.

After funds have moved through the entire motorcade, they are typically converted back into Tether (USDT) through a centralized exchange such as one of the exchanges depicted in Figure 4.[147]

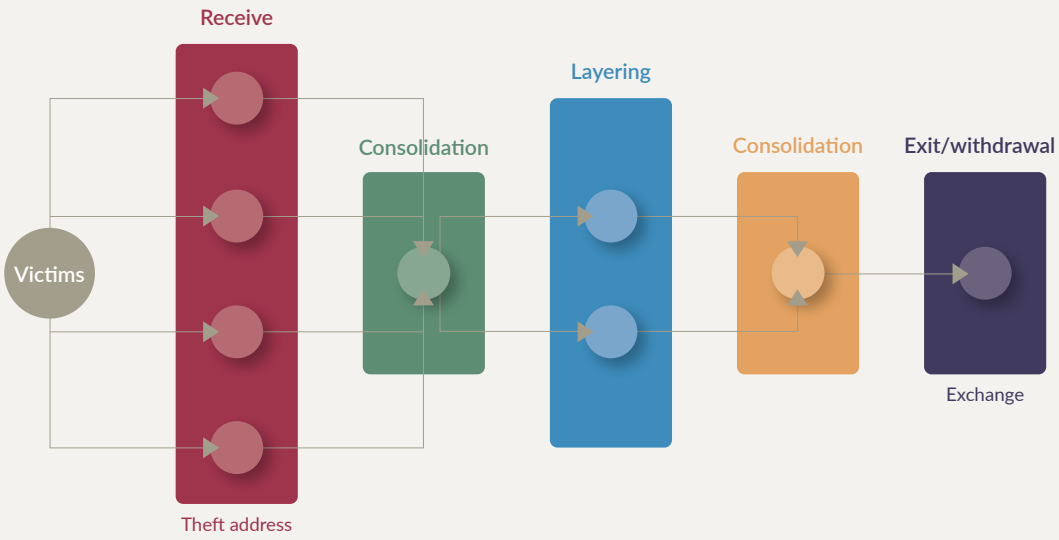


FIGURE 3 How scam funds are dispersed through several accounts and consolidated before moving on to the next motorcade to repeat the process. This layering creates a complex financial trail.

SOURCE: Adapted from Chainbrium, Pig butchering scams global total 2020–2023, May 2024, https://www.chainbrium.com/post/report-pig-butchering-scams-global-total-2020-2023

Finally, cashing out requires a crypto-to-fiat currency dealer. A variety of entities provide this service, including centralized exchanges, cryptocurrency fintech platforms, casinos and unlicensed money exchangers advertised through Telegram channels or located in physical locations in Southeast Asian countries.[148] Some gateway companies also exchange crypto to fiat currencies.[149] Both the gateway company and motorcades deduct fees based on the amount of funds laundered, the jurisdictions involved and the degree of risk involved.[150]

Some gateway companies may take a more direct role in the laundering process by operating their own motorcades. One source claimed that the company they worked for maintained a motorcade that received funds from victims in the US. They purportedly used the personal information of Chinese nationals residing in the US to open shell companies and bank accounts into which scam victims deposited their funds.[151] While the GI-TOC cannot corroborate this claim, US officials have in recent years investigated and arrested individuals suspected of involvement in investment scam-related money laundering schemes that conform to this description.[152]

In addition to the process described above, evidence suggests money launderers also use physical cash, informal money transfers systems (including *hawala*, *hundi*, *fei qian* and others)[153] and prepaid cards to move scam proceeds in the region.[154] Cash is also smuggled across borders in large quantities, converted between currencies and deposited into accounts belonging to individuals or shell companies. Law enforcement officials have documented this cross-border activity in several locations, notably between Cambodia and Vietnam, and Thailand and Myanmar. In one significant case, authorities intercepted US$2.17 million en route to Myawaddy in Myanmar.[155]

Finally, there is a high degree of overlap between the investors, physical locations and technical infrastructure involved in the online illegal gambling industry and scams in Southeast Asia.[156] In addition to the processes described above, therefore, scam funds are believed to be laundered through online gambling websites, physical casinos and junkets.[157]

It is important to note that this process is continuously evolving in response to regulatory changes, legal actions, law enforcement tactics and innovation in unregulated services. There is also variation between organized crime groups; for example, some operations might not use external money laundering services, but instead receive and launder money from scams directly.[158] Regardless of the process used, however, the fundamental goal remains the same: to create a complex, difficult-to-trace financial trail.

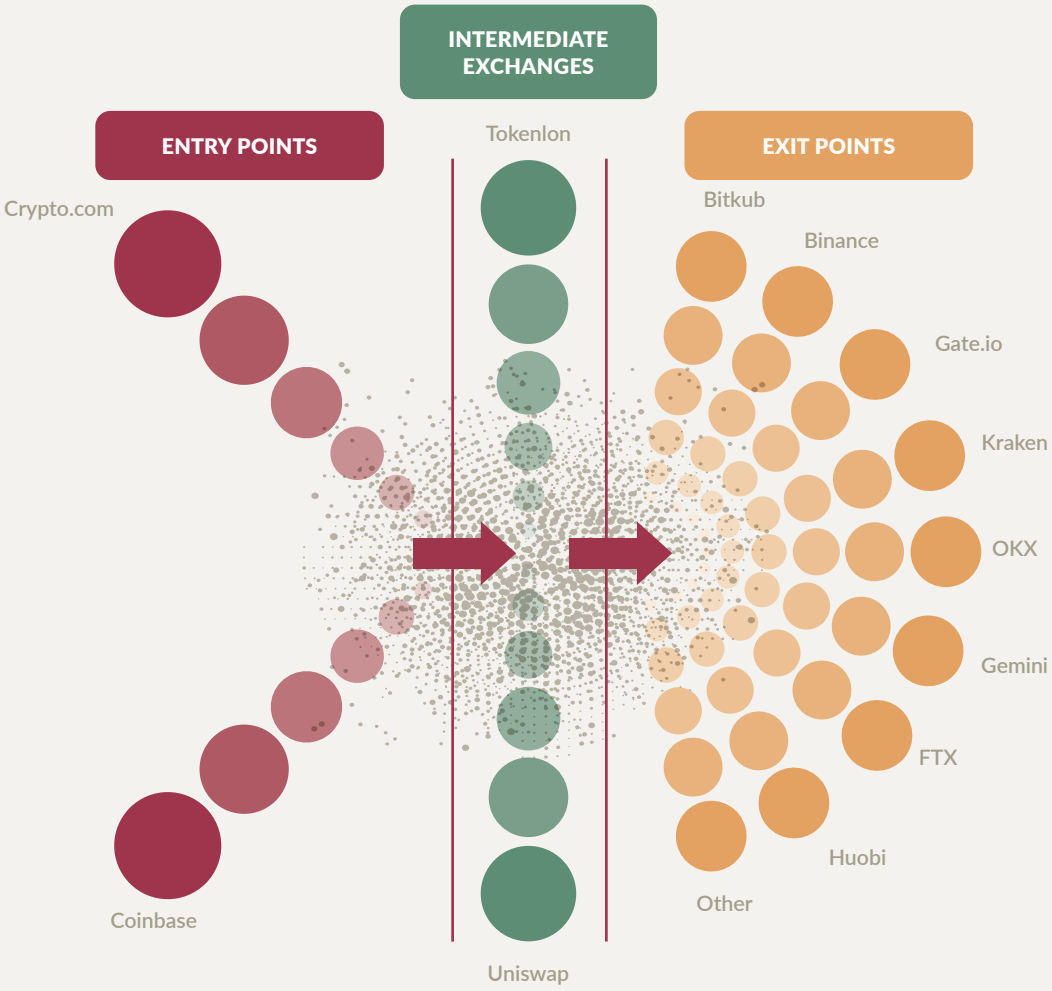


FIGURE 4 Examples of cryptocurrency exchanges used as entry points, intermediate exchanges and exit points during the laundering of scam proceeds on blockchains.

NOTE: The size of the circles does not correspond with the amount of funds sent and received.
SOURCES: Blockchain analysis of 1 018 crypto addresses commissioned by the GI-TOC; Chainalysis, The on-chain footprint of Southeast Asia's 'pig butchering' compounds: Human trafficking, ransoms, and hundreds of millions scammed, 24 February 2024, https://www.chainalysis.com/blog/pig-butchering-human-trafficking/; John M. Griffin and Kevin Mei, How do crypto flows finance slavery? The economics of pig butchering, SSRN, February 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235

WHO BENEFITS?

Following the money along the blockchain, through mixers, mule accounts and across fintech platforms is challenging but possible. However, it rarely reveals the so-called 'big fish' – those profiting most from the scam operations. Indeed, while high level political, business and criminal elites have previously been identified as key actors driving the spread of cyber scam operations, it remains largely unclear the extent to which they financially benefit from these operations and where the illicit funds ultimately end up.

Money laundering techniques will differ depending on the amount that needs laundering or the intended final use. Key final destinations for the illicit funds often include real estate, luxury goods, precious metals and bank accounts. Charitable donations represent another way to spend large amounts of money without declaring the origin.[159] Actors connected to scams in the region have engaged in all these activities.

Some rare insights into money flows and beneficiaries are provided by investigations, particularly a S$3 billion (US$2.2 billion) money laundering case in Singapore that hit headlines in 2023. The case investigated 34 foreign nationals for allegedly forging documents and engaging in other types of fraud to conceal criminal proceeds from scams, online gambling and other criminal activities. Ten of the 34 suspects arrested in 2023 were convicted, with seized assets totaling S$3 billion in cash, cryptocurrency, property, luxury bags, jewellery, cars and other high-value items.[160] Several defendants allegedly had links to scam compounds, illegal betting or compound owners in the region.[161]

To conceal their illicit funds, the defendants appear to have used shell companies and bank accounts across multiple jurisdictions, including Singapore, the UK, Cambodia, Australia and likely other countries.[162] Some forged financial statements to make the criminal proceeds appear as legitimate business income,[163] including some S$370 million (US$274 million) spread across 16 financial institutions, including three of Singapore's biggest banks.[164] Much of the illicit gains were ultimately invested in other assets within the jurisdiction of Singapore.[165] Some of the shell companies also helped register suspected fronts for scam operations. One London-based company associated with a defendant was linked to 9 000 other companies worldwide, with at least 47 of these companies suspected of running scams targeting British citizens.[166]

Defendants in the Singapore case (as well as others alleged to be profiting from the cyber scam industry) invested illicit proceeds into high-value properties in multiple countries.[167] Some of the defendants, for example, reportedly owned multi-million-dollar properties in Singapore and Dubai.[168]

One of multiple luxury cars confiscated in Singapore's 2023 money laundering investigation. Defendants allegedly used such high-value purchases to launder profits from scam operations and other criminal activities. *© Ore Huiying/Bloomberg via Getty Images*

Those convicted in the Singapore case were originally from Mainland China, but all held second passports from countries such as Saint Lucia, Saint Kitts and Nevis, Dominica, Cyprus, Cambodia, Türkiye and Vanuatu.[169] Nine out of the ten had Cambodian passports,[170] some of which may have been acquired through the country's citizenship-by-investment schemes. Cambodia offers a 10-year 'golden visa' to any adult without a criminal record who invests at least US$100 000, a scheme that graduates to passport eligibility after five years and an investment of US$245 000.[171] Cambodia reportedly stopped publishing data on new passports granted to foreigners in September 2024, around three months after the last conviction in the Singapore case.[172]

This is not the first time that citizenship-by-investment schemes have attracted attention, as several foreign nationals linked to scam compounds are also naturalized Cambodian citizens. This includes She Zhijiang, a dual citizen of China and Cambodia who was sanctioned by the US and the UK for his alleged ties to scam compounds in Myanmar and Laos.[173] He is currently detained in Thailand on illegal gambling charges and faces extradition to China.[174] While the Organisation for Economic Co-Operation and Development and the Financial Action Task Force (FATF), two leading global bodies driving policies on economic development and financial regulation, have expressed concerns about these passport schemes, criminal actors continue to use them to access investment opportunities and avoid repercussions when those investments involve criminal activities.[175]

Some beneficiaries – particularly elite players who hold positions in government and/or high-level business enterprises[176] – are believed to invest criminal proceeds into other illicit markets such as illegal gaming and gambling, the illegal wildlife trade and drugs.[177] This reinforces the poly-criminality of cyber scam operations as greater profits enable transnational criminal groups to expand their influence, including over public officials and the financial sector, which in turn reduces scrutiny of cyber scam compounds and related suspicious financial transactions. With their growing wealth, these criminal networks invest further into other types of organized crime and crime-as-a-service infrastructure, generating additional profits that allow them to strengthen their influence and market position.

Recent police seizures in the region have recovered large quantities of assets from individuals connected to scam operations, including gold bars, cash, art, cars, luxury bags, jewellery, electronics, expensive alcohol and cryptocurrencies.[178] However, experts have also noted that there appears to be minimal need to move illicit proceeds directly into Southeast Asian countries where scam compounds are located. Such movements are likely limited to those required to meet the cost of operations. Most proceeds from cyber scam operations are therefore assumed to remain offshore.

CONCLUSION AND RECOMMENDATIONS

Cyber scam operations in Southeast Asia generate tens of billions of dollars in illicit funds annually. This policy brief maps the extraordinarily diverse illicit financial flows involved, ranging from those derived from scams, trafficking in persons and forced labour, to those required to pay bribes and fund the basic operations of scam compounds. Professional money laundering service providers continue to adapt their techniques and enable organized criminal groups to profit significantly from these intersecting crimes.

This policy brief exposes major regulatory and enforcement gaps across both digital and traditional financial systems. While following and intercepting illicit money on the blockchain remains a major challenge for law enforcement, there are many other challenges, such as cash-based illicit economies, weak AML regimes and limited political will to change the status quo.

However, scrutiny of payments made to and from scam compounds has opened new opportunities for intervention and disruption. Establishing 'follow the money' strategies as a policy priority is essential to combat the economic impact and broader societal harms inflicted by this particular illicit economic model.

Cyber scam operations, like other forms of organized crime, prioritize both profit and risk mitigation. As long as laundering the proceeds of scams remains low-risk and lucrative for transnational criminal groups, operations will continue to expand and evolve. Disrupting illicit money flows is crucial to altering this incentive, even (or especially) in areas with weak governance or corruption. The more profits authorities seize, the more criminals must invest in complex laundering schemes and the less attractive scam operations will become.

'Taking the profit out of cyber scam operations' is a central part of the required response. Given the diverse mechanisms used to generate, move and launder illicit proceeds from cyber scams, a follow-the-money response needs to look at all these mechanisms. Failure to account for the broader spectrum of payment mechanisms (and the actors involved) risks missing the wider structural vulnerabilities across Southeast Asia that enable these flows. Key recommendations are summarized below.

Banks

This policy brief has shown that banks and the formal financial system play a much larger role in facilitating scams and related financial flows than generally acknowledged. Serving as entry and exit points for illicit funds and providing cross-border correspondent accounts for P2P platforms, traditional banking systems are integral to the financial infrastructure used by cyber scam operations and money laundering networks. Indeed, scam-related money laundering networks often receive funds through bank transfers, either to mule accounts or accounts linked to shell companies.[179] After laundering illicit proceeds, funds are exchanged back into fiat currency and deposited into offshore bank accounts.

And yet, awareness of cyber scam operations – and the scale at which they operate – appears to remain low among traditional banking institutions. It seems that few financial institutions in Southeast Asia and beyond are identifying and closing mule accounts at an appreciable scale. Instead, criminal groups are circumventing KYC screenings by using stolen identities and (more recently) deepfake technology.[180]

Southeast Asia's formal financial system is riddled with deficiencies, which can be easily exploited by transnational criminal groups. These vulnerabilities have also been recognized and widely reported on by the FATF. For example, Myanmar's serious 'strategic deficiencies' in countering money laundering landed it on the FATF blacklist in October 2022. In addition, Laos is on the FATF grey list alongside other jurisdictions that are subjected to increased monitoring.[181] The FATF removed the Philippines from the grey list in February 2025 and Cambodia in early 2023.[182] The FATF is often criticized for focusing primarily on ticking technical compliance boxes rather than scrutinizing the genuine effectiveness of AML regulation.[183] However, the low adherence to even basic technical compliance with global standards by most countries covered by this research points to significant shortcomings.

As noted above, compliance with FATF requirements alone does not constitute financial integrity. For example, the FATF perceives that Singapore possesses a strong legal and institutional framework against money laundering, but this city state also ranks third globally in terms of financial secrecy, meaning there tend to be fewer questions asked about the origins of money.[184] Furthermore, its good reputation, strong currency and international connectivity make it – as well as other key money laundering hubs such as Hong Kong, the UAE and the UK – highly attractive for money laundering purposes. These factors may well have fed into those implicated in the S$3 billion money laundering case choosing Singapore as an end-destination for much of their illicit gains.

To reduce these vulnerabilities, Southeast Asian policymakers, international organizations and financial institutions operating in the region and globally should consider:

- Investing more resources and capacity in mapping and blocking intersection points between the formal financial system and entities involved in cyber scam operations and money laundering networks.
- Raising awareness of cyber scam operations, including their scale, payment mechanisms and the impact they are having on societies and economies globally. This could be done through targeted briefings to financial institutions to improve the understanding of compliance teams that monitor suspicious transactions or onboard new clients. International organizations could also provide safe spaces for data sharing across industries and countries.

- Strengthening risk-based KYC requirements for financial institutions. While it is not realistic to spot all illicit actors through enhanced KYC measures – and the responsibility for this should not be borne solely by the financial sector – screening for high-risk indicators is critical. For example, this should include enhanced screenings for clients with multiple passports based on a regularly updated list of high-risk jurisdictions (or clients who maintain many bank accounts linked to their name).
- Enhancing frameworks for information and data exchange among financial institutions and financial intelligence units (FIUs), including cross-border collaboration. Public-private partnerships that facilitate exchange – such as the Singapore Anti-Scam Center and its Thai equivalent – represent good practice, but should involve a wider group of stakeholders, including civil society; they should also work across borders. The Association of Southeast Asian Nations (ASEAN) and other international organizations could play a key role in facilitating these partnerships and in promoting legislative coherence. In addition, industry driven thematic study groups could help share information and experiences more informally.
- Closing legislative loopholes, criminalizing the practice of money muling and making follow-the-money and AML issues a policy priority. Money laundering should be made a predicate offence to allow governments to prioritize money laundering investigations alongside trafficking in persons investigations (or other predicate crimes) and to prosecute money laundering independently. This approach should be more openly supported by ASEAN, since independent money laundering investigations may also support trafficking in person investigations.
- Strengthening the capacity of local law enforcement and FIUs, and ensuring they are adequately resourced to trace and seize illicit financial flows and enforce financial regulation. Countries should also consider making seized funds available to victims and/or civil society organizations that support trafficking victims.
- Urging the FATF to ensure that its assessment teams are speaking with a more diverse range of stakeholders and drawing on diverse sources of evidence when conducting their mutual evaluation reports. Given that FATF typologies and assessments are widely used to assess risks in countries and sectors, there is a clear need to assess the risks stemming from cyber scam operations more comprehensively.

Crypto platforms

Cryptocurrencies are integral to cyber scam operations, enabling fraud, worker compensation, ransom payments and the receipt of scam proceeds. They are also crucial for the money laundering process – particularly to layer and obscure the illegal origin of funds as well as move them across borders.[185]

There appear to be thousands of crypto addresses connected to scam compounds in Southeast Asia and there are many factors that make cryptocurrencies popular with criminal networks globally, including their pseudo-anonymous nature, transaction speeds, low costs and global access. The limited KYC checks performed by some cryptocurrency exchanges and other companies also makes them attractive to money launderers. This appears particularly true among service providers in the DeFi sector, many of which claim their decentralization as a pretext to argue that applying AML regulations is incompatible with their technology.[186]

Regulation so far has failed to keep pace with innovation in the sector. Many DeFi protocols and applications globally remain widely under-regulated or indeed entirely unregulated.[187] Although recent

cryptocurrency-related legislation and enforcement in the EU and the US sought to define and increase accountability in these systems, this progress may be rolled back.[188] In the US, the new administration set a goal of 'eliminating regulatory overreach on digital assets' and cut staff and resources dedicated to financial fraud investigations and enforcement (including of the National Cryptocurrency Enforcement Team and the Securities and Exchange Commissions' Crypto Assets and Cyber Unit).[189]

Another challenge is presented by the significant differences in regulatory approaches across jurisdictions. This limits cooperation across borders and creates opportunities to go 'jurisdiction shopping'.[190]

To reduce these vulnerabilities, Southeast Asian policymakers and private sector actors such as financial institutions should consider:

- Introducing and enhancing comprehensive and regionally cohesive cryptocurrency regulation that is aligned with FATF guidelines. This would include adequate AML regulation and enforcement — including but not limited to KYC requirements — for all money service providers, including DeFi platforms. International organizations should support Southeast Asian governments in these efforts. The level of requirements imposed should be proportionate to the risks inherent in these service providers, to avoid disproportionately high compliance costs. Given the rapidly changing nature of the digital assets industry, requirements will need to be monitored and updated regularly.
- Introducing nuanced and new types of regulation and enforcement that encompasses all types of cryptocurrency platforms, even if they only facilitate transfers and do not hold funds directly. These should be coherent across ASEAN and can be promoted by international organizations.
- Strengthening AML measures through enhanced transaction monitoring and risk screening (e.g. by including screening for unexplained wealth), particularly at centralized exchanges where most illicit funds enter and exit DeFi platforms. These should be coherent across ASEAN and can be promoted by international organizations.
- Enhancing collaboration between government agencies and the private sector to clarify the legal implications of technical terms (for example, decentralization) and develop regulations for the rapidly growing DeFi sector.
- Strengthening the capacity of local law enforcement and FIUs and ensuring they are adequately resourced to trace and seize digital assets, investigate the misuse and abuse of cryptocurrencies and enforce crypto regulation.
- Bolstering public-private collaboration, including with crypto technology firms as well as crypto analytics and investigation companies. This could include establishing working groups to discuss draft legislation, sharing technical expertise between these stakeholders, and scaling up capacity building efforts and other opportunities to foster dialogue, networking and cooperation.

Fintech platforms

Fintech platforms, which often utilize blockchain technology and are therefore connected to crypto platforms, also play an important role in facilitating illicit transfers. Like cryptocurrencies, they are commonly used by scam operations to pay operational expenses, including paying scam workers and managers. Most importantly, fintech companies that provide cryptocurrency-to-fiat exchange are a core part of the 'exit strategy' for criminal networks seeking to layer and launder their illicit gains.

Money transfer kiosks such as the one shown here are commonly used in Cambodia and throughout the region to send funds to friends and family. Some also offer services through apps. © *Khmer Times*

Fintech apps that facilitate P2P payments have gained popularity across Southeast Asia due to their speed, low cost and ability to send remittances across borders. For example, they offer money transfer services at kiosks (like the one pictured above) and digital payment apps, which customers can use to send money across international borders.[191] Such services are offered by numerous companies in the region and serve legitimate purposes, most notably the sending of remittances, but their easy accessibility and at times limited regulation and compliance regimes (compared to traditional financial institutions) make them vulnerable to abuse by criminals. Illicit proceeds can be easily concealed among legitimate transfers to and from these apps, where they can also be intermingled with funds coming from other high-volume sites such as online casino or betting apps.[192]

What stands out across Southeast Asia is that many fintech platforms hold financial service licences despite evidence of their misuse by criminal groups. This suggests limited political will for AML regulation and/or inadequate enforcement mechanisms. Additionally, some platforms are owned or influenced by members of the ruling elite (and/or people with close connections to them), suggesting that lax oversight may exist by design.[193]

Finally, there are many other fintech apps in development or use that fail to meet basic licensing criteria or are designed to operate informally (without regulation).

To reduce these vulnerabilities, ASEAN, national policymakers in Southeast Asia and private sector actors should consider:

- Strengthening licensing processes for payment apps through enhanced criminal exposure checks and a greater emphasis on establishing beneficial ownership. Financial regulators should shut down companies that own or host apps found to facilitate cyber scams and revoke the licences of inactive or non-functional apps to prevent future abuse. Existing licensing regulation needs to be enforced more comprehensively.
- Strengthening (and in some cases initiating) regulation of fintech companies and enforcing KYC requirements on these firms that are proportionate to the level of risk posed and are coherent across ASEAN.

- Updating fintech regulations and enforcement to address evolving money laundering tactics across P2P payment apps, gambling and betting sites, and crypto exchanges. These should likewise be coherent across ASEAN.
- Promote enhanced monitoring to identify high-risk and illicit transactions.
- Increasing financial literacy through public and private campaigns to help users to distinguish between legitimate and illicit financial platforms. This could be a public-private partnership where government agencies and financial institutions jointly develop and implement a comprehensive financial education strategy that includes public awareness campaigns. Additionally, legitimate financial institutions and governments could use social media and public advertisements to share bite-sized financial safety tips.

Cash

Cash remains a significant payment modality for those engaged in cyber scam operations and affiliated criminal networks. It is used to pay bribes to officials and armed groups, as well as operational costs like wages and utilities. Recent large-scale cash seizures at the Thai–Myanmar border near a scam compound highlight its continued importance to criminal networks in the region.

Southeast Asia's large informal economies present significant opportunities to move and launder illicit proceeds by comingling these funds with legitimate payments to small businesses such as restaurants, bars or entertainment companies. Cash payments are also widely used in construction and real estate. Because the origin cannot be easily established, cash transactions remain outside formal financial monitoring systems and offer criminal networks opportunities to move value undetected.

To reduce these vulnerabilities, Southeast Asian policymakers should consider:

- Promoting financial inclusion through expanded access to formal banking services. This can help reduce the informal economy and opportunities for criminal groups to exploit it. Increasing financial inclusion can also serve to prevent cyber scam operations as it is widely agreed that such inclusion helps reduce poverty and unemployment, key factors that make populations vulnerable to trafficking in persons.
- Implementing non-conviction-based confiscations, including civil asset forfeiture laws allowing authorities to seize suspicious cash found during investigations. This principle is not new but has been encouraged by the UN Convention Against Corruption. In Southeast Asia, Singapore has updated its law to support this approach.[194] Such laws can grant law enforcement authority to seize cash that is suspected to have derived from a crime and take custody of it while criminal investigations proceed, reducing the risk of it being hidden during any probe.
- Building forums on financial inclusion, fintech and financial regulation that comprise diverse stakeholders. This needs to extend to the international development community and also include those communities that are most affected by financial exclusion in the first place.
- Tracing cash seizures to understand how transnational criminal groups were able to obtain such large quantities of local currencies. This needs to be carried out in close cooperation with the central banks that issue and the financial institutions that disburse the cash.

NOTES

1 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

2 Chainalysis, The 2025 crypto crime report: The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation, February 2025, https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf; UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

3 International Organization for Migration, IOM's regional situation report on trafficking in persons into forced criminality in online scamming centres in Southeast Asia, February 2024, https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-02/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023.pdf; Huizhong Wu, Jintamas Saksornchai and Martha Mendoza, They were forced to scam others worldwide. Now thousands are detained on the Myanmar border, Associated Press, 9 March 2025, https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2.

4 Fiat currency is a government-issued form of money that holds value because of trust and legal recognition, rather than being backed by a physical commodity like gold or silver. Examples of fiat currencies include the Thai Baht (THB), Cambodian Riel (KHR) or the US Dollar (USD). TRM Lab, Glossary: Learn definitions and explore examples of common blockchain, crypto and digital asset terms, https://www.trmlabs.com/glossary/fiat-currency#what-is-fiat-currency-1.

5 Chainalysis, The 2025 crypto crime report: The rising role of cryptocurrency in all forms of crime and how its transparency is creating unique opportunities for investigation, February 2025, https://www.chainalysis.com/wp-content/uploads/2025/03/the-2025-crypto-crime-report-release.pdf; John M. Griffin and Kevin Mei, How do crypto flows finance slavery? The economics of pig butchering, SSRN, February 2024, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235; Elliptic, Huione: The company behind the largest ever illicit online marketplace has launched a stablecoin, 14 January 2025, https://www.elliptic.co/blog/huione-largest-ever-illicit-online-marketplace-stablecoin.

6 There is no universal definition of what exactly constitutes a *hawala* system (popular in the Middle East and South Asia) or other similar systems such as *hundi* (Myanmar) or *fei qian* networks (in China). In fact, these can refer to many kinds of informal money-transfer systems that often do not involve the physical transfer of cash and are frequently used by people to send remittances within and between countries. Commonly, customers use brokers based in their respective locations to send and receive money, with the senders paying a small commission and the receivers sometimes using a password to release the funds. Traditional *hawala* and similar systems are based on trust, meaning they can function in areas that lack a functional banking system; Julia Kagan, What is Hawala? Money transfer without money movement, Investopedia, https://www.investopedia.com/terms/h/hawala.asp; The Economist, How Chinese networks clean dirty money on a vast scale, 22 April 2024, https://www.economist.com/china/2024/04/22/how-chinese-networks-clean-dirty-money-on-a-vast-scale; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

7 People who conduct scams sometimes do so willingly and sometimes under duress. Forced labour is often the result of trafficking in persons, while willing labour is provided by low-level criminals. Some enter willingly but are later unable to leave or are trafficked but decide to stay as they are able to make a profit. See GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

8 Ivan Franceschini, Ling Li and Mark Bo, Compound capitalism: A Political economy of Southeast Asia's online scam operations, Critical Asian Studies, 2023, 55:4, 575-603, DOI: 10.1080/14672715.2023.2268104.

9 For examples of alleged scam workers given medical care at public or other external clinics, see: CNE News, Chinese woman dies after jumping from O'Smach hotel, 6 December 2020, https://cne.wtf/2020/12/06/chinese-woman-dies-after-jumping-from-osmach-hotel/; Al Jazeera, She Zhijiang: Discarded Chinese spy or criminal mastermind?, 26 September 2024, https://www.

aljazeera.com/program/101-east/2024/9/26/she-zhijiang-discarded-chinese-spy-or-criminal-mastermind.

10 Jack Adamović Davies, Torture, forced labor alleged at Prince Group-linked compound, Radio Free Asia, 12 February 2024, https://www.rfa.org/english/news/cambodia/prince-group-investigation-02122024143012.html.

11 This refers to scams where scammers built trust and romantic relationships with victims before directing them to fraudulent investment platforms; Cezary Podkul, What's a pig butchering scam? Here's how to avoid falling victim to one, ProPublica, 19 September 2022, https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one; US Institute of Peace, Transnational crime in Southeast Asia: A growing threat to global peace and security, May 2024, https://www.usip.org/publications/2024/05/transnational-crime-southeast-asia-growing-threat-global-peace-and-security.

12 For examples, see: Mael Le Touz, Vigorish viper: A venomous bet, Infoblox, https://insights.infoblox.com/resources-report/infoblox-report-vigorish-viper-a-venomous-bet.

13 For more information on these and other types of scams see: UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

14 FBI, Cryptocurrency investment fraud, https://www.fbi.gov/how-we-can-help-you/victim-services/national-crimes-and-victim-resources/cryptocurrency-investment-fraud; Nazarudin Latif, Indonesia deports 153 Chinese nationals accused of running online love scams, Benar News, 20 September 2023, https://www.benarnews.org/english/news/indonesian/china-love-scammers-deported-09202023145154.html.

15 RFA Lao and Eugene Whong, Debt-trapped Lao 'chat girls' forced to sell sex in China-run economic zone, 19 December 2021, https://www.rfa.org/english/news/laos/sez-trafficking-12192021113055.html; U Sudhakar Reddy, Chinese scammers in Cambodia force Indian women to make nude calls back home: Victim, *The Times of India*, 9 July 2024, https://timesofindia.indiatimes.com/city/hyderabad/chinese-scammers-in-cambodia-exploit-indian-women-in-cybercrime-scheme/articleshow/111590199.cms; Zhang Pengxiang, Five young people trapped in a fraud den in Laos, Huining police successfully rescued them, Gansu Daily, 28 September 2024, https://gansu.gansudaily.com.cn/system/2023/09/28/030883181.shtml.

16 Securities and Exchange Commission, Ponzi schemes using virtual currencies, https://www.sec.gov/files/ia_virtualcurrencies.pdf.

17 Federal Bureau of Investigation, Scammers target and exploit owners of cryptocurrencies in liquidity mining scam, 21 July 2022, https://www.ic3.gov/Media/Y2022/PSA220721; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

18 Ministry of Science and Technology, Most prominent online scams in VN: Game fraud, fake traffic fines and job scams, 1 December 2024, https://english.mic.gov.vn/most-prominent-online-scams-in-vn-game-fraud-fake-traffic-fines-and-job-scams-197240923080352007.htm; Ministry of Public Security of the PRC, quoted in China Daily, Telecom fraudsters target younger generation, 27 June 2024, https://www.chinadaily.com.cn/a/202406/27/ WS667cbc2da31095c51c50b10e.html.

19 Quoc Vu, Man says he's trapped in a scam compound with 'thousands', Radio Free Asia, 11 January 2024, https://www.rfa.org/english/news/vietnam/human-trafficking-01112024095958.html.

20 Information provided by an investigative journalist, November 2024; The scamdemic targeting the young and vulnerable, Rappler, 23 December 2024, https://www.rappler.com/technology/scamdemic-targeting-young-vulnerable/; Nelson Moura, Southeast Asia illegal online gaming and scam industries booming since mid-2010s: Monitoring group, Asia Gaming Brief, 26 February 2024, https://agbrief.com/intel/deep-dive/26/02/2024/southeast-asia-illegal-online-gaming-and-scam-industries-booming-since-mid-2010s-monitoring-group/; Jason Tower and Priscilla Clapp, Myanmar's casino cities: The role of China and transnational criminal networks, US Institute of Peace, https://www.usip.org/sites/default/files/2020-07/20200727-sr_471-myanmars_casino_cities_the_role_of_china_and_transnational_criminal_networks-sr.pdf.

21 Valentina Casulli, Mina Chiang, Larry Cameron, Aaron Kahler and Ian Mitchell, From fake job ads to human trafficking – the horrifying reality of the human trafficking scam trade, The Mekong Club, 27 July 2023, https://themekongclub.org/wp-content/uploads/2023/07/From_Fake_Job_Ads_to_Human_Trafficking_The_Horrifying_Reality_of_the_Human_Trafficking_Scam_Trade_2023.pdf; Emily Fishbein and Peter Guest, Inside a romance scam compound – and how people get tricked into being there, Pulitzer Center, 27 March 2025, https://pulitzercenter.org/stories/inside-romance-scam-compound-and-how-people-get-tricked-being-there.

22 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

23 United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

24 Smart contracts are computer programmes that automatically execute transactions when conditions are met. In the context of cryptocurrency transactions, a smart contract might automatically transfer funds from one wallet to another when a certain price point is reached.

25 Chainalysis, Money laundering and cryptocurrency: Trends and new techniques for detection and investigation, 11 July 2024, https://www.chainalysis.com/blog/money-laundering-cryptocurrency/; Internet Crime Complaint

Center, Cryptocurrency, https://www.ic3.gov/CrimeInfo/Cryptocurrency.

26 UNODC, Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

27 UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

28 Cezary Podkul and Cindy Liu, Human trafficking's newest abuse: Forcing victims into cyberscamming, ProPublica, 13 September 2022, https://www.propublica.org/article/human-traffickers-force-victims-into-cyberscamming; Department of Financial Protection & Innovation, Crypto scam tracker, https://dfpi.ca.gov/crypto-scams/; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

29 Cezary Podkul, What's a pig butchering scam? Here's how to avoid falling victim to one, ProPublica, 19 September 2022, https://www.propublica.org/article/whats-a-pig-butchering-scam-heres-how-to-avoid-falling-victim-to-one; Department of Financial Protection & Innovation, Crypto scam tracker, https://dfpi.ca.gov/crypto-scams/.

30 Office of Inspector General, Pig butchering scams, https://www.fdicoig.gov/pig-butchering-scams.

31 Chainalysis, The 2024 crypto crime report: The latest trends in ransomware, scams, hacking, and more, February 2024, https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf.

32 Department of Financial Protection & Innovation, Crypto scam tracker, https://dfpi.ca.gov/crypto-scams/.

33 Adam Hayes, Doretha Clemon and Suzanne Kvilhaug, Blockchain facts: What is it, how it works, and how it can be used, 24 March 2025, Investopedia, https://www.investopedia.com/terms/b/blockchain.asp.

34 Tether, Why use Tether?, https://tether.to/en/why-tether/.

35 This does not mean that TRON may not decline in popularity going forward; TRM Labs, Category deep-dive: Overall 2024 figures and declining illicit crypto volume on TRON, 18 February 2025, https://www.trmlabs.com/resources/blog/category-deep-dive-overall-2024-figures-and-declining-illicit-crypto-volume-on-tron; Chainalysis, The 2024 crypto crime report: The latest trends in ransomware, scams, hacking, and more, February 2024, https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf.

36 An ETF, or exchange-traded fund, gives investors exposure to multiple underlying assets. A crypto ETF allows for exposure to cryptocurrency markets without needing to have a digital wallet.

37 Investopedia, Cryptocurrency, https://www.investopedia.com/terms/c/cryptocurrency.asp.

38 Investopedia, What are smart contracts on the Blockchain and how do they work?, 12 June 2024, https://www.investopedia.com/terms/s/smart-contracts.asp.

39 Investopedia, Cryptocurrency, https://www.investopedia.com/terms/c/cryptocurrency.asp.

40 Ethereum, Decentralized finance (DeFi), https://ethereum.org/en/defi/; Jared Ronis, DeFi 101: The good, the bad, and the regulatory, 29 September 2023, https://www.wilsoncenter.org/article/defi-101-good-bad-and-regulatory.

41 Ethereum, Decentralized finance (DeFi), https://ethereum.org/en/defi/.

42 Elliptic, Typologies in focus: the threat of cross-chain crime, 23 October 2023, https://www.elliptic.co/blog/typologies-in-focus-the-threat-of-cross-chain-crime; TRM Labs, TRM Phoenix solves crypto investigators' 'chain-hopping' problem, 25 August 2022, https://www.trmlabs.com/resources/blog/trm-phoenix-solves-crypto-investigators-chain-hopping-problem.

43 Robert Stevens, Bitcoin mixers: How do they work and why are they used? Coindesk, March 2022, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/.

44 For example, a cross-chain bridge can convert Bitcoin on the Bitcoin blockchain to Tether on the Tron blockchain. This cross-chain movement complicates auditing, as investigators must track flows across multiple blockchains simultaneously; Elliptic, Typologies in focus: the threat of cross-chain crime, 23 October 2023, https://www.elliptic.co/blog/typologies-in-focus-the-threat-of-cross-chain-crime.

45 Coinbase, What is a DEX?, https://www.coinbase.com/learn/crypto-basics/what-is-a-dex; imToken, Multi-chain wallets management, https://token.im/wallet?locale=en-us.

46 A non-custodial wallet is one that allows users to maintain complete control of their private keys and funds rather than the exchange acting as intermediary. Crypto.com, Custodial vs non-custodial wallets, 17 February 2023, https://crypto.com/en/university/custodial-vs-non-custodial-wallets.

47 TRM Labs, The illicit crypto economy report, April 2024, https://www.trmlabs.com/the-illicit-crypto-economy-report; Chainalysis, The 2024 crypto crime report: The latest trends in ransomware, scams, hacking, and more, February 2024, https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf.

48 Filip Dimkovski and Marcel Deer, DEX vs. Dapp: What's the difference?, DefiPedia, 3 April 2022, https://defipedia.com/answers/dexs/dex-vs-dapp-what-s-the-difference.

49 TRM Labs, The illicit crypto economy report, April 2024, https://www.trmlabs.com/the-illicit-crypto-economy-report.

50 Chainalysis, The 2024 crypto crime report – the latest trends in ransomware, scams, hacking, and more, February 2024, https://www.chainalysis.com/wp-content/uploads/2024/06/the-2024-crypto-crime-report-release.pdf.

51 John M. Griffin and Kevin Mei, How do crypto flows finance slavery? The economics of pig butchering, SSRN, February 2024,

https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4742235; Jan Santiago, Money changers that front as tech companies, 24 November 2024, https://cannabiccino.substack.com/p/money-changers-that-front-as-tech.

52 Miles Johnson, James Fontanella-Khan, Alex Rogers and Joe Miller, The criminal's 'go-to cryptocurrency' has a new friend in the White House, *Financial Times*, 10 December 2024, https://ft.com/content/b3c5b67d-1df8-4417-8dd5-2c86d76d6392?accessToken=zwAGKP4adAQYkdOzxbZ9HfhEF9ON1SyG121jkg.MEYCIQCexOU242aqdkfeI72A9tz12x2Eb2chn8ced8kgmW6FVglhAMNFA9xfK69m5SSErmJCQeC2iQzBMyxGAn13ATTwnWG7&sharetype=gift&token=aad6bcaa-4c55-4f32-bd04-2c59e8cc22ec.

53 Denis Omelchenko, TRON teams up with TRM Labs to monitor USDT transactions, 10 September 2024, https://crypto.news/tron-teams-up-with-chainalysis-to-monitor-usdt-transactions/.

54 Office of the United Nations High Commissioner for Human Rights, Online scam operations and trafficking into forced criminality in Southeast Asia: recommendations for a human rights response, August 2023, https://bangkok.ohchr.org/wp-content/uploads/2023/08/ONLINE-SCAM-OPERATIONS-2582023.pdf; Valentina Casulli, Mina Chiang, Larry Cameron, Aaron Kahler and Ian Mitchell, From fake job ads to human trafficking – the horrifying reality of the human trafficking scam trade, The Mekong Club, 27 July 2023, https://themekongclub.org/wp-content/uploads/2023/07/From_Fake_Job_Ads_to_Human_Trafficking_The_Horrifying_Reality_of_the_Human_Trafficking_Scam_Trade_2023.pdf.

55 Ibid; Emily Fishbein and Peter Guest, Inside a romance scam compound – and how people get tricked into being there, Pulitzer Center, 27 March 2025, https://pulitzercenter.org/stories/inside-romance-scam-compound-and-how-people-get-tricked-being-there.

56 Indulekha Aravind and ET Bureau, The man who escaped the scam rings of Cambodia, *The Economic Times*, 2 June 2024, https://economictimes.indiatimes.com/jobs/mid-career/the-man-who-escaped-the-scam-rings-of-cambodia/articleshow/110626511.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst; Vincent MacIsaac, Myanmar's scam hells can't release their captives, 6 September 2024, https://www.irrawaddy.com/news/burma/myanmars-scam-hells-cant-release-their-captives.html; Frontier, Scam City: How the coup brought Shwe Kokko back to life, 23 June 2022, https://www.frontiermyanmar.net/en/scam-city-how-the-coup-brought-shwe-kokko-back-to-life/.

57 Frontier, Scam City: How the coup brought Shwe Kokko back to life, 23 June 2022, https://www.frontiermyanmar.net/en/scam-city-how-the-coup-brought-shwe-kokko-back-to-life/.

58 Online interview with a representative of an NGO supporting cyber scam victims, October 2024.

59 International Organization for Migration, IOM's regional situation report on trafficking in persons into forced criminality in online scamming centres in Southeast Asia, February 2024, https://roasiapacific.iom.int/sites/g/files/tmzbdl671/files/documents/2024-02/iom-southeast-asia-trafficking-for-forced-criminality-update_december-2023.pdf.

60 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

61 Ivan Franceschini, Ling Li & Mark Bo, Compound capitalism: A Political economy of Southeast Asia's online scam operations, Critical Asian Studies, 2023, 55:4, 575-603, DOI: 10.1080/14672715.2023.2268104; Vincent MacIsaac, Myanmar's scam hells can't release their captives, 6 September 2024, https://www.irrawaddy.com/news/burma/myanmars-scam-hells-cant-release-their-captives.html.

62 Humanity Research Consultancy, Uncovering the spread of human trafficking for online fraud into Laos and Dubai, July 2024, https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66a9db2e56d3b112ae6eff39_USAID-Asia-CTIP-Laos-Dubai-Investigation.pdf; Tara Siegel Bernard, Lured by a promising job, he was forced to scam people, *The New York Times*, 10 September 2024, https://www.nytimes.com/2024/09/10/business/scammers-trafficking-cybercrime.html; Humanity Research Consultancy, The horrible 5-month life in scamming compounds, 13 July 2024, https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds.

63 Suneth Perera and Issariya Praithongyaem, 'My hell in Myanmar cyber slavery camp', BBC News, 20 April 2024, https://www.bbc.com/news/articles/cw076g5wnr3o; RFA Lao, Four Laotian trafficking victims freed from Myanmar casino faced regular beatings, Radio Free Asia, 16 February 2023, https://www.rfa.org/english/news/laos/casino-02162023163151.html; Tara Siegel Bernard, Lured by a promising job, he was forced to scam people, *The New York Times*, 10 September 2024, https://www.nytimes.com/2024/09/10/business/scammers-trafficking-cybercrime.html; Affidavit from a Filipino rescued from O'Smach, September 2023.

64 Tan Hui Yee, China says controversial Myanmar city not a Belt and Road Initiative project, *The Straits Times*, https://www.straitstimes.com/asia/se-asia/china-says-controversial-myanmar-city-not-a-belt-and-road-initiative-project; Humanity Research Consultancy, The horrible 5-month life in scamming compounds, 13 July 2024, https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds;

65 Online interview with a representative of an NGO supporting cyber scam victims, October 2024.

66 Input received from experts working on cyber scam operations. See also: Indulekha Aravind and ET Bureau, The man who escaped the scam rings of Cambodia, *The Economic Times*, 2 June 2024, https://economictimes.indiatimes.com/jobs/mid-career/the-man-who-escaped-the-scam-rings-of-cambodia/articleshow/110626511.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst; Huo Beixiong, The escape of the Myawaddy

telecom fraud group in Myanmar (Part 2): 'Piggy' waiting to go home, Wainao, 5 March 2024, https://www.wainao.me/wainao-reads/Myanmar-telecom-scam-group-escape-ch2-03052024; Daphne Galvez, Torture den found in Pasay POGO hub, The Philippine Star, 1 November 2023, https://www.philstar.com/nation/2023/11/01/2308078/torture-den-found-pasay-pogo-hub; Isabelle Qian, 7 months inside an online scam labor camp, *The New York Times*, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html.

67 Vincent MacIsaac, Myanmar's scam hells can't release their captives, 6 September 2024, https://www.irrawaddy.com/news/burma/myanmars-scam-hells-cant-release-their-captives.html.

68 UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A Shifting Threat Landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

69 Frontier, Scam City: How the coup brought Shwe Kokko back to life, 23 June 2022, https://www.frontiermyanmar.net/en/scam-city-how-the-coup-brought-shwe-kokko-back-to-life/.

70 Ivan Franceschini, Ling Li and Mark Bo, Compound capitalism: A political economy of Southeast Asia's online scam operations, *Critical Asian Studies*, 2023, 55, 4, 575-603, 10.1080/14672715.2023.2268104; Humanity Research Consultancy, Uncovering the spread of human trafficking for online fraud into Laos and Dubai, July 2024, https://cdn.prod.website-files.com/662f5d242a3e7860ebcfde4f/66a9db2e56d3b112ae6eff39_USAID-Asia-CTIP-Laos-Dubai-Investigation.pdf.

71 Online interviews conducted with cyber scam experts in October 2024.

72 Isabelle Qian, 7 months inside an online scam labor camp, *The New York Times*, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html.

73 UNODC, Casinos, cyber fraud and trafficking in persons for forced criminality in Southeast Asia, Policy brief, August 2023, https://www.unodc.org/roseap/uploads/documents/Publications/2023/TiP_for_FC_Summary_Policy_Brief.pdf; Emily Fishbein, 'A global monster': Myanmar-based cyber scams widen the net, Frontier Myanmar, 24 August 2024, https://www.frontiermyanmar.net/en/a-global-monster-myanmar-based-cyber-scams-widen-the-net/.

74 Christian Shepherd, Shibani Mahtani and Pei-Lin Wu, A Chinese actor was enslaved in a compound running online scams, *The Washington Post*, 22 July 2024, https://www.washingtonpost.com/world/2024/07/22/myanmar-cyberscams-china-trafficking/.

75 Dave Grunebaum, In Southeast Asia's scam centers, human trafficking worsens, VOA, 5 December 2024, https://www.voanews.com/a/in-southeast-asia-s-scam-centers-human-trafficking-worsens/7888452.html.

76 Chainalysis, The on-chain footprint of Southeast Asia's 'pig butchering' compounds: Human trafficking, ransoms, and hundreds of millions scammed, 24 February 2024, https://www.chainalysis.com/blog/pig-butchering-human-trafficking/.

77 Site visits, Cambodia, January – May 2024; Mech Dara, Cindy Liu and Danielle Keeton-Olsen, Victims allege Sihanoukville precincts with ties to major businesses are sites of scams, torture, detention, Voice of Democracy, 18 February 2022, https://vodenglish.news/victims-allege-sihanoukville-precincts-with-ties-to-major-businesses-are-sites-of-scams-torture-detention/; Mech Dara and Cindy Liu, From timber to human trafficking: rescued victims allege major scam operations in tycoon's SEZ, Voice of Democracy, 17 November 2021, https://vodenglish.news/from-timber-to-human-trafficking-rescued-victims-allege-major-scam-operations-in-tycoons-sez/.

78 Interviews conducted with cyber scam experts in October 2024.

79 Isabelle Qian, 7 months inside an online scam labor camp, *The New York Times*, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

80 Komsan Tortermvasana, Fraud raid seizes 58 satellite devices, *Bangkok Post*, 19 June 2024, https://www.bangkokpost.com/business/general/2813459/fraud-raid-seizes-58-satellite-devices; Matt Burgess, Elon Musk's Starlink is keeping modern slavery compounds online, Wired, 27 February 2025, https://www.wired.com/story/starlink-scam-compounds/; Starlink, https://www.starlink.com/.

81 Starlink, Service plans, https://www.starlink.com/us/service-plans.

82 Interviews with residents, O'Smach, Cambodia, March 2024; Coby Hobbs and Khuon Narim, Mystery raids: Over 1,000 potential trafficking victims unaccounted for, CamboJA News, 9 December 2024, https://cambojanews.com/mystery-raids-over-1000-potential-trafficking-victims-unaccounted-for/; Hannah Beech, On a lawless tropical border, the global scam industry thrives, *The New York Times*, 27 February 2025, https://www.nytimes.com/2025/02/27/world/asia/scam-centers-myanmar-thailand-china.html.

83 For instance, Cambodian garment workers earn US$208 per month; Sen David, Minimum wage for workers raised by $4 for next year, *Khmer Times*, 20 September 2024, https://www.khmertimeskh.com/501562708/minimum-wage-for-workers-raised-by-4-for-next-year/.

84 Emily Fishbein and Nu Nu Lusan, Trapped in Myanmar's cyber-scam factories, Al Jazeera, 29 July 2024, https://www.aljazeera.com/news/longform/2024/7/29/trapped-in-myanmars-cyber-scam-mills; The Irrawaddy, Sex, drugs and cyber scams: Inside Myanmar's notorious online crime hub, 8 May 2024, https://irrawaddy.com/in-person/interview/sex-drugs-and-cyber-scams-inside-myanmars-notorious-online-crime-hub.html; Isabelle Qian, 7 months inside an online scam labor camp, *The New*

York Times, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html; Interviews, O'Smach residents, Cambodia, March 2024; C4ADS, Zoned out: A comprehensive impact evaluation of Mekong economic development zones, 2021, https://c4ads.org/wp-content/uploads/2021/06/ZonedOut-Report.pdf; GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

85 UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf; Elliptic, Huione guarantee: The multi-billion dollar marketplace used by online scammers, 10 July 2024, https://www.elliptic.co/blog/cyber-scam-marketplace; Will Jackson, Cambodian online marketplace outed as one-stop shop for scammers' money laundering and 'detention equipment' needs, Australian Broadcasting Corporation, 26 July 2024, https://www.abc.net.au/news/2024-07-27/online-marketplace-for-money-laundering-and-scammers/104131624.

86 Huione Guarantee recently changed its name to Haowong Guarantee. This report uses Huione Guarantee for consistency; Hao wang dan bao [Haowang Guarantee], Huan ying lai dao hao wang dan bao, https://www.yu444.com/.

87 Chainalysis, 2024 crypto crime mid-year update part 2: China-based CSAM and cybercrime networks on the rise, pig butchering scams remain lucrative, https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/.

88 Ibid; Elliptic, Huione guarantee: The multi-billion dollar marketplace used by online scammers, 10 July 2024, https://www.elliptic.co/blog/cyber-scam-marketplace.

89 Crunchbase, Fincy: Financials, https://www.crunchbase.com/organization/fincy-30fc/company_financials; Blockchain, Singapore fintech pulls out of Myanmar border city amid allegations, *The Business Times*, 7 October 2020, https://www.businesstimes.com.sg/startups-tech/startups/singapore-fintech-pulls-out-myanmar-border-city-amid-allegations.

90 Crunchbase, BCB Blockchain, https://www.crunchbase.com/organization/bcb-blockchain.

91 GBCI, Our team, https://gbci.ventures/our-team/; Jason Tower and Priscilla A. Clapp, Myanmar: Casino cities run on blockchain threaten nation's sovereignty, US Institute of Peace, 30 July 2020, https://www.usip.org/publications/2020/07/myanmar-casino-cities-run-blockchain-threaten-nations-sovereignty.

92 Sainul Abudheen K, This Singapore startup is set to turn Myanmar's Yatai City to a blockchain-powered smart city, e27, 1 October 2019. https://e27.co/this-singapore-startup-is-set-to-turn-myanmars-yatay-city-to-a-blockchain-powered-smart-city-20191001/; Stephanie Pearl Li, Singapore payment app Fincy exits Myanmar border city project after accusations, 8 October 2020, https://kr-asia.com/singapore-payment-app-fincy-exits-myanmar-border-city-project-after-money-laundering-accusations; fintech startup Fincy secures $11 mn from parent company GBCI Ventures; Entrepreneur Asia Pacific, 12 June 2020, https://www.entrepreneur.com/en-au/news-and-trends/fintech-startup-fincy-secures-11-mn-from-parent-company/351794.

93 Jason Tower and Priscilla A. Clapp, Myanmar: Casino cities run on blockchain threaten nation's sovereignty, US Institute of Peace, 30 July 2020, https://www.usip.org/publications/2020/07/myanmar-casino-cities-run-blockchain-threaten-nations-sovereignty; Sainul Abudheen K, This Singapore startup is set to turn Myanmar's Yatai City to a blockchain-powered smart city, e27, 1 October 2019. https://e27.co/this-singapore-startup-is-set-to-turn-myanmars-yatay-city-to-a-blockchain-powered-smart-city-20191001/.

94 *The Straits Times*, Myanmar: China says controversial Shwe Kokko New City has nothing to do with Belt and Road Initiative, 27 April 2020, https://www.straitstimes.com/asia/se-asia/china-says-controversial-myanmar-city-not-a-belt-and-road-initiative-project.

95 Fincy, In response to recent media allegations about the use of the Fincy app in Yatai City, Myanmar: A letter from the CEO, Medium, 14 October 2020, https://medium.com/fincy/in-response-to-recent-media-allegations-about-the-use-of-the-fincy-app-in-yatai-city-myanmar-cf8189185ec3.

96 LongPay, https://www.long-pay.net/en; Google Play, LongPay, https://play.google.com/store/apps/details?id=com.longbay.pay&hl=en_US&pli=1.

97 Humanity Research Consultancy, The horrible 5-month life in scamming compounds, 13 July 2024, https://www.humanity-consultancy.com/updates/the-horrible-5-month-life-in-scamming-compounds; Mary Ann Jolley and David Boyle, Cambodia's cyber slaves, Al Jazeera, 11 August 2022, https://www.aljazeera.com/features/longform/2022/8/11/meet-cambodia-cyber-slaves.

98 The director of ZhengHeng Group stated they sold part of the property and have 'no control over the activities therein'. The director of the Long Bay Casino claimed to have no knowledge of criminal activities in the casino; Jack Brook and Runn Sreydeth, Company linked to scams, human trafficking ousted from Cambodia property awards, 26 July 2023, Camboja News, https://cambojanews.com/company-with-ties-to-scams-human-trafficking-ousted-from-cambodia-property-awards/.

99 Jason Tower and Priscilla A. Clapp, Myanmar: Casino cities run on Blockchain threaten nation's sovereignty, United States Institute of Peace, 30 July 2020, https://www.usip.org/publications/2020/07/myanmar-casino-cities-run-blockchain-threaten-nations-sovereignty; Information provided by an investigative journalist, November 2024.

100 Information provided by an investigative journalist, May 2024.

101 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/; US Department

of State, 2024 trafficking in persons report: Burma, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/burma/; US Department of State, 2024 trafficking in persons report: Thailand, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/thailand/; US Department of State, 2024 trafficking in persons report: Cambodia, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/cambodia/; US Department of State, 2024 trafficking in persons report: Laos, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/laos/.

102 Naw Betty Han, South for the winter: Myanmar's cyber scam industry migrates, Frontier Myanmar, 29 August 2024, https://www.frontiermyanmar.net/en/south-for-the-winter-myanmars-cyber-scam-industry-migrates/; Vincent MacIsaac, Myanmar's scam hells can't release their captives, The Irrawaddy, 6 September 2024, https://www.irrawaddy.com/news/burma/myanmars-scam-hells-cant-release-their-captives.html; Christian Shepherd, Shibani Mahtani and Pei-Lin Wu, A Chinese actor was enslaved in a compound running online scams, *The Washington Post*, 22 July 2024, https://www.washingtonpost.com/world/2024/07/22/myanmar-cyberscams-china-trafficking/.

103 Lindsey Kennedy and Nathan Paul Southern, 'Just as scared': Cyberscam victims in Cambodia find no freedom in rescue, Al Jazeera, 24 November 2023, https://www.aljazeera.com/features/2023/11/24/just-as-scared-cyberscam-victims-in-cambodia-find-no-freedom-in-rescue.

104 Interview with a local journalist, March 2024, by online call; Jason Tower and Priscilla A. Clapp, China forces Myanmar scam syndicates to move to Thai border, 22 April 2024, US Institute of Peace, https://www.usip.org/publications/2024/04/china-forces-myanmar-scam-syndicates-move-thai-border.

105 US Department of State, 2024 trafficking in persons report: Burma, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/burma/; US Department of State, 2024 trafficking in persons report: Thailand, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/thailand/; US Department of State, 2024 trafficking in persons report: Cambodia, 2024, https://www.state.gov/reports/2024-trafficking-in-persons-report/cambodia/; Interview with trafficking survivor, 29 March 2024, online call.

106 Interview with local journalist, March 2024, by online call; Jason Tower and Priscilla A. Clapp, China forces Myanmar scam syndicates to move to Thai border, 22 April 2024, US Institute of Peace, https://www.usip.org/publications/2024/04/china-forces-myanmar-scam-syndicates-move-thai-border; The Irrawaddy, Myanmar's BGF: A family-run criminal enterprise with friends across Asia, 22 May 2024, https://www.irrawaddy.com/news/burma/myanmars-bgf-a-family-run-criminal-enterprise-with-friends-across-asia.html.

107 Isabelle Qian, 7 months inside an online scam labor camp, *The New York Times*, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html; Frontier Myanmar, Junta trade policies spark a smuggling revival at Thai border, 5 October 2022, https://www.frontiermyanmar.net/en/junta-trade-policies-spark-a-smuggling-revival-at-thai-border/; Naw Betty Han and Thomas Kean, On the Thai-Myanmar border, COVID-19 closes a billion-dollar racket, 7 June 2020, Frontier Myanmar, https://www.frontiermyanmar.net/en/on-the-thai-myanmar-border-covid-19-closes-a-billion-dollar-racket/.

108 Aung Naing, Karen BGF taxes Shwe Kokko workers as it moves away from Myanmar's military, Myanmar Now, 26 February 2024, https://myanmar-now.org/en/news/karen-bgf-taxes-shwe-kokko-workers-as-it-moves-away-from-myanmars-military/.

109 Jason Tower, China-linked transnational organized crime in Southeast Asia: A rising threat to US national security, Testimony before the US – China Economic and Security Review Commission, 20 March 2025, https://www.uscc.gov/sites/default/files/2025-03/Jason_Tower_Testimony.pdf.

110 Ibid; David Hutt, Chinese crime gangs descend on Southeast Asia, *Asian Times*, 22 August 2017, https://asiatimes.com/2017/08/chinese-crime-gangs-descend-southeast-asia/; Enze Han, Non-state Chinese actors and their impact on relations between China and Mainland Southeast Asia, *Trends in Southeast Asia*, January 2021, 1, https://www.iseas.edu.sg/wp-content/uploads/2020/12/TRS1_21.pdf.

111 Interviews with employees at three gateway companies, February – March 2024, a Southeast Asian country.

112 Possible scenarios may resemble this money laundering case using transnational diamond trade: Customs and Excise Department, Hong Kong Customs detects first-ever money laundering case through transnational diamond trading with about $500 million laundered, The Government of the Hong Kong Special Administrative Region, 28 December 2023, https://www.customs.gov.hk/en/customs-announcement/press-release/index_id_4031.html; ET Bureau, India, Hong Kong bust money laundering racket via diamond trade, *The Economic Times*, 29 December 2023, https://economictimes.indiatimes.com/industry/cons-products/fashion-/-cosmetics-/-jewellery/india-hong-kong-bust-money-laundering-racket-via-diamond-trade/articleshow/106388354.cms.

113 Selam Gebrekidan and Joy Dong, How scammers launder money and get away with it, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html.

114 An investigation by the *The New York Times* found one gateway company took a 15% cut to launder money in the United States. Selam Gebrekidan and Joy Dong, How we investigated money laundering, and what we found, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/takeaways-money-laundering-investigation.html.

115 Jason Tower, China-linked transnational organized crime in Southeast Asia: A rising threat to US national security, Testimony before the US – China economic and security review

commission, 20 March 2025, https://www.uscc.gov/sites/default/files/2025-03/Jason_Tower_Testimony.pdf; Selam Gebrekidan and Joy Dong, How scammers launder money and get away with it, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html.

116 Chainalysis, 2024 Crypto crime mid-year update part 2: China-based CSAM and cybercrime networks on the rise, pig butchering scams remain lucrative, 29 August 2024, https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/; Yanyu Chen, Moving bricks: Money laundering practices in the online scam industry, Global China Pulse, 24 September 2024, https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

117 Escrow accounts are designed to hold funds, securities or other assets pending the completion (or fulfilment) of certain conditions to release or distribute the escrow property. These are typically laid out in an escrow agreement and are managed through a tripartite agreement between a depositor, a beneficiary and an independent third-party provider – or escrow agent. Deutsche Bank, Escrow accounts explained, 24 August 2023, https://flow.db.com/trust-and-agency-services/escrow-accounts-explained.

118 Information on gateway companies collected from on-site research, interviews with current and former staff members, Telegram chat groups and channels used by people in the money-laundering industry, and internal documents from the gateway companies, including employee training manuals, trading rules, and fees; Blockchain analysis by GI-TOC researchers; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

119 Interviews with employees at three gateway companies, February – March 2024, a Southeast Asian country.

120 Ibid; Selam Gebrekidan and Joy Dong, How scammers launder money and get away with it, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html; Yanyu Chen, Moving bricks: Money laundering practices in the online scam industry, Global China Pulse, 24 September 2024, https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

121 The Economist, How Chinese networks clean dirty money on a vast scale, 22 April 2024, https://www.economist.com/china/2024/04/22/how-chinese-networks-clean-dirty-money-on-a-vast-scale; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

122 U.S. Department of Treasury, National money laundering risk assessment, 2024, https://home.treasury.gov/system/files/136/2024-National-Money-Laundering-Risk-Assessment.pdf; Ng Kang-chung, 124 suspects arrested in Hong Kong for allegedly lending accounts to fraudsters, *South China Morning Post*, 24 December 2024, https://www.scmp.com/news/hong-kong/article/3292173/124-suspects-arrested-hong-kong-allegedly-lending-accounts-fraudsters.

123 Binance Square, Lawyer: What are the criminal legal risks of U-business? How to prevent them?, 11 April 2024, https://www.binance.com/en/square/post/6656933148001.

124 Yanyu Chen, Moving bricks: Money laundering practices in the online scam industry, Global China Pulse, 24 September 2024, https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

125 Fully Light Group, Company profile, https://fullylight.com/profile.html; The Irrawaddy, China detains Myanmar Kokang Group including high-profile figures, 9 October 2023, https://www.irrawaddy.com/news/burma/china-detains-myanmar-kokang-group-including-high-profile-figures.html.

126 UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf; Cezary Podkul, Southeast Asian casinos emerge as major enablers of global cybercrime, ProPublica, 5 October 2023, https://www.propublica.org/article/casinos-cambodia-myanmar-laos-southeast-asia-fraud-cybercrime; UNODC, Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

127 RFA Burmese, Myanmar company director and regional officials 'arrested in China', 4 October 2024, https://www.rfa.org/english/news/myanmar/yunnan-arrests-10042023073528.html; The Irrawaddy, Myanmar junta transfers six suspected cyber scam bosses to China, 31 January 2024, https://www.irrawaddy.com/news/burma/myanmar-junta-transfers-six-suspected-cyber-scam-bosses-to-china.html; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

128 Huione Group subsidiaries are involved in various sectors, including tourism (hotels, yachts and helicopter leasing for 'Cambodians and Chinese'), logistics, entertainment (e.g, a 'military club' described as a 'military weapon experience place in cooperation with the local military') and finance.

129 NBC, List of payment service institutions, 30 June 2024, https://www.nbc.gov.kh/download_files/data/khmer/KH/PSIs.pdf.

130 Huìwàng, Huānyíng lái dào huìwàng zhīfù Xīn yī dài hùliánwǎng yínháng, https://www.huionepay.com.kh/; Huione, Who we are, https://www.huione.com/html/about.jsp; Huione Group, Huìwàng, https://play.google.com/store/apps/details?id=com.huione.huionenew&hl=en_US.

131 Elliptic, Huione Guarantee: The multi-billion dollar marketplace used by online scammers, 10 July 2024, https://www.elliptic.co/blog/cyber-scam-marketplace; Chainalysis, 2024 Crypto crime mid-year update part 2: China-based CSAM and cybercrime networks on the rise, pig butchering scams remain lucrative, 29 August 2024, https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-2/; Tom Wilson, Exclusive: North Korean hackers sent stolen crypto to wallet used by Asian payment firm, Reuters, 15 July 2024, https://www.reuters.com/technology/cybersecurity/north-korean-hackers-sent-stolen-crypto-wallet-used-by-asian-payment-firm-2024-07-15/.

132 Will Jackson, Cambodian online marketplace outed as one-stop shop for scammers' money laundering and 'detention equipment' needs, Australian Broadcasting Corporation, 26 July 2024, https://www.abc.net.au/news/2024-07-27/online-marketplace-for-money-laundering-and-scammers/104131624.

133 Jack Adamović Davies, Exclusive: World's 'largest online black market' loses banking license, 6 March 2025, https://www.rfa.org/english/cambodia/2025/03/06/huione-cambodia-cyberscam-cryptocurrency/.

134 Huione Pay, Telegram post, 9 March 2025, https://t.me/Huione7572/4560.

135 US Financial Crimes Enforcement Network, FinCEN finds Cambodia-based Huione group to be of primary money laundering concern, proposes a rule to combat cyber scams and heists, 1 May 2025, https://www.fincen.gov/news/news-releases/fincen-finds-cambodia-based-huione-group-be-primary-money-laundering-concern.

136 Andy Greenberg, The internet's biggest-ever black market just shut down amid a Telegram purge, Wired, 14 May 2025, https://www.wired.com/story/the-internets-biggest-ever-black-market-shuts-down-after-a-telegram-purge/.

137 Chainalysis, Huione carries on: Chinese-language platform's persistence reveals the complexity of on-chain financial crime disruption, 12 June 2025, https://www.chainalysis.com/blog/huione-guarantee-still-active-despite-shutdown/.

138 Interviews with employees at three gateway companies, February – March 2024, a Southeast Asian country; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

139 Ibid.

140 United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/; Input from financial crime experts, GI-TOC cyber scam expert meeting, Bangkok, 8 November 2024.

141 Chainalysis, Understanding crypto drainers, 16 May 2024, https://www.chainalysis.com/blog/crypto-drainers/; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/.

142 Selam Gebrekidan and Joy Dong, How we investigated money laundering, and what we found, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/takeaways-money-laundering-investigation.html.

143 A blockchain analysis commissioned by the GI-TOC analyzed illicit transactions to 1018 crypto addresses (190 Bitcoin, 599 Ethereum and 299 Tron addresses).

144 For example, a cross-chain bridge can convert Bitcoin on the Bitcoin blockchain to Tether on the Tron blockchain. This cross-chain movement complicates auditing, as investigators must track flows across multiple blockchains simultaneously; Elliptic, Typologies in focus: the threat of cross-chain crime, 23 October 2023, https://www.elliptic.co/blog/typologies-in-focus-the-threat-of-cross-chain-crime.

145 DeFi 'mixers' scramble cryptocurrencies between multiple wallets and redistribute equivalent amounts randomly, making them particularly effective for obscuring the connection between receiving and cash-out wallets; Robert Stevens, Bitcoin mixers: how do they work and why are they used? Coindesk, 11 March 2022, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/.

146 Robert Stevens, Bitcoin mixers: How do they work and why are they used? Coindesk, 11 March 2022, https://www.coindesk.com/learn/bitcoin-mixers-how-do-they-work-and-why-are-they-used/; Blockchain analysis of 1018 crypto addresses commissioned by the GI-TOC.

147 Blockchain analysis of 1018 crypto addresses commissioned by the GI-TOC; Chainalysis, The on-chain footprint of Southeast Asia's 'pig butchering' compounds: Human trafficking, ransoms, and hundreds of millions scammed, 24 February 2024, https://www.chainalysis.com/blog/pig-butchering-human-trafficking/.

148 Danielle Keeton-Olsen, In Cambodia's 'underground' crypto economy, Tether becomes coin of choice for Chinese-linked activities, 17 December 2023, *South China Morning Post*, https://www.scmp.com/week-asia/economics/article/3245224/cambodias-underground-crypto-economy-tether-becomes-coin-choice-chinese-linked-activities; UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

149 Interview with employees at three gateway companies, February – March 2024, a Southeast Asian country; Review of documents from gateway companies; UNODC, Inflection point: Global implications of scam centres, underground banking and illicit online marketplaces in Southeast Asia, April 2025, https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.

150 Interview with employees at three gateway companies, February – March 2024, a Southeast Asian country; Review of documents and Telegram posts from gateway companies.

151 Ibid; Yanyu Chen, Moving bricks: Money laundering practices in the online scam industry, Global China Pulse, 24 September

2024, https://globalchinapulse.net/moving-bricks-money-laundering-practices-in-the-online-scam-industry/.

152 U.S. Department of Justice, Two foreign nationals arrested for laundering at least $73m through shell companies tied to cryptocurrency investment scams, 17 May 2024, https://www.justice.gov/opa/pr/two-foreign-nationals-arrested-laundering-least-73m-through-shell-companies-tied; United States Attorney's Office, Eastern District of Texas, Chinese national charged in 'pig butchering' scheme, 21 May 2024, https://www.justice.gov/usao-edtx/pr/chinese-national-charged-pig-butchering-scheme; United States v. Li, Docket Number 2:24-cr-00311, Court Listener, 28 April 2024, https://www.courtlistener.com/docket/68539688/1/united-states-v-li/; James Reddick, Chinese national faces 20 years in US prison for laundering pig-butchering proceeds, 13 November 2024, https://therecord.media/chinese-national-faces-20-years-money-laundering-pig-butchering.

153 Center for Operational Analysis and Research, Hundi networks: Transferring into post-coup Myanmar, 28 September 2023, https://reliefweb.int/report/myanmar/hundi-networks-transferring-post-coup-myanmar; The Economist, How Chinese networks clean dirty money on a vast scale, 22 April 2024, https://www.economist.com/china/2024/04/22/how-chinese-networks-clean-dirty-money-on-a-vast-scale.

154 FATF, Money laundering through money remittance and currency exchange providers, June 2010, https://www.fatf-gafi.org/en/publications/Methodsandtrends/Moneylaunderingthroughmoneyremittanceandcurrencyexchangeproviders.html; Input from financial crime experts and the private sector, GI-TOC cyber scam expert meeting, Bangkok, 8 November 2024; UNODC, Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

155 UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf; Jason Tower and Priscilla A. Clapp, Myanmar scam hubs revive fast after China eases pressure on junta, 26 September 2024, https://www.usip.org/publications/2024/09/myanmar-scam-hubs-revive-fast-after-china-eases-pressure-junta.

156 Jason Tower, China-linked transnational organized crime in Southeast Asia: A rising threat to US national security, Testimony before the US – China Economic and Security Review Commission, 20 March 2025, https://www.uscc.gov/sites/default/files/2025-03/Jason_Tower_Testimony.pdf; Jonathan Head, Casinos, high-rises and fraud: The BBC visits a bizarre city built on scams, BBC, 6 February 2025, https://www.bbc.com/news/articles/c04nx1vnw17o; Lindsey Kennedy and Nathan Paul Southern, Cambodia's billion dollar scam, 15 October 2024, https://www.thedial.world/articles/news/issue-20/cambodia-cyber-scams-human-trafficking.

157 Interview with money exchanger at a Cambodian casino, March 2024; Cezary Podkul, Southeast Asian casinos emerge as major enablers of global cybercrime, ProPublica, 5 October 2023, https://www.propublica.org/article/casinos-cambodia-myanmar-laos-southeast-asia-fraud-cybercrime; UNODC, Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf.

158 Isabelle Qian, 7 months inside an online scam labor camp, *The New York Times*, 17 December 2023, https://www.nytimes.com/interactive/2023/12/17/world/asia/myanmar-cyber-scam.html; *Shendu: Mian bei pianzi de sha zhu pan, shi zenme rang ren qingjiadangchan de?* [Mandarin], August 2021, https://www.xinghuozhiku.com/59618.html.

159 Sophie Lemaître and Anrike Visser, Kleptocrats' trusted helpers: The professions that enable illicit financial flows, Anti-Corruption Resource Centre, 2023, https://www.u4.no/publications/kleptocrats-trusted-helpers.pdf.

160 Gyro Finance, *Xinjiapo baiyi xiqian an beihou: Wangzha, dubo, 'Fujian bang' de shemi yu zui'e* [Mandarin], 26 September 2023, https://www.tuoluo.cn/article/detail-10109660.html; Ashley Tham, Billion-dollar money laundering case: Three men deported to Japan, Cambodia, CNA, 2 June 2024, https://www.channelnewsasia.com/singapore/3-deported-japan-cambodia-billion-dollar-money-laundering-case-4380856.

161 Xinghui Kok, Assets seized in Singapore money laundering case swell to $2.2 bln – media, Reuters, 19 January 2024, https://www.reuters.com/world/asia-pacific/assets-seized-singapore-money-laundering-case-swell-22-bln-media-2024-01-19/; Kelly Ng, The $2bn dirty-money case that rocked Singapore, BBC, 12 April 2024, https://www.bbc.com/news/world-asia-66840450; Zaihan Mohamed Yusof, Billion-dollar money laundering probe widens to include precious metals; 24 more suspects named, *The Straits Times*, 29 August 2023, https://www.straitstimes.com/singapore/money-laundering-probe-precious-metal-dealers-given-34-names-to-check-for-suspicious-deals; James Porteous, and Jeremy Leung, The invisible empire: How Singapore court cases unmasked a multi-billion-dollar illegal betting syndicate, Asian Racing Federation, 1 August 2024, https://www.asianracing.org/email/202408qb-the-invisible-empire-how-singapore-court-cases-unmasked-a-multi-billion-dollar-illegal-betting-syndicate.

162 David Sun and Nadine Chua, Billion-dollar money laundering case: 9 out of 10 accused in S'pore have Cambodian links, *The Straits Times*, 21 September 2023, https://www.straitstimes.com/singapore/billion-dollar-money-laundering-case-9-out-of-10-accused-in-s-pore-have-cambodian-links.

163 Samuel Devaraj, Accused in $3 billion money laundering case handed six new charges related to forgery, *The Straits Times*, 20 February 2024, https://www.straitstimes.com/singapore/courts-crime/accused-in-3-billion-money-laundering-case-handed-six-new-charges-related-to-forgery; Rachel Lim, Billion-dollar money laundering case: Man charged with falsifying accounts, forgery, Channel News Asia, 23 January 2025, https://www.channelnewsasia.com/singapore/billion-dollar-money-laundering-case-wang-junjie-charged-forgery-falsifying-accounts-4891006.

164 Bloomberg, Singapore banks tighten screenings after scandal, *Taipei Times*, 11 June 2024, https://www.taipeitimes.com/News/biz/archives/2024/06/11/2003819158.

165 According to the Singaporean Minister for Home Affairs and Minister for Law, as of December 2024, 55% (S$1.54 billion) of the assets 'surrendered to the state' were cash and financial assets, while 45% (S$1.25 billion) were non-cash assets such as real estate, vehicles and luxury goods; Ministry of Home Affairs, Written replies to parliamentary questions: Total value of assets surrendered to the state in connection with the $3 billion money laundering case as of 31 December 2024, 26 February 2025, https://www.mha.gov.sg/mediaroom/parliamentary/total-value-of-assets-surrendered-to-the-state-in-connection-with-the-3-billion-money-laundering-case-as-of-31-december-2024; Lydia Lam, All the convicts in Singapore's S$3 billion money laundering case have been sentenced. What now?, Channel News Asia, 14 June 2024, https://www.channelnewsasia.com/singapore/billion-dollar-money-laundering-case-recap-cna-explains-conclusion-4401811.

166 UK Government, Jinying Invest Company Limited, https://find-and-update.company-information.service.gov.uk/company/11797729/officers; David Sun and Nadine Chua, Billion-dollar money laundering case: 9 out of 10 accused in S'pore have Cambodian links, *The Straits Times*, 21 September 2023, https://www.straitstimes.com/singapore/billion-dollar-money-laundering-case-9-out-of-10-accused-in-s-pore-have-cambodian-links; 47 companies estimated by an investigative journalist, November 2024.

167 Ashley Tham, Billion-dollar money laundering case: Three men deported to Japan, Cambodia, CNA, 2 June 2024, https://www.channelnewsasia.com/singapore/3-deported-japan-cambodia-billion-dollar-money-laundering-case-4380856; Jack Adamović Davies, Red flags abound in Prince Group's offshore dealings, 8 February 2024, Radio Free Asia, https://www.rfa.org/english/news/cambodia/prince-group-investigation-02082024130529.html.

168 Joyce Lim, Nadine Chua, Zaihan Mohamed Yusof and Andrew Wong, Who are the 10 charged after the billion-dollar anti-money laundering raid in Singapore?, *The Straits Times*, 22 August 2023, https://www.straitstimes.com/singapore/courts-crime/who-are-the-10-charged-following-the-billion-dollar-anti-money-laundering-raid-in-s-pore; David Sun, S'pore's alleged money launderers named alongside terrorist financiers, drug lords in Dubai probe, *The Straits Times*, 19 May 2024, https://www.straitstimes.com/singapore/s-pore-s-alleged-money-launderers-named-alongside-terrorist-financiers-drug-lords-in-dubai-probe.

169 Andrew Wong and Nadine Chua, $3b money laundering case: 10 convicted, 17 on the run; police are after the rest, 9 June 2024, *The Straits Times*, https://www.straitstimes.com/singapore/3b-money-laundering-case-10-convicted-17-on-the-run-police-are-after-the-rest.

170 Joyce Lim, Nadine Chua, Zaihan Mohamed Yusof and Andrew Wong, Who are the 10 charged after the billion-dollar anti-money laundering raid in Singapore?, *The Straits Times*, 22 August 2023, https://www.straitstimes.com/singapore/courts-crime/who-are-the-10-charged-following-the-billion-dollar-anti-money-laundering-raid-in-s-pore.

171 *Khmer Times*, Become a Cambodian citizen through investment: Everything you need to know, 10 October 2023, https://www.khmertimeskh.com/501374000/become-a-cambodian-citizen-through-investment-everything-you-need-to-know/; MLMUPC Cambodia, Law on Nationality, 9 October 1996, https://cdc.gov.kh/wp-content/uploads/2022/05/LAW-96-Nationality-E.pdf; Cambodia My 2nd Home, The official launch of Cambodia My 2nd Home, https://cm2h.com/.

172 Andrew Wong, Cambodia stops publishing details of new citizenships issued to foreigners, *The Straits Times*, 30 September 2024, https://www.straitstimes.com/singapore/cambodia-stops-publishing-details-of-new-citizenships-issued-to-foreigners; Andrew Wong and Nadine Chua, $3b money laundering case: 10 convicted, 17 on the run; police are after the rest, 9 June 2024, *The Straits Times*, https://www.straitstimes.com/singapore/3b-money-laundering-case-10-convicted-17-on-the-run-police-are-after-the-rest.

173 Office of Financial Sanctions Implementation HM Treasury, Global Human Rights, 8 December 2023, https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf; US Department of the Treasury, Treasury sanctions the Zhao Wei Transnational Criminal Organization, 30 January 2018, https://home.treasury.gov/news/press-releases/sm0272.

174 The Irrawaddy, Chinese mega project in Myanmar 'not affected' by owner's arrest: company official, 15 August 2022, https://www.irrawaddy.com/news/burma/chinese-mega-project-in-myanmar-not-affected-by-owners-arrest-company-official.html; Andrew Nachemson, The mystery man behind the Shwe Kokko project, Frontier Khmer, 7 July 2020, https://www.frontiermyanmar.net/en/the-mystery-man-behind-the-shwe-kokko-project/.

175 OECD, Residence/citizenship by investment schemes, https://web-archive.oecd.org/tax/automatic-exchange/crs-implementation-and-assistance/residence-citizenship-by-investment/index.htm; Henry Pope, Golden passports make it too easy for criminals, FATF report finds, OCCRP, 24 November 2023, https://www.occrp.org/en/news/golden-passports-make-it-too-easy-for-criminals-fatf-report-finds.

176 GI-TOC, Compound crime: Cyber scam operations in Southeast Asia, May 2025, https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

177 For example, as is reported for Zhao Wei, for example; US Department of the Treasury, Treasury sanctions the Zhao Wei Transnational Criminal Organization, 30 January 2018, https://home.treasury.gov/news/press-releases/sm0272; Office of Financial Sanctions Implementation HM Treasury, Global Human Rights, 8 December 2023, https://assets.publishing.service.gov.uk/media/6572d548049516000d49be78/Notice_Global_Human_Rights_081223.pdf; Environmental Investigation Agency, Footage reveals criminal-run tiger 'farms' in Laos have actually been expanded, 8 March 2022, https://eia-international.org/press-releases/footage-reveals-criminal-run-tiger-farms-in-laos-have-actually-been-expanded/.

178 UNODC, Transnational organized crime and the convergence of cyber-enabled fraud, underground banking and technological innovation in Southeast Asia: A shifting threat landscape, October 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf; Associated Press, Gold, watches and other luxury items totaling $1.75B seized in Singapore money laundering scheme, 21 September 2021, https://apnews.com/article/singapore-money-laundering-asset-seizure-7640db7f784c05ac9024ef877aba1045.

179 More research is needed to determine the amount of funds entering money laundering networks via banks as compared to alternative methods, such as cryptocurrency exchanges.

180 UNODC, Casinos, money laundering, underground banking, and transnational organized crime in East and Southeast Asia: A hidden and accelerating threat, January 2024, https://www.unodc.org/roseap/uploads/documents/Publications/2024/Casino_Underground_Banking_Report_2024.pdf; Alanna Titterington, How fraudsters bypass customer identity verification using deepfakes, Kaspersky, 15 August 2024, https://www.kaspersky.com/blog/how-deepfakes-threaten-kyc/51987/.

181 FATF, 'Black and grey' lists, https://www.fatf-gafi.org/en/countries/black-and-grey-lists.html.

182 FATF, Cambodia, https://www.fatf-gafi.org/en/countries/detail/Cambodia.html.

183 An upcoming round of 'mutual evaluation' – the process by which the FATF assesses AML measures – will seek to focus more on the genuine effectiveness of measures.

184 Tax Justice Network, Financial Secrecy Index 2022, https://fsi.taxjustice.net/.

185 Chainalysis, Money laundering and cryptocurrency: Trends and new techniques for detection and investigation, 11 July 2024, https://www.chainalysis.com/blog/money-laundering-cryptocurrency/; Selam Gebrekidan and Joy Dong, How scammers launder money and get away with it, *The New York Times*, 23 March 2025, https://www.nytimes.com/2025/03/23/world/asia/cambodia-money-laundering-huione.html.

186 Iwa Salami, Challenges and approaches to regulating decentralized finance, Cambridge University Press, 6 December 2021, https://doi.org/10.1017/aju.2021.66; Jan Santiago, Money changers that front as tech companies, 24 November 2024, https://cannabiccino.substack.com/p/money-changers-that-front-as-tech.

187 District of Columbia Department of Insurance, Securities & banking, beware of decentralized finance (DeFi), https://disb.dc.gov/page/beware-decentralized-finance-defi; Iwa Salami, Challenges and approaches to regulating decentralized finance, Cambridge University Press, 6 December, 2021, https://doi.org/10.1017/aju.2021.66.

188 Thomas Gentle, Preparing for DeFi regulation: The role of portable KYC, 7 August 2024, https://www.coindesk.com/opinion/2024/08/07/preparing-for-defi-regulation-the-role-of-portable-kyc; European Commission, Crypto-assets, https://finance.ec.europa.eu/digital-finance/crypto-assets_en; Commodity Futures Trading Commission, CFTC issues order against Uniswap Labs for offering illegal digital asset derivatives trading, 4 September 2024, https://www.cftc.gov/PressRoom/PressReleases/8961-24.

189 The White House, Fact Sheet: Executive Order to establish United States leadership in digital financial technology, 23 January 2025, https://www.whitehouse.gov/fact-sheets/2025/01/fact-sheet-executive-order-to-establish-united-states-leadership-in-digital-financial-technology/; Todd Blanche, Memorandum for all department employees: Ending regulation by prosecution, U.S. Department of Justice, 7 April 2025, https://www.justice.gov/dag/media/1395781/dl?inline; Matthew Goldstein, Eric Lipton and David Yaffe-Bellany, S.E.C. moves to scale back its crypto enforcement efforts, *The New York Times*, 4 February 2025, https://www.nytimes.com/2025/02/04/business/sec-crypto-task-force.html; Anna Betts, Trump's justice department to disband unit investigating crypto fraud, *The Guardian*, 8 April 2025, https://www.theguardian.com/us-news/2025/apr/08/trump-crypto-doj.

190 Input from financial crime experts, GI-TOC cyber scam expert meeting, Bangkok, 8 November 2024.

191 Wing Bank, World transfer, https://www.wingbank.com.kh/en/personal/money-transfer/international-money-transfer/; Wing and ABA Bank launch fund transfers and cash deposit services, 28 January 2020, https://www.wingbank.com.kh/en/wing-aba-bank-launch-fund-transfers-cash-deposit-service/.

192 Information provided by an investigative journalist, May 2024.

193 Interviews conducted with cyber scam experts, October 2024.

194 Ministry of Home Affairs, Phased Commencement of the Anti-money Laundering and Other Matters Act, Government of Singapore, 13 November 2024, https://www.mha.gov.sg/mediaroom/press-releases/phased-commencement-of-the-anti-money-laundering-and-other-matters-act/.

GLOBAL INITIATIVE
AGAINST TRANSNATIONAL ORGANIZED CRIME

ABOUT THE GLOBAL INITIATIVE

The Global Initiative Against Transnational Organized Crime is a global network with over 700 Network Experts around the world. The Global Initiative provides a platform to promote greater debate and innovative approaches as the building blocks to an inclusive global strategy against organized crime.

www.globalinitiative.net