July 2026

The Accountability Gap – Tackling Cyber Fraud Across Legal Frameworks

Assessing the role of anti-trafficking, cybercrime, and financial regulations in the fight against online scams

By Allison Pytlak, Courtney Weatherby, Kathleen Scoggin

Cyber-enabled fraud and scams have become a global crisis, laundering billions of dollars annually and capturing victims across every region. Yet, the legal tools built to fight back, anti-trafficking protocols, cybercrime laws, and anti-money laundering frameworks, remain unevenly applied and inconsistently enforced. Fragmented enforcement and jurisdictional challenges leave gaps that sophisticated transnational networks exploit. This report takes stock of where these three frameworks are gaining traction, where they are falling short, and what governments, financial institutions, and international bodies must do to close the gaps.

Contents

Introduction

Cyber-enabled fraud ("online scam operations") have emerged as an increasingly urgent security concern in recent years. The facilities out of which they operate exist in multiple locations globally but have been most prolific in the special economic zones (SEZs) and fragile spaces in the Indo-Pacific region, especially Southeast Asia, where they have rapidly altered the landscape of transnational organized crime. Technological developments, combined with rapid digitalization, weak governance, limited law enforcement capability in the areas where scam centers are most concentrated, and lax regulation of key markets like cryptocurrency have created a perfect storm for criminal enterprises to rapidly and efficiently scale-up their operations.

These are not victimless crimes. The United States Institute of Peace (USIP) offers a conservative estimate of funds stolen worldwide by transnational crime syndicates in Southeast Asia to be $64 billion.[1] Analysis shows that cyber fraud criminals use a "scattergun" approach that prioritizes scale over precision, in which situational vulnerabilities such as stress, bereavement, distraction, or divorce are exploited.[2] The general population is the most targeted group, irrespective of age, language, gender or other immutable characteristics.

Online scam operations challenge the rule of law in countries where operations are based, while causing ripple effects and economic burdens for primary victim economies and increasingly threatening national, regional, and global security. They pose unique governance challenges. Scams are often treated as individual instances both socially and in the legal system, but these are also not isolated crimes. Rather, they are sophisticated criminal money-making business models developed as part of a market ecosystem unconstrained by geography or traditional jurisdictions, while exploiting gaps between law enforcement, financial intelligence, and the private sector.

---

[1] United States Institute of Peace Senior Study Group, *Transnational Crime in Southeast Asia: A Growing Threat to Global Peace and Security* (Washington, DC: United States Institute of Peace, May 2024), https://www.usip.org/sites/default/files/2024-05/ssg_transnational-crime-southeast-asia.pdf.
[2] Emily Taylor, "Large Scale, AI Analysis of Scam Signals Calls for Safeguarding Approach to Scam Prevention," *Oxford Information Labs (OXIL)*, March 16, 2026, https://oxil.uk/news/large-scale-ai-analysis-of-scam-signals-calls-for-safeguarding-approach-to-scam-prevention.

As criminal networks grow more sophisticated, the need for robust, coordinated legal accountability has never been more urgent. The question is not whether society has an obligation to confront these harms, but whether the frameworks and tools at our disposal are equal to the scale of the problem. If legal frameworks aren't up to task, what needs to change? And if they are, what are the challenges and obstacles which inhibit effective responses?

As other Stimson Center work in this area has noted, a primary challenge in countering cyber-enabled fraud and scams is that there is no single agency, community, or sector that can address this problem alone.[3] The threat is transboundary *and* sits at the intersection of other cross-border threats: organized crime, money laundering, human trafficking, and corruption, making it a prime example of polycriminality. The digital platforms and infrastructure through which scams operate present their own governance gaps in which questions of content moderation, data governance, and platform accountability remain contested across jurisdictions, with tech sector self-regulation often outpacing or even substituting for coherent legal guardrails. Existing legal frameworks address many of the components of the "scam lifecycle," but the way in which they intersect and are unevenly applied or enforced makes it challenging to fully leverage the full legal and normative toolkit in bringing perpetrators to account.

Responses should look to leverage multiple areas of law. Legal frameworks against trafficking-in-persons and forced labor correspond with one of cyber-enabled fraud's more brutal aspects: the false recruitment and coercion of people into "working" within scam centers, often transforming victims into instruments of criminal enterprise. Financial crime law and anti-money laundering (AML) regimes are relevant because fraud rarely ends with the initial theft: Stolen funds must be moved, hidden, laundered, and re-integrated within legitimate economies before they can be used. Cybercrime law governs the digital infrastructure, activities, and even many of the tools which underpin most aspects of a cyber-enabled fraud operation, from phishing activities to AI-generated deception, and can facilitate law enforcement cooperation across jurisdictions.

Existing laws, policies, and regulations across the three areas described above are distinct, but the nature of cyber-enabled fraud is creating new interdependencies. For

[3] Allison Pytlak, Courtney Weatherby, Brian Eyler, Shreya Lad, and Kathleen Scoggin, "Countering Digital Deception: National Responses to Online Scams," *Stimson Center*, August 11, 2025, https://www.stimson.org/2025/countering-digital-deception-national-responses-to-online-scams/.

example, a criminal syndicate running a cryptocurrency investment scam may simultaneously be violating securities law, AML obligations, and computer fraud statutes while its operators sit beyond the reach of any single jurisdiction, and operations are being implemented by individuals that have been trafficked or coerced. Recent efforts to disrupt and dismantle fraud centers and operators are encouraging and also offer lessons in how to draw from multiple legal frameworks against common targets. Effective accountability demands that investigators, prosecutors, regulators, and policymakers understand how these legal regimes interact, where they reinforce each other, and where gaps in coverage allow harm to persist.

This report examines relevant laws, policies, and normative frameworks in three areas: anti-trafficking in persons, financial crime and anti-money laundering, and cybercrime at international, regional, and national levels. Each chapter contextualizes the issue of fraud and scams within the respective topic; breaks down relevant treaties, laws, regulations, and practices; identifies gaps and challenges; provides examples of good practice; and offers suggestions on the way forward. Together, they make the case that combating fraud and scams is a fundamental question of justice, institutional integrity, and the rule of law. The core issue is not a lack of laws or legal frameworks but rather the constraints on effective implementation and enforcement. Each brief identifies some of these constraints and explores potential pathways to working through or around them. Many of these constraints are shared across sectors, while others may be unique to the trafficking, cyber, and financial sectors.

The report is the culmination of a two-year consultative process in which the Stimson Center convened a multi-national and cross-sectoral group of experts to discuss these and other areas of law, including through four online roundtables and one in-person capstone workshop in Bangkok, Thailand.[4] This occurred in the context of a wider capacity-building project focused primarily on five countries (Cambodia, Lao, the Philippines, Thailand, and Vietnam). The project has been supported by Global Affairs Canada. We are grateful to all contributors and participants in our roundtables and workshop.

[4] Courtney Weatherby and Allison Pytlak, "Breaking Silos to Beat Scams: Why Holistic Law Enforcement Matters," *Stimson Center*, March 19, 2026, https://www.stimson.org/2026/breaking-silos-to-beat-scams-why-holistic-law-enforcement-matters/.

Anti-Trafficking in Persons Law and Frameworks

Online scam compounds based largely in Southeast Asia have rapidly emerged as a major destination for trafficking in persons (TIP), challenging the application of existing anti-trafficking laws and frameworks. While the situation is in flux, the United Nations has estimated at least 300,000 people have been trafficked into compounds across the region, with victims drawn from more than 60 countries through fraudulent job offers – typically promises of legitimate employment in technology, customer service, or hospitality.[5] Once inside these compounds, individuals are subject to confinement, physical coercion, debt bondage, systemic violence, and sexual violence and abuse, with their documents being confiscated and freedom of movement denied.[6]

What distinguishes trafficking into scam compounds from other forms of forced labor or exploitation is the name of the harm inflicted on victims and the role they are compelled to play. Unlike most historical trafficking contexts — which targeted precisely because they lacked formal skills or education — trafficked persons in scam compounds are coerced into committing cyber-enabled fraud. This work is not merely exploitative but directly criminal, and it demands a workforce with meaningful digital literacy and technical aptitude, a distinct victim demographic. The most common crimes in scam compounds are “pig butchering” investment scams, romance fraud, and cryptocurrency manipulation against victims in third countries. This creates a layered victimization dynamic in which trafficked persons simultaneously suffer serious human rights violations and are instrumentalized perpetrators of crime. This duality has proven to be a significant obstacle for recognition, protection, and prosecution: Authorities in destination countries have in practice been more likely to treat scam workers as criminal suspects than as trafficking victims, and the relative cost of prosecution or deportation compared to victim rehabilitation and support has, in many jurisdictions, skewed responses away from a protection-centered approach.[7]

---

[5] United Nations Office of the High Commissioner for Human Rights. *A “Wicked Problem": Seeking Human Rights-Based Solutions to Trafficking into Cyber Scam Operations in South-East Asia.* United Nations, 2026. https://www.ohchr.org/sites/default/files/documents/issues/trafficking/report-a-wicked-problem.pdf.
[6] Lawler, Siobhan, Samantha Lyneham, and Christopher Dowling. *Gender, Technology and Trafficking in Persons: Women's Experiences of Forced Criminality in South-East Asia's Cyber-Scam Centres*. Australian Institute of Criminology, 2026. https://doi.org/10.52922/sp78274.
[7] United Nations Office of the High Commissioner for Human Rights, A "*Wicked Problem*."

The scale and geographic scope of the online scam operations (OCOs) phenomenon have grown substantially and continue to evolve. While Myanmar, Cambodia, and Laos remain central hubs and are those discussed here, it is important to note that enforcement pressure – including an estimated 200 compound closures as of early 2026 – have prompted operators to adapt rapidly, relocating operations within the region and expanding outward in what amounts to jurisdiction shopping.[8] East Africa and Sri Lanka have emerged as notable new destination zones, and Timor-Leste has more recently come to attention as an emerging site. Simultaneously, the operational model for scam compounds continues to shift.[9] As fraud tools become more sophisticated and accessible, with some being sold as a "scam tool suites," compounds require fewer highly specialized workers, and the roles individuals are forced to perform have become more fluid, complicating both victim identification and the application of legal frameworks that were created around more static exploitation classifications.[10]

Many individuals working in scam compounds have been trafficked, making this dimension of the OCO phenomenon one of the most acute and fast-moving human trafficking challenges. Existing international and regional frameworks provide a foundation for response, but their application on the ground often remains uneven. This issue brief first outlines those relevant international and regional standards and guidance applicable to the trafficking into OCOs, then highlights key gaps and challenges in applying those frameworks in practice. It also presents examples of promising and emerging good practices in prevention, protection, and prosecution that may help bridge the current implementation gap.

RELEVANT FRAMEWORKS

Multilateral efforts to combat modern human trafficking have existed for decades. The primary international instrument is the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, which supplements the UN

[8] Tanakasempipat, Patpicha. "Crime Syndicates in Southeast Asia Go Global, Defying Crackdowns." *Bloomberg*. April 21, 2025. https://www.bloomberg.com/news/articles/2025-04-21/crime-syndicates-in-southeast-asia-go-global-defying-crackdowns.
[9] Hale, Erin. "UN warns online scam centres hitting Southeast Asia moving to East Timor." *Al Jazzera*. September 12, 2025. https://www.aljazeera.com/news/2025/9/12/un-warns-online-scam-centres-hitting-southeast-asia-moving-to-east-timor.
[10] Meda, Kennedy. "Fraud-as-a-Service: Creating a new breed of fraudsters." *Thomson Reuters*. February 21, 2025. https://www.thomsonreuters.com/en-us/posts/corporates/faas-new-fraudsters/.

Convention against Transnational Organized Crime.[11] Adopted in 2000, the “Palermo Protocol” was a landmark instrument and provided the first universally accepted, legally binding definition of human trafficking, as well as establishing the "3Ps" framework — Prevention, Protection, and Prosecution.[12]

The Palermo Protocol defines trafficking in persons as the recruitment, transportation, transfer, harboring, or receipt of persons, by means such as coercion, abduction, fraud, deception, abuse of power or vulnerability, or the giving or receiving of payments to achieve control over a person, for the purpose of exploitation.[13] Exploitation is understood to include sexual exploitation, forced labor or services, slavery or practices similar to slavery, servitude, and organ removal; contemporary practice and guidance also recognize forced begging, exploitative marriage, and forced criminality as forms of exploitation.

Online scam operations frequently exhibit the acts, means, and purpose of trafficking under this definition. Individuals are often recruited through deceptive offers of legitimate employment, transported across borders, and then subjected to restrictions on movement, confiscation of documents, threats, physical abuse, and debt bondage. They are compelled to run online fraud schemes under coercive conditions, working long hours, having to adhere to strict quotas, and are punished for non-compliance. There is also growing evidence of sexual abuse and exploitation, notably against women.[14] In such circumstances, participation in OCOs constitutes forced labor or forced criminality within a trafficking framework, even if the initial movement was voluntary.

Numerous countries have adopted national legal legislation to implement the Protocol. All ASEAN Member States have criminalized trafficking in persons in broad alignment with the definition of trafficking in persons as set out in both the Palermo Protocol and the ASEAN Convention Against Trafficking in Persons (ACTIP). Many ASEAN countries

[11] United Nations. “Protocol to Prevent, Suppress and Punish Trafficking in Persons Especially Women and Children, Supplementing the United Nations Convention against Transnational Organized Crime.” 2000. https://www.ohchr.org/en/instruments-mechanisms/instruments/protocol-prevent-suppress-and-punish-trafficking-persons.
[12] Ibid.
[13] Ibid.
[14] Global Initiative Against Transnational Organized Crime, *Compound Crime: Cyber Scam Operations in Southeast Asia*. Global Initiative Against Transnational Crime, 2024. https://globalinitiative.net/analysis/compound-crime-cyber-scam-operations-in-southeast-asia/.

have dedicated TIP legislation as well as provisions in their Criminal Codes that can be used to confront trafficking into criminal activities.

An important aspect of anti-TIP efforts is the "non-punishment principle," which sets out that trafficked persons should not be subject to arrest, charge, detention, prosecution, or be penalized or otherwise punished for illegal conduct that they committed as a direct consequence of being trafficked. While not explicitly included in the Protocol, this principle has since been widely reflected in regional and national legislation and is considered foundational.

Other legal, normative and functional initiatives are relevant. The International Labour Organization's Forced Labor instruments complement and intersect with the Protocol by offering important definitions and compelling governments to criminalize forced labor, enforce penalties, protect victims, and ensure access to compensation. The Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime is a regional forum that promotes cooperation, dialogue, and the development of policies addressing irregular migration across the Asia-Pacific region and beyond. The UN Office on Drugs and Crime (UNODC) has recently developed a set of indicators to identify victims of Trafficking in Persons for Forced Criminality to Commit Cyber Enabled Crime, recognizing the unique challenges of trafficking in the scams and cyber context.[15] The Greater Mekong Subregion's Coordinated Mekong Ministerial Initiative against Trafficking (COMMIT)[16] focuses on combating human trafficking through prevention, victim protection, repatriation, and prosecution via a Sub-regional Plan of Action.

GAPS AND CHALLENGES

Despite a solid legal framework to prevent and address trafficking-in-persons, the unique nature of the recent online scam operations epidemic has created challenges for the full implementation or application of these frameworks.

---

[15] United Nations Office on Drugs and Crime, *Key Indicators of Trafficking in Persons for Forced Criminality to Commit Cyber Enabled Crimes*. United Nations, 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2025/TIP/TIP_for_FC_indicators_EN_FINAL.pdf.

[16] International Organization for Migration. "Coordinated Mekong Ministerial Initiative against Trafficking (COMMIT Process)." International Organization for Migration. Accessed June 1, 2026. https://www.iom.int/coordinated-mekong-ministerial-initiative-against-trafficking-commit-process.

Weak Upstream Prevention of Trafficking

A foundational gap in existing anti-trafficking frameworks is the insufficient attention paid to preventing recruitment into trafficking situations before they occur. While frameworks address identification and response after exploitation has begun, they have not kept pace with the sophisticated, technology-enabled recruitment pipelines that funnel workers into scam compounds.

Entry-point controls remain inadequate across source and transit countries. Recruitment portals, job boards, and visa processes can fail to be cross-referenced against lists of known fraudulent employers or flagged job advertisement patterns. Workers traveling on employment visas may be provided with documentation that appears legitimate but leads to exploitative conditions upon arrival, with no systematic mechanism to verify the legitimacy of the employer or the working conditions promised. Notably, India updated its screening guidance in 2023 to specifically address nationals traveling to Laos, Cambodia, and Myanmar for employment purposes as well as posting signs in airports with warnings – an example of targeted upstream action that remains the exception rather than the rule.[17]

Compounding this gap, scam operators have become more sophisticated in their recruitment efforts, fabricating company profiles, synthetic positive reviews, and AI-generated recruitment content to attract trafficking victims. AI tools now enable the mass production of convincing fake job postings and recruitment communications at low cost, making it significantly harder for prospective workers to distinguish a legitimate offer from a fraudulent one.[18]

---

[17] India, Ministry of External Affairs. "Advisory on Overcharging by Agents for Overseas Recruitment, Offering Fake Overseas Jobs and Illegal Recruitment." Ministry of External Affairs, Government of India. December 14, 2023. https://www.mea.gov.in/press-releases.htm?dtl/37425/Advisory_on_overcharging_by_agents_for_overseas_recruitment_offering_fake_overseas_jobs_and_illegal_recruitment; ASEAN Skyline Rising. "The Ministry of Home Affairs of India Has Issued Public Warnings..." Facebook, January 3, 2026. https://www.facebook.com/61574261780854/posts/122156997950808726/.

[18] Bennett, Phil. *New Frontiers: The Use of Generative Artificial Intelligence to Facilitate Trafficking in Persons.* Policy Brief. Vienna and Bangkok: OSCE Office of the Special Representative and Coordinator for Combating Trafficking in Human Beings and Regional Support Office of the Bali Process, 2024. https://s3.ap-southeast-2.amazonaws.com/assets.rso.baliprocess.net/app/uploads/2024/11/01112800/OSCE-RSO-AI-TIP-Policy-Brief-FINAL.pdf.

Labor Ministries and immigration authorities, despite being the first institutional point of contact for outbound migrant workers, are often not integrated into anti-trafficking prevention architectures. Their potential role in vetting employers, issuing alerts, and verifying job offers remains largely untapped.

Victim identification and non-punishment

An additional challenge is around victim identification and the inconsistent application of the non-punishment principle. The fluid and overlapping roles of people in scam compounds create a central challenge to applying anti-trafficking frameworks. Potential movement between willing and forced labor complicates legal classification and victim identification, highlighting the need for nuanced and context-sensitive approaches rather than rigid categories. Additionally, states may have different definitions of trafficking in ways that complicate cooperation between source, transit, and destination countries.

As well, frameworks of cybercrime, trafficking, and financial crimes — all of which are applicable to online scam operations — are often seen as mutually exclusive rather than complementary. The primary lens by which a law enforcement agency or government views the issue determines the characteristics with which they classify individuals, what evidence they collect, and how they proceed with prosecution. This, in conjunction with different international and domestic laws, makes both victim protection and conviction difficult.

As a result, workers found in scam compounds during raids or that have escaped are often being treated primarily as offenders, facing detention, prosecution, or deportation before any systematic screening for trafficking indicators. Existing indicators of trafficking for forced criminality, including the COMMIT[19] guidebook on supporting the reintegration of trafficked persons and guidelines put out by the UNODC, are not consistently disseminated or applied, so key signs of trafficking are often missed.

This combination of fluid roles, weak identification, and inconsistent use of non-punishment norms undermines victim protection, discourages cooperation with

[19] International Organization for Migration, "COMMIT Process."

authorities, impacts the collection of testimony, and risks reinforcing impunity for higher level actors.

Jurisdictional Challenges and Institutional Silos

Compounding the above challenges are the gaps that exist across how countries define trafficking in persons and what that means for prosecution. Some jurisdictions require proof of movement across borders as a threshold element, meaning that a person trafficked within a single country may fall outside the statutory definition entirely and be treated instead as a labor dispute or immigration violation. Others set a high evidentiary bar for demonstrating coercion, requiring physical restraint or direct threats of violence, which fails to capture the subtler psychological and debt-bondage mechanisms that characterize scam compound trafficking, where victims may have initially traveled voluntarily and only later found themselves unable to leave.

The transnational nature of online scam operations exploits the fragmented nature of international law enforcement to operate with near impunity: A scam compound based in Myanmar, for example, staffed by trafficked workers recruited under false pretenses in Vietnam, Philippines, or China, and targeting victims in the United States or Europe, raises questions about whose law applies, and who has the authority to act.

The silo problem is both international and domestic. In several countries, different police units are tasked with responding to trafficking and cybercrime respectively, and these units frequently do not share information, coordinate investigations, or agree on how to classify individuals found in scam compound situations. The question of whether agencies are oriented toward apprehending low-level workers or toward dismantling the criminal networks at the top further shapes the outcome of an investigation. These siloed mandates allow operators and organizers to benefit from the gaps between enforcement jurisdictions while lower-level workers bear the primary burden of prosecution.

Limited Capacity

Online scam operations are highly digitized, relying on encrypted communications, complex platform infrastructures, and online payment systems. This means there is a financial and logistical paper trail behind trafficking and other aspects of the

operations. Trafficking responses, however, have often been built around testimonial evidence and visible, physical forms of exploitation. This industrial-scale, digital-first approach to recruitment does leave a trail to follow in the form of social media messages, IP addresses, e-payments for transit, etc., but the nature of the evidence requires digital forensics investigations to build a case. Where law-enforcement agencies lack robust capacity to capture, preserve, and analyze digital evidence, they may struggle to prove coercion, control, and financial benefit, particularly against organizers who remain remote from compound-level abuses.[20] This evidentiary gap constrains the effective use of trafficking provisions and encourages reliance on narrower cybercrime or fraud charges.

Current events show that authorities may also lack the ability and capacity to process large numbers of escaped or released workers at once, to quickly record and corroborate their accounts, and integrate these testimonies into cross-border investigations.[21] They are often not trained in conducting victim-centered and trauma-informed methods to process victims or escapees. Such testimony helps to build the case for other legal action, including against leaders. Prosecutorial capacity is similarly limited, with many offices focusing on lower-level offenders because they lack the resources or international cooperation channels needed to target higher-ranking organizers.

A structural incentive problem compounds these capacity constraints. When prosecutors can achieve a conviction on cybercrime or fraud charges without building a trafficking case, there is little institutional pressure to pursue the more resource-intensive investigation that would be required to implicate leadership. A financial audit trail consisting of evidence obtained by tracing the financial flows associated with scam compounds could support building a case against the criminal leadership responsible for trafficking-in-persons charges. Yet, this work requires sustained resourcing, specialized skills, and inter-agency coordination that is unsustainable in some jurisdictions. Metrics that reward conviction counts over network disruption further push investigators and prosecutors toward lower-hanging fruit.

---

[20] United Nations Office of the High Commissioner for Human Rights, A "*Wicked Problem*."
[21] United States Department of State, Office to Monitor and Combat Trafficking in Persons. *2025 Trafficking in Persons Report.* U.S. Department of State, 2025. https://www.state.gov/reports/2025-trafficking-in-persons-report/.

Technological Enablement

Technology is significantly lowering the barriers to recruiting people fraudulently and bypassing traditional markers of trafficking, creating new prevention challenges for states and businesses. As mentioned above, the explosion of generative AI has enabled increasingly realistic recruitment processes. Online job boards, social media, messaging apps, and professional networking sites allow traffickers to target many individuals quickly, cheaply, and across borders, often under the guise of legitimate employment.[22] Artificial intelligence tools have been used to generate synthetic voices or deepfake video personas, making the deception even more convincing and harder for victims to detect.[23] The geographic reach that technology enables is also critical, because a recruiter sitting in one country can simultaneously groom dozens of potential victims across multiple countries.

Existing trafficking prevention measures struggle to keep up with this level of digital sophistication and are often programmed to detect only traditional red flags — such as obvious document confiscation, physical confinement, implausibly low wages, or third-party control of a worker's earnings — rather than online processes that appear fully legitimate. Prevention also requires greater coordination with the private sector (notably the tech companies who own the platforms where recruitment occurs) and financial institutions.

Corruption and Political Will

Finally, corruption remains a critical but insufficiently addressed challenge in the context of online scam operations. Existing trafficking frameworks often acknowledge corruption in general terms but do not embed concrete, coordinated measures to detect and respond to official collusion in recruitment, border crossing, and the overall

---

[22] United Nations Office on Drugs and Crime. *Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape.* United Nations, 2024. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf.

[23] Mathieson, Rosalind. "AI Helps Scam Centers Evade Clampdown in Asia, Dupe More Victims." Bloomberg. February 9, 2026. https://www.bloomberg.com/news/articles/2026-02-09/ai-helps-scam-centers-evade-clampdown-in-asia-dupe-more-victims.

protection of scam sites.[24] Weak safeguards for whistle-blowers and limited integration of anti-corruption measures allow these relationships to persist, undermining investigations and prosecutions.

The broader political will challenge is equally significant. As has been observed across multiple country contexts, the laws and policies necessary to address scam compound trafficking largely exist. Enforcement is the challenge. Where criminal networks have the resources to co-opt officials, compromise investigations, and insulate leadership from accountability, even well-designed legal frameworks will fail at implementation. Anti-corruption measures must therefore be treated not as a separate concern but as a prerequisite for effective anti-trafficking enforcement in this context.

EXAMPLES OF APPLYING ANTI-TIP LAW

Recent cases from the region illustrate how authorities are beginning to apply anti-trafficking law to prosecute online scam operators particularly where victims are deceptively recruited. The following examples highlight emerging approaches to charging, sentencing, and victim redress in such cases:

- In June 2025, a court in Vietnam sentenced four defendants for human trafficking, including the trafficking of minors, facilitating illegal entry into Vietnam, and involvement in overseas online scam operations. This case marked a successful prosecution for facilitation of illegal entry and TIP prosecution for forced criminality; the longest sentence was 13 years and 3 months.[25]
- In October 2024, two men pleaded guilty for coercing five citizens from Hong Kong into forced criminality in cyber-scam centers in Cambodia and Myanmar,

[24] Wojcik, J. et al. *Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia.* United Nations, 2025. https://www.unodc.org/roseap/uploads/documents/Publications/2025/Inflection_Point_2025.pdf.
[25] "Four jailed for trafficking Vietnamese teens to work in Cambodian scam ring." *Viet Nam News*. July 1, 2025. https://vietnamnews.vn/society/1720564/four-jailed-for-trafficking-vietnamese-teens-to-work-in-cambodian-scam-ring.html.

where the victims experienced severe abuse. The traffickers were charged for conspiracy to defraud.[26]

- In November 2022, three perpetrators were arrested and went to trial in Batam, Indonesia, for the trafficking of persons into Cambodia. Victims were forced to commit crypto-currency scams and were physically punished if they did not meet their targets. The traffickers were convicted for 3-4 years and ordered to pay restitution to the victims.[27]

Across these examples, certain elements stand out as emerging good practice. It sets a precedent that authorities are willing to treat deceptive recruitment into scam centers, combined with coercive condition and forced participation in fraud, as trafficking or as exploitation. Trafficking charges may be combined with other offenses to address not only exploitation but also broader criminality.

Other recommended good practice that has emerged from Stimson's research in this area[28] includes: prioritizing prosecutions of high-level organizers, recruiters, and enabling businesses rather than individual workers; increasing prosecutorial resources to support complex casework on these issues; the dissemination and application of existing indicators of trafficking for forced criminality[29]; and ensuring that victims are not criminalized and are treated appropriately throughout the identification and legal process.

[26] Wong, Brian. "Human traffickers jailed for luring 5 Hongkongers into forced labour in Southeast Asia." *South China Morning Post*. November 1, 2024. https://www.scmp.com/news/hong-kong/law-and-crime/article/3284837/human-traffickers-jailed-luring-5-hongkongers-forced-labour-southeast-asia.
[27] "Indonesian Court Sentences Three Perpetrators Guilty of Human Trafficking for Forced Labour in Cyberscamming." *International Justice Mission*. March 15, 2023. https://ijm.org.au/news/indonesian-court-sentences-three-perpetrators-guilty-of-human-trafficking-for-forced-labour-in-cyberscamming.
[28] Stimson Center. "Countering Cyber Scam Operations." Accessed June 3, 2026. https://www.stimson.org/project/countering-cyber-scams/.
[29] United Nations Office on Drugs and Crime, *Key Indicators of Trafficking in Persons for Forced Criminality.*

WAYS FORWARD

Recommendation 1: Design and implement appropriate screening mechanisms for individuals seeking employment in other jurisdictions to prevent and mitigate against potential trafficking.

- Governments across the region should establish standardized pre-departure screening protocols, in partnership with civil society and regional authorities, that help identify individuals who may be at heightened risk of labor exploitation before they travel abroad for employment. Screenings should include verified employment contract review, employer legitimacy checks, and accessible grievance channels, while taking care to avoid overly restrictive measures that could inadvertently limit legitimate labor mobility or push migration through informal channels.
    - Since individuals coached by recruiters or traveling on tourist visas may evade detection through self-reporting alone, protocols should also consider contextual indicators such as travel patterns, point-of-contact information, and destinations often associated with trafficking routes.
- Governments should invest in targeted public awareness campaigns, in partnership with civil society, tech platforms, and employers, that can help prospective migrants recognize fraudulent job offers before they travel.
    - Materials should be available in relevant languages and distributed through channels that reach vulnerable populations, including social media, community organizations, and recruitment offices.
    - Physical signage at airports and border crossings flagging the warning signs of trafficking and providing accessible reporting channels can also serve as a low-cost, high-visibility prevention measure.

Recommendation 2: Mandate trafficking screening or an assessment of possible trafficking before any processing of people found in scam compounds.

- Governments should establish a legal presumption against the prosecution of individuals found in scam compound contexts until trained personnel complete a systematic trafficking screening — prior to detention, deportation, or criminal proceedings.
    - Screening protocols should draw on existing tools, including the COMMIT guidebook and UNODC forced criminality indicators.

- Protection and immigration authorities should refer individuals who screen as potential victims to protection services regardless of immigration status or conduct occurring while under coercion.
- Governments and international organizations should invest in scaling capacity to rapidly process large numbers of escaped or released workers.
- Regional bodies and international partnerships should lead translation and socialization of screening mechanisms across Southeast Asia to secure buy-in from the most affected countries.

Recommendation 3: Establish shared case classification criteria across trafficking, cybercrime, and immigration agencies

- Governments should establish inter-agency task forces with agreed criteria for classifying individuals found in scam compound contexts, specifically to prevent the investigative lens from defaulting to whichever agency encountered the case first.
- Task forces should embed the principle that victim identification precedes offender classification, not the reverse.
- Government and task force leadership should orient mandates and performance metrics towards dismantling criminal network leadership rather than prosecuting low-level actors.
- Companion recommendations in the cybercrime and AML issue briefs address the broader coordination and financial investigation architecture.

Recommendation 4: Redesign reintegration programs for non-identifying victims

- Governments and service providers should recognize that some individuals exiting scam compound situations will not voluntarily identify as trafficking victims, due to shame, fear of stigma, distrust of authorities, or concern that victim identification will trigger legal consequences and will not seek formal assistance.[30]

[30] Beltran, Sam. "Southeast Asia's scam compound survivors suffer in stigma and silence." *South China Morning Post*. March 15, 2026. https://www.scmp.com/week-asia/people/article/3346532/southeast-asias-scam-compound-survivors-suffer-stigma-and-silence.

- Reintegration programs should offer non-coercive pathways to support that do not require self-identification or cooperation with prosecution as a condition of access.
- Livelihoods support should specifically address the risk that returnees apply scam-related skills to further criminal activity in their home communities, combining economic transition assistance with behavioral support and community-level monitoring through civil society partners.
- Governments should provide support to on the ground organizations prioritizing this work.

The core legal frameworks needed to address scam compound trafficking largely exist — in the UN Trafficking in Persons Protocol, regional instruments, and an increasing number of national laws. The challenge is enforcement: institutional silos, incentive structures that favor easier prosecutions, the corrupting influence of criminal networks, and the political economy of countries where scam operations have become embedded economic actors. Reform efforts must therefore focus on implementation architecture, accountability mechanisms, and political will — not additional framework design.

Cybercrime Law and Frameworks

Cyber-enabled fraud and scams (or, online scam operations, OSOs) have rapidly evolved into sophisticated cyber operations powered by the same tools, infrastructure, and criminal ecosystems that drive other digital threats such as ransomware attacks and nation-state intrusions. Individuals who lose money to a romance scam, impersonation, or a cryptocurrency scheme are, in almost every case, the targets of a cyber operation that could have involved any number of digital tools employed for other forms of malicious behavior: credential-stealing malware[31], stalkerware[32], or remotely controlled botnets.[33] Phishing[34] kits allow low-skill fraudsters to impersonate banks, government agencies, and retailers with ease. One 2026 study[35] identified a sophisticated malware-as-a-service (MaaS) platform capable of facilitating real-time surveillance, credential theft, data exfiltration and financial fraud. It linked the platform to locations known to be associated with cyber-enabled fraud and scams, notably the K99 Triumph City compound in Cambodia, and cyber threat actors.

---

[31] Malware, short for malicious software, refers to any intrusive software developed by cybercriminals (often called hackers) to steal data and damage or destroy computers and computer systems. Examples of common malware include viruses, worms, Trojan viruses, spyware, adware, and ransomware. Palo Alto Networks, "What Is Malware?," accessed June 4, 2026, https://www.paloaltonetworks.com/cyberpedia/what-is-malware-vs-ransomware.

[32] Software, made available directly to individuals, that enables a remote user to monitor the activities on another user's device without that user's consent and without explicit, persistent notification to that user in a manner that may facilitate intimate partner surveillance, harassment, abuse, stalking, and/or violence. See Coalition Against Stalkerware, "What Is Stalkerware?," accessed June 4, 2026, https://stopstalkerware.org/.

[33] A botnet is a coordinated network of internet-connected devices—including computers, mobile phones, and IoT hardware—infected with specialized malware that grants remote control to a single attacking party. These hijacked devices, often called zombies, act in unison under the command of a bot-herder to execute automated, large-scale cyberattacks that would be impossible for a single machine to perform. Palo Alto Networks, "What Is a Botnet?," accessed June 4, 2026, https://www.paloaltonetworks.com/cyberpedia/what-is-botnet.

[34] Phishing is a form of social engineering that uses deception to manipulate individuals into disclosing sensitive information or executing unauthorized transactions. It remains the most pervasive initial access vector in modern cyber attacks, often serving as the entry point for credential theft, account compromise, ransomware deployment, and supply chain infiltration. Palo Alto Networks, "What Is Phishing?," accessed June 4, 2026, https://www.paloaltonetworks.com/cyberpedia/what-is-phishing.

[35] Infoblox Threat Intel and Chong Lua Dao, "Scams, Slaves and (Malware-as-a) Service: Tracking a Trojan to Cambodia's Scam Centers," Infoblox Blog, April 10, 2026, https://www.infoblox.com/blog/threat-intelligence/scams-slaves-and-malware-as-a-service-tracking-a-trojan-to-cambodias-scam-centers/.

Part of the rapid industrialization of scamming is tied to the recent explosion of AI and automation into mainstream use and availability. Whether it be through instant language translation, deepfakes and voice impersonation, or automated content management tools and smart chatbots, AI tools are changing the cyber scams landscape.[36]

Yet, OSOs have not always been approached as a cybercrime issue in the way that ransomware operations or hack-and-leak breaches are, for example, and the full extent to which cybercrime law can be a tool for accountability is under-studied. This is likely because while the acts are cyber-enabled, the core crime or transgression that results in financial loss more easily tracks back to anti-fraud efforts. There has also been significant, and important, emphasis on the forced labor and trafficking of individuals into scam compounds and the legal and normative frameworks. However, continuing to address cyber-enabled fraud and scams purely as consumer protection or a monetary issue risk addressing the symptoms of the problem rather than tackling the underlying structures and tools that have facilitated the evolution of scams into a global, industrialized criminal economy.

This Issue Brief presents a general overview of cybercrime law and how it relates to cyber-enabled fraud and scams. It will describe several relevant legal instruments and frameworks, and an overview of national laws amongst ASEAN Member States. Based on this analysis, the Issue Brief will consider gaps and challenges in advancing accountability for cyber-enabled fraud and scams through cybercrime law and offer a set of recommendations.

UNDERSTANDING CYBERCRIME LAW

While there is no universally accepted definition of cybercrime, it is widely considered to be any act using "information technology" to perpetrate or facilitate a crime. There are generally understood to be two types of cybercrime[37]:

[36] Di Girolamo, Michael. *Deceptive by Design: The AI-Enabled Tools Fueling the Scam Industry*. C4ADS, February 25, 2026. https://c4ads.org/wp-content/uploads/2026/02/DeceptiveByDesign-C4ADS.pdf.
[37] United Nations Office on Drugs and Crime. *Cybercrime in Brief*. Cybercrime Module 1: Introduction to Cybercrime. United Nations Office on Drugs and Crime, 2019. https://www.unodc.org/e4j/en/cybercrime/module-1/key-issues/cybercrime-in-brief.html.

Cyber-dependent crime is any crime that can only be committed using computers, computer networks, or other forms of information communication technology, such as hacking and ransomware operations.

Cyber-enabled crime is generally understood to refer to a traditional crime that is facilitated and enhanced by using information and communications technology.

Cyber-enabled fraud (or "online scams") fall into this latter category, although the tools and tactics used for fraud may also constitute other forms of cybercrime (phishing, social engineering, etc.) and some of these actions are also covered by traditional fraud statutes, widening the spectrum of legal liability. For example, when scammers impersonate banks or create fake websites to harvest credentials, prosecutors can charge them with computer fraud, wire fraud, and identity theft simultaneously. Perpetrators can be individuals or organized networks or groups, some with links to nation-state actors. Cybercrime activities can range from large-scale attacks on national critical infrastructure to espionage and hack-and-leak operations, or targeting businesses, schools, and hospitals and banks through ransomware.

Cybercrime law identifies standards of acceptable behavior for information and communication technology (ICT) users. It protects ICT users, in general, and mitigates and/or prevents harm to people, data, systems, services, and infrastructure. Cybercrime law can also protect human rights; enables the investigation and prosecution of crimes committed online; and facilitates cooperation between countries on cybercrime matters. In the words of the UNODC, "Cybercrime is notoriously difficult to prosecute due to the borderless nature of the internet, which creates complex jurisdictional conflicts, alongside advanced anonymity tools that hide perpetrators' identities. Furthermore, digital evidence is fragile, technically complex to gather, and often requires international cooperation that is slow or nonexistent."[38]

Not surprisingly, there are multiple types and forms of cybercrime law, ranging from those that cover online safety, computer safety and computer misuse (phishing, hacking), to those relating to identity theft or protecting sensitive materials. Laws exist at national, regional, and multilateral levels. Some countries have amended existing

[38] United Nations Office on Drugs and Crime. *Obstacles to Cybercrime Investigations*. Cybercrime Module 5: Cybercrime Investigation. United Nations Office on Drugs and Crime, n.d. https://www.unodc.org/cld/en/education/tertiary/cybercrime/module-5/key-issues/obstacles-to-cybercrime-investigations.html.

national legislation or criminal codes to account for cybercrime whereas others introduce new laws, some of which are informed by regional or global conventions and frameworks, as outlined below.

It is often challenging to enforce cybercrime law because a significant amount of activity is transboundary, making attribution and evidence collection even more difficult. Mutual Legal Assistance Treaties (MLATs) are the formal mechanism for countries to share evidence and cooperate on investigations, but they are often criticized as being too slow vis-à-vis the pace of cybercrime. International agencies such as Interpol, Afripol, Asiapol and Europol are important channels for threat intelligence sharing and managing operations but lack the ability to make arrests. At a national level, cybercrime law enforcement tends to be fragmented as well across various agencies and departments; locally, law enforcement agencies frequently lack the human resources, staffing capacity, tools, and training to fully investigate digital crimes including cyber fraud.

New models have emerged to combat other forms of cybercrime. The Counter Ransomware Initiative, for example, is one promising multilateral initiative bringing together more than 70 countries to cooperate on disrupting ransomware infrastructures, build resilience, facilitate cooperation between government agencies and private sector actors, and advance policy.[39]

In other areas of cybercrime or cybersecurity, sanctions are an increasingly common tool for accountability and a way to introduce consequences for breaching laws or norms[40]. These have been applied in relation to ransomware groups (i.e. Evil Corp[41], LockBit[42]) as well against the vendors of spyware. In 2022, the U.S. sanctioned Hydra

[39] Counter Ransomware Initiative. Accessed June 5, 2026. https://counter-ransomware.org/.
[40] Bartlett, Jason, and Megan Ophel. *Sanctions by the Numbers: Spotlight on Cyber Sanctions*. Center for a New American Security, 2021.https://www.cnas.org/publications/reports/sanctions-by-the-numbers-cyber.
[41] United States Department of the Treasury. “Treasury Sanctions Members of the Russia-Based Cybercriminal Group Evil Corp in Tri-Lateral Action with the United Kingdom and Australia.” U.S. Department of the Treasury, 2024, https://home.treasury.gov/news/press-releases/jy2623.
[42] U.S. Department of State. "United States, Australia, and United Kingdom Jointly Sanction Ransomware Infrastructure Providers.” U.S. Department of State, 2025, https://www.state.gov/releases/office-of-the-spokesperson/2025/11/united-states-australia-and-united-kingdom-jointly-sanction-ransomware-infrastructure-providers.

Market[43], a dark web marketplace, for facilitating cybercrime and money laundering. Earlier this year, the first sanctions were issued by the U.S. and the UK against networks in Southeast Asia connected to online fraud[44]; there may be lessons learned from the effectiveness of past "cyber sanctions" for cracking down on the criminal networks engaged in cyber-enabled fraud. It is not clear to what extent this may become the case for cyber-enabled fraud.

RELEVANT FRAMEWORKS

The 2001 Council of Europe's Convention on Cybercrime (Budapest Convention) is an internationally binding framework for harmonizing national cybercrime laws, standardizing definitions of offenses, and creating mechanisms for cross-border cooperation and evidence sharing in an effort to address the jurisdictional fragmentation that criminal actors exploit.[45] Its enforcement power remains limited, but it is viewed as a baseline legal framework that facilitates cooperation on investigation and prosecution across borders, closing some of the safe harbor space that fraud networks, ransomware operators, and other cybercriminal enterprises depend upon. The Convention further provides signatories with guidance on mutual assistance and acts as a mutual legal assistance treaty for countries that do not have one with the country requesting assistance. There are presently 81 states parties to the Budapest Convention. Sovereignty-based concerns about cross-border data sharing and human rights safeguards are among the reasons why some countries have refused to join.

In 2022, states parties negotiated a new addition to the Convention. The Second Additional Protocol to the Cybercrime Convention on enhanced co-operation and

---

[43] U.S. Department of Justice. "Justice Department Investigation Leads to Shutdown of Largest Online Darknet Marketplace." Office of Public Affairs, 2022, https://www.justice.gov/archives/opa/pr/justice-department-investigation-leads-shutdown-largest-online-darknet-marketplace.
[44] U.S. Department of the Treasury. "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia." U.S. Department of the Treasury, 2025, https://home.treasury.gov/news/press-releases/sb0278.
[45] Council of Europe, *Convention on Cybercrime (Budapest Convention, ETS No. 185)*, Council of Europe, 2001. https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680081561.

disclosure of electronic evidence.[46] was developed to respond to the challenge of obtaining electronic evidence that may be stored in foreign, multiple, shifting, or unknown jurisdictions. It provides tools for enhanced cooperation and disclosure of electronic evidence such as direct cooperation with service providers and registrars, effective means to obtain subscriber information and traffic data, as well as immediate cooperation in emergencies or joint investigations. It is subject to a system of human rights, including data protection safeguards. As of April 2026, there are 3 Parties and 49 signatories. It will enter into force once there are five ratifications.

For many years, the Budapest Convention was regarded as the primary multilateral cybercrime instrument. In 2021 however, a new UN General Assembly treaty negotiation process led to the 2024 adoption of the United Nations Convention against Cybercrime; Strengthening International Cooperation for Combating Certain Crimes Committed by Means of Information and Communications Technology Systems and for the Sharing of Evidence in Electronic Form of Serious Crimes (UN Cybercrime Convention).[47] The UN Cybercrime Convention opened for signature in Hanoi, Vietnam in October 2025. Its proponents argued that the Budapest Convention was not universal enough in its membership, and that a new global framework was needed.[48] Despite significant pushback and a contentious negotiation process, the convention was ultimately adopted by the UNGA and now has 76 signatures and three ratifications.[49] It will enter into force after the 40th ratification and then become binding international law.

---

[46] Council of Europe. *Second Additional Protocol to the Convention on Cybercrime on Enhanced Co-operation and Disclosure of Electronic Evidence (CETS No. 224).* Council of Europe Treaty Office, 2022. https://www.coe.int/en/web/conventions/full-list?module=treaty-detail&treatynum=224.
[47] United Nations General Assembly, *United Nations Convention against Cybercrime*.
[48] Chatham House. *What Is the UN Cybercrime Treaty and Why Does It Matter?* Chatham House, August 2, 2023. https://www.chathamhouse.org/2023/08/what-un-cybercrime-treaty-and-why-does-it-matter.
[49] Australian Strategic Policy Institute. *The UN Cybercrime Convention: A Victory for State Sovereignty*. The Strategist, August 16, 2024. https://www.aspistrategist.org.au/the-un-cybercrime-convention-a-victory-for-state-sovereignty/; Lawfare. "Has Russia Overplayed Its Hand in UN Cyber Negotiations?" *Lawfare*, May 21, 2026. https://www.lawfaremedia.org/article/has-russia-overplayed-its-hand-in-un-cyber-negotiations; Electronic Frontier Foundation. *Joint Statement on the UN Cybercrime Convention: EFF and Global Partners Urge Governments Not to Sign*. Electronic Frontier Foundation, October 24, 2025. https://www.eff.org/deeplinks/2025/10/joint-statement-un-cybercrime-convention-eff-and-global-partners-urge-governments-not-to-sign.

The UN Convention is grounded in existing criminal justice treaties (related to drug trafficking, organized crime, and corruption), counter-terrorism instruments (which exist but are not as thorough as the above treaties), as well as regional cybercrime treaties of the Council of Europe, Arab States, and African Union. It is organized across six substantive sections: criminalization, procedural measures, jurisdiction, international cooperation, preventative measures, and technical assistance/information exchange, as well as mechanisms for implementation.[50]

Two articles are understood to be most relevant for cyber-enabled fraud and scams:

Article 12 on ICT-related forgery is a complex article but essentially focuses on three actions: input, alteration, or deletion of data resulting in the creation of inauthentic data *with the intent* that it be considered or acted upon as authentic data.

Article 13 on ICT-related theft or fraud addresses any input, alteration, deletion, or suppression of data as well as interference with the functioning of an information or IT system. It also covers the use of deception through ICT systems that cause a person to do anything which they would normally not do (or to not do something which they would normally do) with the fraudulent or dishonest intent of procuring money or other gains which they would normally not have rights to.

Various regional agreements complement these multilateral frameworks. Regional groups and blocs including the Commonwealth of Independent States, the Arab League, the African Union, and the Shanghai Cooperation Organization have regional cybercrime frameworks or agreements, although most pre-date the widespread emergence of scams and fraud. Some, however, can facilitate MLATs and/or information sharing. The 2025 ASEAN Declaration on Combating Cybercrime and Online Scams includes nine action points for forward action, including deepening law enforcement and other cooperation; building capacity; improving policy, regulation and legislation; and establishing dedicated points of contact.[51]

---

[50] United Nations Office on Drugs and Crime. *Chapters of the Convention against Cybercrime*. United Nations Office on Drugs and Crime, 2024. https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html.

[51] Association of Southeast Asian Nations, *ASEAN Declaration on Combatting Cybercrime and Online Scams*, Association of Southeast Asian Nations, 2025. https://asean.org/wp-content/uploads/2025/09/03.-ASEAN-Declaration-on-Combatting-Cybercrime-and-Online-Scams.pdf.

Many ASEAN countries have cybercrime laws or acts that apply to various aspects of the online fraud and scams lifecycle and that establish authorities responsible for enforcement, including investigation. Some of these laws, however, are now being updated or supplemented by other legislation that focus on more precise concerns, such as money mule accounts or cryptocurrency. For example, the 2007 Computer Crime Act in Thailand penalized activities like hacking and phishing, and computer-related fraud. It was updated in 2017 to address fake news and misinformation. In 2020, the King passed a Royal Decree creating the Cyber Crime Investigation Bureau (CCIB) within the Royal Thai Police.[52] This specialized unit is responsible for preventing and investigating technological crimes, establishing operational procedures, and supporting evidence analysis for cybercrimes. In November 2023, multiple government agencies launched the Anti-Online Scam Operation Centre (AOC) as a centralized reporting mechanism. The Royal Thai Police maintains a Technology Crime Suppression Division within the Central Investigation Bureau, and the Department of Special Investigation has its Bureau of Technology and Cyber Crime.[53]

In the Philippines, the Cybercrime Prevention Act of 2012 (Republic Act 10175) established a legal foundation for addressing cybercrime. It identified a concrete definition and list for cybercrime acts, relevant penalties for such acts, and mandated the creation of specialized cybercrime units within the National Bureau of Investigation (NBI) and the PNP, as well as an Office of Cybercrime within the Department of Justice (DOJ).[54] The Cybercrime Investigation and Coordinating Center (CICC) is the lead agency for implementing the Cybercrime Prevention Act of 2012. The Senate is considering potential amendments to the Cybercrime Prevention Act to update it further; in particular, Senate Bill 2570[55] – proposed in February 2024 – would grant the CICC greater mandate to coordinate on cybercrime prevention and investigation, ensuring the implementation of updated cybercrime laws, and integrate

[52] Royal Thai Police, *Royal Decree on the Division of the Royal Thai Police Office*, Royal Thai Police, September 6, 2020. https://www.royalthaipolice.go.th/downloads/laws/laws_04_17.pdf.
[53] See Council of Europe, "Thailand," Octopus Cybercrime Community, accessed June 5, 2026, https://www.coe.int/en/web/octopus/thailand.
[54] Republic of the Philippines, "Republic Act No. 10175: Cybercrime Prevention Act of 2012," Republic of the Philippines, September 12, 2012, https://www.officialgazette.gov.ph/2012/09/12/republic-act-no-10175/.
[55] Republic of the Philippines, Nineteenth Congress, "Senate Bill No. 2570: An Act Strengthening Cybercrime Prevention Measures, Amending for the Purpose Republic Act No. 10175, Otherwise Known as the 'Cybercrime Prevention Act of 2012,'" Republic of the Philippines, February 26, 2024, https://legacy.senate.gov.ph/lisdata/4355139600!.pdf.

additional service providers into the prevention efforts.

Other countries studied as part of this project including Cambodia, Lao PDR, and Vietnam similarly have updated and/or are updating relevant cybercrime legislation.

GAPS AND CHALLENGES

The current cybercrime law landscape offers many promising tools for advancing accountability for the perpetrators of fraud and scams, but there are also notable gaps and challenges. Some are not unique to fraud and scams, but there are additional complexities.

Legal loopholes. Despite a strong legislative foundation addressing cybercrime, there are significant disparities in the national cybercrime laws of ASEAN member states and other countries affected by cyber-enabled fraud and scams, leading to a patchwork that hinders cross-border cooperation and generates loopholes that can be exploited by cyber criminals. Relatedly, there are disparities in how a cybercrime or a cyber-enabled crime is defined, and punished, across jurisdictions, leading to a practice of "jurisdiction shopping" in which countries lacking effective cybercrime laws and/or law enforcement potentially become safe havens for criminals. Some countries do not recognize the links between cyber-enabled fraud and organized crime, creating further legal loopholes. Harmonizing cybercrime laws and penalties across ASEAN countries has been encouraged but is challenging due in part to cultural differences that lead to a variation in the types of law and constitutions in each country. Existing multilateral frameworks similarly have substantive shortcomings that could hinder their utility for counter fraud and scams or lack sufficient membership at present.

Capacity. There are multiple capacity gaps that hinder full use of cybercrime law. Smaller economies such as those that are often on the front lines of fraud and scams face challenges in developing advanced technological tools and enforcement mechanisms. Across all countries affected by cyber-enabled fraud, law enforcement agencies are reporting the need to upskill their workforces for cybercrimes more broadly and especially regarding online fraud and scams, including relevant technical skills. Where the technical and human capacity for digital investigations exist, they are often still under-resourced given the digital first nature of modern economies and intersections between traditional crimes and digital evidence trails. In addition, resource constraints mean that law enforcement has tended to prioritize investigating other forms of criminal activities over scams, which are often reported in individual

instances with a lesser overall financial impact. The collective impact of scams and fraud raises questions about the possibility of whether these crimes can be prosecuted under international law. The UN Cybercrime Convention, for example, requires offenses to meet a "serious crime threshold." While a single scam may not meet this threshold, large-scale, organized criminal scam operations may do so.[56]

Victim identification. Cyber-enabled fraud and scam victims face unique challenges compared to victims of conventional or even other forms of cybercrime. In many cases, they may feel shame or guilt, or even a sense of responsibility for their own victimization. This correlates to under-reporting of the issue. Another challenge on the other side of the scam stems from the emergence of a category of people who are simultaneously victims *and* unwitting participants in cybercrime. In the context of scam compounds, where trafficking victims are coerced into committing cyber-enabled fraud, existing legal frameworks struggle to distinguish perpetrator from victim, often criminalizing the exploited rather than their exploiters who ultimately benefit from scams. This puts many of the laws used to prosecute fraud and scams at odds with the anti-trafficking frameworks described in the corresponding Issue Brief on anti-trafficking in persons law and frameworks.

Lost digital evidence. The evidence needed to prosecute for a cybercrime disappears notoriously quickly. Many platforms and email providers retain detailed logs for only a short period of time and scammers deliberately exploit this by using temporary websites, burner email accounts, and messaging apps with disappearing messages. Law enforcement agencies, already poorly resourced, may not be able to issue preservation requests or subpoenas quickly enough to capture time-sensitive data. The situation worsens in cross-border cases where evidence sits on servers in foreign jurisdictions with different data retention policies and complex legal assistance procedures, creating gaps where critical evidence simply ceases to exist before investigators can secure it.

Plausible deniability. This is a constant challenge for all cyber accountability because the technical foundation of digital environments is such that attribution of responsibility is challenging. Criminal networks operating across jurisdictions exploit the same attribution difficulties such as anonymized infrastructure, layered financial

[56] United Nations General Assembly. *United Nations Convention against Cybercrime*. United Nations Office on Drugs and Crime, 2024. https://www.unodc.org/unodc/en/cybercrime/convention/convention-against-cybercrime-chapters.html.

systems, and legal differences between states to conduct cyber-enabled fraud and scams with near impunity.

Tech sector regulation. The digital technologies and networks used in the majority of online fraud and scams are privately owned and operated, including companies registered in third-party countries. Liability laws exist but are not universally or consistently applied, and privately owned platforms have their own policies and enforcement mechanisms, leading to a patchwork approach to accountability. Within relevant technology companies, there are also challenges in how to frame the scams and fraud issues to senior leadership in ways that enable and incentivize large corporations to take action or determine company policies. The technical limitations of companies are not always fully understood by governments, leading to misunderstandings about roles and responsibilities. Governments have historically treated cyber-enabled fraud as a problem for platforms and financial institutions to solve through self-regulation, while industry has argued that fraud prevention is a law enforcement responsibility, leaving victims caught in the middle.

Human rights. There has traditionally been a risk of cybercrime laws being overly restrictive of content in ways that suppress freedom of expression and dissent and turn technological tools against users and/or restrict their access. International human rights law (IHRL) can act as an international standard to guard against these risks and thus is also relevant for consideration as a legal framework. However, in many countries and some regions, IHRL is perceived as a Western construct that may be at odds with long held cultural values.

WAYS FORWARD

Recommendation #1: Leverage relevant multilateral cybercrime instruments through joining and robustly implementing treaty obligations and make use of the cooperation channels such instruments provide.

Governments should leverage the opportunities provided by the Budapest Convention and new UN Cybercrime Convention to counter cyber-enabled fraud and scams in ways that are complementary and do not create new silos. Both instruments should be implemented in a rights-respecting way that does not expand state powers beyond what is necessary and proportionate to combat cybercrime.

States that have not yet ratified the Budapest Convention, especially those in Southeast Asia, should be actively supported and incentivized to accede to it, with capacity-building assistance provided as needed. States Parties should make use of the Convention's relevant Guidance Notes[57], notably on Botnets (#2), Transborder Access (#3), and Identity Theft (#4), among others, in order to fully utilize the capacities of the treaty to address fraud and scams.

Governments committed to tackling cyber-enabled fraud, and which have signed and will ratify or later accede to the UN Cybercrime Convention, could seek interpretative guidance or implement the Convention in ways that treat participation in the cyber-enabled fraud and scam industry as meeting the serious crime threshold. Improved evidence collection, research, and mapping of scam industry actors and syndicates is needed to demonstrate the scale of these operations and the gravity of crimes being committed.

Recommendation #2: Harmonize national laws and establish common definitions to strengthen implementation to resolve loopholes across the ASEAN region, and to resolve tensions between cybercrime frameworks and anti-trafficking in persons (anti-TIP) obligations.

ASEAN Member States are encouraged to improve shared understanding about their respective relevant cybercrime laws, including gaps or inconsistencies, as well as complementarity.

While a regional cybercrime convention has been suggested by some as an admirable goal, it has also been acknowledged that this would be time consuming and resource heavy. Agreeing on common standards or definitions could be an important immediate step towards closing legal loopholes.

Governments should review and, where necessary, amend their cybercrime and fraud legislation to incorporate clear provisions that distinguish between voluntary perpetrators and those coerced into committing cyber-enabled crimes. Prosecutorial guidelines and judicial training should reinforce this distinction to prevent the

[57] Council of Europe, *Guidance Notes*, Council of Europe, n.d., accessed June 5, 2026, https://www.coe.int/en/web/cybercrime/guidance-notes.

criminalization of the exploited in place of those who ultimately direct and profit from these schemes.

Recommendation #3: Invest in capacity-building initiatives for cybercrime investigators and law enforcement.

Governments should invest in specialist units that bring together cybercrime investigators, financial intelligence analysts, and prosecutors under a single operational mandate covering cyber-enabled fraud and scams.
National cybercrime training centers are a good model and should be encouraged, as well as training at all ranks and levels about cyber-enabled fraud, including digital evidence collection and digital forensics, and about the cybercrime marketplace and infrastructures.

Bilateral and multilateral assistance programs should support specialist cybercrime and fraud units in regions where scam infrastructure is concentrated, with technical assistance covering digital forensics, cryptocurrency tracing, and mutual legal assistance procedures, among other topics.

Recommendation #4: Encourage public-private cooperation and information exchange and support the use of technological innovation to counter online scam operations.

Improve understanding and collaboration between public and private sectors, notably the technology sector, about each other's respective roles, capacities, priorities, and internal processes, to close the resulting accountability deficit. Reviewing and harmonizing existing legal frameworks in the areas of data protection and privacy, as well as anti-fraud and consumer safety, would assist in reducing ambiguities.

Technology-based initiatives or actions to disrupt scam operations should be explored and encouraged, while avoiding adverse negative effects. Such initiatives may include geofencing, halting satellite internet, DNS blocking and web authentication efforts, and leveraging artificial intelligence.

Financial Crimes and Anti-Money Laundering Law and Frameworks

Scamming is ultimately about the money — criminal organizations are raking in an estimated $442 billion to $1 trillion per year through online scams. Currently, scamming remains a low-risk, high-reward activity, and as a result, many pre-existing criminal organizations are diversifying into scams to derisk their business, even as new criminal actors have entered the market. To be effective, efforts to counter online scams require disruption of these financial flows and raising the risk of prosecution for criminals engaging in online fraud and money laundering.

Online scam operations make use of complicated processes to transfer funds, often utilizing multiple bank accounts (usually money mule accounts), cryptocurrency wallets, as well as real and fake cryptocurrency platforms, to transfer stolen and illicit funds and eventually launder them back into normal circulation. These processes echo the behaviors of more traditional criminal organizations — and indeed, many online scam operations are run by criminal enterprises with deep familiarity and access to money laundering services from more traditional activities such as drug trafficking or trafficking in persons.

Many scam operations in Southeast Asia have large physical infrastructure associated with compounds — offices, dormitories, restaurants, entertainment, trafficked workers, and all the associated supply chains. This means there is a clear financial and logistical trail that can be followed for investigations and used to pinpoint vulnerabilities for disruption. Within this context, governments can leverage existing institutions and legal frameworks designed to counter money laundering to counter illicit funding flows from online scam operations with the right updates in approach, effective national implementation, and impactful cross-border coordination.

EXISTING LEGAL FRAMEWORKS AND INSTITUTIONS

The most comprehensive international institution related to countering money laundering is the *Financial Action Task Force (FATF)*, which is an independent inter-governmental body established in 1989 with the intent of setting standards for legal, regulatory, and operational measures to combat money laundering, terrorist financing, proliferation financing, and other threats to the international financial system. Originally, the FATF membership included the G7, European Commission, and eight other countries; as of 2026, there are 37 full members and a global network of more than 200 countries and 20 international organizations which are involved in

providing feedback on and implementing its recommendations.[58] The FATF's mandate has also evolved over time, focusing originally on countering misuse of financial systems to launder drug money in 1990 and then expanding over subsequent years to track other illicit flows, terrorist financing, and more recently, guidance and regulations for virtual asset management.

While each country needs to implement policies at the national level and in accordance with specific national circumstances, the FATF's primary role is to coordinate and update the *International Standards on Combatting Money Laundering and the Financing of Terrorism and Proliferation,* also known as The FATF Recommendations. These were approved in 2012 and are regularly updated — virtual assets and service providers were included as targets for AML recommendations in 2019, and the last update was in October 2025 — and cover a range of preventative measures such as know-your-customer (KYC) principles and other due diligence measures, payment transparency and use of new technologies, and internal controls; transparency and beneficial ownership of accounts to track real owners of the funds rather than just public business names; guidance on establishing appropriate national authorities such as Financial Intelligence Units (FIUs) or supervisory bodies to regulate, manage, investigate, and enforce the laws; and approaches and requirements for international cooperation such as mutual legal assistance or freezing and confiscation of assets.[59]

One major challenge in this space is that developments consistently outpace regulatory efforts — it takes time for the FATF bureaucratic processes to convene stakeholders, establish best practices, and then enforce them. This lag is necessary but leaves loopholes for criminal actors. For instance, Article 16 of the recommendations, often known as the Travel Rule, explicitly expands requirements on due diligence to cover virtual asset service providers and requires that information travels along with the funds to prevent illicit activities. This recommendation will only go into effect by 2030, and more than many others is still only partially implemented.[60] The delay has

[58] Financial Action Task Force. "FATF Global Network." Accessed June 4, 2026. https://www.fatf-gafi.org/en/countries/global-network.html.
[59] Financial Action Task Force. "International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation: The FATF Recommendations." 2025, 5–6. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.
[60] Financial Action Task Force. "FATF Updates Standards on Recommendation 16 on Payment Transparency." June 2025. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/update-Recommendation-16-payment-transparency-june-2025.html.

contributed to online scams flourishing through rapid transfers of stolen funds from traditional financial institutions into less regulated cryptocurrency and other digital assets. In addition to providing guidelines, the FATF also monitors enforcement and implementation of recommendations through regionally specific bodies. Indonesia, Malaysia, and Singapore are official members of the FATF, and the Asia/Pacific Group on Money Laundering (APG) regional body includes the other seven Southeast Asian nations as well as others around the region in its analysis. As part of the monitoring and enforcement procedures, the FATF and bodies like the APG provide regular evaluations of individual economies, which inform decisions to place individual countries under jurisdiction for increased monitoring or call to action when analysis identifies deficiencies.

Beyond FATF, individual countries have adopted anti-money laundering protocols, procedures, and regulations to implement the recommendations. Within Southeast Asia — where many online scam operations are based — the following institutions and regulations are also relevant:

Most countries have a Financial Intelligence Unit (FIU) which is responsible for receiving reports from financial institutions and the public and disseminating information to law enforcement. In Southeast Asia, these units are mostly housed within the national central banks such as PPATK (Indonesia), the Bank of Thailand, and Bank Negara Malaysia. In some countries such as the United States with the Financial Crimes Enforcement Network (FinCEN), these are housed within a direct government department, such as Department of Treasury.

The Association of Southeast Asian Nations (ASEAN) holds regular meetings related to countering Transnational Crime. At the 19th ASEAN Ministerial Meeting on Transnational Crime in September 2025, ASEAN adopted the ASEAN Declaration on Combatting Cybercrime and Online Scams, with particular commitments to increase understanding of illicit financial flows and money laundering associated with cyber scams.[61] ASEAN also committed to establishing a Working Group on Money Laundering in September 2025, with operations planned to begin in 2026 and coordinate across national borders. These also build on the existing Working Group on Anti-Online Scams, which was established in 2024 and engages on countering scams

[61] Association of Southeast Asian Nations. "ASEAN Declaration on Combatting Cybercrime and Online Scams." 2025. https://asean.org/wp-content/uploads/2025/09/03.-ASEAN-Declaration-on-Combatting-Cybercrime-and-Online-Scams.pdf.

through a digital economy lens and seeks to convene relevant officials and the private sector.[62]

Most countries in the region have one or more national laws which directly reference or address online scams. Some rely on older cyber security laws or are in the process of considering or updating national approaches.

GAPS AND CHALLENGES

Interlinkages between fraud and other crimes (trafficking and broader money laundering) are not sufficiently explored. Online scam operations didn't emerge out of a vacuum; many of the groups responsible had their roots in other criminal or crime-adjacent sectors including casinos and online gambling. Money laundering for proceeds of fraud is often done by the same operations which launder proceeds for other criminal actors ranging from trafficking organizations to North Korean cybercriminals. These are sophisticated services which often mix illicit and legitimate infrastructure, and which allow fraud and scam operations to thrive.

FATF watch lists are based on analysis that happens every few years, and which leaves it liable to miss rapid expansion of illicit flows at the scale that has occurred with online scam operations. For instance, as of early 2026, two of the three countries in Southeast Asia which are known to host scam compounds have identified deficiencies and are on FATF lists: Lao PDR is subject to increased monitoring, and Myanmar is considered high-risk and under a call-to-action.[6] Notably, while Cambodia was previously under monitoring twice from 2011-2015 and again from 2019-2023, it graduated in 2023 despite recognized deficiencies related to online casinos. As a result, the rapid evolution and expansion of online scam operations occurred largely after the latest FATF review and is unaccounted for with the current watch list status.[63]

While the FATF has recommendations for virtual assets, they are not fully implemented, and many countries either don't yet mandate or don't enforce the application of KYC and other security protocols to fin-techs, digital payment

---

[62] Mario Masaya et al. "Governments Across Southeast Asia Are Committed to Combatting the Rise of AI-Related Scams." US-ASEAN Business Council, 2025. https://www.usasean.org/article/governments-across-southeast-asia-are-committed-combatting-rise-ai-related-scams.
[63] David Whitehouse. "FATF Is Behind the Curve on Cambodia's Cyber-Scam Compounds." The Diplomat, July 18, 2025. https://thediplomat.com/2025/07/fatf-is-behind-the-curve-on-cambodias-cyber-scam-compounds/.

systems, cryptocurrency, or other virtual assets. The FATF only included virtual assets as subject to its recommendation starting in 2019, and while there has been progress — for instance, Thailand's second Royal Decree on Prevention and Suppression of Technological Crimes was updated in 2025 to expand due diligence mandates to digital asset providers — it is still an ongoing transition. Since significant numbers of scams utilize cryptocurrency and other frictionless payment services providers to move funds, limited deployment or enforcement of due diligence protections leaves gaps that scammers can exploit. Many fintechs and other digital financial operators do hold licenses to act as financial vehicles; government should equally implement the associated due diligence requirements and, when necessary, should revoke licenses to ensure compliance.

Mule accounts at conventional banks remain a major vector for fraudulent funding flows. Global anti-money laundering efforts are designed to address wholesale fund transfers, but many scammers operate at the retail level, using numerous "money mule" accounts to transfer smaller amounts of money and avoid detection. Current practices allow for relatively frictionless opening of bank accounts online, which is increasingly vulnerable to artificial intelligence to avoid due diligence processes. A lack of awareness among community members about the illegality and risks of being a money mule allows criminals to take advantage, for instance, through paying citizens in some communities for access to their personal information or accounts. More screening is needed — not just at account opening, but for suspicious behavior.

Existing bases for cooperation are reactive and case-specific, rather than proactive. The ASEAN Mutual Legal Assistance Treaty (MLAT) already enables cooperation on criminal matters including things like evidence collection, asset recovery, and other information sharing. However, it is limited by bureaucratic processes and is ultimately reactive as it requires one side to request cooperation and often requires an active investigation into an individual given data privacy protections. This stands in counterpoint to many industry approaches and FATF recommendations about real-time or near-real-time information sharing under the Travel Rule.

Criminals adapt more quickly than authorities do. Ensuring that regulations are consultative and not overly impactful on key sectors often requires a long time to design, review, and implement new regulations. Criminals' adaptability ranges from jumping across national borders when local enforcement increases in one location to shifting the types of scams and target focus when regulations are enforced.

EXAMPLES OF GOOD PRACTICE

While every country context is unique and policies are not directly transferable to other jurisdictions, some countries have successfully implemented changes to laws or regulations which can act as inspiration or guidance on how to successfully harden key sectors and communities against the threat of scams. The following examples address some of the gaps identified above and provide lessons-learned for other countries or regulatory bodies seeking to address online scams and fraud.

- **Numerous countries — including the UK, Australia, Singapore, and Thailand — have adopted penalties for financial institutions (and FI-adjacent companies like fintech and virtual asset providers) which do not take necessary steps to create friction for scammers and prevent losses.** All four of the named countries have passed laws in the last two years that will penalize financial institutions for losses incurred by their customers. Such regulations may not be appropriate in all markets, but they provide a clear incentive for increased monitoring and prevention activities to protect consumers.
    - In the United Kingdom, starting in October 2024, the government's payment regulator began requiring service providers to reimburse losses of up to 85,000 GBP for authorized fraud, with liability for both sending and receiving banks. Anecdotal reports indicate push payment fraud is trending downward since these policy changes.
    - The Monetary Authority of Singapore provided guidance in October 2024 indicating that financial institutions and telecoms are liable for losses incurred if they did not meet a set of clear security and due diligence criteria to identify and block scam or fraud losses, including for seemingly authorized payments.[64]
    - Thailand adopted the Emergency Decree on Measures for the Prevention and Suppression of Cybercrimes No 2 in April 2025, which built on a previous law to significantly expand the scope of options and responsibilities for telecommunications and financial institutions,

[64] Monetary Authority of Singapore and Infocomm Media Development Authority. "Guidelines on Shared Responsibility Framework." 2024. https://www.mas.gov.sg/-/media/mas-media-library/regulation/guidelines/pso/guidelines-on-shared-responsibility-framework/guidelines-on-shared-responsibility-framework.pdf.

including liability for losses if not compliant with regulatory standards. The new emergency decree requires that virtual asset service providers follow the same approach as banks do towards data collection, sharing, and transaction suspension for suspected cybercrime.[65]
    - Australia's National Scam Prevention Framework, which went into effect in January 2025, requires businesses in key sectors (specifically telecommunications, banks, and digital platforms) to take reasonable steps to prevent, detect, and disrupt scams or face fines of up to AUS $50 million.
- Singapore's Online Criminal Harms Act allows the government to direct key sectors (social media, telecoms, banks) to take measures to halt scams and requires stricter verification for things like advertisements. After its adoption and enforcement, the number of users doing scams on Meta platforms dropped by 36.5%.[66]
- The Global Signal Exchange (GSE), established in 2024 by Global Anti-Scam Alliance in partnership with Google and the Oxford Information Labs, serves as a clearinghouse for business, government, and civil society to share data and related information (signals) about actors of concern.[67] The platform has shared more than one billion individual signals of threat intelligence in the two years since its launch, including details ranging from suspicious IP addresses to merchant IDs or bank account numbers. The GSE is one of many platforms that seek to fill gaps in data and understanding of scam impacts within existing legal constraints surrounding privacy laws or uncertainties.
- **Monitoring bank accounts not just at opening but in an ongoing manner for suspicious behavior can help limit the flow of illicit funds.** Thailand has

[65] Thailand Securities and Exchange Commission. "SEC Is Ready to Elevate Restrictions on Illegal Digital Asset Platforms after the New Laws Take Effect Today." Bangkok: Securities and Exchange Commission, Thailand, 2025. https://www.sec.or.th/EN/Pages/News_Detail.aspx?SECID=11698. The announcement refers to the Act on Prevention and Suppression of Technology Crime (No. 2), B.E. 2568 (2025), full text (Thai).
[66] Nadine Chua. "Over 9 in 10 Pieces of Criminal Cybercontent Taken Down Were Scams: Online Criminal Harms Act Office." *Straits Times*, February 28, 2026. https://www.straitstimes.com/singapore/more-than-9-in-10-criminal-cyber-content-taken-down-were-scams-online-criminal-harms-act-office.
[67] Global Signal Exchange. "About the Global Signal Exchange." Accessed June 4, 2026. https://www.globalsignalexchange.org/about.

piloted this approach through adopting "speed bump" approaches to digital transfers. In 2025, this included a limit on transactions for accounts which are seen as a fraud risk or have insufficient history of operation to only 50,000 THB per day (or about $1,500 USD).[68] In 2026, this "speed bump" approach was expanded to cryptocurrency and other digital assets, leading to a 24-hour pause for additional know-your-customer verification before transactions go through.[69] These small friction-adding steps are an additional pain point for criminal actors, who rely on speed to rapidly collect multiple illicit transfers and shift them through multiple accounts and/or wallets to obfuscate their origin.

WAYS FORWARD

Building on the gaps and best practices above, the following are a series of specific needs that should be addressed in order to better position regional governments, businesses, and other actors to effectively address online scam operations.

Recommendation 1: Invest more in data-sharing and coordination across sectors and national borders to improve response times when scams are reported. There is almost always a lag between when a fund transfer happens and when the person who lost funds identifies it as a scam and reports it. Financial institutions have developed near-real-time information sharing to track the movement of funds through traditional vehicles. However, most law enforcement investigations are reactive and require lengthy bureaucratic processes to access information.

Improve the rate of information sharing between governments to be more proactive and include real-time or near-real-time information when appropriate. Scammers rely on systematic blind spots by pushing funds across multiple platforms and national borders; improved information-sharing could make it easier to identify and halt suspicious transfers.

---

[68] "Bank of Thailand Clarifies 50,000 Baht Transfer Limit Applies Only to Vulnerable Groups." *The Nation*, August 20, 2025. https://www.nationthailand.com/business/banking-finance/40054282.
[69] Nuntawun Polkuamdee. "Crypto Operators Freeze 10,000 Suspect Accounts." *Bangkok Post*, March 10, 2026. https://www.bangkokpost.com/business/general/3213543/crypto-operators-freeze-10000-suspect-accounts.

Improve investment and resourcing for data sharing and coordination among key actors across sectors and national borders. Simply providing a mandate would be insufficient to implement improved processes.

Recommendation 2: Laws should be improved to clearly identify fraud and scams as a real and serious crime, including updates to penalties to match the severity of the crime. Despite their prevalence, scams and fraud are generally considered to be lower severity than other crimes, and the punishments vary widely across national borders. Countries should update penalties on the books to recognize the severity of fraud and scams — and where possible, harmonize these penalties so that crimes are treated similarly across national borders.

Recommendation 3: Financial investigations should be a natural follow-on when a cyber or trafficking crime is identified. Lawmakers often pursue criminal investigations through the particular lenses of the reported crime. For instance, when a trafficking investigation occurs, it often treats the case as an individual instance and does not necessarily include an associated digital forensics investigation. This risks losing crucial digital and financial evidence not only to prove that the trafficking occurred but also to understand how an individual trafficking case is linked to a broader online scam operation network. Similar challenges of investigative silos exist for cyber crimes and fraud as well. If investigations explore linkages between individual crimes and the broader criminal ecosystem and marketplace rather than as one-offs, then prosecution and disruption are more feasible.

Recommendation 4: Law enforcement organizations and development partners should provide capacity-building and resource support to local digital forensics investigations so that funds can be better identified, tracked, and then potentially seized and returned to rightful owners. As investigations and seizures increase in response to greater political will and international attention, capacity building will be crucial for law enforcement as well as for judiciaries so there is a clear understanding of how to identify and return lost funds.

Ensure that there are appropriate processes for remediation and victim restitution in target countries. Increasingly, as countries like the United States and Australia seize or forfeit proceeds from known mule and other suspended bank and crypto accounts, there is a need to ensure it is appropriately disposed of. Governments should provide such clarity.

Recommendation 5: Coordination needs to occur across sectors (telecoms, financial institutions, fintech/non-traditional finance actors, and social media platforms) and between countries to ensure that crackdowns in one sector do not simply push criminal actors to adapt and utilize other approaches.

Recommendation 6: Financial institutions and law enforcement should prioritize disruption of criminal enterprises through improving halts on suspicious transfers and other deterrence mechanisms. As financial institutions improve detection of unusual transactions and identification of mule accounts, and can respond quickly to requests to halt funds when they are reported in a timely manner, it is increasingly possible to disrupt individual scam losses. As detection improves, it is increasingly clear that disruption needs to be more of a focus given limited halting of suspicious transactions and other deterrence mechanisms.

Recommendation 7: Governments need better data transparency to track and understand how legitimate businesses benefit from illicit advertisements for scams or other fraudulent services. Criminal entities take advantage of weak KYC protocols and due diligence to launder funds back into the legitimate economy, as seen in numerous sectors ranging from real estate to precious metals. Recent investigations[70] show that some tech companies are receiving funds for scams or other illicit activities, which can create conflicts of interest. This is likely widespread due to limited requirements for advertiser verification across numerous online platforms.
Given widespread concern and attention from regulators and reputational damage among consumers, tech companies may benefit from improving industry standards to reduce future risks.

Governments should consider how to incentivize better control to prevent this from re-occurring, but decision-makers need better data to understand the scale of the problem.

Addressing some of these gaps in enforcement and implementation can help right the current imbalance that treats scams and fraud as a low-risk, high-reward activity. While this problem will remain endemic given human greed and the easy efficiency gains of scams and fraud that technological advancements provide, adding friction to

[70] Jeff Horwitz. "Meta Is Earning a Fortune on a Deluge of Fraudulent Ads, Documents Show." *Reuters*, November 6, 2025. https://www.reuters.com/investigations/meta-is-earning-fortune-deluge-fraudulent-ads-documents-show-2025-11-06/.

the process, increasing risk for criminals who make use of systemic vulnerabilities, and disrupting efforts can significantly reduce its attractiveness to criminal actors and stem losses.

Conclusion

This publication has examined relevant laws, policies, and normative frameworks in three areas: anti-trafficking-in-persons, cybercrime, and financial crime/anti-money laundering, at international, regional, and national levels. Each of the above sections has presented and explored relevant treaties, laws, regulations, and practices; identified gaps and challenges; and provided recommendations for forward action in preventing, disrupting, and responding to online fraud and scams.

A goal of this project has also been to bridge divides across national borders, communities of practices, and industry sectors. In almost every event and dialogue on this topic, at least one expert noted that improving practices and enforcement in only one sector would simply push scammers to adapt their approach and take advantage of loopholes elsewhere.

To that end, we offer the following overarching recommendations that cut across the topics studied or that may foster better cooperation and information sharing between them.

1. Interagency task forces or national anti-scam centers are strongly recommended as a valuable way to promote collaboration and cooperation across agencies and departments, and often with law enforcement. This was repeatedly recommended by diverse participants in project activities. Such national bodies are being established in a growing number of countries, including Singapore (the first to establish one) as well as Malaysia and Thailand.[71] While these are tailored to national contexts and ways of working,

[71] As of 2025-2026, Singapore, Malaysia, and Thailand have established dedicated national centers with interagency cooperation and real-time response mandates: Singapore's Anti-Scam Centre was created in 2019 under the Singapore Police Force (SPF); Malaysia launched its National Scam Response Centre in 2022, a joint operation between the National Anti-Financial Crime Centre, Royal Malaysian Police, Bank Negara Malaysia, and the Malaysian Communications and Multimedia Commission; Thailand operates two parallel bodies, the Anti-Online Scam Operation Center (AOC, est. 2023) and the Royal Thai Police's Anti-Cyber Scam Centre (ACSC); and Indonesia launched the Indonesia Anti-Scam Centre/IASC (est. 2024), led by the Financial Services Authority (OJK) in coordination with Satgas PASTI and the financial services industry. The Philippines coordinates through the Cybercrime Investigation and Coordinating Center (CICC), without a single dedicated center, but are pushing for its creation. Vietnam, Brunei, Lao PDR, Cambodia, and Myanmar lack formal national centers, though some participate in ASEAN-level

they can provide a blueprint for other interested states to create their own. Establishing task forces, committees, or similar entities at the regional level could provide a further layer of coordination and act as a clearinghouse for regional information sharing.

   a. Finding ways for such centers to establish regularized dialogue with private sector stakeholders remains a priority challenge, given the valuable information such actors hold and how many of their platforms and services are affected by online fraud.

2. Governments should pursue a coordinated, multi-pronged strategy to disrupt and dismantle the criminal networks behind scam centers, such as through targeted sanctions on key actors and complicit businesses, sustained diplomatic pressure on governments that harbor or tolerate these operations, and rigorous financial investigations that follow illicit money flows across borders and into offshore havens. A greater emphasis on disruption and tackling the root causes of cyber fraud was encouraged by project participants, including through methods that disincentivize scamming, that focus on individuals in leadership roles, and make it more challenging for criminal networks to operate overall.

   a. Targeted sanctions are emerging as one of the most potent instruments of accountability for cyber fraud, although sanctions frameworks vary from country to country, which may affect the ability of some to pursue this route. Ideally, sanctions could be coordinated across multiple regimes, but even one effective use of targeted sanctions can have a ripple effect. A good example of this is sanctions against the Prince Group, which began in October 2025 when the U.S. designated the Prince Group as a transnational criminal organization and sanctioned 146 associated

---

working groups. Singapore Police Force, "Opening of Anti-Scam Command Office," March 22, 2022, https://www.police.gov.sg/media-room/news/20220906_opening_of_anti-scam_command_office; National Anti-Financial Crime Centre (NFCC), "About NSRC," Prime Minister's Department, Malaysia, October 14, 2022, https://nfcc.jpm.gov.my/index.php/en/about-nsrc; Thailand Ministry of Digital Economy and Society, "Anti-Online Scam Centre Gets Off the Ground," *The Nation Thailand*, November 2, 2023, https://www.nationthailand.com/thailand/general/40032467; Otoritas Jasa Keuangan (OJK), "OJK Luncurkan Indonesia Anti-Scam Centre," November 22, 2024, https://ojk.go.id/id/berita-dan-kegiatan/info-terkini/Pages/Waspada-Penipuan-Website-Mengatasnamakan-Indonesia-Anti-Scam-Centre-IASC.aspx; Philippine News Agency, "CICC Eyes National Anti-Scam Hub as One-Stop Complaint Center," April 29, 2026, https://www.pna.gov.ph/articles/1274007.

individuals and entities.[72] The U.K. joined on to these sanctions the same day the U.S. issued them, and this kickstarted a series of follow-on efforts: In November 2025, South Korea sanctioned the Prince Group;[73] in March 2026, Singapore arrested three as part of related investigations;[74] and Taiwan indicted 62 people over operating scam centers for the Prince Group.[75] If similar efforts against other criminal organizations are coordinated further in the future, the impact could be even broader.

   b. Concerted diplomatic action and consolidated positions from countries affected by scams are also important to elevate the issue, direct resources accordingly, and reduce loopholes and related jurisdiction shopping.

3. Local NGOs and journalists are indispensable to understanding and documenting scam center operations in Southeast Asia, yet they remain chronically under-resourced relative to the risks they bear. On-the-ground insight into what is happening has been crucial for information-gathering and public exposure of scam compounds, but individual journalists don't always fit well into the traditional grant funding model. International stakeholders should prioritize direct, flexible funding for these individuals and organizations and ensure they are meaningfully included in research partnerships, policy consultations, and advocacy coalitions.
4. Regional or other multilateral events and convenings focused on a single aspect of cyber fraud are encouraged to take stock of, and potentially integrate, what is occurring in other fora. For example, convenings relating to anti-TIP conventions or processes could be spaces to include voices with expertise on

---

[72] U.S. Department of the Treasury, "U.S. and U.K. Take Largest Action Ever Targeting Cybercriminal Networks in Southeast Asia," press release, October 14, 2025, https://home.treasury.gov/news/press-releases/sb0278.
[73] "South Korea Introduces Sanctions over Online Crimes in Southeast Asia," *Reuters*, November 27, 2025, https://www.reuters.com/world/asia-pacific/south-korea-introduces-sanctions-over-online-crimes-southeast-asia-2025-11-27/.
[74] Singapore Police Force, "Police Arrest Three Singaporeans in Money Laundering Investigation Relating to Transnational Scam Syndicate Prince Holding Group," press release, March 3, 2026, https://www.police.gov.sg/media-hub/news/2026/03/20260303_police_arrest_three_singaporeans_in_money_laundering_investigation.
[75] "Taiwan Indicts 62 over Suspected Scam Centre Operator Prince Group," *Reuters*, March 4, 2026, https://www.reuters.com/world/china/taiwan-indicts-62-over-suspected-scam-centre-operator-prince-group-2026-03-04/.

cybercrime law or who are following financial flows as the relate to scams, or vice versa.

5. In addition to improved application of the non-punishment principle and improved legal clarity on support for victims of trafficking, there is a need to improve the legal framework to provide support for victims of fraud who suffer monetary, reputational, social, and emotional losses. Laws to support (fraud) victim assistance and remediation efforts.

The criminal networks behind scam centers are sophisticated, adaptive, and operating across borders. Responses must match that complexity. No single law, agency, or sector can address this problem alone. Progress will require sustained cooperation across disciplines and jurisdictions: between anti-trafficking advocates and cybercrime investigators, between financial regulators and diplomatic corps, and between international bodies and the local NGOs doing difficult work on the ground. The frameworks examined in this series provide a foundation to build on. What is needed now is the political will to use them, including in concert, close the gaps between them, and resource the actors best positioned to make a difference. The scale of harm caused by scam centers demands nothing less.