US-ASEAN BUSINESS COUNCIL, INC.

Southeast Asia Public Policy Institute

TOWARDS AN ASEAN RESPONSE TO SCAMS

September, 2025

This paper has been researched and produced by the Southeast Asia Public Policy Institute in collaboration with the US ASEAN Business Council, with support from lead industry member Meta. The information and analysis presented are based on interviews with relevant stakeholders, publicly available information, and analysis by the authors. It does not represent the views of Meta or the US ASEAN Business Council directly. It is not intended to be an exhaustive review of policy, legislation, or regulation and should be used with due caution and consideration of its scope and limitations.

We would like to thank Thailand's Ministry of Digital Economy and Society (MDES), the U.S. ASEAN Business Council and lead industry member Meta, the U.S. Department of State's Bureau of Cyberspace and Digital Policy (CDP), the U.S. Embassy in Bangkok, and the U.S. Mission to ASEAN for supporting the gathering of insights for the paper.

CONTENTS

ABOUT THIS PAPER

This policy white paper has been prepared by the Southeast Asia Public Policy Institute in coordination with the US-ASEAN Business Council, supported by Meta.

The aim of the paper is to develop a set of actionable policy recommendations to combat scams across the Association of Southeast Asian Nations (ASEAN) member states. This is done through a review of the state of scams in the region, an in-depth review of policy responses in ASEAN and around the world, an analysis of the key challenges the region faces in combating scams, and the development of a set of policy recommendations, including a specific set of recommendations that can be taken forward by the ASEAN Secretariat and ASEAN member states, potentially in collaboration with ASEAN Dialogue Partners.

The paper was developed through desk research, analysing a range of sources from ASEAN, international organisations, individual ASEAN member states, other countries' approaches to scams, and private sector sources. Initial findings were tested and supplemented with expert interviews with a range of sources from the private sector (telecommunications, technology platforms, finance sector), civil society (especially those involved in combating scam centres and regional trafficking), as well as government ministries and law enforcement.

The draft findings of this paper were presented for discussion at a workshop co-hosted by the Ministry of Digital Economy and Society (MDES) of Thailand and the US-ASEAN Business Council, in coordination with the U.S. Department of State's Bureau of Cyberspace and Digital Policy (CDP), the U.S. Mission to ASEAN, and the U.S. Embassy in Bangkok on 20 August 2025.

ASEAN Workshop and Recommendations on Public-Private Partnership to Tackle Scams

Context

Scams have evolved into one of the most pervasive criminal threats in Southeast Asia, undermining financial stability, social trust, and human security. Globally, scams are now part of a cybercrime economy valued at over US$10.5 trillion, with consumers losing more than US$1 trillion in 2023 alone. In Southeast Asia, the problem is compounded by the presence of large-scale scam compounds that intertwine illicit online activity with human trafficking, money laundering, and organized crime. These compounds exploit tens of thousands of trafficked individuals coerced into forced criminality, making scams both a digital and humanitarian crisis.

In response to the alarming threats, governments across Southeast Asia have taken significant measures such as establishing centralized anti-scam task forces, updating legislation, and introducing technical safeguards. These efforts are reinforced by the private sector, where technology platforms, banks, and telecom providers are investing in AI-powered detection, intelligence sharing, and user education. Civil society has also played a vital role in reducing vulnerabilities of citizens, documenting abuses within scam compounds, and advocating for victims. Despite this progress, scams remain fast evolving: criminal groups shift operations across borders, exploit regulatory and regional governance gaps, and continually develop new methods, keeping enforcement perpetually one step behind. ASEAN member states bring a wealth of experience in this area, and are well placed to take the lead in developing a holistic approach to tackle fraud and scams, involving regulators, private companies, and civil society to address these challenges effectively.

Insights from the Workshop

The Ministry of Digital Economy and Society (MDES) and the U.S. ASEAN Business Council - in coordination with the U.S. Department of State's Bureau of Cyberspace and Digital Policy (CDP), U.S. Embassy in Bangkok, and U.S. Mission to ASEAN hosted a workshop on August 20, 2025 to explore the response to-date in Southeast Asia to scams, and discuss opportunities for a way ahead, focusing on intra-national coordination, and regional coordination at the ASEAN level.

The workshop was attended by Member state representatives from Singapore SPF, MDDI, and GovTech, Malaysia MCMC and BNM, Philippines CICC, Thailand MDES, Indonesia Komdigi, Myanmar mmCert/MOTC, Brunei AITI and many more from civil society such as Vietnam Chong Lua Dao and Philippines Citizen Watch contributed input. It was also attended by key regional and international organizations such as the United Nations Office on Drugs and Crime, the Global Initiative Against Transnational Organized Crime, Bali Process on People Smuggling, Trafficking in Persons and Related Transnational Crime, and International Justice Mission.

ASEAN Workshop and Recommendations on Public-Private Partnership to Tackle Scams

Workshop discussions identified recommendations for ASEAN to combat scams:

1. **Priorities to disrupt scam compounds:**
In order to tackle scams at the root, ASEAN requires not only law enforcement operations but also political will, financial monitoring, and cross-sector intelligence sharing through joint operations, oversight of special economic zones, and disruption of the criminal infrastructure. Human trafficking tied to forced scamming must be understood as central to the scam economy, with stronger victim support, rescue, and reintegration systems. Financial disruption is essential: illicit funds often move across borders within hours, facilitated by cryptocurrencies, shell companies, and weak Know Your Customer (KYC) regimes. Strengthening anti-money laundering (AML) frameworks and aligning with Financial Action Task Force (FATF) standards will be critical.

2. **Priorities to reduce vulnerability to scams:**
Bad actors rely on regional governance gaps, which must be reduced by tightening infrastructure loopholes (such as fraudulent job ads and spoofed telecom channels), improving digital literacy, engaging all stakeholders, and promoting public-private partnerships across the scam attack chain. The workshop also helped identify opportunities for ASEAN to coordinate and convene work between member states, the private sector and international partners to combat scams

3. **Priorities for ASEAN:**
ASEAN now has a critical opportunity to lead a coordinated regional response. Recommendations identified during the workshop include:

- Empower the ASEAN Working Group on Anti-Online Scams (WG-AS) with dedicated funding to enable it to centralize intelligence, propose joint projects, and engage in the development of policy guidelines towards a common response to scams.
- Elevate scams onto the agendas of all relevant ASEAN Ministerial Meetings and dialogues to recognise it as a shared priority and to leverage existing frameworks.
- Initiate a 'track 1.5 dialogue' between ASEAN member state governments and relevant stakeholders including civil society and the private sector (including telecoms operators, technology platforms, and the finance sector) to foster public-private collaboration, intelligence exchange, and coordinated cross-border responses.
- Strengthen engagement with international governments and organizations to expand cooperation on cross-border investigations, legal assistance, and align standards on due diligence and asset recovery.
- Support regional intelligence and data sharing among governments and law enforcement by coordinating threat intelligence, including alerts e.g. on fraudulent URLs, phishing domains, and mule account identifiers.

Ultimately, the successful implementation of these recommendations requires unprecedented collaboration across governments, law enforcement, the private sector, and civil society, both regionally and internationally, to effectively disrupt criminal networks, protect vulnerable populations, and safeguard the economic prosperity and well-being of Southeast Asia's citizens.

EXECUTIVE SUMMARY

Scams have become a global epidemic, costing consumers over US$1 trillion in 2023 and eroding trust in digital services while also fueling organized crime. Increasingly enabled by AI, deepfakes, and cryptocurrencies, scams now range from investment and romance fraud to business email compromise, phishing, and social engineering-based scams. Southeast Asia has emerged as a global hub for the "scam-industrial complex," where transnational crime networks run large compounds and exploit trafficked workers as coerced "victim-perpetrators" to scam consumers and businesses worldwide. Weak financial oversight, cryptocurrency misuse, and links to under-regulated casinos make scams both a cybersecurity challenge and a human rights crisis with far-reaching socio-economic consequences.

Responding to scams requires a comprehensive, multi-stakeholder approach. Effective strategies combine proactive measures—including education, prevention, detection, and disruption—with reactive responses including victim support, enforcement, and recovery. Governments worldwide are experimenting with new institutional frameworks, legislation, and technical protocols, while public engagement campaigns have proven valuable in building resilience and intelligence. Yet the policy landscape remains fragmented; no single actor has oversight of the full "attack chain" of scams, making coordinated contributions across government, industry, and civil society essential.

In Southeast Asia, governments have introduced a range of measures, from SIM card re-registration and e-KYC rules to centralized scam response centres. Some states are taking comprehensive, multi-agency approaches, while others remain constrained by capacity or governance challenges. Regionally, initiatives through ASEANAPOL, the ASEAN Regional CERT, and the ASEAN Working Group on Anti-Online Scams have begun to take shape, but cooperation remains uneven and often reactive. A more strategic and inclusive regional framework is needed—one that also systematically engages industry, civil society, and international partners.

Private sector and civil society initiatives already provide an essential layer of defence, bringing speed, scale, and innovation. Technology companies deploy AI-driven detection, banks and telecoms invest in real-time analytics and fraud prevention, and NGOs advocate for victims and expose human trafficking in scam compounds. Emerging systemic responses—such as cross-industry intelligence sharing and proof-of-human tools—show the potential of innovation to counter evolving threats. Together, these efforts underscore that addressing scams requires a whole-of-society approach rooted in cross-border collaboration.

To build resilience, Southeast Asia must focus on dismantling scam compounds, disrupting illicit financial flows, and addressing the trafficking that underpins forced criminality. Nationally, governments should strengthen coordination, deepen public-private partnerships, and invest in digital literacy and victim support. Regionally, ASEAN can play a catalytic role by empowering its anti-scams working group, elevating scams onto ministerial agendas, convening Track 1.5 dialogues with industry and civil society, and aligning with global partners such as INTERPOL, the Financial Action Task Force (FATF), and the Global Informal Regulatory Antifraud Forum (GIRAF). With a coordinated response, scams can be treated not as isolated crimes but as systemic threats to digital trust, economic stability, and human security.

Discussions at the ASEAN Workshop contributed to the recommendations below that identify key priorities for ASEAN Member States to disrupt scam compounds and reduce the vulnerability of their economies to scams, and to define a role for ASEAN to drive a regional response to scams:

1. PRIORITIES TO DISRUPT SCAM COMPOUNDS

In order to tackle scams at the root, ASEAN requires not only law enforcement operations but also political will, financial monitoring, and cross-sector intelligence sharing through joint operations, oversight of special economic zones, and disruption of the criminal infrastructure. Human trafficking tied to forced scamming must be understood as central to the scam economy, with stronger victim support, rescue, and reintegration systems. Financial disruption is essential: illicit funds often move across borders within hours, facilitated by cryptocurrencies, shell companies, and weak Know Your Customer (KYC) regimes. Strengthening anti-money laundering (AML) frameworks and aligning with Financial Action Task Force (FATF) standards will be critical.

2. PRIORITIES TO REDUCE VULNERABILITY TO SCAMS

Bad actors rely on regional governance gaps, which must be reduced by tightening infrastructure loopholes (such as fraudulent job ads and spoofed telecom channels), improving digital literacy, engaging all stakeholders, and promoting public-private partnerships across the scam attack chain. Bringing together the various relevant arms of the state for a coherent government response has already delivered results in many jurisdictions. Exploring ways to engage private sector and other stakeholders to gain from their expertise and intelligence is also an essential part of the policy response. Creating a policy landscape that supports individual actors to take action is also an important step.

3. PRIORITIES FOR ASEAN

ASEAN now has a critical opportunity to lead a coordinated regional response. Recommendations identified during the workshop include:

1. Empower the ASEAN Working Group on Anti-Online Scams (WG-AS) with capacity and funding to enable it to centralize intelligence, propose joint projects, and engage in the development of policy guidelines towards a common response to scams.
2. Elevate scams onto the agendas of all relevant ASEAN Ministerial Meetings and dialogues to recognise it as a shared priority and to leverage existing regional coordination frameworks.
3. Initiate a 'track 1.5 dialogue' between ASEAN member state governments and relevant stakeholders including civil society and the private sector (telecoms operators, technology platforms, payments and the finance sector) to foster public-private collaboration, intelligence exchange, and coordinated cross-border responses.
4. Strengthen engagement with international governments and organizations to expand cooperation on cross-border investigations, legal assistance, and align standards on due diligence and asset recovery.
5. Support regional intelligence and data sharing among governments and law enforcement by coordinating threat intelligence, including alerts e.g. on fraudulent URLs, phishing domains, and mule account identifiers

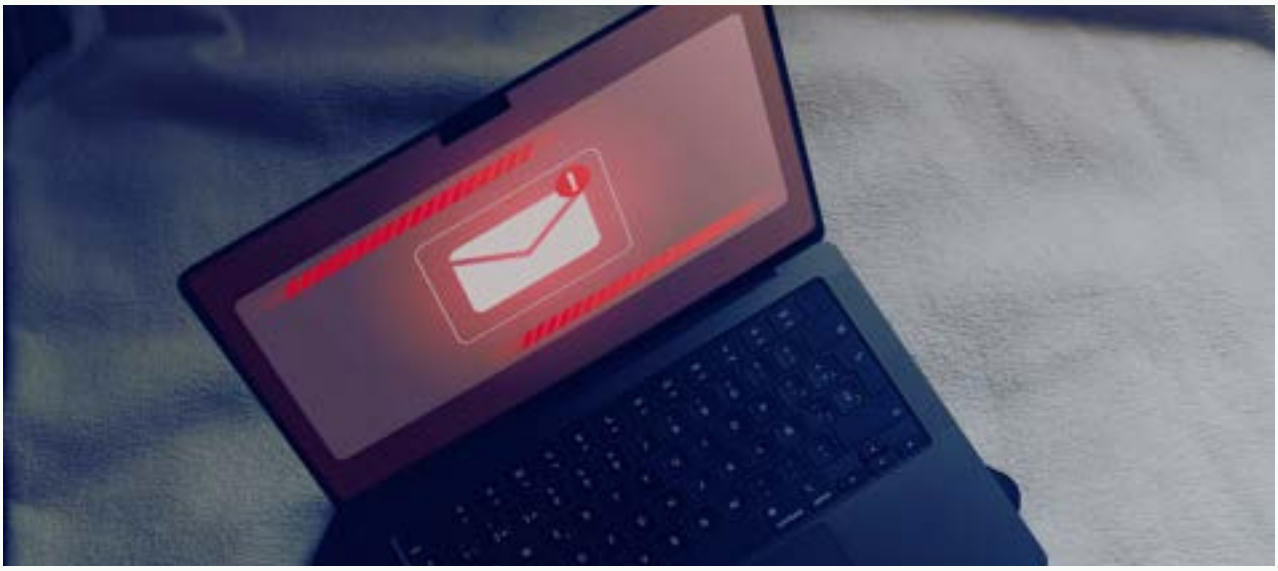
This final version of the white paper incorporates the discussions at the workshop, as well as additional insights from US-ASEAN Business Council members, building on the research and stakeholder interviews undertaken by the Southeast Asia Public Policy Institute.

PART I
UNDERSTANDING SCAMS IN 2025

SCAMS – A GLOBAL EPIDEMIC

As societies and economies have embraced digital technology, online crime has surged in scale and sophistication. The global cybercrime economy is now worth US$10.5 trillion, positioning it as equivalent to the world's third-largest economy by GDP.[1] Scams are a specific and growing type of cybercrime, where individuals, businesses or other organisations lose money or sensitive information to criminal actors.

According to the Global Anti-Scam Alliance (GASA), consumers lost more than US$1 trillion to scams in 2023.[2] However, the costs of scams go far beyond individual financial impact. For victims of scams, it can be a life-changing event, affecting mental health and wellbeing, and eroding trust in digital services.[3] There are also broader social and economic effects – money extracted through scams can fuel other types of criminality and governments are being forced to spend increasingly large amounts of money to combat scams through investments in law enforcement, public awareness, and national cybersecurity.



Focus on the victims and the economies targeted by scams hides a much darker social cost – the many victims of human trafficking that have been coerced into criminality in scam centres. The nature of these 'victim-perpetrators,' is complex, predominantly featuring people from low socio-economic backgrounds looking to escape poverty. The same countries from which scam centres recruit and operate are also often the least able to respond to the challenge, due to capacity constraints and other issues such as corruption.

Indeed, even the best-resourced governments struggle to keep up with the rapid evolution of scam methods, buoyed by the abuse of new technologies. Artificial intelligence (AI) and deepfakes are now being weaponized to better facilitate scams, with more than 42% of fraud attempts detected in the financial sector now attributed to AI.[4] New financial technologies such as cryptocurrencies support the broader scam business model.

Among this global epidemic of scams, Asia stands out as the region most heavily impacted. So-called pig-butchering scams, which refer to scammers who build relationships with a victim and deceive them into making investments (henceforth referred to as investment or romance scams), are especially widespread. These are often initiated through social media, messaging and SMS services before moving to alternative platforms, or completely offline.

Many of these schemes are operated by transnational crime syndicates running scam compounds concentrated in a handful of countries in Southeast Asia, targeting victims globally.[567] This scam centre model, that has been perfected in Southeast Asia, is being exported, with similar set-ups seen in the Middle East, West Africa, and South America.

Scams are thus at the centre of a set of global issues with profound implications for governance, socio-economic consequences, and the development agenda in an increasingly digital world.[8]

UNDERSTANDING SCAMS – SCAM TYPOLOGIES AND VECTORS

While scams are a seemingly pervasive and global experience, there are several factors why they remain such a significant challenge. Each scam is not just a single problem: it comprises a series of problems cutting across different parts of society and the economy. Each stakeholder involved only has a limited view of what is going on, meaning collaboration across government, across industry sectors, and across borders is essential.

Acknowledging this, we outline three complementary ways to frame scams: by tracing money movement, by categorizing typologies of scam schemes, and by examining the vectors through which the scams are executed.

The first approach is to trace the movement of money by distinguishing between authorized and unauthorized payments. In unauthorized cases, scammers gain access to accounts and make payments without the victim's consent, often enabled by stolen credentials or account takeover. These scams can be traced to broader issues of cybersecurity including data leaks and the installation of malware.

By contrast, authorized push payment (APP) scams occur when victims themselves are deceived into transferring funds under false pretenses, for example through impersonation, romance, or investment scams. This distinction is now widely used by regulators and the financial industry, with the U.S. Federal Reserve's ScamClassiferSM providing a clear example.[9]

The second approach is to use a more complex typology of scam schemes, as outlined in the UNDP's Anti-Scam Handbook, which categorizes scams by structure, purpose, and victim targeting. Most of the below are types of APP scam, though in some cases the ultimate objective is to obtain sensitive information that can later be used to facilitate unauthorised payments:[10]

TYPE	Description
E-Commerce / Shopping Scams	Fraudulent sellers exploit online marketplaces and social media platforms by offering products at attractive prices. Victims either never receive the goods or receive counterfeit or substandard items.
Investment Scams	Fraudsters lure victims with promises of high returns through fake or fraudulent investment opportunities.
Social Engineering Scams	Exploitation of human psychology to deceive individuals into divulging sensitive information or transferring funds.
Fake Charity Scams	Fraudulent solicitations for donations, often during crises or disasters, where funds are misused or stolen.
Business Email Compromise (BEC) Scams	Scammers promise victims large rewards, payments, or donations in exchange for an upfront fee.
Advance Fee Schemes	Scammers promise victims large rewards, payments, or donations in exchange for an upfront fee.
Romance Scams	Scammers use fake profiles on social media or dating apps to form emotional relationships with victims, ultimately exploiting them for financial gain.
Fake Job Scams	Fraudsters offer fake employment opportunities to extort money from job seekers or harvest their personal information.

A third approach, highlighted by the Global System for Mobile Communications Association (GSMA), looks at the vectors of communication that scammers exploit to reach victims. This lens shifts attention away from the typology or payment mechanics and instead examines the channels through which scams are actually delivered. Understanding these delivery mechanisms is critical because the same scam can spread through multiple vectors, and different vectors demand different forms of detection, regulation, and user protection. The wide range of techniques include:[11]

TYPE	Description
Authorized Push Payment fraud	Victim is tricked into sending money to a fraudster posing as a trusted payee.
Baiting	Offering something enticing (e.g. free software) to lure victims into giving up data or access.
Business Email Compromise	Criminals infiltrate business email to deceive staff into transferring money or information.
Identity fraud	Using another person's identity or creating a fictitious one to commit fraud.
Identity theft	Stealing personal details (e.g. ID numbers, passwords) to impersonate victims.
Impersonation	Pretending to be someone else (bank, colleague, official) to gain trust.
Phishing	Fake emails, SMS, or websites that trick users into revealing sensitive information.
Pretexting	Fabricating a scenario to obtain information, often by posing as a trusted figure.
Robocall	Automated calls with recorded messages used to deceive recipients into sharing data or money.
SIM Swap fraud	Convincing a mobile operator to transfer a victim's number to a fraudster's SIM.
Smishing and Vishing	Fraudulent SMS (smishing) or calls (vishing) to trick victims into revealing data.
Spear phishing	Targeted phishing, impersonating someone the victim knows to gain information or funds.
Spoofing	Falsifying caller ID, email, or contact details to disguise the scammer's identity.

Despite the different types of scam, most follow a similar, multi-step process—often referred to as the "life cycle" or "attack chain" of a scam. Each step in the attack chain builds on the previous; the earlier in the attack chain a fraudster is stopped, the more scams can be prevented.

Scam Journey Map, Source: UNDP Anti-Scam Handbook

The UNDP *Anti-Scam Handbook* illustrates the "scam journey map," which traces the typical sequence of steps taken by perpetrators. On the scammer's side, the process can be summarized as follows:

- **Establish operations:** set up the infrastructure to run scams at scale, which may include scam compounds, call centers, mule networks, bank accounts, or fake websites. Some scammers operate without heavy infrastructure, relying instead on digital platforms and small groups.
- **Research victims:** collect or purchase personal data, identify vulnerable groups, and target by geography, language, or profession to increase success rates.
- **Target and contact:** reach potential victims through ads, phishing emails, spoofed websites, social media, messaging apps, or unsolicited calls.
- **Communicate and convince:** build trust by impersonating legitimate actors or offering fraudulent opportunities, such as investments, jobs, or romantic relationships.
- **Call-to-action and payment:** persuade victims to transfer money, disclose credentials, or hand over sensitive information.
- **Hide proceeds:** launder illicit funds using cryptocurrencies, shell companies, online gambling platforms, or layered banking transactions to obscure financial trails.
- **Re-scam:** return to the same victims with new schemes, such as recovery scams or supposed opportunities to recoup earlier losses.

Understanding the attack chain is crucial to coordinating a robust response to scams, with each stakeholder – from construction companies and utilities that may be involved in supplying scam centres transport service providers that may be exploited for human trafficking, to mobile network operators, to banks, social media and messaging platforms, to law enforcement and government – identifying their possible role in the attack chain, creating a mechanism or method to identify and flag fraud, and intervening to disrupt the fraud in action. Combating fraud cannot be undertaken by any individual operator; a coordinated approach is essential.

SCAMS AND THE SCAM-INDUSTRIAL COMPLEX IN SOUTHEAST ASIA

Southeast Asia's digital economy is growing rapidly, expanding by 15% from 2023 alone, underscoring increasing prosperity across the region. As of 2024, internet penetration across the region reached 83%, supporting robust growth in sectors such as e-commerce.[12]

Yet, the same forces driving economic growth and digital inclusion are enabling a surge in scams. According to a survey of ASEAN member states conducted in 2023 by the ASEAN Working Group on Anti-Online Scams (WG_AS), half of all internet users in the region acknowledge having fallen victim to online fraud,[13] with phishing, impersonation, and the use of fake websites and social media platforms reported as the most widespread tactics across all ASEAN member states.[14]

While all regions host both scammers and victims, Southeast Asia is unique in the scale of the scam-industrial complex, which links scams, illicit activities such as drug production, human trafficking, and money laundering, all managed through transnational crime networks.[15] Large-scale scam compounds, often purpose-built or repurposed to coordinate these activities, sprung up during the COVID-19 pandemic, as lockdowns closed off both legitimate and illicit revenue opportunities.

According to a study by the UNODC in 2024, compounds can be found primarily in Cambodia, Laos, and Myanmar,[16] with the model prevalent in Southeast Asia spreading to Africa, South America, Eastern Europe, the Middle East, South Asia, and Pacific islands.[17]

The scam compounds frequently exploit trafficked individuals who are coerced into perpetrating scams. Estimates suggest that at least 120,000 people in Myanmar and 100,000 in Cambodia were at one time trapped in such operations.[18] A separate report by the United States Institute of Peace (USIP) places the total number of forced labourers involved in scam activities across Myanmar, Laos, and Cambodia at over 300,000, sourced from over 100 countries.[19]

Trafficking victims are typically job seekers lured by exploitative employment offers who interact with traffickers posing as recruiters targeting places with high unemployment rates. INTERPOL found that the keywords mentioned in the traffickers' fraudulent work advertisements have expanded over time from requirements for basic skills such as "phone operator" for "call centre" jobs, to technical skills to recruiting "information technology workers" and "digital sales executives." The United Nations Office of Drugs and Crime (UNODC) corroborates this finding: the need for victims with language skills is being surpassed by the need for victims with IT skills who can develop new programs including data scientists, digital marketers, and social media managers to help them further "professionalize" their operations.[20]

In the event of a successful operation against a scam centre operation, the treatment of these "victim-perpetrators" varies greatly, and poses significant challenges for law enforcement, justice systems, immigration, diplomatic and consular services. Many of the workers in the scam compounds are trafficking victims coerced into online fraud, yet they are also caught in active roles as perpetrators, blurring the line between protection and prosecution. Law enforcement must balance organized crime charges with obligations under anti-trafficking frameworks, while immigration and consular authorities face pressure to process and repatriate large groups of foreign nationals. In 2023, for example, Cambodian authorities rescued more than a thousand trafficked workers from scam centres, yet some were detained for immigration violations before being returned home. Such inconsistent approaches leave many in legal limbo and complicate regional cooperation against the scam-industrial complex.

Additionally, the scale of illicit profits generated from scam centres has driven the rapid professionalization of money laundering. Criminal groups now rely heavily on cryptocurrencies to layer and obscure transactions, making cross-border tracing difficult for law enforcement. Weak banking regulations and limited KYC enforcement in parts of Southeast Asia further enable shell companies, mule accounts, and underground remittance networks. Scam proceeds are also funnelled through under-regulated casinos and online gambling platforms, where illicit funds can be commingled with legitimate revenues. This convergence of scams, gambling, and opaque financial channels has created entrenched illicit economies that are difficult to disrupt.

PART II
RESPONDING TO SCAMS

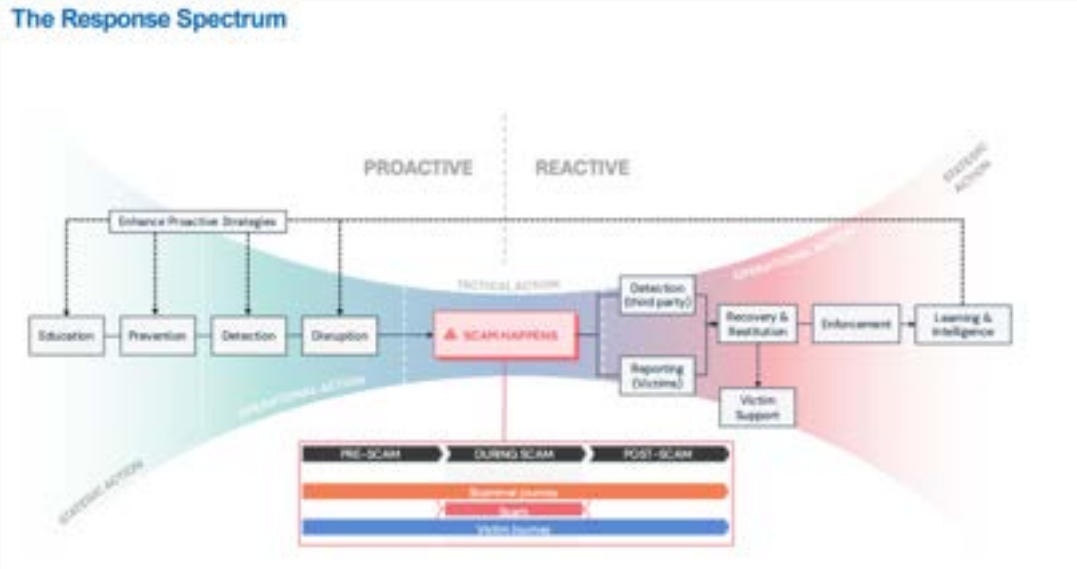
Addressing scams and fraud requires a comprehensive, multifaceted response involving a wide range of stakeholders at the global, regional, and country levels. Governments can respond to this set of challenges in a number of ways, including through developing a foundation of cybercrime law with targeted offences as well as specific sectoral arrangements through co-regulation and technical protocols. However, there is a significant amount of work that must be developed beyond this foundation from funding and training law enforcement, raising public awareness about scams and scam centres, to addressing corruption and transnational crime.

A common thread of response in expert interviews and at the ASEAN scams workshop was that to be effective, any fraud prevention initiative must mobilise all the relevant actors across government and across industry sectors, taking into account the need for local, national and international collaboration. The lack of any one entity having oversight over the whole journey of a scam means that understanding the roles and responsibilities of each potential actor is equally important.

To that end, government responses to scams can be significantly amplified by engaging stakeholders along the journey of a scam including the private sector – technology platforms (e-commerce, social media, messaging, etc.), telecommunications providers, payments operators, and financial services – many of whom are already deeply involved in combating scams. These entities continue to invest in their own cybersecurity, as well as sharing threat intelligence, and educating their own customers to recognize and report scams.

The UNDP *Anti-Scam Handbook* frames these diverse efforts through a "Response Spectrum," which maps interventions across the scam lifecycle. Proactive measures such as education, prevention, detection, and disruption complement reactive measures like recovery, enforcement, and learning. The model underscores that no single actor can address every stage, making coordinated contributions across government, industry, and civil society essential.

RESPONDING TO SCAMS



Source: UNDP Anti-Scam Handbook 2.0

To better frame the roles of different actors, the UNDP *Anti-Scam Handbook* introduces the idea of a "Response Spectrum." The model distinguishes between proactive actions that occur before or during a scam, and reactive actions that take place once a scam has been detected. Proactive measures include broad strategies such as education and prevention, alongside more targeted interventions like detection and disruption of scam operations. Once a scam occurs, responses shift into the reactive space, ranging from third-party detection and victim reporting to recovery, restitution, enforcement, and longer-term learning.

The framework also categorizes these interventions as strategic, operational, or tactical, depending on how close they are to the scam itself. Strategic actions like education and intelligence aim to shape the wider environment, while operational actions—such as prevention programs, victim support, and enforcement—directly address systemic risks. Tactical measures, by contrast, act at the point of exploitation, including disrupting scams in progress or tracing illicit financial flows. By setting interventions on this spectrum, the model illustrates that effective scam responses require both early-stage prevention and coordinated post-scam mechanisms, linking together multiple actors across government, industry, and civil society.

Against this backdrop, governments around the world have begun implementing their own policy responses, each emphasizing different parts of this spectrum with varying degrees of success. It is difficult to identify a single 'best practice,' especially in terms of legislation, given the recent and fast-changing nature of scams and the increasing role of technology in their execution.

REVIEWING RESPONSES FROM AROUND THE WORLD

Governments around the world have implemented policy responses to address the rise of scams with varying degrees of success. It is difficult to identify a 'best practice', especially in terms of policy and legislation, given the relatively recent emergence of these forms of scams, their fast-changing nature, and the increasing use of technology to execute them. In the expert stakeholder interviews undertaken for this paper, stakeholders regularly referenced the United Kingdom, Singapore and Australia as pursuing some of the earliest or most ambitious responses.

As the next pages show, the global policy landscape is fragmented, displaying disparate ways in which each jurisdiction is tackling the issue. However, there are common responses which we have identified across five key areas, including:

1. Creating a unified response across government - responding to the challenges of coordinating a government response across digital, communications, justice and law enforcement, many countries have established an anti-scam centre, commission or command, that brings together different arms of the state and, often, engages private sector stakeholders. These can vary greatly in their capacity, powers and focus, and the stakeholders involved.

2. Legislative responses – legislative responses are nascent, ranging from foundational cybercrime laws to laws specifically responding to scams, sometimes setting out new offences, creating new powers, and creating responsibilities for key stakeholders.

3. **Regulatory measures and technical protocols** – distinct from the broader legislative approach are targeted interventions, often sector-specific regulations for the banking, digital platform, or telecommunications sectors, for example to implement technical protocols such as SIM e-registration.

4. Coregulation and voluntary measures – these may stand alongside or in place of broader legislative responses and provide the framework for voluntary coordination between government and, in particular, private sector stakeholders.

5. Public engagement – public engagement by government ranges from campaigns, often in coordination with the private sector, to educate consumers, to more sophisticated schemes that allow victims to report scams and feed into government data and analysis.

The following section highlights examples of responses by different governments around the world (NB: responses from the ASEAN region are included in the following section). This is not an exhaustive list, a ranking, or a value judgement on the efficacy of these approaches. However, these are generally the most frequently referenced examples from stakeholder interviews and overall reporting on government-led responses to scams.

I. CREATING A UNIFIED APPROACH ACROSS GOVERNMENT

Some of the most robust responses to scams have been founded on the creation of a centralized authority, a single body responsible for overseeing and coordinating anti-scam efforts. Whether this is a newly established agency or a dedicated unit within an existing organization, such an organisation plays a critical role in ensuring systematic procedures, effective response, and strategic decision-making.

In Canada, the Canadian Anti-Fraud Centre (CAFC)[21] has operated since 1993 as the government-affiliated organization responsible for collecting reports of scams, identity theft, and fraud. It is run jointly by federal police, Ontario Provincial Police and the Competition Bureau Canada, bringing in various government agencies to execute its functions. The CAFC works with agencies focused on financial security and consumer protection. The centre also acts as a focal point for reporting, encouraging individuals and businesses to share information—even if they're not victims—so that law enforcement can act. It coordinates with relevant agencies and supports investigations, helping streamline case management across jurisdictions and also collaborates with the private sector on reporting, investigations, prevention, and information sharing.

In Australia, the National Anti-Scam Centre (NASC),[22] operated by the Australian Competition and Consumer Commission (ACCC), brings together experts from across government, law enforcement, and the private sector to disrupt scams proactively. The NASC partners with regulators including the Australian Securities and Investments Commission (ASIC), the Australian Communications and Media Authority (ACMA) and agencies administrating tax, services, and signals, as well as the Department of Home Affairs. Representatives from industry sectors, consumer advocacy groups and victims support organisations comprise an advisory board for the centre. Through its Scamwatch website, the NASC collects data, identifies trends, and alerts the public to emerging threats. It also publishes reports like the Targeting Scams Report, which documents the scope of scam activity and reported losses. In 2024, NASC reported a 25.9% reduction in scam-related financial losses, totalling AU$2 billion—a strong signal that coordinated action can yield measurable results.

In the United Kingdom, the National Economic Crime Centre (NECC), established in 2018 within the National Crime Agency, provides a similar coordinating function. The NECC brings together law enforcement, regulators, government departments, and the private sector to oversee a unified response to fraud and scams. Its role as "system leader" is complemented by Action Fraud, the national reporting platform for individuals and businesses to flag suspicious activity. Alongside reporting, the *Stop! Think Fraud* campaign—backed by the Home Office, City of London Police, and the National Cyber Security Centre—seeks to raise public awareness and simplify how victims understand and report scams. While Action Fraud has faced criticism over limited follow-through into investigations, the integration of data from both public and private sources has strengthened analysis of fraud patterns and informed prevention efforts. Together, these initiatives demonstrate how a centralized authority, when paired with dedicated reporting and outreach mechanisms, can provide a more consistent national response to scams.

II. LEGISLATIVE RESPONSES

Developing laws against scams is a challenge, given the pace of change and the cross-border nature of many online scams. Many countries have basic cybercrime laws making the use of technology for criminal purposes illegal. However, a small number of countries have been taking a different approach to the development of laws specifically targeting online fraud and scams.

Australia has taken an early approach to scams legislation with the passage of the Scams Prevention Framework (SPF) Bill 2025.[23] This legislation is among the world's first to impose specific legal duties on key industries vulnerable to scams—including banks, telecom providers, and digital platforms offering social media, paid advertising, or messaging services. Entities must take reasonable steps to prevent, detect, disrupt, and report scams, and the law empowers the ACCC to monitor compliance and enforce penalties where necessary.

Taiwan's Fraud Crime Prevention Act (2024) requires financial institutions, virtual asset service providers, telecom enterprises, online advertising platform operators, third-party payment service providers, e-commerce, and online gaming companies to respectively take certain fraud prevention measures. Businesses that fail to comply face heavy fines and serious reputational risk.

While the UK has generally taken a collaborative approach (see co-regulation section below), scams are addressed in a limited way in the Online Safety Act. The Act requires in-scope services (including platforms and marketplaces) to consider scams in their risk assessments for managing user-generated content on their platforms and remove suspected fraudulent content. The Act also bans paid-for fraudulent advertising e.g. advertising fake investment scams, which will be based on codes of practice to be developed with consultation by the communications regulator Ofcom.

In addition to addressing online content, the UK has also recently updated measures to further protect consumers against APP fraud. The UK Payment Systems Regulator announced new mandatory requirements for all UK financial providers to reimburse customers who fall victim to APP scams in all but exceptional circumstances. The new framework, which started in October 2024, stipulates reimbursement costs will now be shared between the sending and receiving financial providers.

III. REGULATORY MEASURES AND TECHNICAL PROTOCOLS

In addition to a legislative response which set out new frameworks for an approach to scams, there are a wide number of technical protocols and other measures that can improve the security of services, including telecommunications and payments.

In the United States, the Caller ID Authentication (STIR/SHAKEN) protocol was introduced by the Federal Communications Commission (FCC) to combat phone-based scams.[24] This system reduces spoofed robocalls by verifying caller identity across major telecom networks, making it harder for scammers to impersonate legitimate phone numbers—a tactic widely used in fraud schemes.

At the regional level, the European Union's Payment Services Directive (PSD) offers another example. Under PSD2, payment service providers are required to apply Strong Customer Authentication (SCA), a multi-factor verification system that significantly reduces unauthorized transactions. The upcoming PSD3 aims to go further by addressing fraud-related gaps in PSD2. It proposes enhanced real-time fraud monitoring and improved data-sharing between financial institutions for more targeted authentication and consumer protection.[25] A related but separate EU regulation on instant credit transfers[26] mandates a solution fronted by banks and payments service providers regarding the verification of the payee in instant transfers in the eurozone.

In 2025, the Irish Commission for Communications Regulation (ComReg) launched a new SMS Sender ID Protection Registry to reduce fraud through SMS spoofing. Legitimate organizations can register their SMS Sender IDs, allowing mobile service providers and messaging aggregators to tap into the registry to detect and block messages sent from unregistered or spoofed sender IDs.[27]

IV. COREGULATION AND VOLUNTARY MEASURES

Some of the most comprehensive responses have been based around a co-regulation approach, implemented through frameworks, strong industry codes, and targeted actions by stakeholders.

The UK provides a notable example, with structured engagement and collaboration with key industry sectors. In 2023 the UK introduced the Online Fraud Charter, a voluntary agreement between the government and the tech sector to minimize fraud on their platforms.[28] Actions to address fraud are agreed and implemented and are targeted to the specific risks on the individual platforms. This charter builds on similar agreements focused on the telecommunications (in 2021)[29] and retail banking (2021)[30] sectors, though notably both telecommunications and banking are also regulated sectors.

The UK's Joint Fraud Taskforce (a cross-government coordinating body) monitors progress against the commitments in the sector charters.[31] The coordination has also helped deliver several private sector partnerships. For example, in March 2025, major UK banks including Barclays, Lloyds, HSBC, and Santander, together with tech companies such as Google, Amazon, and Meta, signed a fraud charter to share real-time fraud indicators and monitoring data.[32]

Australia has also piloted voluntary models through the Fintel Alliance, which is led by the Australian Transaction Reports and Analysis Centre (AUSTRAC) a government agency responsible for monitoring financial transactions to identify money laundering and organised crime, including scams. The Alliance is a public-private partnership that brings together law enforcement and financial institutions to share intelligence and jointly develop advanced technological tools to prevent and detect scams and financial crime.[34]

Meanwhile, the Australian National Anti-Scam Centre's Job Scam Fusion Cell was a highly targeted initiative that aimed to combat scams targeting work-from-home job hunters. The taskforce brought together government, law enforcement, and industry for a six-month period in 2024 and successfully led to the referral of 836 scammer cryptocurrency wallets to digital currency exchanges for investigation, leading to blocking and blacklisting. The taskforce also leveraged intelligence sharing, enabling technology group Meta to remove around 29,000 accounts engaged in job scams on Australian Facebook groups, in addition to the referral of 1,850 scam enablers such as websites and scam job advertisements for removal.

There are several other examples in the Asia-Pacific region, including Hong Kong's voluntary Anti-Scam Consumer Protection Charter, which outlines six key principles to combat fraud and promote online safety. Tech companies including Google, Meta, LinkedIn, Weibo, Douyin and WeChat are signatories of the charter, with each company implementing actions that apply based on its unique business models.

The commitments and actions in the Charter are voluntary and non-legally binding and are intended to be applied on a proportionate basis.

At the regional level, the European Union's Europol-led European Money Mule Action (EMMA) showcases the value of cross-border, cross-sector collaboration.[35] EMMA enables public and private actors—ranging from Interpol and Eurojust to Microsoft and the European Banking Federation—to share intelligence on money mules, resulting in coordinated arrests and disruption of illicit financial flows across countries.[36]

V. PUBLIC ENGAGEMENT

Public awareness campaigns are sometimes dismissed as short-lived or superficial. However, international case studies—particularly from the United Kingdom, Australia, and the United States—demonstrate that when well-designed, sustained, and adaptive, these campaigns can significantly reduce scam victimization and build long-term public resilience. These campaigns can also develop to become more sophisticated tools that integrate reporting and data analysis that provides essential information for law enforcement strategy and policymaking.

In the United Kingdom, the government launched the "Take Five to Stop Fraud" campaign,[37] which delivers simple but powerful messages: Stop, Think, and Verify before sharing information or money. By 2022, 73% of the United Kingdom public recognized the campaign, and over half reported being more cautious in responding to unsolicited requests. The campaign aligned closely with Action Fraud, which centralizes reporting for a broad range of fraudulent activities, from cybercrime and investment fraud to business-related scams. It works closely with the National Crime Agency (NCA) and the National Cyber Security Centre (NCSC) to investigate threats and support victims.[38]

Australia's "Stop. Check. Protect." Campaign follows a similar approach. Launched by the federal government, it educates the public about sophisticated scam tactics, emphasizes that anyone can fall victim, and empowers people to report scams to Scamwatch.[39] The campaign encourages behavioural change, helping Australians pause and verify before responding to suspicious calls, messages, or online content.

There is also a role for the private sector in public engagement. The Stop Scams UK Coalition network of major banks, telecom providers, and technology companies collaborates closely with government agencies. One of its key achievements is the launch of the "159" fraud hotline, a pilot helpline that connects consumers directly with their bank's security team.[40] This model shows how public-private action can provide simple, scalable tools to empower and protect the public.

CONSIDERATIONS FOR EFFECTIVE LEGISLATION AND REGULATION

Through the research and interviews for this report, there were limited calls for new legislation and regulation. In many cases, the building blocks required to address scams exist, although they may require updating, and in all cases require better enforcement or capacity building. A further point made repeatedly at the workshop was that the scams challenge must be recognised as an international challenge, and was beyond domestic containment.

The following contains some insights to inform a cautious approach to new legislation:

Most of the legislative and regulatory approaches tend to focus on regulating industries, instead of focusing on efforts to deter bad actors. Furthermore, while more strictly regulating scams and fraud might seem intuitive, over-regulation can undermine user protection and privacy, as well as impede innovation and effective anti-scam efforts in the long run.

- **Impeding innovation:** Heavy-handed regulatory measures that fail to meet principles of proportionality can create an environment of uncertainty and excessive caution, which may result in companies merely focusing on compliance to avoid penalties.[41]

- **Undermining privacy:** Regulators overseeing scams often propose onerous obligations that run counter to global privacy obligations and regulations, making it difficult for global companies to comply.

- **Disincentivising effectiveness:** Regulators have been focused on prescriptive ideas without providing flexibility or room for innovation, which requires companies to divert resources in order to comply, rather than build for effectiveness of harm reduction.

CONSIDERATIONS FOR EFFECTIVE LEGISLATION AND REGULATION

Disincentivizing industry innovation and flexibility might lead to a less effective fight against scams, given the paramount role of industry in providing expertise and resources as well as new technologies to combat scams and fraud. It may also lead to less effective cross-industry collaboration which is key to tackling scams.

Over-regulation when it comes to information sharing typically relies on establishing a low threshold for sharing intelligence on scams and fraud, without insight into what intelligence is useful and actionable across industries. This can lead to false positives and over-removal, whereby legitimate content will be blocked or removed.[42]

For example, if a compromised email is used to facilitate scams, and that email is then shared, the real user may be blocked from other services, and therefore revictimized. Further, significant amounts of scams originate from fake or inauthentic accounts. That signal is likely useless but mandated sharing would mean investigative resources used to process this information would be taken away from other scam fighting work. It may also compromise user privacy, as a low threshold for monitoring content will inevitably subject users to more data collection for checks and control.

Further, regulation which requires more and more service providers to compensate victims for scam losses can reduce user vigilance and make the relevant jurisdiction more attractive to scammers by creating an insurance policy for bad actors. A barrage of regulations and warnings can also desensitize users to potential threats. Users might also become overwhelmed by the sheer amount of control and information, leading them to ignore or filter out important safety features or messages against scams.

To this end, a balanced approach to regulating online scams must uphold justice, fairness, and due process by carefully weighing the rights of victims against those of publishers, creators, or alleged perpetrators. Strict enforcement actions should be reserved for cases of demonstrable and high-severity harm, supported by clear evidence and robust procedural safeguards.

PART III

SOUTHEAST ASIA'S RESPONSE TO SCAMS

With Southeast Asia as a global epicentre for scams, governments and law enforcement across the region have responded with a range of measures to combat scams. This ranges from specific measures, such as the enforced e-registration of SIM cards (in Brunei, Cambodia and Myanmar) or better KYC for bank accounts, to more strategic efforts such as the creation of an anti-scam task force or command.

As in Part II, we have identified policy actions across five key areas. The below table gives an overview of key actions taken by governments in the region.

SOUTHEAST ASIA'S ANTI-SCAM AND FRAUD POLICY OVERVIEW

Country	Unified approach across government	Legislative response	Coregulation and voluntary measures	Public engagement	Technical protocols (e.g.)
Brunei	-	Penal Code Sec. 417; Computer Misuse Act – (no specific scam law)	-	-	SIM re-registration
Cambodia	Commission for Combatting Online Scams	Criminal Code; Sub-Decree No. 41 (SIM ID registration); cybercrime law in progress	-	-	SIM ID regulation
Indonesia	Indonesia Anti-Scam Centre (IASC) led by OJK	Penal Code; Electronic Information and Transactions (ITE) Law; OJK Regulation No. 12/2024	Indonesia Anti-Scam Centre (IASC) supported operationally by banks, payment associations, and e-commerce partners	"Beware of The Bad Guys" campaign (#AwasJebakanBadman)	e-KYC with biometrics
Laos	-	Cybercrime Law (2015) – no specific scam law	-	-	SIM registration
Malaysia	National Scam Response Centre (NSRC); National Fraud Portal under NSRC	Penal Code & CPC amendments; Comm. & Multimedia Act (2024); FSA 2013 updates	National Scam Response Centre (NSRC) with police, central bank, MCMC, and operational support from banks and telcos	#JanganKenaScam campaign	SMS content filtering; cross-border intelligence with SG

Country	Unified approach across government	Laws & Regulations	Coregulation and voluntary	Awareness & Literacy Campaigns	Technical Policies and protocols
Myanmar	-	Cyber Security Law (2025) - no specific scam law	CBM fraud task force engaging banks and financial institutions	-	SIM re-registration
Philippines	Cybercrime Investigation and Coordinating Center (CICC)	Cybercrime Prevention Act; AFASA (2024); SIM Card Reg. Act	AFASA with bank and fintech cooperation	"Kontra Scam Attitude" campaign	Multi-factor authentication requirements under AFASA
Singapore	Anti-Scam Command (ASCom) and ASC with co-located bank teams	OCHA (2024); Protection from Scams Bill (2025); CMA amendments; MAS' Shared Responsibility Framework for financial institutions and telecommunication companies (2024)	IMCS involving MHA, SPF, MAS, IMDA with Technical Reference 76 e-commerce standard	"Spot The Signs. Stop The Crimes" campaign; ""I can ACT against scams" campaign	SMS Sender ID Registry (SSIR); real-time fraud detection
Thailand	Anti-Online Scam Operation Centre (AOC)	Royal Decree on Tech Crimes (2023, amended 2025); Bank of Thailand Ann. No. 4/2025 on payments and money laundering; Royal Decree on Digital Platform Services (2022)	MDES-led Anti-Online Scam Operation Centre coordinating with CCIB, BOT, banks and telcos	The Online Safety Campaign Roadshow, aimed at raising awareness on internet safety including scams in over 10,000 public schools and universities.	"DE Fence" scam detection sandbox; SIM rules tightened
Vietnam	-	Personal Data Protection Decree No.13; Anti-Money Laundering Law; Law on Credit Institutions (2025); Decree No. 147 on management, provision and use of internet services and online information including user identification requirement (2024)	Ongoing development of cross-sectoral collaboration	-	Biometric ID required for large mobile transactions

NATIONAL RESPONSES IN SOUTHEAST ASIA

I. CREATING A UNIFIED APPROACH ACROSS GOVERNMENT

Several countries in Southeast Asia are implementing models that address the need for a unified approach across government.

In 2022, Malaysia established the National Scam Response Centre (NSRC) multi-agency body. It integrates law enforcement (Royal Malaysia Police), the central bank (Bank Negara Malaysia), the communications regulator (Malaysian Communications and Multimedia Commission), and consumer protection bodies to provide a coordinated and round-the-clock response to online financial fraud. The NSRC's structure aims to facilitate faster detection of stolen funds and enforcement actions by bringing together diverse resources and expertise.[44]

Singapore employs a comprehensive, multi-agency framework. The Inter-Ministry Committee on Scams (IMCS) draws expertise from various government agencies, including the Ministry of Home Affairs and the Monetary Authority of Singapore. Operationally, the Anti-Scam Command (ASCom) consolidates scam investigation, incident response, intervention, enforcement, and sense-making capabilities. This includes co-location of bank staff within ASCom premises for real-time coordination in tracing funds and freezing accounts suspected of involvement in scams.[45][46]

Thailand has advanced its centralized approach with the launch of the Anti-Online Scam Operation Centre (AOC) in November 2023. The AOC functions as a one-stop centre, centralizing response, investigation, and victim assistance. It is vested with the authority to freeze accounts and manage interagency data sharing. A Royal Decree requires active coordination from both the telecommunications and finance sectors with the AOC, with participation also from the National Cyber Security Agency and other ministries.[47][48]

Cambodia has also taken a step towards a centralized model with the establishment of the Commission for Combatting Online Scams in mid-2024. This high-level, government-sanctioned task force is chaired by the Prime Minister and tasked with leading and coordinating national efforts against online scams, involving multiple government ministries, law enforcement agencies, and telecommunications regulators.[49]

Brunei Darussalam, Laos, Myanmar, and Vietnam have not yet established dedicated or unified cross-sector anti-scam authorities. Anti-scam initiatives in these countries are led by individual ministries or agencies, which can limit systematic coordination. In Laos, for example, efforts such as mandatory SIM card registration are directed by the Ministry of Technology and Communications, but a standing, dedicated inter-agency body for real-time response is not in place.[50] In Vietnam, while various ministries and the state bank are active in fighting cyber fraud, efforts are managed through separate directives rather than a single, unified command centre.[51]

II. LEGISLATIVE RESPONSES

Several Southeast Asian countries have taken an early approach to targeted laws to combat scams, though there is significant variation in the approaches.

Singapore's Online Criminal Harms Act (OCHA) gives the government the power to issue directions to online service providers to restrict exposure to criminal activities, including scams.[52] This is complemented by the Shared Responsibility Framework (SRF), which regulates financial services and telecommunications. Under the SRF, the Monetary Authority of Singapore introduced 'waterfall liability'[53] for banks and telcos, as well as an SMS Sender ID Registry (SSIR)[54] which has blocked millions of scam messages by placing obligations on financial institutions and telecom providers.[55] It mandates real-time alerts and introduces a self-service kill switch, allowing users to instantly block access to their account during a suspected breach.

While the Monetary Authority of Singapore (MAS) and Infocomm Media Development Authority (IMDA) drove the policy, the detailed duties – such as the specific obligations of banks to scrutinize high-risk transactions or the responsibility of telecommunication providers to block fraudulent SMS with sender IDs—were developed in consultation with the respective industries.

Furthermore, Singapore's Protection from Scams Bill, passed in 2025, empowers authorities to issue Restriction Orders against financial institutions for individuals suspected of being targeted, a last resort measure to protect victims' funds.[56]

Similarly, Malaysia has strengthened its legal framework by amending the Communications and Multimedia Act 1998 to prohibit unsolicited electronic commercial messages.[57] Financial institutions are required to enhance transaction monitoring and security under directives from the central bank, Bank Negara Malaysia (BNM), pursuant to the Financial Services Act 2013. Operationally, the National Scam Response Centre (NSRC) provides a 24/7 rapid response, while the National Fraud Portal streamlines reporting for victims.[58] The Malaysian Communications & Multimedia Commission (MCMC) also mandates providers to filter and block "Prohibited Content" in all SMS messages.

Thailand has actively responded to rising online fraud with a series of legislative measures. The Royal Decree on Measures for Protection and Suppression of Technology Crimes (2023) requires financial institutions to freeze suspicious transactions and mandates information sharing.

Amendments hold financial institutions and mobile operators accountable for customer losses, requiring their active collaboration.[59] The Office of the National Broadcasting and Telecommunications Commission (NBTC) has tightened SIM card regulations, and the Bank of Thailand (BOT) prohibits banks from sending links in SMS/email and mandates real-time fraud detection systems. This collaborative approach is centralized through the Anti-Online Scam Operation Centre (AOC), which has been instrumental in suspending hundreds of thousands of mule bank accounts.[60]

Other countries are also making significant progress. Vietnam is enhancing its legal and regulatory measures through several key laws, including Decree No. 13 on Personal Data Protection to strengthen data security and the Anti-Money Laundering Law (2023) to enhance financial monitoring.[61] The State Bank of Vietnam (SBV) has also mandated biometric authentication for certain high-value online transactions, effective from July 2025.[62]

In Indonesia, while the Penal Code addresses fraud, Regulation No. 12 of 2024 by the Financial Services Authority (OJK) has significantly strengthened anti-fraud measures, expanded the legal definition of fraud and mandated that all financial institutions implement comprehensive anti-fraud strategies.[63]

The Philippines made legislative strides with the passage of the Anti-Financial Scamming Act (AFASA), which criminalizes money mule operations and increases financial institutions' obligations to implement enhanced fraud management systems, building upon the SIM Card Registration Act. The Cybercrime Investigation and Coordinating Centre (CICC) serves as the primary agency for combating cybercrime.[64]

Specific to tackling human trafficking in addition to scams, in 2024 the Philippines cracked down on illegal Philippine Offshore Gambling Operators 'POGOS', which have been linked to scams and human trafficking.

Despite this progress, some countries face some constraints. Brunei Darussalam relies on general provisions in its Penal Code and Computer Misuse Act rather than comprehensive legislation specifically targeting scams.[65] While measures like mandatory SIM card registration have been implemented, the absence of a dedicated legal framework can hinder a coordinated response.[66] Cambodia, despite recent initiatives, still grapples with weak law enforcement and a slow pace in enacting a dedicated cybercrime law, allowing it to remain a major hub for scam operations.[67] Similarly, Laos faces substantial difficulties with the Golden Triangle Special Economic Zone (SEZ).[68] Its Cybercrime Law does not explicitly list online fraud as a specific criminal offense, creating legal loopholes exploited by criminal enterprises.[69]

III. REGULATORY MEASURES AND TECHNICAL PROTOCOLS

Across Southeast Asia, governments are moving beyond isolated interventions to adopt multi-layered technical protocols that strengthen resilience against scams. Key areas of focus include enhancing identity verification during digital transactions and closing the net on the abuse of SIM cards.

In Vietnam, biometric authentication is now required for high-value mobile transactions,[70] while Indonesia has mandated electronic Know-Your-Customer (e-KYC) protocols that also incorporate biometric data.[71] In the Philippines, the newly enacted Anti-Financial Scamming Act (AFASA) reinforces mandatory multi-factor authentication requirements for financial institutions.[72]

In the telecommunications sector, several countries are working to sanitize messaging channels and prevent spoofing. Singapore's SMS Sender ID Registry (SSIR) serves as a regional model, enabling telecom providers to verify and block spoofed messages.[73] Malaysia complements this with mandates for telecoms to implement SMS content filtering,[74] while Thailand has tightened SIM card registration rules to limit the proliferation of mule SIMs used in scams.[75]

Real-time detection and intelligence sharing are also emerging as central elements of the regional response. Financial institutions in Singapore have broadly adopted real-time fraud detection systems.[76] Thailand's "DE Fence" initiative—a government-run sandbox—provides a space to test and develop scam detection technologies.[77] Malaysia and Singapore have also formalized cross-border intelligence sharing, setting an example for regional cooperation against transnational scam networks.[78]

Among the remaining ASEAN member states, implementation of advanced technical protocols remains at an early stage. Brunei has focused on foundational measures such as mandatory SIM card re-registration and public scam alerts through its central bank. Cambodia and Laos have taken similar steps on SIM registration, but face capacity constraints in developing broader technical frameworks. In Myanmar, the ongoing conflict and governance crisis have significantly hindered the deployment of cohesive national strategies, creating space for transnational scam operations to expand with little resistance.[79]

IV. COREGULATION AND VOLUNTARY MEASURES

Singapore Technical Reference 76 is the national standard for e-commerce transactions including anti-scam guidelines. The model for TR76 is unique as a multistakeholder convening of industry, industry associations, and government, representing the value chain of e-commerce, to help design new e-commerce and consumer protection industry standards. The model relies on consensus building, with industry providing expertise, and partnership with the government to agree on content and language of the standard. The process is iterative, with opportunities for future amendments and review to keep the standard relevant.

In Indonesia, the Financial Services Authority (OJK) is institutionalizing public-private partnerships to combat fraud. Through its regulatory authority, OJK mandates that all banks and payment system providers implement comprehensive anti-fraud strategies, including stricter electronic Know Your Customer (e-KYC) protocols with biometric verification. These efforts are being expanded to include fintech and other digital financial services, requiring broader private sector participation.[80]

The Philippines shows progress in public-private collaboration, with the Cybercrime Investigation and Coordinating Centre (CICC) partnering with law enforcement, financial regulators, and the telecommunications sector. The Anti-Financial Scamming Act (AFASA) also imposes new obligations on financial institutions, requiring them to implement multi-factor authentication and enhance fraud management systems.[81]

While Vietnam's State Bank of Vietnam (SBV) mandates measures for financial institutions, broader, institutionalized cross-sectoral efforts are still developing.[82] In other countries, systemic public-private partnerships are less mature. In Cambodia, weak law enforcement and corruption have historically hindered effective collaboration, though recent government initiatives aim to address this.[83] Laos faces unique challenges where limited state capacity and the semi-autonomous nature of Special Economic Zones, like the Golden Triangle SEZ, complicate coordinated public-private action against powerful criminal syndicates.[84] In Brunei Darussalam, while government agencies and private companies cooperate on general cybersecurity, a formal, integrated public-private framework specifically for combating scams across all sectors is not yet established.[85]

V. PUBLIC ENGAGEMENT

Malaysia has actively pursued public awareness through its #JanganKenaScam campaign. Led by banks under the Association of Banks in Malaysia (ABM) and the Association of Islamic Banking and Financial Institutions Malaysia (AIBIM), this campaign includes nationwide events, experiential booths, and an online resource center (JanganKenaScam.com). The campaign emphasizes that public awareness is a strong defense and uses public figures as brand ambassadors to amplify its message across various demographics.[86]

Singapore employs a multi-pronged approach to public education. The National Crime Prevention Council (NCPC) manages the ScamAlert.sg website, which provides information on scam types and victim experiences.[87] The ScamShield app, a government initiative, not only blocks scam calls and filters suspicious SMS messages, but also enables users to verify potential scams by submitting links, phone numbers, messages, or screenshots for assessment.[88] The national Digital for Life Movement aims to equip citizens of all ages with digital skills to navigate the online world safely.[89] Meta, in collaboration with the Singapore Police Force and NCPC, has also run "Staying safe online" campaigns and launched a "Youth Online Safety Program" in schools to educate teens on online harms, including scams.[90] Several other private companies are also launching services with similar functionality, including Scamnetic, Feedzai ScamAlert, Rangers AI, Ask Silver.

Thailand's Anti-Online Scam Operation Centre (AOC) also functions as a resource for public advice. Its 24/7 hotline (1441) provides guidance, and the Ministry of Digital Economy and Society (MDES) uses official channels to actively disseminate information on new scam methods and warn the public against impersonators.[91]

In Vietnam, the Ministry of Public Security's Department of Cybersecurity and Hi-tech Crime Prevention and Control has partnered with Google to launch a "social-first" educational initiative. This campaign leverages over 200 YouTube creators to integrate anti-scam messages into engaging content, aiming to arm Vietnamese citizens with knowledge to identify and avoid sophisticated online fraud.[92]

Indonesia's Financial Services Authority (OJK), through its Regulation No. 12 of 2024, mandates that financial service institutions include anti-fraud awareness programs for consumers as part of their comprehensive anti-fraud strategies. This regulation underscores the importance of institutional efforts in educating their customer base directly.[93]

Despite these efforts, challenges remain. In Laos, while the Ministry of Education has warned residents about specific threats like fake scholarship scams, broader, systematic digital literacy campaigns against various scam types are less evident.[94] Similarly, in Brunei Darussalam, the Brunei Darussalam Central Bank (BDCB) issues alerts on suspicious entities and advises the public on recognizing scam signs, but a comprehensive national digital literacy strategy focused solely on scams is not prominently detailed.[95] In Myanmar, the ongoing conflict and resulting breakdown of state services severely limit the capacity for widespread public awareness campaigns, leaving many citizens vulnerable to sophisticated scam operations.[96]

TOWARDS A REGIONAL RESPONSE — ASEAN AND MULTI-COUNTRY EFFORTS

In recent years, regional coordination in response to the rise of scams and fraud in Southeast Asia has also ramped up. National law enforcement agencies in some ASEAN member states, for instance, have cooperated in joint action targeting scam centres and rescuing human trafficking victims. Yet, the level of policy development and enforcement capacity varies significantly across the region.

ASEAN-WIDE RESPONSE

At present, Southeast Asia lacks a strategic framework specifically dedicated to combating scams. The ASEAN Cybersecurity Cooperation Strategy (2021–2025) outlines broad priorities for enhancing cybersecurity and addressing digital threats – though it does not explicitly address scams.[97]

Nonetheless, several regional initiatives and action plans are underway. The ASEAN National Police (ASEANAPOL) 2025 Action Plan largely focuses on identifying crime trends accurately, identifying law enforcement gaps, and addressing training needs among member countries. As part of its regional action plan for 2025, ASEANAPOL will prioritize the dismantling of scam call centres linked to human trafficking and forced criminal activities.[98] ASEANAPOL is also coordinating capacity-building initiatives and establishing an anti-scam centre, in addition to supporting police operations against cyber scams in all ASEAN member states.

At the October 2024 ASEAN Ministerial Conference on Cybersecurity, ASEAN also established the ASEAN Regional Computer Emergency Response Team (ASEAN Regional CERT).[99] The ASEAN Regional CERT is backed by a US$10 million commitment by Singapore over the next decade and aims to leverage partnerships with the private sector and academia, conduct cyber exercises, and exchange intelligence related to cyber threats.

The ASEAN Working Group on Anti-Online Scam was established in 2024, with a proposal put forward by Thailand, and the establishment welcomed at the 4th ASEAN Digital Ministers' Meeting (ADGMIN) in Singapore. The working group serves as the principal collaborative platform for ASEAN member states to coordinate a regional response to scams on digital and telecommunications channels.

Cybersecurity and scams featured significantly at the 5th ASEAN Digital Ministers' Meeting (ADGMIN), with call scams formally placed on the regional agenda with ministers expressing an urgent need for collective action.[100] There were also discussions on efforts to build strong digital identification systems, strengthening cross-border data governance and digital interactions, as well as the critical role of international partnerships in strengthening regional cybersecurity frameworks.[101]

BILATERAL COORDINATION

Efforts to coordinate across borders have emerged but remain largely *ad hoc* and reactive. Joint crackdowns, such as those between Thailand and Myanmar, Thailand and Cambodia, or Malaysia and Singapore, have helped disrupt scam compounds and cross-border fraud. Still, these actions are isolated responses rather than part of a systematic, long-term strategy for regional enforcement.

However, the development of government-led scam coordination centres has presented an opportunity for international cooperation. For example, between April and May 2025, the Singapore Police Force Anti-Scam Command (ASCom) – discussed in greater detail in Part III – collaborated with Hong Kong, South Korea, Malaysia, Maldives, Thailand, and Macao law enforcement agencies to conduct a major anti-scam operation. With a combined force of 2,784 officers, the operation resulted in the arrests of more than 1,800 subjects and investigations of 33,900 subjects for their suspected involvement in scam and fraud activities—including government official impersonation scams, investment scams, love scams, and e-commerce scams, among others.[102]

The existing ASEAN initiatives, whether ASEANAPOL, the ASEAN Regional CERT, or the ASEAN Working Group on Anti-Online Scam, currently government-focused, with minor participation from industry, NGOs, and academics or independent experts. There is opportunity to establish more regular and formalized mechanisms to engage and consult with private sector stakeholders to maximize or identify best practices, resources and opportunities.

PART IV

PRIVATE SECTOR AND NON-GOVERNMENTAL INITIATIVES

PROACTIVE PRIVATE SECTOR RESPONSES

Beyond formal public-private partnerships, a diverse ecosystem of private sector and non-governmental initiatives provides another critical layer of defence against scams. These efforts, driven by corporate responsibility, business necessity, and humanitarian concern, often operate with an agility that can complement and sometimes outpace government responses.

Global technology platforms are at the forefront of this fight, leveraging their scale and technical capabilities.

Google employs a multi-layered approach combining AI-powered detection that blocks billions of malicious ads and phishing attempts across its services like Search and Gmail, with proactive user education through its "Safer with Google" initiatives.[103] In June 2025, the company launched its Safety Charter for India, introducing new AI-powered security measures designed to protect users from increasingly sophisticated online fraud.[104] Visa has also stepped up its role through a dedicated “scam disruption” team, which uses generative AI and dark-web monitoring to block more than USD 350 million in fraud attempts and prevent an estimated USD 27 million in losses.[105]

Similarly, Meta has deployed advanced AI tools to detect and remove fraudulent accounts and pages across Facebook, Instagram, and WhatsApp, while also partnering with local fact-checking organizations in markets such as the Philippines and Indonesia to debunk viral scams and provides users with tools to report suspicious content.[106] These global measures are being adapted to the regional context. Across Asia Pacific, Meta worked with over 30 partners on the Staying Safe Online scam education campaign from 2021 to2023, spanning 18 countries including Singapore, Malaysia, Thailand, Cambodia, the Philippines, and Indonesia. The campaign delivered resources in local languages, reached more than 717 million people and generated over 2.8 billion impressions. Since 2024, the company has continued to expand its educational efforts, focusing on emerging scam styles such as ecommerce, romance, and investment scams.

In addition to individual company initiatives, the private sector has begun to act collectively. Meta, Match Group, and Coinbase have joined forces to establish Tech Against Scams, a global industry coalition that continues to expand with new partners. The coalition functions as a convening body where members share best practices, coordinate threat intelligence, and develop joint strategies to address the evolving tactics used by scammers. This first-of-its-kind collaboration underscores the role of cross-industry cooperation in strengthening consumer protection.[107]

Alongside these measures, new collaborative intelligence-sharing platforms have emerged. The Global Signals Exchange (GSE), led by the Global Anti-Scam Alliance (GASA) and the DNS Research Foundation (DNSRF), enables participants such as Microsoft, Meta, and Google to exchange scam-related alerts in real time. In the first quarter of 2025, Google expanded its contributions, connecting additional product areas and boosting signal sharing to 10 million received and 4 million shared, a tenfold increase over the initial pilot in October 2024.[108] This kind of global clearing house is vital given the cross-border nature of online scams. Meta has also piloted the Fraud Intelligence Reciprocal Exchange (FIRE), which allows financial institutions to flag scams directly to Meta for investigation. Confirmed cases trigger both enforcement actions on Meta's platforms and improvements to detection systems, while lessons learned are shared back with partner banks. This initiative is incremental as bad actors tend to operate globally, so global and independent cross signal clearing houses will help to tackle scams effectively.

The financial and telecommunications sectors have also moved beyond compliance to launch proactive, independent measures. Across the region, major banks are investing in proprietary real-time fraud analytics, using machine learning to detect anomalous transactions and alert customers instantly. They are also rolling out more secure authentication methods and leading awareness campaigns to safeguard clients and strengthen trust.[109] Telecommunication providers, meanwhile, have deployed sophisticated SMS firewalls and systems to block traffic from known fraudulent international numbers, creating a crucial first line of defence against many common scam delivery methods.

Other actors are contributing through public-private partnerships. In early 2025, Mastercard pledged support to ASEANAPOL's capacity-building programs on cybercrime and financial fraud, offering expertise, tools, and anti-scam methodologies.[110] Mobile anti-fraud app Whoscall, developed by Gogolook, has also established partnerships with ASEAN government and law enforcement agencies, including the Thai Royal Police and Royal Malaysian Police, to block scam calls and share real-time intelligence.[111]

EMERGING TECHNOLOGICAL CHALLENGES AND SYSTEMIC RESPONSES

Beyond individual company efforts and sectoral initiatives, private actors are increasingly responding to the technological frontier of scams. The growing sophistication of artificial intelligence has made fraudulent interactions harder for victims to detect. AI-driven chat systems can convincingly mimic human conversation, while deepfake technology enables video calls that trick targets into believing they are speaking to colleagues, superiors, or trusted contacts. AI-generated documents—such as fabricated bills or identity cards—are also being used to bypass anti-fraud checks in banking and financial services. These developments complicate detection and require new forms of verification.

In response, cross-border and cross-industry partnerships have begun to emerge. One Consortium, for example, brings together international telecommunications companies, industry organizations, and regulators to address unwanted and fraudulent voice calls and messages on a global scale. By working with National Regulatory Authorities (NRAs) and linking to the broader *Restore Trust* initiative, it develops harmonized best practices, technologies, and enforcement mechanisms that no single entity could achieve alone. ASEAN regulators stand to benefit from stronger participation in such efforts. Engagement with initiatives like One Consortium and the *Global Informal Regulatory Antifraud Forum (GIRAF)* would allow the region to contribute to, and learn from, collective approaches to scam prevention.

Financial-sector initiatives are also moving to the network level. In April 2024, Mastercard launched a multi-layered anti-scam program in collaboration with the Global Anti Scam Alliance (GASA) and the UNDP Digital Scams Coalition to strengthen global resilience. In the United Kingdom, 15 banks representing 90 percent of account-to-account payments now use an AI-powered real-time transaction scoring service. Since its rollout in 2023, the system has helped reduce authorized push payment (APP) fraud cases by 20 percent in 2024. These examples show the potential for scalable, systemic defences that operate across institutions and borders.

Finally, new tools are emerging to distinguish between human and non-human activity online. In May 2025, Match Group and Tools for Humanity announced an integration between Tinder and *World ID* as a proof-of-human safeguard against AI scams. By verifying that an account is operated by a unique human rather than an automated bot or scam farm, such tools enable service providers to take further steps—such as KYC processes or compliance screening—confident that they are dealing with a real individual. Similarly, advances in technologies like World ID help service providers confirm both that a user is human and that they are unique, limiting the ability of scammers to generate multiple fake accounts or recycle blocked identities. These innovations could prove especially valuable in curbing fake accounts and malvertising, where the scale of abuse often hinges on automation.

Together, these responses illustrate how the private sector and civil society are adapting to the evolving technological landscape of scams. By combining AI-driven detection, proof-of-human systems, and global coalitions, they highlight a path toward more resilient defences that ASEAN regulators and industry actors can build upon.

CIVIL SOCIETY AND NON-GOVERNMENTAL ORGANIZATIONS

Civil society and non-governmental organizations (NGOs) play a vital role in filling gaps that governments and corporations may overlook. Consumer advocacy groups, such as the Consumers' Association of Singapore (CASE), provide direct assistance and advice to scam victims, mediate disputes, and campaign publicly for stronger consumer protection laws.[112] Singapore has also positioned itself as a regional hub of collaboration, hosting the APAC Summit of the Global Anti-Scam Alliance (GASA), which brings together governments, law enforcement, consumer protection organizations, financial authorities and providers, brand protection agencies, social media and internet service providers, and cybersecurity companies to share knowledge and define joint action against scams.

In the Mekong region, human rights organizations have focused on exposing the darker side of the scam industry. Groups such as Human Rights Watch and the Global Initiative Against Transnational Organised Crime (GI-TOC) have published detailed reports on forced labour in scam compounds in Cambodia and Myanmar, advocating for victim protection and urging governments to dismantle these criminal networks.[113]

Taken together, these independent efforts of technology companies, financial institutions, and civil society actors form a more resilient and multi-faceted defence, underscoring that addressing the evolving threat of scams requires a whole-of-society approach.

PART V
BUILDING RESISTANCE TO SCAMS THROUGH ASEAN

Parts II, III and IV reviewed the actions being taken by governments in Southeast Asia, authorities around the world, and efforts being taken by the private sector to combat scams. In Part V, we synthesize what Southeast Asian countries and ASEAN as a regional coordinator can do to better coordinate the response to scams in the region, attacking the scams at their source, reducing the vulnerability of economies and societies to scams, and coordinating a regional response.

The following comprises two sets of priorities identified through our research, regarding disrupting the scam centres in the region and reducing the vulnerability of regional economies to scams. The paper then concludes with a set of tangible recommendations for actions that can be coordinated through ASEAN, for consideration by the ASEAN Anti-Scams Working Group.

PRIORITIES FOR ADDRESSING SCAM CENTRES AND HUMAN TRAFFICKING

I: DISRUPT AND DISMANTLE THE SCAM COMPOUNDS

Governments in the region must address the dismantling of scam compounds around Southeast Asia. This effort will require using technological and intelligence tools to map and identify the organizational networks and criminal actors behind the compounds' operations. It will also require collaboration and joint security operations between countries, such as the joint crackdowns conducted by Cambodia and Thailand, to conduct raids and dismantle the hard infrastructure and digital infrastructure of these scam operations.

Several pathways exist. Individual countries must strengthen oversight of special economic zones (SEZs), border regions, and contested areas where scam compounds are typically located. Law enforcement organizations, in coordination with regional and national agencies and utilities providers, can also improve due diligence and oversight of development projects and migrant flows in these regions, with an eye towards identifying cover for illicit activities.

Governments can collaborate with the private sector and civil society organizations in this effort. More broadly, private sector actors can also be helpful in disrupting organized crime; for instance, tech companies have continued to investigate criminal organizations involved in scam compounds, looking for new scam compounds and taking down the associated online accounts, and rolling out new product features that can protect users against known scam tactics.[114]

II: ADDRESS HUMAN TRAFFICKING AND FORCED CRIMINALITY

Human trafficking is at the core of Southeast Asia's scam compounds. While direct victims of scam operations are the main focus of anti-scam policies, it is equally important to address the other victim category: the trafficked labour forced into criminality.

Efforts to combat human trafficking linked to scam compounds begin with strengthening victim identification and rescue operations. Law enforcement officials and authorities must improve victim-screening procedures at key transit points—airlines, ports, borders—and have a planned response to safely extract and repatriate victims. As raised during the workshop, solutions must be found to make use of the large amount of potential evidence and intelligence on devices recovered from scam centres and from the many thousands of human trafficking victims working in the scam centres.

Licensing and oversight of employment agencies must also be strengthened and improved, including a more strategic oversight of online job advertisements that lure vulnerable jobseekers into forced labour. The use of emerging technology such as AI, as well as the assistance of internet platforms, can greatly complement efforts by governments and law enforcement agencies.

A more robust approach towards cross-border cooperation, one that ties scam-related human trafficking to countries and the region's greater obligations and commitment to human rights, is needed. Partnerships such as the ASEAN-Australia Counter-Trafficking initiatives (ASEAN-ACT) and UNDOC's Emergency Response Network enhance coordination among law enforcement agencies across the region through training, intelligence sharing, synchronized operations, and joint investigations across different jurisdictions.[115]

III: DISRUPT ILLICIT FINANCIAL FLOWS

It is only possible to steal billions of dollars if criminals have access to sophisticated financial and money laundering operations. These exploit weak financial and regulatory oversight, unregulated technologies such as cryptocurrencies, corruption, and shell companies.

To begin, the region needs harmonized and robust cross-border collaboration on anti- money laundering (AML). Aligning with global standards such as those of the Financial Action Task Force (FATF), countries should commit to mutual legal assistance, intelligence gathering and sharing, and coordinated investigations and sanctions against illicit financial service activities. For instance, the Monetary Authority of Singapore (MAS), Bank of Thailand (BoT), and Bank Negara Malaysia (BNM) have introduced new measures for banks to comply with. These include requiring the ban on clickable links, limits to the number of mobile devices per user, enhanced authentication and verification controls, and installation of real-time scam detection and monitoring solutions, among others.[116]

Meanwhile, private sector collaboration is critical. Banking consortia such as MAS' Collaborative Sharing of Money Laundering/Terrorism Financing Information & Cases (COSMIC) in Singapore and the Financial Intelligence Evaluation Sharing Tool (FINEST) launched by the Hong Kong Association of Banks utilize analytics-driven detection of money laundering networks to disrupt fund flows before they exit the financial system. More broadly, they also shed light on how financial institutions can contribute to the fight against Southeast Asia's scam and fraud operations.

PRIORITIES FOR BUILDING RESILIENCE AND REDUCING VULNERABILITY TO SCAMS

I: FACILITATE CROSS-GOVERNMENT COORDINATION FOR A WHOLE-OF-GOVERNMENT RESPONSE

A centralized body – a commission, command or coordination centre is a proven means to align the efforts of the various government entities that must be involved for a coherent response to scams. This ideally engages government actors from justice, digital, communications, finance, as well as regulators, and law enforcement. This body can streamline activities, enhance real-time information sharing and develop an essential single source of feedback and analysis for future policy response.

II: FOSTER STRONGER FORMALIZED PUBLIC-PRIVATE PARTNERSHIPS FOR INTELLIGENCE SHARING AND RAPID RESPONSE

Further to the above priority, it is also clear that the involvement of all non-government stakeholders with relevance to combating scams is also essential to a coherent response. Scammers exploit multiple layers of infrastructure—from finance and telecommunications to social media and e-commerce. Tackling this complexity requires close collaboration between public agencies and private-sector actors, leveraging the expertise of different entities, and enabling real-time information sharing.

This paper has described the various approaches to public-private partnerships – joint taskforces, charters, data-sharing arrangements, or cross-industry collaborations that help prevent fraud and help improve public confidence in the digital economy. In general, these groupings have clear mandates, involve the relevant stakeholders to achieve their objectives, and introduce accountability for the stakeholders involved.

III: ENABLE A WHOLE-OF-SOCIETY RESPONSES THROUGH PUBLIC ENGAGEMENT

Even with advanced technology and legal tools, an informed public remains one of the strongest defences against scams. In Southeast Asia, rapid internet adoption—particularly among underbanked or digitally inexperienced populations—has outpaced efforts to build digital literacy.

Public education campaigns can significantly reduce victimization by equipping users with knowledge to spot and avoid scams. These initiatives should be localized, multilingual, and ongoing, delivered through schools, universities, community centres, digital media, and public services.

As seen in several examples in this paper, public education can be expanded to public engagement, encouraging the public to report scams, creating a useful stream of data and intelligence to inform law enforcement's response and policy development.

Awareness and literacy must also extend to better cybersecurity for all organizations and institutions that handle data, which will contribute to reducing sensitive data being leaked which can feed scams at a later date.

IV: DEVELOP THE POLICY LANDSCAPE TO SUPPORT A STRONG SCAMS RESPONSE

Foundational laws such as cybercrime laws are essential for providing the legal basis for action. Beyond these, governments in the region can consider targeted regulatory actions that allow further bold action, such as powers to freeze digital assets.

On the technical side, governments in the region should consider adopting international standard protocols for technologies such as SMS, e-commerce, and online payments and financial services. Standardizing security measures across these systems can reduce vulnerabilities—for instance, making it harder to spoof phone numbers or exploit SIM cards. Governments can also promote or mandate the use of technologies like fraud analytics, secure authentication, and AI-powered scam detection to stay ahead of evolving threats.

Regulators should also seek to reduce obstacles created by existing rules. One clear example of this is in the development of appropriate exemptions in data protection and privacy laws that allow reasonable processes and procedures to uphold data protection standards, while allowing the sharing of relevant data for analysis to fight fraud. A 'fighting fraud' special use exemption would also allow for data to move across borders to help power AI-enabled cybersecurity technologies that sustain and protect global commerce. Similarly, limiting data localisation to allow for the mapping of suspicious activity is essential to the maintenance of global threat intelligence and trends analysis.
Alternatively, there are other innovative ways to allow stakeholders, especially financial institutions to securely share data. This may be done via a consortium model, sharing data securely to help financial services providers to accurately analyse money flows and use predictive intelligence to identify fraud and prevent crime before it can take place.

Finally, shared responsibility frameworks help allocate responsibility for scam losses among financial institutions, intermediaries, and users based on their respective roles and risk controls in the payment supply chains. They can help spread the burden of scams. For example, the UK's reimbursement rules mandate automatic compensation for scam victims, typically split between the sending and receiving institutions.

RECOMMENDATIONS FOR ASEAN TO COORDINATE A REGIONAL APPROACH

I: EMPOWER THE ASEAN WORKING GROUP ON ANTI-ONLINE SCAMS (WG-AS)

The ASEAN Working Group on Anti-Online Scams (WG-AS) is a promising collaborative platform to coordinate regional efforts to combat online scams.[117] To fulfil its potential, the capacity of the working group should be expanded to enable deeper policy work and greater authority to coordinate and navigate across ASEAN's various frameworks, meetings, and collaborative channels. The magnitude of the challenge presented by scams warrants greater funding for regional collaboration by ASEAN, members states and donors.

This would enable the working group to address key policy development opportunities such as the development of ASEAN guidelines that can be endorsed by different ASEAN Ministerial Meetings (e.g. ADGMIN). This could include:

- Guidelines for national data regulators on 'fighting fraud' legitimate use exemptions
- Guidelines on improving KYC against scams for the banking, technology and telecommunications sectors
- Guidelines on collaboration between law enforcement and banks, technology and telecommunications sectors
- Guidelines on coregulation and policy coordination with banks, technology and telecommunications sectors
- Guidelines on best practice and protocols for cross-border cooperation

II: PUT SCAMS ON THE AGENDA OF RELEVANT MINISTERIAL MEETINGS

The impact of the Working Group is reliant on its ability to influence existing ministerial groupings. Raising the political profile of scams as a national and regional challenge was a key issue identified during the workshop.

In order to raise the profile of the challenge presented by scams, getting the issue onto the agendas of ASEAN ministerial meetings should be an end in itself. The issue should be integrated into high-level ASEAN ministerial agendas, beyond the ASEAN Digital Ministers Meeting (ADGMIN). Given that it intersects issues such as cybersecurity, money-laundering, human trafficking, and transboundary crime, scams and fraud should be regularly integrated into the ASEAN Ministerial Meeting on Transnational Crime (AMMTC), the meeting of Attorney Generals, the meeting of Finance Ministers', and thematic meetings such as the ASEAN Ministerial Conference on Cybersecurity. As a global challenge, scams could also feature on the agenda or workplans between ASEAN and its Dialogue Partners.

The problem of scams intersects the three pillars of the ASEAN Economic Community (Political-Security, Economic and Socio-Cultural) - with issues ranging from the digital economy to human rights. Elevating scams into ASEAN's ministerial agendas will promote the issues as a priority shared concern among ASEAN nations, one that does not occur in isolation nor affect only one member state. On the ground, this approach would enable a more coordinated and synergistic effort against scams in the region, enabling scams to be tackled through multiple avenues. Integrating scams and fraud into ASEAN's high-level ministerial agendas will also encourage relevant policymakers to address the issue by tapping into ASEAN's existing frameworks and initiatives, and to leverage member states' collective resources and capacity.

III: ENGAGE IN TRACK 1.5 DIALOGUE WITH INDUSTRY

Current ASEAN initiatives, such as the ASEAN Working Group, ASEANAPOL initiatives, and the ASEAN Regional CERT are government-focused, with limited participation from industry, NGOs, and expert academia. Many stakeholders would support the opportunity to establish more regular and formalized mechanisms to engage and consult with private sector and other stakeholders to maximize or identify best practices, resources and opportunities.

ASEAN should initiate Track 1.5 dialogue—discussions involving both government officials and non-government stakeholders to deepen public-private collaboration in combating scams and fraud. These dialogues would provide a structured yet open space for exchanging intelligence and insights, discussing scam technologies and tactics, and coordinating cross-border responses. Given the transnational and interconnected nature of scam networks, involving stakeholders such as telecoms operators, social media platforms, and financial institutions is essential. ASEAN member states could convene Track 1.5 dialogue under existing ministerial meetings such as the ASEAN Digital Ministers' Meeting (ADGMIN—which can enable continuity and policy impact. Ideally, the ASEAN Scams Working Group, would be the main convener and facilitator.

A Track 1.5 dialogue also provides an opportunity for best practice sharing among economic operators across technology, finance, and telecommunications, as well as more regular dialogue between economic operators and civil society. It is essential that the dialogue includes a range of economic operators, especially the most prevalent technology platforms used in the region, some of which do not engage regularly in international dialogues.

The Mekong-U.S. Partnership Track 1.5 Dialogue provides a useful model. Launched by the U.S. government in 2020, the dialogue series aims to explore solutions to key policy and sustainability challenges in the Mekong sub-region.[118] The ninth edition, held in Bangkok, Thailand in October 2024, focused on online scam operations, including preventing scams and trafficking, the role of media and civil society, how to assist trafficking victims, multilateral collaboration, and regulatory efforts.[119] More than 90 participants attended the dialogue, including experts, civil society representatives, government institutions, the private sector, and international organizations from the ASEAN region as well as development partner countries including the United Kingdom and Australia, among others.[120]

IV: STRENGTHEN ENGAGEMENT WITH INTERNATIONAL GOVERNMENTS AND ORGANIZATIONS

ASEAN can support Southeast Asian countries to strengthen engagement with international governments and organizations in fighting scams and fraud. One pathway is by expanding bilateral and multilateral cooperation on cross-border investigations and legal assistance. Scam compounds and operations, particularly those owned and run by criminal syndicates originating or based in third countries, rely on jurisdictional fragmentation to evade investigation and enforcement. Given that citizens of countries such as the US, EU, and Australia have increasingly become victims of scam operations based in Southeast Asia, there is incentive for their governments to share technical expertise and investigative resources to complement enforcement efforts done by ASEAN member states.

Regionally, ASEAN could coordinate and form partnerships more actively with international organizations such as INTERPOL, UNODC, and the Financial Action Task Force (FATF). Joint efforts can be conducted on aligning standards on due diligence, digital and financial surveillance, asset recovery, and the relevant laws. Training and dialogue also provide avenues for ASEAN countries and their international counterparts to learn and share new methods and typologies of scams and fraud, as well as the emerging technologies and tools for more advanced detection and prevention. By strengthening and expanding its engagement with the international community, ASEAN can position itself not just as a reactive actor, but a proactive partner in shaping the global responses and solutions to the threat of scams and fraud.

ASEAN and its member governments may also seek to participate in global initiatives such as the One Consortium and the Global Informal Regulatory Antifraud Forum (GIRAF). These will support collaboration with counterparts worldwide, making it harder for bad actors to operate across jurisdictions. It will also support access to global good practice, tools, expertise and initiatives. Several of these global initiatives also provide global early warning systems, intelligence sharing and coordinated responses that help regulators stay ahead of emerging threats. Finally, they also give ASEAN regulators a seat at the table to comment on the development of coordinated initiatives, global standards development and strategies.

V: SUPPORT INTELLIGENCE AND DATA SHARING AMONG GOVERNMENTS AND LAW ENFORCEMENT

ASEAN – potentially in collaboration with INTERPOL – can coordinate efforts for threat intelligence sharing, enabling the exchange of up-to-date information on scam and fraud types that can inform national policy and strategy. This should include timely alerts on fraudulent URLs and phishing domains, mule account identifiers, and behavioural patterns, drawn from both law enforcement and private sector partners. As participants in the ASEAN scams workshop stressed, no single authority has the full picture of scam activity. Governments, platforms, telecoms, and financial institutions each hold partial insights, and only by combining them can the region build a comprehensive view.

Industry representatives also highlighted the types of signals that can be shared in real time. These include number verification (ensuring transactions match a registered device), SIM swap data, anomalies in call and SMS patterns, device identifiers such as IMEIs, and unusual call durations. Telecoms operators, as the first point of scam contact, are critical players in such exchanges. Singapore's GovTech has already piloted this approach, sharing thousands of scam site URLs daily with Google via the Global Signals Exchange (GSE), which has demonstrated measurable impact. Regional initiatives such as the Asia Pacific Cross-Sector Anti-Scam Taskforce (ACAST) also provide platforms that ASEAN could connect to for broader intelligence sharing.

Experts emphasized that political will and a common baseline are essential. Governments must treat scams as a systemic threat, while industry should proactively target scam enablers—such as fraudulent websites, lax SIM registrations, or weak KYC regimes—that allow scams to scale. At the same time, participants cautioned that intelligence sharing must be coupled with safeguards to prevent false positives and protect data privacy. High-confidence signals and clear governance frameworks will be vital to ensure that cross-border intelligence exchanges both strengthen trust and deliver tangible disruption to scam networks.

METHODOLOGY

This white paper is grounded in two main sources of evidence: desk research and expert consultations.

First, we conducted a comprehensive review of secondary sources, including reports from the UNODC, INTERPOL, ASEAN working groups, GSMA, the Global Anti-Scam Alliance (GASA), and national government agencies across Southeast Asia. These sources provided foundational data on scam prevalence, typologies, and emerging trends, as well as statistics on victimization, economic losses, and regulatory responses.

Second, the analysis draws on primary insights from expert interviews and roundtable discussions. Stakeholder interviews were conducted with:

- Government entities in ASEAN and partner countries leading policy responses on scams;
- Private sector operators across technology, cybersecurity, telecommunications, and payments
- Civil society organizations working on victim support, human trafficking, and awareness-raising;
- International organizations working on scams and scam centres

Particular use was made of findings from the ASEAN Scams Workshop (August 2025), which convened regional stakeholders in a Track 1.5 format to share insights, explore cross-border responses, and discuss good practice response to scams.

NOTES

[1] Cybersecurity Ventures. n.d. “The World’s Third Largest Economy Has Bad Intentions—And It’s Only Getting Bigger.” Accessed August 2025. https://cybersecurityventures.com/the-worlds-third-largest-economy-has-bad-intentions-and-its-only-getting-bigger/.

[2] Feedzai. 2024. “GASA Global State of Scams Report: $1T Lost to Scams.” Accessed August 2025. https://www.feedzai.com/blog/gasa-global-state-of-scams-report-1t-lost-to-scams/.

[3] GSMA. 2025. Fraud and Scams Safety Report. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.

[4] Signicat. 2024. “Fraud Attempts with Deepfakes Have Increased by 2137% over the Last Three Years.” Accessed August 2025. https://www.signicat.com/press-releases/fraud-attempts-with-deepfakes-have-increased-by-2137-over-the-last-three-year.

[5] International Justice Mission. 2023. Trapped Online: An Investigation into Forced Criminality in Southeast Asia’s Cyber-Scamming Crisis. Washington, DC: IJM. https://www.ijm.org/reports/trapped-online-forced-criminality-in-southeast-asias-cyber-scamming-crisis.

[6] International Justice Mission. 2024. Beyond Rescue: A Multi-Sectoral Response to Cyber-Scam Trafficking. Washington, DC: IJM.

[7] United Nations Office on Drugs and Crime. 2024. Transnational Organized Crime in East and Southeast Asia: A Threat to Sustainable Development. Vienna: UNODC.

[8] United Nations Development Programme. n.d. Anti-Scam Handbook. New York: UNDP.

[9] Federal Reserve. n.d. “About the ScamClassifier Model.” FedPayments Improvement. https://fedpaymentsimprovement.org.

[10] United Nations Development Programme. n.d. Anti-Scam Handbook. New York: UNDP.

[11] GSMA. 2025. Fraud and Scams Safety Report. London: GSMA. https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2025/02/Fraud-and-scams-safety-report.pdf.

[12] Google, Temasek, and Bain & Company. 2023. e-Conomy SEA 2023 Report. https://economysea.withgoogle.com/intl/ALL_th/report/.

[13] Google, Temasek, and Bain & Company. 2023. e-Conomy SEA 2023 Report. https://economysea.withgoogle.com/intl/ALL_th/report/.

[14] ASEAN Working Group on Anti-Online Scam (WG-AS). 2024. Report of the Online Scams Activities in ASEAN (2023–2024).

[15] United Nations Office on Drugs and Crime. 2024. Convergence of Transnational Organized Crime in East and Southeast Asia: 2024 Report. Vienna: UNODC. https://www.unodc.org/roseap/uploads/documents/Publications/2024/TOC_Convergence_Report_2024.pdf

[16] United Nations Office on Drugs and Crime. 2024. “Crushing Scam Farms: Southeast Asia’s Criminal Service Providers.” UNODC, July 2024. https://www.unodc.org/unodc/frontpage/2024/July/crushing-scam-farms--southeast-asias-criminal-service-providers.html.

[17] Reuters. 2025. “Cancer Billion-Dollar Cyberscam Industry Spreading Globally—UN.” Reuters, April 21. https://www.reuters.com/world/china/cancer-billion-dollar-cyberscam-industry-spreading-globally-un-2025-04-21/.

[18] Reuters. 2023. “Hundreds of Thousands Trafficked into SE Asia Scam Centres—UN.” Reuters, August 29. https://www.reuters.com/world/asia-pacific/hundreds-thousands-trafficked-into-se-asia-scam-centres-un-2023-08-29/.

[19] Khaosod English. 2025. “They Were Forced to Scam Others Worldwide, Now Thousands Are Held in Detention on the Myanmar Border.” March 9. https://www.khaosodenglish.com/featured/2025/03/09/they-were-forced-to-scam-others-worldwide-now-thousands-are-held-in-detention-on-the-myanmar-border/.

[20] CSIS. 2024. “Cyber-Scamming Goes Global: Sourcing Forced Labor for Fraud Factories.” Washington, DC: Center for Strategic and International Studies. https://www.csis.org/analysis/cyber-scamming-goes-global-sourcing-forced-labor-fraud-factories.

[21] Canadian Anti-Fraud Centre. n.d. “About the Canadian Anti-Fraud Centre.” https://antifraudcentre-centreantifraude.ca/index-eng.htm.

[22] National Anti-Scam Centre (NASC). n.d. “About NASC.” Government of Australia. https://www.nasc.gov.au/.

[23] Australian Competition and Consumer Commission. 2024. “ACCC Welcomes Passage of World-First Scams Prevention Laws.” ACCC, September. https://www.accc.gov.au/media-release/accc-welcomes-passage-of-world-first-scams-prevention-laws.

[24] Federal Communications Commission. n.d. “Call Authentication.” FCC. https://www.fcc.gov/call-authentication.

[25] Association of Certified Anti-Money Laundering Specialists. 2023. “The European Union’s Battle against Financial Fraud: Confronting the Threats Ahead.” ACAMS Today. https://www.acamstoday.org/the-european-unions-battle-against-financial-fraud-confronting-the-threats-ahead/.

[26] European Union. 2024. Regulation (EU) 2024/886. Official Journal of the European Union. https://eur-lex.europa.eu/eli/reg/2024/886/oj/eng.

[27] Access Partnership. 2024. “Ireland Launches SMS Sender ID Registry.” Accessed August 2025. https://accesspartnership.com/ireland-launches-sms-sender-id-registry.

[28] UK Government. 2023. Online Fraud Charter. London: HM Government. https://www.gov.uk/government/publications/online-fraud-charter-2023.

[29] UK Government. 2023. Joint Fraud Taskforce: Telecommunications Charter. London: HM Government. https://www.gov.uk/government/publications/joint-fraud-taskforce-telecommunications-charter.

[30] UK Government. 2023. *Joint Fraud Taskforce: Retail Banking Charter.* London: HM Government. https://www.gov.uk/government/publications/joint-fraud-taskforce-retail-banking-charter.

[31] UK Government. 2023. Joint Fraud Taskforce Collection. London: HM Government. https://www.gov.uk/government/collections/joint-fraud-taskforce.

[32] Financial Times. 2024. “Article on Fraud and Scams.” Financial Times. https://www.ft.com/content/12bbd99e-ed46-418d-bc15-04433e13db30.

[33] AUSTRAC. n.d. “Fintel Alliance.” Australian Government. https://www.austrac.gov.au/partners/fintel-alliance.

[34] The Australian. 2024. “Fast-Growing Scam Targets WFH Job Hunters.” The Australian, April. https://www.theaustralian.com.au/breaking-news/fastgrowing-scam-targets-wfh-job-hunters/news-story/32e97ce408468ad5d8060ddebe24bc6e.

[35] Europol. n.d. “Money Muling.” https://www.europol.europa.eu/crime-areas/forgery-of-money-and-means-of-payment/money-muling.

[36] European Banking Federation. 2024. “European Money Mule Action Leads to 1,803 Arrests.” Brussels: EBF. https://www.ebf.eu/innovation-cybersecurity/european-money-mule-action-leads-to-1-803-arrests/.

[37] Take Five to Stop Fraud. n.d. “About Us.” UK Finance. https://www.takefive-stopfraud.org.uk/.

[38] Action Fraud. n.d. “Report Fraud and Cyber Crime.” UK Police. https://www.actionfraud.police.uk/.

[39] NASC. 2024. “Australians Urged to Stop, Check, Protect to Stay Scam Safe.” https://www.nasc.gov.au/news/australians-urged-to-stop-check-protect-to-stay-scam-safe.

[40] Stop Scams UK. n.d. “About.” https://stopscamsuk.org.uk/about/.

[41] Meta. 2024. Submission on the Scams Prevention Framework Bill 2024. London: Meta Platforms.

[42] Parliament of Australia. 2024. Scams Prevention Framework Bill 2024: Submissions. Canberra: Commonwealth of Australia. https://www.aph.gov.au/DocumentStore.ashx?id=4e98f789-2d3f-482d-86cd-d88a42071c0f&subId=775666.

[44] National Anti-Financial Crime Centre (Malaysia). n.d. “About NSRC.” https://nfcc.jpm.gov.my/index.php/en/component/content/article/about-nsrc?catid=17&Itemid=114.

[45] Infocomm Media Development Authority (Singapore). n.d. “Anti-Scam Measures.” https://www.imda.gov.sg/how-we-can-help/anti-scam-measures.

[46] Singapore Police Force. 2022. “Opening of Anti-Scam Command Office.” September 6.

[47] Siam Legal. n.d. “What Is Thailand’s Anti-Online Scam Operation Center?” https://library.siam-legal.com/what-is-thailands-anti-online-scam-operation-center/.

[48] Siam Legal. n.d. “Thailand’s Anti-Online Scam Operation Center: Using AI and Big Data to Combat Cybercrime.” https://library.siam-legal.com/thailands-anti-online-scam-operation-center-using-ai-and-big-data-to-combat-cybercrime/.

[49] Khmer Times. 2024. “PM Chairs First Meeting of the Commission for Combatting Online Scams.” June 13. https://www.khmertimeskh.com/501506489/pm-chairs-first-meeting-of-the-commission-for-combatting-online-scams/.

[50] Laotian Times. 2023. “Lao Government Orders Nationwide SIM Card Registration to Combat Online Scams.” February 10. https://laotiantimes.com/2023/02/10/lao-government-orders-nationwide-sim-card-registration-to-combat-online-scams/.

[51] VietnamNet Global. 2024. “Vietnam Strengthens Measures to Prevent Online Fraud.” June 5. https://vietnamnet.vn/en/vietnam-strengthens-measures-to-prevent-online-fraud-228809.html.

[52] Monetary Authority of Singapore. 2023. “Consultation Paper on Proposed Shared Responsibility Framework.” https://www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework.

[53] Monetary Authority of Singapore. 2023. “Consultation Paper on Proposed Shared Responsibility Framework.” https://www.mas.gov.sg/publications/consultations/2023/consultation-paper-on-proposed-shared-responsibility-framework.

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

[55] Malaysian Communications and Multimedia Commission. 2023. “MCMC to Enforce Mandates to Block Fraudulent Content in SMS.” October 11. https://www.mcmc.gov.my/en/media/press-clippings/mcmc-to-enforce-mandates-to-block-fraudulent-cont.

[56] Singapore Parliament. 2025. Protection from Scams Bill. Singapore: Parliament of Singapore.

[57] Malaysian Communications and Multimedia Commission. 2023. “MCMC to Enforce Mandates to Block Fraudulent Content in SMS.” October 11. https://www.mcmc.gov.my/en/media/press-clippings/mcmc-to-enforce-mandates-to-block-fraudulent-cont.

[58] Bank Negara Malaysia. 2023. “Update on Measures to Reinforce Safeguards against Financial Scams.” September 26. https://www.bnm.gov.my/documents/20124/5911400/Measures_to_Reinforce_Safeguards_Against_Financial_Scams.pdf.

[59] Wotton + Kearney. 2023. “Thailand’s New Law Expands Cybercrime Prevention and Enforcement Powers.” April 20. https://www.wottonkearney.com/thailands-new-law-expands-cybercrime-prevention-and-enforcement-powers/.

[60] Siam Legal. (n.d.). Thailand's Anti-Online Scam Operation Center: Using AI and Big Data to Combat Cybercrime. Retrieved from https://library.siam-legal.com/thailands-anti-online-scam-operation-center-using-ai-and-big-data-to-combat-cybercrime/

[61] Vietnam Briefing. 2023. “An Introduction to Vietnam’s Law on Anti-Money Laundering.” April 20. https://www.vietnam-briefing.com/news/an-introduction-to-vietnams-law-on-anti-money-laundering.html/.

[62] State Bank of Vietnam. 2023. “Decision No. 2345/QD-NHNN on Deploying Solutions for Security and Safety in Online Payments and Bank Card Payments.” December 18.

[63] Antara News. 2024. “OJK Issues New Regulation to Strengthen Anti-Fraud Strategy.” March 4. https://en.antaranews.com/news/307455/ojk-issues-new-regulation-to-strengthen-anti-fraud-strategy.

[64] Republic of the Philippines. 2024. Republic Act No. 12010: Anti-Financial Scamming Act. Official Gazette of the Republic of the Philippines. July 12.

[65] U.S. Department of State. 2024. 2024 Investment Climate Statements: Brunei. Washington, DC: Department of State. https://www.state.gov/reports/2024-investment-climate-statements/brunei/.

[66] Authority for Info-communications Technology Industry of Brunei Darussalam. n.d. “Mandatory Registration for Prepaid SIM Cards.” https://www.aiti.gov.bn/sim-card-registration.

[67] United States Institute of Peace. 2024. “Cambodia’s Cyber Scammers Are a Global Problem.” February 21. https://www.usip.org/publications/2024/02/cambodias-cyber-scammers-are-global-problem.

[68] United Nations Office on Drugs and Crime. 2024. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat. Vienna: UNODC. https://www.unodc.org/roseap/uploads/documents/Publications/2024/UNODC_Transnational_Crime_Report_2024.pdf.

[69] National Assembly of the Lao PDR. n.d. Cybercrime Law. Vientiane: Government of Laos. http://www.na.gov.la/index.php/cybercrime-law.

[70] Vietnam Ministry of Information and Communications. 2024. Circular on Mobile Financial Transactions.

[71] Indonesia Financial Services Authority (OJK). 2023. "Regulation on Digital Financial Innovation." https://ojk.go.id/en/fungsi-utama/itsk/regulatory-sandbox/default.aspx.

[72] Republic of the Philippines. 2024. Republic Act No. 11975: Anti-Financial Scamming Act. Manila: Government of the Philippines. https://lawphil.net/statutes/repacts/ra2024/ra_12010_2024.html.

[73] Infocomm Media Development Authority (Singapore). 2022. SMS Sender ID Registry (SSIR) Guidelines. October. https://www.imda.gov.sg/-/media/imda/files/news-and-events/media-room/media-releases/2022/10/media-factsheet---full-ssir-regime14102022.pdf.

[74] Malaysian Communications and Multimedia Commission. 2024. "Directive on SMS Content Filtering." September 2. https://www.thestar.com.my/tech/tech-news/2024/09/02/mcmc-bans-sms-with-hyperlinks-callback-numbers-and-personal-info-requests-from-sept-1.

[75] National Broadcasting and Telecommunications Commission (Thailand). 2023. "SIM Card Regulations." https://developingtelecoms.com/telecom-business/telecom-regulation/17889-thailand-s-nbtc-to-mandate-biometrics-for-sim-registrations.html.

[76] Monetary Authority of Singapore. 2024. "Shared Responsibility Framework – Combatting Scams." https://www.mas.gov.sg/regulation/combatting-scams.

[77] Ministry of Digital Economy and Society (Thailand). 2024. "DE Fence Initiative Overview." Bangkok Post, June. https://www.bangkokpost.com/business/general/2974926/thailands-digital-ministry-rolls-out-anti-scam-sandbox.

[78] Infocomm Media Development Authority and Malaysian Communications and Multimedia Commission. 2024. "Malaysia–Singapore Bilateral Cooperation on Scam Intelligence." Press release. https://www.imda.gov.sg/resources/press-releases-factsheets-and-speeches/press-releases/2024/sg-and-my-sign-mou.

[79] United Nations Office on Drugs and Crime. 2025. Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia. Vienna: UNODC.

[80] Otoritas Jasa Keuangan (Indonesia). 2024. "OJK Strengthens Anti-Fraud Strategy in Financial Services Sector." March 7.

[81] Cybercrime Investigation and Coordinating Centre (Philippines). n.d. "Home." https://cicc.gov.ph/.

[82] Vietnam Investment Review. 2025. "Vietnamese Lenders Seek Unified Anti-Fraud Shield." July 25. https://vir.com.vn/vietnamese-lenders-seek-unified-anti-fraud-shield-133206.html.

[83] United States Institute of Peace. 2024. "Cambodia's Cyber Scammers Are a Global Problem." February 21. https://www.usip.org/publications/2024/02/cambodias-cyber-scammers-are-global-problem.

[84] United Nations Office on Drugs and Crime. 2024. Casinos, Money Laundering, Underground Banking, and Transnational Organized Crime in East and Southeast Asia: A Hidden and Accelerating Threat. Vienna: UNODC.

[85] U.S. Department of State. 2024. 2024 Investment Climate Statements: Brunei. Washington, DC: Department of State.

[86] JanganKenaScam. 2023. “Banking Associations Launch Nationwide Anti-Scam Campaign.” October 3. https://www.jangankenascam.com/my/berita/banking-associations-launch-nationwide-anti-scam-campaign/.

[87] National Crime Prevention Council (Singapore). n.d. “ScamAlert.” https://www.scamalert.sg/.

[88] Government of Singapore. n.d. “ScamShield App.” https://www.scamshield.org.sg/.

[89] Infocomm Media Development Authority (Singapore). n.d. “Digital for Life Movement.” https://www.imda.gov.sg/digitalforlife.

[90] Meta. n.d. “Online Scam Prevention: Spotting and Reporting Scams.” https://about.meta.com/sg/actions/safety/anti-scam/education/.

[91] Royal Thai Government. 2024. “MDES Warns Public against Scammers Impersonating AOC 1441 Officials.” May 15. https://www.thaigov.go.th/news/contents/details/82829.

[92] VietnamPlus. 2025. “Google, Public Security Ministry Join Hands in Anti-Scam Campaign.” June 26. https://en.vietnamplus.vn/google-public-security-ministry-join-hands-in-anti-scam-campaign-post321729.vnp.

[93] SW Indonesia. 2025. “New Anti-Fraud Framework: Deadlines and Reporting of LJK POJK 12/2024.” February 17. https://sw-indonesia.com/insights/legal-update/new-anti-fraud-framework-deadlines-and-reporting-of-ljk-pojk-12-2024/.

[94] Laotian Times. 2023. “Lao Education Ministry Warns Residents about Fake Scholarships from China, Vietnam.” September 7. https://laotiantimes.com/2023/09/07/lao-education-ministry-warns-residents-about-fake-scholarships-from-china-vietnam/.

[95] Brunei Darussalam Central Bank. 2025. “BDCB Alert List Update.” July 24. https://www.bdcb.gov.bn/publications/details?id=01k0xv53gednq05zaan7cedqxa.

[96] United Nations Office for the Coordination of Humanitarian Affairs. 2025. Myanmar Humanitarian Update No. 43. April 2. https://reliefweb.int/report/myanmar/myanmar-humanitarian-update-no-43-2-april-2025.or International Crisis Group consistently detail the collapse of public services and communication channels due to the conflict).

[97] ASEAN. 2021. ASEAN Cybersecurity Cooperation Paper 2021–2025. Jakarta: ASEAN Secretariat. https://asean.org/wp-content/uploads/2022/02/01-ASEAN-Cybersecurity-Cooperation-Paper-2021-2025_final-23-0122.pdf.

[98] VietnamPlus. 2025. “ASEANAPOL Enhances Crackdown on Scam Call Centres.” https://en.vietnamplus.vn/aseanapol-enhances-crackdown-on-scam-call-centres-post308678.vnp.

[99] Asialink (University of Melbourne). 2024. “Fraud Danger: The Rise of Cyber Scams in Southeast Asia.” https://asialink.unimelb.edu.au/diplomacy/article/fraud-danger-rise-cyber-scams-southeast-asia.

[100] Public Relations Department of Thailand. 2025. “Thailand Digital Economy and Society Ministry Campaign.” https://thailand.prd.go.th/en/content/category/detail/id/2078/iid/356340.

[101] Cyble. 2025. “United against Cybercrime: ASEAN Ministers Forge New Security Pathways.” https://cyble.com/blog/united-against-cybercrime-asean-ministers-forge-new-security-pathways/.

[102] Singapore Police Force. 2025. “Seven Law Enforcement Agencies Collaborate in Major Anti-Scam Operations.” May 4. https://www.police.gov.sg/media-room/news/20250504_seven_law_enforcement_agencies_collaborate_in_major_anti-scam_operations.

[103] Google. 2024. “How We’re Using AI to Build a Safer Digital Future in Asia-Pacific.” The Keyword, October 28. https://blog.google/around-the-globe/google-asia/four-ways-google-is-combatting-scams-in-asia-pacific/.

[104] Times of India. 2025. “How Google Plans to Save Indians 20,000 Crore from Cybercrime.” March. https://timesofindia.indiatimes.com/technology/tech-news/how-google-plans-to-save-indians-20000-crore-from-cybercrime-in-2025/articleshow/121908679.cms.

[105] Axios. 2025. “Future of Cybersecurity Newsletter.” https://www.axios.com/newsletters/axios-future-of-cybersecurity-f9cf8cf0-fab8-11ef-b65f-110efff1a746.

[106] Meta. 2024. “How Meta Addresses Coordinated Inauthentic Behavior.” Transparency Center. https://transparency.fb.com/cib/how-we-address-it/

[107] Match Group. 2025. “Company News Release.” https://mtch.com/single-news/985/.

[108] Google. 2024. “Four Ways Google Is Combatting Scams in Asia-Pacific.” The Keyword, October 28. https://blog.google/around-the-globe/google-asia/four-ways-google-is-combatting-scams-in-asia-pacific/

[109] PwC. 2024. Global Economic Crime and Fraud Survey 2024: Asia Pacific Report. London: PwC.

[110] ASEANAPOL. 2025. “Strengthening Cybersecurity: ASEANAPOL and Mastercard Forge Path for Collaboration.” February 28. http://www.aseanapol.org/display/2025/02/28/strengthening-cybersecurity-aseanapol-and-mastercard-forge-path-for-collaboration.

[111] NewsHub Asia. 2025. “Royal Malaysia Police Teams Up with Pos Malaysia and Whoscall in Strategic Partnership to Combat Parcel Scams.” https://www.newshubasia.com/tech/royal-malaysia-police-teams-up-with-pos-malaysia-and-whoscall-in-strategic-partnership-to-combat-parcel-scams/.

[112] Consumers’ Association of Singapore. 2025. “CASE Unveils Top Consumer Complaints of 2024, Calls for Greater Vigilance against Scams.” January 15. https://case.org.sg/.

[113] Human Rights Watch. 2024. “My Soul Is Trapped”: Trafficking and Torture in Myanmar’s Online Scam Operations. New York: HRW. https://www.hrw.org/report/2024/04/03/my-soul-trapped/trafficking-and-torture-myanmars-online-scam-operations.

[114] Meta. 2024. “Cracking Down on Organized Crime Scam Centers.” November. https://about.fb.com/news/2024/11/cracking-down-organized-crime-scam-centers/.

[115] ASEAN–Australia Counter-Trafficking (ASEAN-ACT). n.d. “About Us.” https://www.aseanact.org/.

[116] Oliver Wyman. 2024. “Cracking Scams with Analytics in Southeast Asia.” March. https://www.oliverwyman.com/our-expertise/insights/2024/mar/cracking-scams-with-analytics-southeast-asia.html.

[117] ASEAN. 2025. Joint Media Statement of the 5th ASEAN Digital Senior Officials Meeting (ADGSOM). Jakarta: ASEAN Secretariat. https://asean.org/wp-content/uploads/2025/01/15-ENDORSED-JOINT-MEDIA-STATEMENT-5th-ADGSOM-v2-Cleaned.pdf.

[118] Stimson Center. 2025. “Mekong–U.S. Partnership Track 1.5 Policy Dialogue on Countering Scam Operations.” https://www.stimson.org/2025/mekong-u-s-partnership-track-1-5-policy-dialogue-on-countering-scam-operations/.

[119] Ibid.

[120] Ibid.