

RESEARCH PAPER

Bridging the Gaps: Rethinking Regional Efforts Against Online Scams in APAC

PANEL 1

Deepfakes for Financial Fraud

Adinova Fauri

Adinova is a researcher at CSIS Indonesia's Department of Economics. He currently holds a bachelor's degree in economics from the University of Indonesia and an MSc in Economics from Tilburg University, The Netherlands. Ever since he joined CSIS in 2015, Adinova has worked in various research projects related to the issue of digital literacy and skills, digital governance and privacy, and the economic impact of digital economy. In 2023, he spent three months as a research fellow at Istituto Affari Internazionali (IAI) in Italy, where he examined the potential opportunities and risks of CBDC. Additionally, He is also an active member of Indonesian Economists Association (ISEI) and Indonesia Fintech Society (IFSoc).

Rojwa Rachmiadi

Rojwa Rachmiadi is a Project Research Assistant at CSIS. With an interdisciplinary background rooted in qualitative research, her broader work spans across multiple domains, including tech, business, and education. She is particularly interested in analyzing policy challenges from structural angles and how research can better inform decision-making. In this paper, she explores the regulatory challenges of tackling cross-border online scams.

This paper is circulated for discussion and feedback. The views expressed are solely those of the author(s) and do not represent an official position of SAIL, CSIS, Google, CfDS, Faculty of Social and Political Sciences UGM or any other organization. The author(s) welcome comments on this version and invite you to contact them directly with any feedback or questions.



Bridging the Gaps: Rethinking Regional Efforts Against Online Frauds and Scams in Asia Pacific

Adinova Fauri, Rojwa Rachmiadi

As the most cyber-attacked region in the world, the Asia-Pacific urgently needs to explore policy options to effectively combat online fraud and scams. While several domestic initiatives, such as establishing anti-scam centers, fostering public-private partnership, and removing fraudulent online advertisements, have been implemented, there remains a lack of international commitment to coordinated cross-border actions. By utilizing data governance framework, this paper assesses domestic, bilateral, and regional efforts to address these threats, aiming to evaluate the depth of international commitment and identify the key challenges in tackling them. Despite some obstacles, we believe that leveraging existing ASEAN regional agreements and expanding their scope across the broader Asia-Pacific could provide a strategic entry point to strengthen regional commitment and collective action against online fraud and scams.

Keywords: online frauds and scams, data governance, regional cooperation



Introduction

The Asia Pacific was the most cyber-attacked region, bearing 31 percent of global cyberattacks in 2022. In the first quarter of 2023, global cyberattacks increased by 1.8 percent year-on-year.¹ SEA emerged as the global hub for online fraud and scam operations, with industrial-level scam centers concentrated in Special Economic Zones and vulnerable areas across the region.² The UNODC estimated that cyber-enabled frauds in SEA generate between US\$27.4 - 36.5 billion (about 0.9 % of the economy³) annually, with the Global Anti-Scam Alliance (GASA) reporting over US\$1.03 trillion in scam proceeds globally in 2024.⁴

Ample evidence illustrates that SEA countries exhibited multiple roles, such as headquarters of scam compounds, sources of trafficked or recruited scam laborers and victims, and hubs for transit and laundering activities. For example, Chinese actors may lead scam groups operating in Cambodian compounds where SEA laborers from multiple countries execute them, and proceeds are laundered in neighboring countries.⁵ On the other hand, Australia is not a source of scam activity but is a victim and a regulatory actor actively contributing to collaborative measures against it.

The increasing use of digital tools, such as Artificial Intelligence (AI), has enabled perpetrators to bypass language and cultural barriers, expand their markets, and build more trust with victims. From 2022 to 2023, AI-driven scams, such as voice cloning, facial simulation, and plug-and-play scam kits, were increasingly used to impersonate identities and enhance credibility in APAC, with significant growth across China, Vietnam, the Philippines, Indonesia, and Thailand.⁶ For example, a Taiwanese woman believed she was video calling a Hong Kong celebrity from a website, a well-known entrepreneur, a celebrity, and government officials

¹ Olajide O Oyadeyi, Oluwadamilola Adeola Oyadeyi, and Rofiat Omolola Bello, "[Cybercrime in the Asia-Pacific](#)," June 2024

² UNODC, "[Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia](#)," April 2025.

³ [IMF 2024 Data](#), Southeast Asia's GDP is 3,952,665 in 2024

⁴ UNODC, "[Inflection Point: Global Implications of Scam Centres, Underground Banking and Illicit Online Marketplaces in Southeast Asia](#)," April 2025.

⁵ Hai Thanh Luong and Hieu Minh Ngo, "[Understanding the Nature of the Transnational Scam-Related Fraud: Challenges and Solutions from Vietnam's Perspective](#)," *Laws* 13, no. 6 (2024): 1–15.

⁶ Danielle Watson, "[Transnational and Organised Crime in Pacific Island Countries and Territories: Police Capacity to Respond to the Emerging Security Threat](#)," October 2024.

were used to promote bogus investment schemes in Japan, South Korea, Singapore, and Indonesia.⁷

Several efforts have been done domestically to tackle online scams, including forming anti-scam centers, public-private partnerships between banks and telecommunication industries, mandating laws that require platforms to remove fraudulent ads and close accounts or numbers used in scams, and requiring financial institutions to implement an immediate deactivation feature and fraud detection for high-risk transactions. On the side, public education campaigns and outreach to increase digital literacy and awareness on scam identification were also delivered.⁸

In terms of joint efforts, INTERPOL has concluded a transcontinental police operation, which resulted in seizures of USD 300 million worth of assets from cyber-enabled fraud across 34 countries.⁹ Commendable actions include Australia's collaboration with the Philippines for offshore raids to dismantle foreign scam centers targeting Australians, cooperation with the UK's Ofcom to combat phone scams, and, along with New Zealand, supporting the Pacific Transnational Crime Network (PTCN).¹⁰

Although extensive domestic efforts to tackle online scams have been observed in various countries, considering the cross-border nature of online scams, there is a lack of international commitment to joint action beyond borders. Without standards and agreements across other countries in APAC, regulatory bodies are limited to local jurisdictions, which makes tracing and prosecuting perpetrators who operate servers and use encrypted applications increasingly challenging.

Furthermore, an absence of shared definitive terms and enforcement standards regarding online frauds and scams across APAC may lead to fragmented laws that further entangle cross-border collaborations. The lack of coordination between stakeholders within or across borders often contributes to overlapping and redundant jurisdictions, creating compliance fatigue that may slow progress toward preventive and proactive measures.¹¹ Although some


⁷ Safer Internet Lab., ["Online Fraud and Scam Trends Across APAC,"](#) June 2025.

⁸ Kenechi Okelele, ["Towards a Digital Nation: Addressing the Scam Economy in Asia Pacific,"](#) March 2025.

⁹ INTERPOL, ["INTERPOL Global Financial Fraud Assessment,"](#) 2024.

¹⁰ Kenechi Okelele, ["Towards a digital nation: addressing the scam economy in Asia Pacific,"](#) March 2025.

¹¹ William A. Carter and William Crumpler, ["Financial Sector Cybersecurity Requirements in the Asia-Pacific Region,"](#) April 30, 2019.



dialogues shared between ASEAN member states have led to bilateral and multilateral MoUs for resource-sharing and internal capacity building, they lack binding treaties for collaborative enforcement measures. Further challenges persist as scam perpetrators are continuously ahead of policy responses by evolving to newer and more sophisticated trends.

This paper aims to discuss existing bilateral and regional collaborations and their potential challenges in the APAC region and offers policy recommendations to strengthen regional efforts against online cross-border frauds and scams. In the following sections, we will examine the conceptual literature regarding data governance, data protection, and data sharing, case studies of jurisdictional challenges, a mapping of existing bilateral and regional partnership documents and their potential challenges, and policy recommendations to improve mitigation against online cross-border frauds and scams in the APAC region.

Literature Review

The terms “scam” and “fraud” are often used interchangeably in academic discourse. While “scams” is sometimes used to refer to a specific type of fraud, typically involving interactive acts that exploit trust to manipulate victims, “fraud” encompasses a broader range of deceptive acts, such as identity theft and accounting fraud.¹² In this paper, the two terms are used interchangeably. Meanwhile, the terms “cybercrime,” is employed to present a broader term of crimes committed using computers or computer networks, which includes online scams in the discussion.

Online frauds and scams continue to evolve at an alarming rate, outpacing the development of an effective regulatory framework to address them. The absence of good data governance risks widening regulatory gaps and has left increased vulnerabilities to cyber threats. Data governance encompasses the factors necessary to ensure data protection and compliance against online frauds and scams in the APAC region. The data governance framework consists of core principles (accountability, transparency, data stewardship), data policies and standards (establishing clear rules on how data is collected, stored, processed, and shared, defining roles and responsibilities in data management), data ownership and access control

¹² Liu, Xiao Fan, Yushi Ai, Li Crystal Jiang, Xiaohui Wang, and Ye Wu. 2025. “Understanding the Human Element in Scams: A Multidisciplinary Approach.” *Journal of Information Technology Case and Application Research* 27 (1): 9–24. <https://doi.org/10.1080/15228053.2024.2439192>.

(assigning data ownership roles, implementing role-based access controls to sensitive data), data quality management (ensuring accuracy, consistency, and reliability of data), and compliance with regulations (e.g., the General Data Protection Regulation in Europe, the California Consumer Privacy Act in the United States).¹³

Data governance, when integrated with risk management and legal requirements, can reduce vulnerabilities and enhance data security, thereby protecting against online scams, such as through security breaches, data leaks, attacks, and compliance failures. For example, a bank that deploys advanced encryption protocols conducts regular cybersecurity audits to identify vulnerabilities and implement prompt improvements. An e-commerce company has also significantly reduced the risk of unauthorized access by implementing multi-factor authentication.¹⁴

However, there is limited research regarding the relationship between data governance and the prevalence of online scams globally. From 1996 to 2018, a review of 64 papers published on data governance and cybercrime revealed that only 2 papers explicitly discussed both topics in the same study.¹⁵ This finding underscores a gap in the literature that indicates a fragmented foundation for a regulatory assessment of online scams.

One notable study discussing data governance and cybercrime was conducted by the World Bank, which applied a Global Data Regulation Diagnostic framework. The paper assessed global data governance laws and regulations based on a survey in 80 countries, providing insights into regulatory strengths and gaps related to cybercrime. Cybersecurity and cybercrime are among the dimensions scored under the safeguards pillar. This includes the presence of a regulatory framework that criminalizes illegal cyber activities, specifies cybersecurity measures, and requires the establishment of response teams as components of robust data governance. While over 60 percent of countries surveyed have enacted cybercrime regulations, only 7 percent of high-income and 5 percent of upper-middle-income countries have comprehensive requirements to facilitate cross-border data transfers.

¹³ "Data Governance and Risk Management: Mitigating Data-Related Threats," 2020.

¹⁴ "Kishore Reddy Gade, "Data Governance and Risk Management: Mitigating Data-Related Threats" 3 (2020)

¹⁵ Gerald Onwujekwe, Manoj Thomas, and Kweku-Muata Osei-Bryson, "Using Robust Data Governance to Mitigate the Impact of Cybercrime," in *Proceedings of the 2019 3rd International Conference on Information System and Data Mining* (ICISDM 2019: 2019 The 3rd International Conference on Information System and Data Mining, Houston TX USA: ACM, 2019), 70–79, <https://doi.org/10.1145/3325917.3325923>

In addition, only 33 percent of lower-income countries have established official bodies with supervisory authorities for data protection measures.¹⁶

The uneven implementation of regulatory frameworks globally highlights a broader challenge to developing good data governance, where cybersecurity is enforced with data privacy measures and data sharing. While principles of data privacy and security must be safeguarded, responsible cross-border data sharing enables a deeper understanding of the scam landscape from a holistic perspective; it provides comprehensive information to study past cases, map the recent development of scam tactics, and alert neighboring areas. However, although data sharing is often encouraged to improve decision-making and promote joint research efforts, it risks the misuse of personal data.¹⁷ While some regulations restrict financial institutions from sharing clients' personal information, other laws mandate them to share sensitive information to combat financial crimes.¹⁸ For instance, the US favors the free flow of data as a commodity, the EU exclusively protects and limits the transfer of personal data, while China mandates data localization and centralized control.¹⁹

In response to legal and regulatory complexities, global cooperative frameworks have emerged to facilitate data exchange and joint enforcement in coordinating responses against online scams. As of 2013, over 50 percent of countries surveyed reported having established public-private partnerships to combat cybercrime.²⁰ Global efforts to exchange knowledge and encourage joint actions to protect users against online scams include: 1) GASA, a member-based organization that brings together governments, law enforcement, consumer protection organizations, financial authorities and providers, social media, internet service providers, and cybersecurity companies 2) International Consumer Protection Enforcement Network (ICPEN), an association of law enforcement and consumer protection organisations

¹⁶ Rong Chen, *Mapping Data Governance Legal Frameworks around the World: Findings from the Global Data Regulation Diagnostic* (World Bank, Washington, DC, 2021), <https://doi.org/10.1596/1813-9450-9615>

¹⁷ Mattia Caldarulo, Jared Olsen, and Mary K. Feeney, "Oversharing: The Downside of Data Sharing in Local Government," *Public Administration* 102, no. 4 (December 2024): 1647–64, <https://doi.org/10.1111/padm.12993>

¹⁸ Panagiotis Chatzigiannis et al., "Privacy-Enhancing Technologies for Financial Data Sharing" (arXiv, June 16, 2023), <https://doi.org/10.48550/arXiv.2306.10200>

¹⁹ Douglas W. Arner, Giuliano Castellano, and Eriks Selga, "The Transnational Data Governance Problem," *SSRN Electronic Journal*, 2021, <https://doi.org/10.2139/ssrn.3912487>

²⁰ UNODC, "[Comprehensive Study on Cybercrime Draft](#)," February 2013.

from 70 countries, and 3) INTERPOL, an organization that has conducted transnational investigations, seizing proceeds and arresting perpetrators of scams.²¹

However, challenges persist in fostering effective international cooperation to combat online scams. The absence of a universal definition and recognition for online frauds and scams further complicates regional responses, as it may fall under the jurisdiction of multiple agencies. The different powers of arrest, procedural laws, and access to data and systems among countries also pose a challenge to mitigating cross-border scams. In the late 1990s, international cybercrime investigators could not prosecute criminals who infected more than 45 million computer users worldwide with malware because their home country, the Philippines, did not have a law against cybercrime.²²

Moreover, digital evidence of a crime may exist in a different country from where the crime occurred. Foreign governments may require domestic private entities to disclose electronic data, while their local laws prohibit them. Although Mutual Legal Assistance Treaties (MLATs) can be submitted to obligate participating countries to summon witnesses, compel evidence, and issue warrants, this request may take an average of approximately 10 months to complete.²³

While there is a growing body of research on online frauds and scams globally, the discussion of cross-border online frauds and scams specific to the APAC region remains underexplored. The explicit discourse on data governance, the balance between privacy and security, and legal harmonization across jurisdictions in the context of online scams in the region is limited, yet it was implied under similar cases, such as the challenges in phishing and cybercrime.

One of the early studies on cross-border online frauds and scams in APAC was observed in 2010, which highlighted the phishing attacks that have entered Australia and New Zealand since 2003, as fake bank websites tricked users into disclosing their banking credentials, which were suspected of coming from Ukrainian spammers. They also found that these syndicates advertise 'internet money mule' jobs in Australia through spam emails, instant

²¹ Mark Button et al., "Policing Cross-Border Fraud 'Above and below the Surface': Mapping Actions and Developing a More Effective Global Response," *Crime, Law and Social Change* 83, no. 1 (June 2025), <https://doi.org/10.1007/s10611-024-10186-2>

²² Andrew Teng, "Jurisdictional Barriers: Cybercrime Prosecution Challenges," May 2017

²³ Stephen P Mulligan, "Cross-Border Data Sharing Under the CLOUD Act," April 23, 2018.

messaging applications, and employment websites to assist them in transferring fraud proceeds to Eastern Europe, and it recognizes the legislative challenges and urgency for proactive government action in cross-border cases.²⁴

Meanwhile, research on cross-border online scams in the SEA region is lagging. In 2017, a paper discussed how cross-border cybercrimes have exploited loopholes in the system, and the absence of coordination, integrated information sharing, and interagency training among relevant bodies pose significant challenges to combat the crime. Although the article was written in a global context, APAC countries were included in the analysis, yet it does not explicitly mention cyber-enabled frauds and scams.²⁵ In 2019, the growing trend of cybercrime began to encourage researchers to assess the cybersecurity requirements in APAC's financial sector, highlighting findings about how complex bureaucratic compliance and stakeholders working in silos may drain talent, resources, and attention away from operational cybersecurity—yet it only briefly mentions cyber frauds and internet banking fraud as a risk for financial institutions.²⁶

The discussion of online frauds and scams shifted in 2024 when UNODC's report on transnational cybercrime extensively revealed the ability of scam perpetrators to operate cross-border in SEA, with an explicit section on the rise of AI-driven techniques, especially deepfakes to impersonate credible figures. The report exposed foreign and local scam syndicates operating in emerging economies with weak law enforcement, using unregulated virtual asset service providers (VASPs), such as cryptocurrencies, to stay anonymous. Due to the local nature of jurisdictions in tackling online scams, syndicates can escape accountability by simply crossing borders and moving illicit proceeds.²⁷ Since then, online scams were assessed through an international lens in need of multistakeholder intervention rather than as individual cases. Hence, advancing international collaboration and establishing harmonised standards are essential to effectively tackle online scams.

²⁴ Stephen McCombie and Josef Pieprzyk, "Winning the Phishing War: A Strategy for Australia," in *2010 Second Cybercrime and Trustworthy Computing Workshop* (2010 Second Cybercrime and Trustworthy Computing Workshop (CTC), Ballarat, Australia: IEEE, 2010), 79–86, <https://doi.org/10.1109/CTC.2010.13>, 2010

²⁵ Andrew Teng, "[Jurisdictional Barriers: Cybercrime Prosecution Challenges](#)," May 2017

²⁶ William A. Carter and William Crumpler, "[Financial Sector Cybersecurity Requirements in the Asia-Pacific Region](#)," April 30, 2019.

²⁷ UNODC, "[Transnational Organized Crime and the Convergence of Cyber-Enabled Fraud, Underground Banking and Technological Innovation in Southeast Asia: A Shifting Threat Landscape](#)," October 2024.

Policy Assessment in APAC and Its Challenges

Driving Factors of Online Scams in APAC

The urgency of building a robust data governance to combat online scams was often discussed in literature, emphasizing the elements of data privacy, data protection, and data sharing to safeguard against threats. While these elements that can be reflected in cybersecurity regulations are crucial, they are not a silver bullet policy. Figure 1 visualizes a positive relationship between the scam encounters and national cybersecurity scores in the APAC region, suggesting that cybersecurity efforts alone may not be sufficient to mitigate this crime. The borderless and anonymous character of the internet alerts organizations that domestic solutions are no longer effective in addressing online scams.

Similar findings were observed in several studies. Cybersecurity laws can backfire if they are introduced abruptly, poorly communicated, or frequently changed. Even within the same country, legislative efforts on cybersecurity may vary between states, which further complicates the regulatory environment. In addition, adapting to comply with new regulations often results in changes, disruptions, and increased expenses, potentially creating new vulnerabilities in the system. Due to the high costs of cybersecurity, firms often delay their cybersecurity investments when regulations are uncertain, and this delay increases the risk of cyberattacks.²⁸ Similarly, another paper argued that despite improved cybersecurity policies in the U.S., the voluntary adoption of these frameworks may result in uneven implementation across sectors and may increase the cost of cybercrime.²⁹ These studies imply that regulations must adopt a consistent structure while aiming for adaptable responses to the advancement of threats.

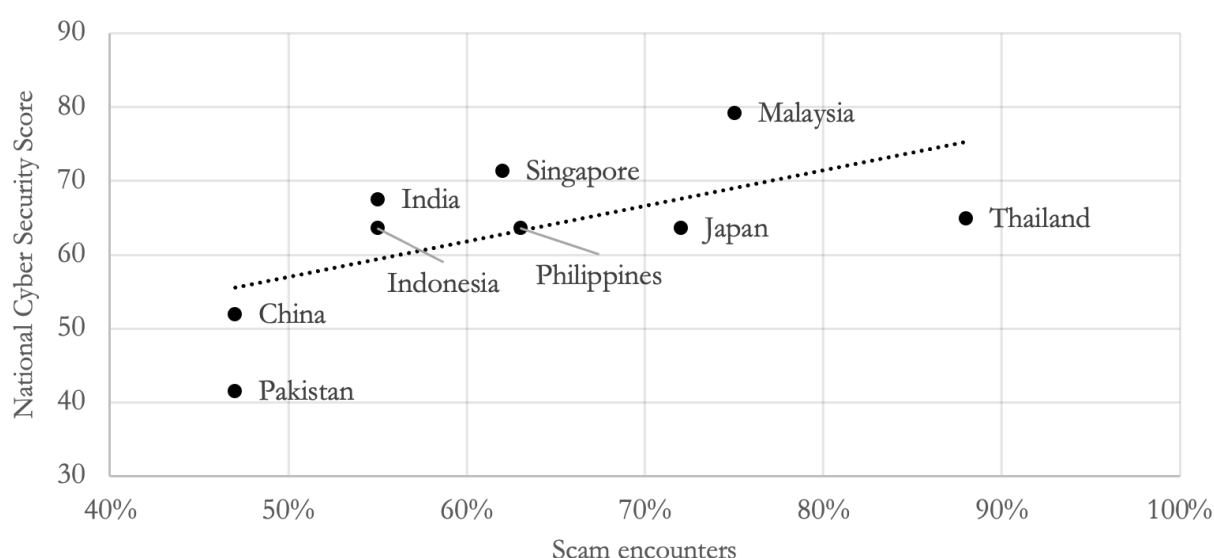
The core problem may not be the absence of cybercrime laws but rather the issue of implementation and political prioritization. The lack of enforcement was observed in the gap between the annual number of cyberattacks and the law enforcement actions taken in

²⁸ Mazaher Kianpour and Shahid Raza, "More than Malware: Unmasking the Hidden Risk of Cybersecurity Regulations," *International Cybersecurity Law Review* 5, no. 1 (March 2024): 169–212, <https://doi.org/10.1365/s43439-024-00111-7>

²⁹ Ejiofor Oluomachi et al., "Assessing the Effectiveness of Current Cybersecurity Regulations and Policies in the US," *International Journal of Scientific and Research Publications* 14, no. 2 (February 24, 2024): 78–85, <https://doi.org/10.29322/ijsrp.14.02.2023.p14610>

response to them, where arrests and prosecutions remain uncommon despite the rise in cyberattacks. Challenges in defining clear roles of different government agencies working on cyber-related cases hinder inter-agency coordination, especially when there is no central authority to supervise them. Furthermore, many national cybersecurity strategies are unclear about what actions should be taken and their objectives.³⁰ Differences in the powers of investigative agencies, the range of jurisdiction in criminal cases, and intermediary services also present loopholes for transnational crime organizations to exploit.³¹

Figure 1. Relationship between scam encounters and the national cybersecurity score



Source: GASA Global State of Scams Report 2024; (Scam encounters), and The Global Cybercrime Report 2024 (National Cybersecurity Score)

Furthermore, digitally mature countries may be more susceptible to online scam cases in terms of frequency and volume. Figure 2 illustrates that countries with higher internet penetration are more likely to encounter scams and greater losses per capita. Digitally mature countries are increasingly vulnerable, as rising digital frauds and scams in high-growth markets shows how digitalization enables fraudsters to operate with greater agility.³² In countries with high levels of digital literacy, like Singapore, overconfidence in identifying

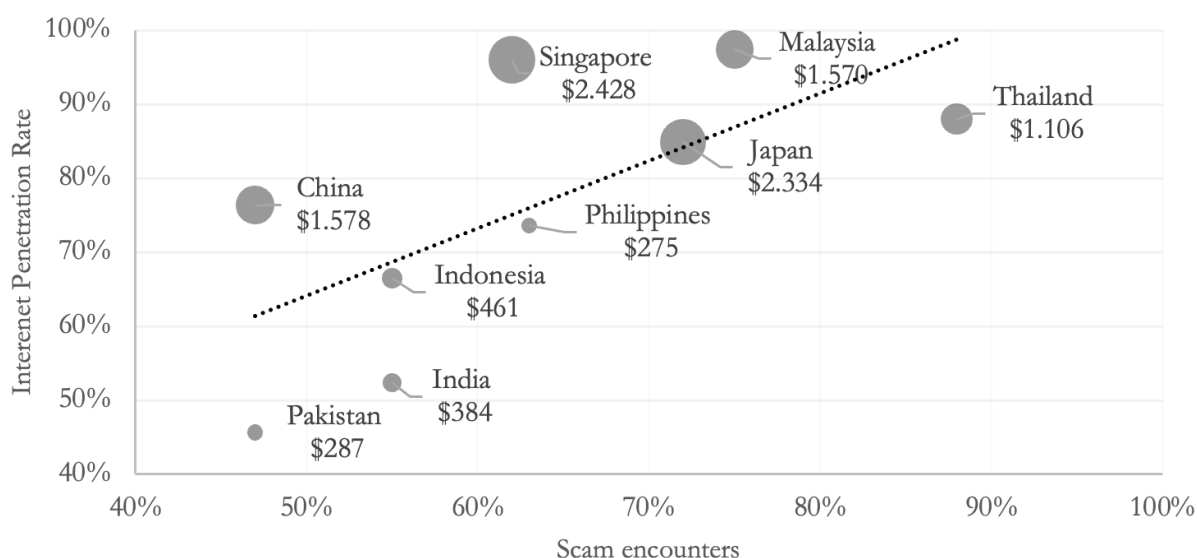
³⁰ Allison Peters and Amy Jordan, "[Countering the Cyber Enforcement Gap: Strengthening Global Capacity on Cybercrime](#)" 10 (May 2020).

³¹ Sylvia Mercado Kierkegaard, "Cracking Down On Cybercrime Global Response: The Cybercrime Convention," *Communications of the IIMA* 5, no. 1 (January 5, 2015), <https://doi.org/10.58729/1941-6687.1255>

³² Bank for International Statements, "[Digital Fraud and Banking: Supervisory and Financial Stability Implications](#)," November 2023

scams can also be a factor that increases vulnerability to being a victim of online scams.³³ Additionally, wealthier countries are also targets of fraud due to their relative wealth.³⁴

Figure 2. Relationship between scam encounters and the internet penetration rate



Source: [GASA Global State of Scams Report 2024](#); (Scam encounters and fraud loss per capita), and [Datareportal](#) (Internet penetration rate 2024)

Domestic and International Policy Responses in APAC Region

As online frauds and scams continue to advance rapidly, countries in the APAC region are responding with varying regulatory measures to mitigate risks (See Table 1). Consumer protection, privacy, data-sharing frameworks, anti-scam centers and others are essential pillars of strong internet governance. Hence, having each components is an important first step for countries to effectively address online fraud and scams. As we can see in Table 1, all countries have enacted consumer protection laws to ensure fair trade and safeguard the public against deceptive transactions. Cases of data-sharing mechanisms between government bodies or within public-private partnerships, and public scam awareness campaigns were also found to be evident in every country. It is important to note that public

³³ Joanna Octavia, "[Online Fraud and Scams in Singapore](#)," May 2025.

³⁴ Basel Governance, "[Basel AML Index 2024: 13th Public Edition Ranking Money Laundering Risks around the World](#)," November 2024.

information on data-sharing frameworks for scam-specific cases is limited, making it challenging to map domestic readiness against online scams in this aspect.

However, the remaining half of the pillars remain fragmented between countries. In terms of personal data protection, Cambodia, Myanmar, and Pakistan have not enacted laws that cover most of the OECD's basic data protection principles, which include collection and usage limitation, data quality, purpose specification, security safeguards, and accountability.³⁵ Furthermore, countries that do not have a designated anti-scam center generally handle scam cases and data sharing through the police or a security agency under a broader cybercrime unit, which can result in a lack of focus and reduced effectiveness. While asset-tracing mechanisms for illicit funds exist, they are generally enacted under an Anti-Money Laundering (AML) law or a Criminal Act.

Table 1. A comparison table of anti-scam regulatory measures among countries in the APAC region

| Country | Consumer Protection Law | Personal Data Protection Law | Designated Anti-Scam Center ¹ | Asset Tracing Framework for Illicit Funds ² | Data Sharing Frameworks for Financial Crime ³ | Public Scam Awareness Campaign |
|-----------|-------------------------|------------------------------|--|--|--|--------------------------------|
| Australia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Brunei | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Cambodia | ✓ | | | ✓ | ✓ | ✓ |
| China | ✓ | ✓ | | ✓ | ✓ | ✓ |
| India | ✓ | ✓ | | ✓ | ✓ | ✓ |
| Indonesia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Japan | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Laos | ✓ | ✓ | | | ✓ | ✓ |

³⁵ OECD, *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (OECD, 2002), <https://doi.org/10.1787/9789264196391-en>.

| | | | | | | |
|-------------|---|---|---|---|---|---|
| Malaysia | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Myanmar | ✓ | | | | ✓ | ✓ |
| Pakistan | ✓ | | | | ✓ | ✓ |
| Philippines | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Singapore | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| South Korea | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Thailand | ✓ | ✓ | ✓ | ✓ | ✓ | ✓ |
| Vietnam | ✓ | ✓ | | | ✓ | ✓ |

[1] Officially established scam units that are not under a criminal or cybercrime unit

[2] Enacted laws or official platforms that include the freezing, seizing, tracing, or recovery of illicit funds

[3] Enacted laws or official platforms that facilitate data sharing to address financial crimes

In addition, the absence of clearly designated key actors to lead efforts against online frauds and scams remains a challenge. We mapped the key actors and their roles in mitigating and tackling online scams in the region, where online scams generally fall under the duties and functions of multiple institutions (See Table 2). We found that overlapping jurisdictions can be observed within the same countries and across borders. In the Philippines, the Department of Information and Communications Technology oversees three other offices that coordinate, ensure compliance, and provide reporting mechanisms for online scams. However, the Department of Justice also has an office of cybercrime, the national police has an Anti-Cybercrime Group, and the National Bureau of Investigation has a cybercrime division. A similar pattern exists in neighboring countries, where most roles may not be mutually exclusive. The lack of a single point of contact in these regions leaves foreign partners uncertain about whom to approach for international cooperation.

Table 2. Table of key actors and their roles in online scams in the APAC region

| Country | Key Actors | Roles in Online Scams |
|-----------|--|---|
| Australia | Australian Competition and Consumer Commission (ACCC) | Leads the National Anti-Scam Centre of Australia (NASC) |
| | Australian Signals Directorate (ASD) | Prevent and disrupt offshore cyber-enabled crime; runs the Australian Cyber Security Centre; coordinates with NASC |
| | Australian Federal Police (FPD) | Enforcing criminal law; leads the Joint Policing Cybercrime Coordination Centre; coordinates with NASC. |
| | Australian Transaction Reports and Analysis Centre (AUSTRAC) | Involved when online scams use money laundering techniques to transfer and layer the criminal proceeds; coordinates with NASC. |
| | Australian Securities and Investments Commission (ASIC) | Regulate and enforce scams related issues in financial products and services, such as the taking down of investment scam websites, and evaluation over banks' scam prevention mechanism; seek civil penalties and prosecute offenders for the purpose of consumer protection in financial products and services; coordinates with the NASC. |
| | Australian Communications and Media Authority (ACMA) | Register and enforce rules to the telecommunications sector on scams issues; coordinate with the NASC. |
| India | Indian Cyber Crime Coordination Centre (I4C) | <ul style="list-style-type: none"> • Tracks transnational scam networks • Trains police in AI fraud detection |
| | CERT-In (Indian Computer Emergency | <ul style="list-style-type: none"> • National nodal agency for cybersecurity threats • Issue alerts on AI scams • Coordinates with ISPs to block fraudulent domains |

| | | |
|-----------------|--|---|
| | Response Team) | |
| | Ministry of Electronics & IT (MeitY) | <ul style="list-style-type: none"> • Coordinate formulate AI and cybersecurity policies • Regulates digital platforms |
| | Reserve Bank of India (RBI) | <ul style="list-style-type: none"> • Safeguards financial systems from AI fraud • Mandates fraud detection for banks |
| | Securities and Exchange Board (SEBI) | <ul style="list-style-type: none"> • Prevents stock market fraud via AI • Monitors fake investment schemes |
| Indonesia | Financial Services Authority (OJK) | <ul style="list-style-type: none"> • Established a multi-sectoral task force called SATGAS PASTI (including the Ministry of Investment, the Ministry of Communication and Digital Affairs, the Ministry of Cooperatives, the National Police, the State Intelligence Agency (BIN), the National Cyber and Crypto Agency (BSSN), and others) to coordinate in combating scams. • The SATGAS PASTI task force established the Indonesia Anti-Scam Center (IASC), providing a platform for the public to report scam activities easily. • Outlined four main pillars (prevention, detection, enforcement, and assessment) for FIs to establish anti-fraud strategies. |
| | Government of Indonesia | <ul style="list-style-type: none"> • Launched the “National Strategy for Artificial Intelligence,” providing a guideline to develop AI from 2020 to 2045 with five priority sectors (health services, bureaucratic reform, education and research, food security, and mobility and smart cities). |
| The Philippines | Department of Information and Communications Technology (DICT) | <ul style="list-style-type: none"> • Oversees policies and programs related to the development of the national ICT sector, data privacy, security, and confidentiality • Develops cybersecurity policies that prevent, address, and minimize cyber threats and attacks |

| | | |
|--|--|---|
| | | <ul style="list-style-type: none"> Facilitates countermeasures to address domestic and transnational cyber cases Monitors cybercrime cases handled by law enforcement agencies <p><i>Includes the following offices:</i></p> <ul style="list-style-type: none"> Cybercrime Investigation and Coordinating Center (CICC): Develops and employs coordinating procedures for law enforcement agencies, the telecommunication industry, and relevant key stakeholders to collaborate in the enforcement, prevention, and investigation of cybercrime. National Telecommunications Commission (NTC): Monitors potential data privacy violations in the collection, storage, processing, and use of personal data, while ensuring individuals and organizations comply with the Data Privacy Act. National Privacy Commission (NPC): Regulates all telecommunications services and facilitates reporting mechanisms for users and providers to report online scam incidents. |
| | Bangko Sentral ng Pilipinas (BSP) | <ul style="list-style-type: none"> Develops, implements, and monitors policies and regulations to guide BSFIs in cybersecurity-related concerns Assists in mediating complaints between BSP-supervised Financial Institutions (BSFIs) and consumers |
| | Department of Trade and Industry (DTI) | <ul style="list-style-type: none"> Develops policies, monitors, and oversees e-commerce transactions Handles consumer complaints about unfair trade practices |
| | Department of Justice – Office of Cybercrime (DOJ-OOC) | <ul style="list-style-type: none"> Handles the prosecution of cybercrime cases, including online scams, that violate the provisions of the Cybercrime Prevention Act Responsible for international cooperation on legal assistance and extradition, which may involve resolving issues related to cross-border fraudulent transactions |
| | Anti-Money Laundering Council (AMLC) | <ul style="list-style-type: none"> Has no mandate to prevent online scams but provides initiatives to create infographics for public awareness. |

| | | |
|-----------|--|---|
| | Philippine National Police – Anti-Cybercrime Group | <ul style="list-style-type: none"> Enforces laws, conducts cybercrime investigations, including online scams, and raises public awareness against online fraud |
| | National Bureau of Investigation - Cybercrime Division | <ul style="list-style-type: none"> Investigate investment scams, cybercrime, and other types of online scams |
| Singapore | Singapore Police Force (SPF) | <ul style="list-style-type: none"> Established the Anti-Scam Command (ASCom), a dedicated unit within the SPF that coordinates efforts across various agencies to address scams in real time. Collaborates with key stakeholders to develop technologies, such as deepfakes detection with the Home Team Science and Technology Agency (HTX) and the Robotic Process Automation technology, successfully recovering losses from online scams. |
| | Ministry of Communications and Information (MCI) | <ul style="list-style-type: none"> Surveyed to identify scam awareness among Singaporeans |
| | Ministry of Home Affairs | <ul style="list-style-type: none"> Launched large-scale national anti-scam campaigns, such as the 'I can ACT against scams,' disseminated across TV, radio, posters, digital ads, and the local news. Launched the ScamShield app with the SPF, the National Crime Prevention Council, and Open Government Products. |
| | Monetary Authority of Singapore (MAS) | <ul style="list-style-type: none"> Established the Shared Responsibility Framework (SRF) to complement legislative efforts by distributing accountability for phishing scams between consumers, financial institutions, and telecommunication operators. |
| | The Cyber Security Agency of Singapore | <i>Mentioned as an information reference, but its roles are not explicitly stated in the document</i> |
| | Ministry of Digital Development and | <i>Mentioned as an information reference, but its roles are not explicitly stated in the document</i> |

| | Innovation (MDI) | |
|-------------|---|--|
| South Korea | Office of Government Policy Coordination | <ul style="list-style-type: none"> Launched the “Whole-of-Government Task Force on Telecommunication Financial Fraud Response” with the Ministry of Science and ICT, the Korea Communications Commission, and the National Policy Agency |
| | National Police Agency | <ul style="list-style-type: none"> Established a ‘Cyber Crime Reporting System,’ especially effective when tackling organized fraud enablers |
| | Financial Service Commission (FSC) | <ul style="list-style-type: none"> A government agency with statutory authority over financial policy and regulatory supervision |
| | Financial Supervisory Service (FSS) | <ul style="list-style-type: none"> A specially legislated quasi-government supervisory authority charged with financial supervision across the entire financial sector. In terms of anti-scam activities, their primary role is consumer protection and preventing voice phishing. |
| | Ministry of Science and ICT and the Ministry of Interior and Safety | <ul style="list-style-type: none"> Coordinate policies with the Office for Government Policy Coordination (OGPC) by allocating budgets for public awareness programs, campaigns, and other supportive initiatives. |
| | Korea Internet & Security Agency (KISA) | <ul style="list-style-type: none"> An organization promoting internet and information security, founded in 2009. Operates ‘Boho Nara & KrCERT/CC’ to countermeasure hacking and virus attacks, developing technical responses to attack tools. For individuals, this operation offers smishing and quishing verification services targeting corporations and entities, as well as small and medium-sized enterprises (SMEs). |
| | Korea Institute of Finance (KIF) | <ul style="list-style-type: none"> Leads research to advance the financial industry and facilitate the realization of the ‘Information Age’ across the financial sector. |
| | Korea Financial Crime Prevention | <ul style="list-style-type: none"> Established to research and counteract serious financial crimes, promoting awareness of the risks |


| | Association (KFCPA) | and effective prevention methods to the public to prevent the spread of damage. |
|--------|--|--|
| Taiwan | Financial Supervisory Commission (FSC) | <ul style="list-style-type: none"> • Promotes the establishment of mechanisms to detect and flag financial accounts suspected of fraudulent activities, while the mandatory reporting and collaboration among financial institutions facilitate the tracking and freezing of fraudulent accounts • Has an alliance with the Ministry of Digital Affairs and several partners in the financial industry in Taiwan, including 35 banks • Is considering new legislation to regulate the cryptocurrency industry, where all VASPs would be classified as financial institutions, and personal trading would be prohibited once the law is enacted. |

Source: Safer Internet Lab., "[Online Fraud and Scam Trends Across APAC](#)," June 2025.

Meanwhile, the proliferation of online scams across transnational borders calls for cross-border efforts in the region. However, the absence of a unified definition regarding what constitutes an online scam remains a challenge in determining the boundaries of this discussion. Differing terms were used across documents, from "cybercrime", "telecom fraud", "digital fraud", "spam", "unsolicited messages", and "online threat", to "malicious intrusions."

In addition, scam units in these countries are housed differently, either under police forces, financial regulators, or other government bodies. For instance, Singapore's police force has an Anti-Scam Command center, Indonesia's Anti-Scam Centre is under the financial regulator, and South Korea's task force for telecommunication financial fraud is a part of the Office of Government Policy Coordination. The varying degrees of institutional power may impose further challenges, where a scam unit in one country may have more authority in law enforcement, supervision, or budget allocation than another (see Table 2).

To assess the region's commitment to combating scams, we identified seven main indicators, based on existing literature, drawn from cross-border MoUs, treaties, strategy documents, joint statements, and official press releases (see Table 3). According to these documents, we found that there is a clear recognition of cross-border coordination to combat scams across



these agreements. In the early 2000s, MLATs laid the groundwork for regions to cooperate in sharing certified records and confiscating properties related to crimes, with no explicit mention of scams. Since the 2020s, MoUs have begun to offer clearer protocols for online scams, such as sharing expertise through training programs, staff exchanges, and exchanging information on suspects, technical solutions, and best practices. In 2025, ASEAN has also formed a Working Group on Anti-Scams, which was modeled after successful initiatives in Singapore, Malaysia, and Thailand, providing specialized training courses and shared databases for scam-related intelligence.³⁶


Private sectors (such as Mastercard and Singtel) have also begun signing MoUs regarding their involvement in the technicalities of online scam prevention, such as providing access to real-time data. Private sector-led initiatives were also observed in neighbouring countries, such as Australia's Banking and Customer-Owned Banking Association, which provides a common threshold for addressing scams, and efforts made by fintech services, telecom providers, e-commerce, and social media platforms in detecting anomalies, flagging scam numbers, and detecting deepfake algorithms.³⁷

In many agreements, consumer protection was also implied in broader terms, such as "secure e-payments," "protection from cyber threats," and "trusted digital services." These documents place more emphasis on enforcement measures, such as supporting countries in maintaining laws that protect against fraudulent and deceptive commercial activities, reducing the number of scam messages, and integrating APIs to reduce fraud risk. However, enforcement-led mechanisms may lack responsive measures, such as providing financial safety nets or legal aid for victims. Additionally, asset-tracing commitments were rarely explicitly addressed, leaving more vulnerabilities to the public.

Furthermore, the lack of joint public awareness campaigns regarding scams is further reflected in GASA's Asia Scam Report 2024. It underscored the differing trends of scam awareness, where Japan, Thailand, and Malaysia were the least informed about AI threats, lagging behind other Asian countries. Moreover, the absence of cross-border asset-tracing agreements also results in differing reactive protocols, where China, Singapore, and Korea

³⁶ Muhammad Anas, "[ASEANAPOL Secretariat Hosts the First Working Group Meeting on Anti-Scam Operations](#)," ASEANAPOL, March 20, 2025.

³⁷ Safer Internet Lab., "[Online Fraud and Scam Trends Across APAC](#)," June 2025.



were more likely to fully recover scam losses, while Hong Kong and Pakistan believed they were less likely to do so.

While there is recognition of joint anti-scam measures to address scams, a clear directive to form a designated anti-scam task force is still rare. A key challenge is to ensure that these agreements translate into actionable steps, and the absence of a task force may present a lack of implementation power in these commitments, where documents may remain symbolic without tangible outcomes. This gap raises concerns about the accountability of bilateral and multilateral agreements, where fragmented mechanisms may hinder the agile responses needed to adapt to the dynamic nature of scams.


Table 3. Mapping of online scam commitments in the APAC region based on MoUs, treaties, and strategy documents

| Documents | Countries involved | Commit to Tackle Scams/Fraud | Cross-Border Coordination | Data or Info Sharing | Consumer Protection | Establish Task Force / Mechanism | Public Awareness Campaign | Asset Tracing |
|---|----------------------|------------------------------|---------------------------|----------------------|---------------------|----------------------------------|---------------------------|---------------|
| Bilateral MoUs / Agreements | | | | | | | | |
| Bank of Thailand – Bank Negara Malaysia MoU (2025) | Thailand, Malaysia | | | | | | | |
| The Office of the Communications Authority (OFCA) of Hong Kong and the Infocomm Media Development Authority (IMDA) of Singapore (2024)* | Singapore, Hong Kong | | | | | | | |
| The Infocomm Media Development Authority (IMDA) of Singapore and Malaysian | Singapore, Malaysia | | | | | | | |



| | | | | | | | | |
|--|------------------------|--|--|--|--|--|--|--|
| Communications and Multimedia Commission (MCMC) (2024)* | | | | | | | | |
| Singapore–Australia Digital Economy Agreement (All 8 MoUs 2022) | Singapore, Australia | | | | | | | |
| Ministry of Digital Economy and Society of Thailand and the Ministry of Posts and Telecommunications of Cambodia (2022)* | Thailand, Cambodia | | | | | | | |
| Australian Communications and Media Authority (ACMA)–NZ Department of Internal Affairs MoU (2024) | Australia, New Zealand | | | | | | | |

| | | | | | | | | |
|--|--|--|--|--|--|--|--|--|
| IMDA–ACMA MoU (2022) | Singapore, Australia | | | | | | | |
| Regional MoUs / Agreements | | | | | | | | |
| 5th ADGMIN Joint Media Statement (2025) – WG on Anti-Online Scams and CERT** | ASEAN member states | | | | | | | |
| ASEAN+3 Consumer Protection MoU (2024)*** | ASEAN + 3 | | | | | | | |
| Regional Comprehensive Economic Partnership (2024) | ASEAN Member States, Australia, China, Japan, Korea, New Zealand | | | | | | | |



| | | | | | | | | |
|--|--|--|--|--|--|--|--|--|
| ASEAN–China MoU on Non-Traditional Security (2017–2023) | ASEAN Member States, China | | | | | | | |
| SAARC MLAT (2008) | Afghanistan, Bangladesh, Bhutan, India, Maldives, Nepal, Pakistan, Sri Lanka | | | | | | | |
| ASEAN MLAT (2004) | ASEAN Member States | | | | | | | |
| Strategy documents | | | | | | | | |
| Regional Transnational Organised Crime Disruption Strategy | Pacific Islands Forum | | | | | | | |



| | | | | | | | | |
|---|-----------------------------|--|--|--|--|--|--|--|
| (2024–2028) | Member Countries | | | | | | | |
| APT Cooperation Work Plan 2023–2027 | ASEAN + China, Japan, Korea | | | | | | | |
| ASEAN Cybersecurity Cooperation Strategy (2021–2025) | ASEAN Member States | | | | | | | |
| ASEAN Plan of Action to Combat Transnational Crime (2012) | ASEAN Member States | | | | | | | |
| Private-sector-related documents | | | | | | | | |



| | | | | | | | | |
|--|---------------------------------|--|--|--|--|--|--|--|
| Singtel–AIS–Maxis MoUs on Telco API Federation for Scam Mitigation (2024)* | Singapore, Thailand, Malaysia | | | | | | | |
| Mastercard–ASEAN Foundation Cybersecurity Resilience MoU (2024)* | ASEAN member states, Mastercard | | | | | | | |

*Information acquired from the official press release

**Information acquired from a joint media statement

***Information acquired from a news article

Legend: **Green** indicates the pillar is explicitly mentioned, **orange** indicates it is implied or partially mentioned, and blank indicates the pillar does not exist in the document.

Way Forward


The rapid development of technology and internet adoption has opened more pathways for scammers to upgrade their methods with the latest advancements in cyberspace, allowing them to operate borderlessly across regions and exploit regulatory loopholes. In the Asia Pacific region, countries have enacted domestic safeguards to protect against online scams. However, these efforts alone were observed to exhibit varying degrees of data governance measures and institutional power among key stakeholders, and this challenge is further exacerbated by the lack of a comprehensive international commitment to cooperate with anti-scam efforts at the regional level.

While there is a clear acknowledgment of the importance of cross-border collaborations in this matter, existing agreements rarely outline the necessity of establishing a formal joint task force. As online scams were found to fall under the jurisdiction of multiple stakeholders, the absence of a centralized coordinating body may lead to overlapping and fragmented responses. Considering the cross-border nature of online scams, there are two alternatives that should be considered.

First, by establishing a joint task force to ensure a tangible strategic alignment, building a strong foundation, and harmonising standards to effectively facilitate data sharing, data protection, public education, and asset recovery mechanisms, among others. However, forming a new joint task force would be challenging, as it requires both the right momentum and strong regional leaders to drive its establishment.

An alternative would be to adapt and expand the existing ASEAN cooperation infrastructure to facilitate coordinated responses in tackling online scams, while ensuring strategic alignment with broader regional and international parties. For example, the likes of the “ASEAN+5” agreement can incorporate members of the APAC region to existing collaborations, such as ASEAN’s Working Group on Anti-Scams and CERT. Binding economic agreements, such as the RCEP framework, can also be leveraged as an entry point to establish shared protocols, standards, and response mechanisms.

As a first step to promote this cooperation, the broad scope and definition of scams across official documents, scholarly articles, and industry reports must be recognized. With the absence of regional standardization, scammers are likely to take advantage of regulatory



gaps by migrating operations to countries with weaker enforcement systems. Thus, this concern calls for the urgency to harmonize anti-scam regulations or legislative frameworks, creating a robust governance system that leaves scammers no gaps to seep in.

At the domestic level, countries can benefit from appointing a single point of contact to coordinate anti-scam efforts not only at the domestic level but also at the multilateral and regional levels to strengthen international cooperation. This centralized body will oversee inter-agency collaboration, and they are expected to lift bureaucratic burdens, such as reducing coordination delays and strengthening institutional accountability. Additionally, this initiative not only streamlines the coordination flow for institutions, but it can also be a top-of-mind contact for the public to reach out to report scams and support anti-scam operations directly.



INFORMATION RESILIENCE & INTEGRITY SYMPOSIUM

Generative AI and Information Resilience
in the Asia-Pacific: Actions and Adaptations

➤ Faculty of Social and Political Sciences
Universitas Gadjah Mada

➤ 21 August 2025