

Workshop Summary Report: APEC Workshop on Combatting Online Fraud and Scams

APEC Digital Economy Steering Group

September 2026



**Asia-Pacific
Economic Cooperation**



**Asia-Pacific
Economic Cooperation**

**Workshop Summary Report:
APEC Workshop on Combatting
Online Fraud and Scams**

Digital Economy Steering Group (DESG)

September 2026

APEC Project: DESG 01 2026S

Produced by
National Center for APEC
601 Union St, Suite 1701
Seattle, WA, 98001, United States
Telephone: (+1) 206-441-9022
Email: office@ncapec.org
Website: www.ncapec.org

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

© 2026 APEC Secretariat

APEC#226-CT-04.10

Table of Contents

I. EXECUTIVE SUMMARY	4
II. INTRODUCTION.....	6
III. BACKGROUND.....	6
IV. KEY ISSUES.....	7
1. COMBATTING ONLINE FRAUD AND SCAMS IN FINANCIAL INSTITUTIONS	7
2. COMBATTING ONLINE FRAUD AND SCAMS IN TELECOMMUNICATIONS	10
3. COMBATTING ONLINE FRAUD AND SCAMS IN DIGITAL PLATFORMS.....	12
V. CONCLUSION.....	14
ANNEX A – “KEY TRENDS SHAPING THE FUTURE OF SCAMS AND FRAUD” PRESENTATION BY WANJING JI, HEAD OF PAYMENT ECOSYSTEM RISK, ASIA PACIFIC, VISA	16
ANNEX B – “AI-BASED VOICE PHISHING PREVENTION POLICY” PRESENTATION BY SUNUP PARK, DEPUTY DIRECTOR AT THE PERSONAL INFORMATION PROTECTION COMMISSION (PIPC) OF THE REPUBLIC OF KOREA	22
ANNEX C – “ASEAN GUIDE ON ANTI-SCAM POLICIES AND BEST PRACTICES” BY EVELYN GOH, DIRECTOR, INTERNATIONAL RELATIONS, POLICY AND STRATEGY, INFOCOMM MEDIA DEVELOPMENT AUTHORITY, SINGAPORE	30
ANNEX D – “COMBATTING SCAMS AND FRAUD IN TELECOMMUNICATIONS” BY DARYL TEO, MANAGER, ECONOMICS STRATEGY, ACCESS PARTNERSHIP	36
ANNEX E – “FIGHTING SCAMS IN SINGAPORE THROUGH PUBLIC-PRIVATE PARTNERSHIPS” BY EVELYN GOH, DIRECTOR, INTERNATIONAL RELATIONS, POLICY AND STRATEGY, INFOCOMM MEDIA DEVELOPMENT AUTHORITY, SINGAPORE.....	38

I. Executive Summary

On 4 February, the National Center for APEC (NCAPEC), in partnership with Australia's Department of Foreign Affairs and Trade, organized the APEC DESG workshop "Combating Online Fraud and Scams" on the margins of the first APEC 2026 Senior Officials' Meeting (SOM1).

Sponsored by Australia and co-sponsored by Indonesia, Singapore, and the United States, the workshop brought together government officials, financial institutions, telecommunications providers, digital platforms, and international organizations to tackle one of the fastest-growing threats to the digital economy, online scams and fraud.

The speakers included:

- Wanjing Ji, Asia Pacific Head of Ecosystem Risk, Visa
- Justin Liu, Head, China Government Affairs and Public Policy, PayPal
- Stanley Wu, Head, Financial Crime Compliance, Hong Kong, China, Standard Chartered Bank
- Evelyn Goh, Director, International Relations, Policy and Strategy, Infocomm Media Development Authority (IMDA), Singapore
- Sunup Park, Deputy Director, Personal Information Protection Commission (PIPC), Republic of Korea
- Daryl Teo, Manager, Economics Strategy, Access Partnership
- Jennifer Chien, Economic Policy Manager, APAC, Meta
- Andrei Skorobogatov, Director of Policy, Global Anti-Scam Alliance

As online scams continue to grow in scale and sophistication, driven by digitalization, emerging technologies, and their cross-border nature, the discussion underscored the urgency of coordinated action. The key takeaways from the discussion are:

- **Scams Are Increasingly Industrialized and Cross-Border:** Fraud operations run by criminal scam syndicates are becoming highly organized, technology-enabled, and coordinated across borders, making detection and enforcement significantly more complex for individual economies acting alone.
- **AI Is Reshaping Both Threats and Defenses:** Scammers are rapidly adopting AI-enabled tools such as impersonation, voice phishing, and automated targeting, while financial institutions, telecommunications providers, and digital platforms are deploying advanced analytics and AI-driven monitoring to detect suspicious activity earlier in the fraud lifecycle.
- **Whole-of-Ecosystem Collaboration Is Essential:** Effective responses require timely and coordinated engagement across governments, financial institutions, telecommunications operators, digital platforms, and international organizations, as each actor sees only a portion of the threat landscape.
- **Intervention across the scam ecosystem is necessary:** Participants emphasized collaborating to detect fraudulent activity across the value chain according to where each ecosystem player has visibility into the scam, through ecosystem-wide intelligence sharing and timely and coordinated prevention measures.
- **Cross-Border Cooperation and Scalability Are Critical:** The transnational nature of scams and criminal scam syndicates requires greater government-to-

government cross-border coordination, scalable data-sharing mechanisms beyond bilateral approaches, and more aligned regulatory approaches to prevent regulatory gaps that criminals exploit.

- **Balancing Protection and Innovation Remains a Key Challenge:** Anti-scam measures must be flexible and proportionate while maintaining privacy protections, minimizing unnecessary friction for legitimate users, preserving trust in digital services, and supporting private sector growth and innovation.
- **Consumer and SME Protection Requires Sustained Education and Capacity Building:** Public awareness campaigns, targeted SME support, and accessible prevention tools are necessary to reduce exposure among the groups most vulnerable to scams, including victims of human trafficking and forced criminality in scam centers.

The panelists recommended:

- Strengthening public-private collaboration, regional information sharing frameworks and cross-sector coordination mechanisms will improve the ability to detect and disrupt evolving scam typologies and criminal scam networks.
- Promoting balanced, proportionate, and scalable anti-scam tools and policy approaches can help economies and industries close cross-border enforcement gaps and improve collective resilience, while supporting digital access and innovation. The data and resources available across the ecosystem could be better leveraged to detect and disrupt scams, and to target friction more precisely at bad actors.

Future APEC and ABAC work should support the development of practical good-practice frameworks, capacity-building initiatives, and public-private cooperation models to combat online fraud and scams across the region.

For more information, please contact Olivia Myhre, Policy Associate at the National Center for APEC.

Introduction

The Digital Economy Steering Group (DESG) Workshop on Combatting Online Fraud and Scams was held on 4 February 2026 on the margins of the First Senior Officials Meeting in Guangzhou, People's Republic of China. The event was organized by the National Center for APEC (NCAPEC), in partnership with the Australian Department of Foreign Affairs and Trade (DFAT). The workshop was sponsored by Australia and co-sponsored by Indonesia, Singapore, and the United States. Speakers included:

- Wanjing Ji, Head of Payment Ecosystem Risk, Asia Pacific, Visa
- Justin Liu, Head, China Government Affairs and Public Policy, PayPal
- Stanley Wu, Head, Financial Crime Compliance, Hong Kong, China, Standard Chartered Bank
- Evelyn Goh, Director, International Relations, Policy and Strategy, IMDA, Singapore
- Sunup Park, Deputy Director, Personal Information Protection Commission (PIPC), ROK
- Daryl Teo, Manager, Economics Strategy, Access Partnership
- Jennifer Chien, Economic Policy Manager, APAC, Meta
- Andrei Skorobogatov, Director of Policy, Global Anti-Scam Alliance

Participants included APEC government officials, private sector representatives, industry associations, and academic experts.

Through three panels, each focusing on a major avenue through which scammers are able to reach consumers, this workshop brought together stakeholders to share best practices, identify opportunities for collaboration, and strengthen the collective response to scams and fraud. Its goal was to better equip APEC economies with the tools to combat scams both domestically and across the region.

II. Background

With the rise of digital technology, the sophistication and prevalence of digital fraud and scams have also grown. While text messages, emails, and calls remain common vectors for scammers, today's fraudulent activity spans the entire digital ecosystem, impersonating household names and brands, including online marketplaces, while operating on financial services platforms, and social media, and impacting lives in the physical world. Nonetheless, the near-constant barrage of fraudulent activity and threats within the digital ecosystem also presents opportunities for earlier detection and intervention by entities with visibility and agency in these spaces.

Consumers can no longer be expected to protect themselves from all of the potential harm they encounter online on a daily basis. They are no longer battling a single perpetrator on the other side of a screen but a network of organized crime. Thus, more comprehensive and systematic protection is needed, which requires the cooperation of governments, law enforcement, businesses, and consumer groups. Pursuing this level of protection is essential, as consumer trust is critical for the growth of digital economies and realizing the potential of digital trade. Declining consumer trust heavily impacts SMEs in particular, as they are much less likely to be able to access and properly utilize the tools needed to protect consumers

online. Instead, they become indirect victims of the one trillion dollar (USD) international fraud industry as of 2024, according to the Global Anti-Scam Alliance.

Governments across the APEC region must strengthen cooperation with one another while also enhancing collaboration with industry stakeholders to better protect citizens and businesses from increasingly sophisticated digital fraud and scams. The cross-border nature of these crimes makes enforcement particularly challenging, as perpetrators often exploit jurisdictional gaps and operate across multiple economies. Without comprehensive and compatible legal frameworks, effective mechanisms for international cooperation, and sufficient technical capabilities, particularly in economies with fewer resources, consumers remain vulnerable to evolving online threats. At the same time, governments often depend on private sector entities for access to the critical data, intelligence, and operational insights needed to investigate and prosecute these crimes effectively. Addressing these challenges requires a coordinated, multi-stakeholder approach that prioritizes legal alignment, technical capacity building, cross-border cooperation, and trusted public-private collaboration. This project directly supports APEC's overarching priorities on innovation, digitalization, and sustainable growth for all. It aligns with the APEC Putrajaya Vision 2040, particularly the pillar on Innovation and Digitalization, recognizing that scams and fraud undermine the trust and integrity essential for realizing the digital economy's full potential. The project contributes to APEC's goal of fostering a trusted and resilient digital ecosystem for all that enables economic growth.

The project also advances the Aotearoa Plan of Action, under the Innovation and Digitalization driver, by promoting interoperable and harmonized policy frameworks that encourage cross-border cooperation and public-private collaboration to strengthen digital trust and consumer protection.

Furthermore, the project aligns with the objectives of the APEC Internet and Digital Economy Roadmap (AIDER) by promoting interoperability, supporting the development of holistic policy frameworks for the Internet and Digital Economy, fostering coherence among regulatory approaches, and enhancing trust and security in the use of digital technologies. It also contributes to APEC's efforts to facilitate the free flow of information and data consistent with domestic laws and to advance cooperation on e-commerce and digital trade. Through these efforts, the project reinforces APEC's shared commitment to a secure digital future for all across the Asia-Pacific region.

III. Key Issues

1. Combatting Online Fraud and Scams in Financial Institutions

Wanjing Ji, Head of Payment Ecosystem Risk for Asia Pacific at Visa, opened the discussion by outlining several key trends shaping the evolution of online fraud and scams. She began by clarifying the distinction between fraud and scams within the payments ecosystem. Fraud generally involves unauthorized transactions conducted without the victim's knowledge, such as through stolen credentials. Scams, by contrast, involve authorized payments in which victims are manipulated into handing over their payment credentials or transferring funds voluntarily through deception. This distinction is important

for both regulatory and technological responses, as scams rely heavily on social engineering rather than direct technical compromise.¹

Ji emphasized that contemporary scams increasingly resemble industrialized, rather than isolated operations. Organized networks operate with sophisticated infrastructure, automated tools, and coordinated operational structures that mirror legitimate business processes. Fraud operations have become strategic, automated, and scalable, with criminal actors leveraging artificial intelligence to accelerate outreach, personalize communications, and automate cyberattacks. Based on Visa's analysis of observed trends, the number of leaked accounts recovered by the company increased by more than 220 percent in the first half of 2025.² Criminal organizations are also adapting their tactics strategically, often stockpiling stolen credentials over long periods before monetizing them quickly once an opportunity emerges. Another significant trend highlighted in the presentation was the global expansion of scam compounds and the increasingly transnational nature of fraud operations.³ These compounds, reported in public and industry sources to be associated with organized criminal networks, rely on layered structures distributing tasks across individuals and jurisdictions. Some workers are reported as having been trafficked or coerced into participating in scams, while others may knowingly engage in specific roles such as initiating calls, opening financial accounts, or processing transactions. This compartmentalized structure enables organizers to conceal their identities and shield core operations from enforcement. Ji illustrated how scam networks may operate across multiple jurisdictions simultaneously, using legitimate front businesses and complex financial pathways to obscure illicit activity.

Ji also noted that scams often change their modus operandi, for example by relying on small, incremental transactions that are less likely to trigger fraud detection systems. In some cases, scammers initially provide small financial returns to victims in order to build trust before requesting larger transfers. These tactics complicate detection and enforcement because victims often perceive early interactions as legitimate. The use of highly personalized information, urgency, and authority can make even highly educated individuals susceptible to deception.

To illustrate Visa's response to the scale and complexity of these operations, Ji described Visa's Scam Disruption Practice, which analyzes payment transaction data alongside other signals such as IP addresses, while complying with applicable privacy requirements, to identify suspicious patterns across networks. Through this approach, Visa has contributed to mapping scam infrastructure and disrupting potential fraudulent merchant networks at scale. In one case study, nearly 12,000 potentially fraudulent merchant entities were identified and this prevented losses of over USD 37 million in fraud.⁴ These efforts demonstrate the importance of proactive detection and intelligence gathering across the payments ecosystem and the increasing ability of the ecosystem to respond at scale.

Ji concluded by emphasizing that combating scams and fraud requires an ecosystem-wide response. Because scams span telecommunications networks, digital platforms, and financial systems, no single institution can effectively address the problem in isolation. Instead,

¹ See Annex A, slide 2

² See Annex A, slide 4

³ See Annex A, slide 5

⁴ See Annex A, slide 10

stronger public–private collaboration and a shared responsibility across ecosystem stakeholders are necessary to protect consumers and maintain trust in digital financial services.

Following her presentation, Ji joined **Justin Liu, Head, China Government Affairs and Public Policy, PayPal**, and **Stanley Wu, Head, Financial Crime Compliance, Hong Kong, China, Standard Chartered Bank**, in a panel discussion that expanded on these themes by examining how regulators and industry actors assess risk and coordinate responses to scams within the financial ecosystem. Panelists noted that both governments and financial institutions increasingly rely on data-driven risk measurement to identify emerging threats. Governments play a critical role in enabling information-sharing infrastructure that allows financial institutions, regulators, and other stakeholders to exchange intelligence on fraudulent activity. In Hong Kong, China, for example, legislative reforms have been introduced to enable government-to-government data sharing platforms that support more effective coordination in combating scams.

Participants also discussed emerging technological approaches to fraud detection. One example highlighted during the discussion was a pilot program in the United Kingdom that applies artificial intelligence to ecosystem-wide data in order to generate real-time risk scores that helps sending and receiving institutions to identify suspicious transactions within account-account payment flows. These models draw on information from multiple participants within the financial ecosystem, allowing financial institutions to identify anomalies earlier in the fraud lifecycle. In addition, financial institutions are experimenting with large language model architectures to map emerging scam patterns and identify new typologies as they appear. However, panelists also emphasized that technological innovation introduces new trade-offs. Panelists noted that as digital payments scale, consumer and merchant expectations increasingly center on seamless, instantaneous experiences. From a network perspective, these expectations must be balanced with robust fraud and security controls, even where this adds steps to the user journey.

The discussion also explored how AI is enabling agent-driven transactions, with intelligent systems increasingly initiating and managing purchases on behalf of users. Panelists noted that while these systems can facilitate fraud detection by enabling analysis of behavioral patterns across the customer journey, they also introduce new considerations around trust, governance, oversight, and accountability in automated decision-making, as well as data privacy.

In this context, participants emphasized that trust must be designed into the ecosystem from the outset. As commerce becomes more agent-driven, merchants need a reliable way to verify who an agent is, confirm it is acting on behalf of a legitimate consumer, and ensure interactions remain secure and authentic. Frameworks such as Visa’s Trusted Agent Protocol were highlighted as an example of how identity, intent, and legitimacy can be clearly established, enabling secure communication between agents and merchants while preserving existing systems and customer relationships.

Looking ahead, the panel outlined several priorities. Participants called for stronger government-led cross-border collaboration, reflecting the inherently transnational nature of scam operations. They also stressed that prevention must shift earlier in the lifecycle of fraud, particularly in agent-led environments, focusing on identifying suspicious activity or

compromised interactions before a transaction is executed. In addition, panelists highlighted the need for greater interoperability of protection mechanisms across financial institutions and ecosystem participants to ensure consistent, coordinated safeguards grounded in shared trust frameworks. Strengthening coordination across detection tools and data-sharing will be essential to improving collective resilience against increasingly sophisticated scams.

2. Combatting Online Fraud and Scams in Telecommunications

The telecommunications session began with context-setting presentations from **Sunup Park, Deputy Director at the Personal Information Protection Commission (PIPC) of the Republic of Korea; Evelyn Goh, Director of International Relations, Policy and Strategy at the Infocomm Media Development Authority (IMDA) of Singapore; and Daryl Teo, Manager of Economics Strategy at Access Partnership.** These presentations established key regulatory, technical, and economic dimensions of scam activity within telecommunications networks, and were followed by a panel discussion that further explored the implications of these trends for policy and industry practice.

Sunup Park's presentation on Korea's approach to AI-based voice phishing prevention illustrated how governments can enable innovation through structured public-private collaboration. Korea has pursued a multi-layered framework combining legal, regulatory, and technical mechanisms to support the deployment of advanced detection systems. A key component of this approach is an inter-agency memorandum of understanding that facilitates the sharing of de-identified call data between government entities and telecommunications providers, enabling the development of machine learning models for detecting suspicious call patterns and voice characteristics.⁵ These models analyze call context, behavioral patterns, and voice data to identify potential phishing attempts, achieving reported detection accuracy rates exceeding 90 percent.⁶

Importantly, Korea's framework also incorporates regulatory innovation mechanisms, including the use of a regulatory sandbox and a prior adequacy review system. These tools allow companies to test AI-driven detection technologies, such as on-device voice recognition, under controlled conditions while ensuring compliance with privacy and data protection requirements. This reflects a broader recognition that effective scam prevention requires access to sensitive data, necessitating governance structures that enable data use while maintaining safeguards such as purpose specification, transparency, and accountability. The Korean model further emphasizes interoperability between telecommunications providers and financial institutions, with detection signals shared across sectors to enable coordinated responses to suspected fraud activity.

Evelyn Goh's presentation on the ASEAN Guide on Anti-Scam Policies and Best Practices developed by Singapore and ASEAN Members (AMS), situated these domestic efforts within a broader regional framework. The Guide was endorsed at the 6th ASEAN Digital Ministers' Meeting in January 2026 and is the region's first comprehensive framework for combatting scams over telecommunication channels. The Guide proposed a structured set of recommendations that could be adopted based on differing levels of technical and regulatory

⁵ See Annex B, slide 7

⁶ See Annex B, slide 10

maturity.⁷ Central to the framework is a tiered approach to implementation, allowing economies to adopt baseline protections, such as mandatory SIM card registration and basic in-network filtering of SMS messages, while progressively advancing toward more sophisticated measures, including AI-driven analytics and real-time threat detection.⁸ The Guide identifies several key intervention points within telecommunications networks. These include strengthening SIM card and equipment controls to limit anonymous or large-scale misuse of telecom infrastructure,⁹ implementing network-level defenses to block scam calls and SMS messages,¹⁰ and preventing identity spoofing through mechanisms such as caller ID authentication and SMS sender ID registries.¹¹ Singapore's experience with its SMS Sender ID Registry demonstrates the potential effectiveness of such measures, with scam cases reportedly declining significantly following its implementation.¹² Beyond technical controls, the Guide places a strong emphasis on regional information sharing and coordinated traceback mechanisms to address the inherently cross-border nature of scam operations. By promoting harmonization of safeguards and collaborative enforcement, the framework seeks to strengthen trust in telecommunications systems across the region.

Daryl Teo's presentation from Access Partnership complemented these policies and technical perspectives by examining the economic and structural challenges facing telecommunications operators. He highlighted that the global cost of scams and fraud is already estimated to exceed USD 1 trillion annually in direct financial losses, but broader societal impacts including erosion of trust in digital interactions and reduced participation in the digital economy remain unaccounted for from an economic standpoint and will amplify this negative impact for years to come.¹³ At the same time, telecommunications providers face growing pressure to invest in anti-fraud infrastructure, even as traditional revenue streams from voice and SMS services continue to decline.

This misalignment of incentives presents a structural challenge for the telecommunications sector. While operators are expected to play a frontline role in detecting and preventing scams, they often lack clear mechanisms to recoup the costs of these investments. As a result, fraud prevention becomes an increasing financial burden, potentially limiting the scalability and sustainability of anti-scam measures. Teo's analysis suggests that addressing scams effectively will require not only technical solutions but also policy interventions that better align incentives across stakeholders to enhance cross-stakeholder involvement and collaboration.¹⁴

The panel discussion that followed built on these presentations, with participants emphasizing the need for a coordinated, ecosystem-wide approach to addressing scams within telecommunications networks. A recurring theme was the importance of balancing security, privacy, and usability. While measures such as call blocking, identity verification, and expanded data sharing can significantly reduce scam activity, they may also introduce friction

⁷ See Annex C, slide 2

⁸ See Annex C, slide 4

⁹ See Annex C, slide 5

¹⁰ See Annex C, slide 7

¹¹ See Annex C, slide 8

¹² See Annex C, slide 9

¹³ See Annex D, slide 2

¹⁴ See Annex D, slide 3

or raise concerns regarding data protection. Participants noted that maintaining trust in telecommunications systems requires carefully calibrated approaches that protect users without undermining accessibility or user experience.

Panelists also underscored the importance of compatibility and cross-sector coordination, particularly between telecommunications providers, financial institutions, and digital platforms. Given that scams often originate in one sector and materialize in another, effective intervention depends on the ability to share information and act across institutional boundaries. In this context, regional and cross-border collaboration was identified as essential, as scam operations frequently exploit jurisdictional fragmentation to evade enforcement.

Overall, the telecommunications session highlighted that network-level interventions are a critical component of a broader strategy to combat online fraud and scams. Strengthening regulatory frameworks, enabling responsible data sharing, and aligning incentives across stakeholders will be essential to disrupting scam activity at its source and reinforcing trust in digital communications infrastructure across the APEC region.

3. Combatting Online Fraud and Scams in Digital Platforms

The digital platforms session opened with a context-setting video from **Andrei Skorobogatov of the Global Anti-Scam Alliance (GASA)**, followed by a presentation from **Evelyn Goh, Director of International Relations, Policy and Strategy at the Infocomm Media Development Authority (IMDA) of Singapore**. These interventions framed the role of digital platforms within the broader scam ecosystem and were followed by a panel discussion examining how platform governance, public-private collaboration, and technological innovation can be leveraged to combat online fraud.

The GASA video highlighted the global scale and systemic nature of scam activity, emphasizing that online fraud has evolved into a highly organized, transnational industry generating significant economic and social harm. Beyond direct financial losses, scams impose broader costs through erosion of trust in digital interactions, reduced participation in the digital economy, and increased operational burdens on both governments and businesses. The presentation underscored that no single actor can effectively address these challenges in isolation. Instead, coordinated, ecosystem-wide responses are required, supported by real-time information sharing and international collaboration.

Building on this global framing, Evelyn Goh's presentation provided a detailed account of Singapore's approach to addressing scams on digital platforms across the digital economy through a whole-of-society approach. She emphasized that high levels of digitalization and social trust, while enabling economic growth, also create conditions that have become exploited by malicious actors. In Singapore, scam incidents and associated losses had risen across recent years, reinforcing the urgency of strengthening trust in digital services.¹⁵

Singapore's response centers on close collaboration between government agencies, digital platforms, e-commerce marketplaces, telecommunications providers, and the public. This approach targets multiple points along the "scam chain," combining prevention, disruption, enforcement, and public education. A key policy instrument is the Online Criminal Harms

¹⁵ See Annex E, slide 2

Act, which enables authorities to require online platforms to implement safeguards against scams and to take action to remove harmful content.¹⁶ This reflects a broader shift toward stronger platform accountability in mitigating fraudulent activity.

In parallel, Singapore has introduced mechanisms to incentivize improved platform practices. The E-commerce Marketplace Transaction Safety Ratings system evaluates major platforms based on the effectiveness of their anti-scam measures, creating transparency and encouraging higher standards of consumer protection.¹⁷ Such approaches signal an increasing emphasis on embedding trust and safety considerations into platform governance frameworks.

Goh also highlighted the importance of upstream interventions designed to prevent scammers from reaching potential victims. These measures include securing communication channels in partnership with telecommunications providers and enhancing device-level protections. For example, the Cyber Security Agency of Singapore has collaborated with Google to pilot an enhanced fraud protection feature within Google Play Protect. In addition, the development of a Safe App Standard establishes best practices for application design, reducing the risk that vulnerabilities can be exploited by malicious actors.¹⁸

Technology plays a central role in Singapore's approach to scam disruption. The Scam Analytics and Tactical Intervention System (SATIS), developed through collaboration between government agencies, leverages artificial intelligence to identify and disable scam-related websites at scale.¹⁹ This capability is complemented by GovTech Singapore's participation in the Global Signal Exchange, an international information-sharing initiative which enables rapid dissemination of scam-related indicators across participating organizations. Through such mechanisms, digital platforms and public authorities can coordinate responses more effectively and reduce the time between detection and intervention.

A further dimension of Singapore's strategy is sustained investment in public education and awareness. Campaigns such as "I can ACT against scams" aim to empower individuals to adopt protective behaviors, verify suspicious communications, and report fraudulent activity. These efforts are supported by tools such as the ScamShield suite, which integrates reporting, alerting, and detection functions across multiple channels.²⁰ The emphasis on user awareness reflects recognition that even the most advanced technical safeguards must be complemented by informed and vigilant users.

Following this presentation, Goh joined **Jennifer Chien, Economic Policy Manager, APAC, Meta**, for a panel discussion that expanded on these themes, emphasizing the increasing collaboration with digital platforms in the scam ecosystem. Chien noted that platforms, alongside upstream and downstream ecosystem players, each serve as both a vector for fraudulent activity and a critical point of intervention. As such, platform governance frameworks must balance flexibility and accessibility with effective risk mitigation, to allow for room to innovate and stay ahead of rapidly evolving bad actor tactics. This includes

¹⁶ See Annex E, slide 3

¹⁷ See Annex E, slide 3

¹⁸ See Annex E, slide 4

¹⁹ See Annex E, slide 5

²⁰ See Annex E, slide 6

strengthening identity verification processes, improving content moderation systems, and enhancing transparency around enforcement actions.

A recurring theme was the importance of early, upstream intervention. Similar to discussions in the financial and telecommunications sessions, panelists emphasized that industry must collaborate to intervene at the earliest point in the scam attack chain. Interventions at the platform level, such as detecting fraudulent advertisements, disrupting scam communications, and removing malicious accounts, can significantly reduce the burden on downstream interventions to stop scam transactions.

The panelists also highlighted the importance of scalability and cross-sector coordination. Effective scam prevention depends on the ability to share signals across platforms, financial institutions, and telecommunications providers. Initiatives such as shared databases of scam indicators and collaborative intelligence platforms were identified as promising tools for strengthening ecosystem-wide resilience.

At the same time, participants acknowledged the challenges associated with expanding platform responsibilities. These include managing trade-offs between privacy and security, ensuring proportionality in regulatory requirements, and maintaining innovation within digital ecosystems. As with other sectors, maintaining user trust requires carefully calibrated approaches that provide robust protection without introducing excessive friction or undermining user experience and access to digital tools.

Overall, the digital platforms session reinforced the view that trust in digital services depends on coordinated action across multiple layers of the ecosystem. By integrating regulatory frameworks, technological innovation, public–private partnerships, and user engagement, economies can strengthen their ability to prevent and disrupt scams at scale. Continued collaboration within APEC and across international networks will be essential to ensuring that digital platforms remain secure, trustworthy, and conducive to sustained economic growth.

IV. Conclusion

The workshop “Combatting Online Fraud and Scams” underscored the scale, complexity, and systemic nature of online fraud as a growing threat to the digital economy in the Asia-Pacific. Across discussions spanning financial services, telecommunications, and digital platforms, a consistent picture emerged: scams are no longer isolated incidents but highly organized, technology-enabled, and increasingly transnational criminal syndicate operations that exploit gaps across sectors and jurisdictions. Addressing this challenge therefore requires coordinated, ecosystem-wide responses that extend beyond traditional enforcement approaches.

Discussions highlighted how scam operations have become increasingly industrialized, leveraging artificial intelligence, globalized infrastructure, and sophisticated social engineering techniques to scale their activities. These developments have made detection and enforcement more difficult, particularly as criminals adapt their tactics to evade existing safeguards. At the same time, rapid digitalization and the expansion of real-time services have increased both the opportunities for fraud and the speed at which harm can occur.

Across sectors, there is a growing shift toward coordinated proactive intervention across the scam value chain, as no one actor has the complete picture of the entire scam. Financial institutions, telecommunications providers, and digital platforms are increasingly deploying data-driven tools and advanced analytics to detect suspicious activity upstream, protecting individuals before they lose their money to scams. However, these efforts are accompanied by structural challenges, including the need to balance security with legitimate user access, ensure privacy protections, and maintain incentives for continued investment in innovative anti-fraud capabilities alongside regulatory frameworks that are outcome-focused.

The discussions also reinforced that no single actor has full visibility into the scam ecosystem. Effective responses depend on coordinated action across governments, industry stakeholders, and international partners. Telecommunications networks, digital platforms, and financial systems each represent critical points of vulnerability as well as opportunities for intervention. Intervention at these points in the scam chain is significantly more effective than acting after financial loss has occurred. Strengthening linkages across these sectors is essential to improving collective resilience.

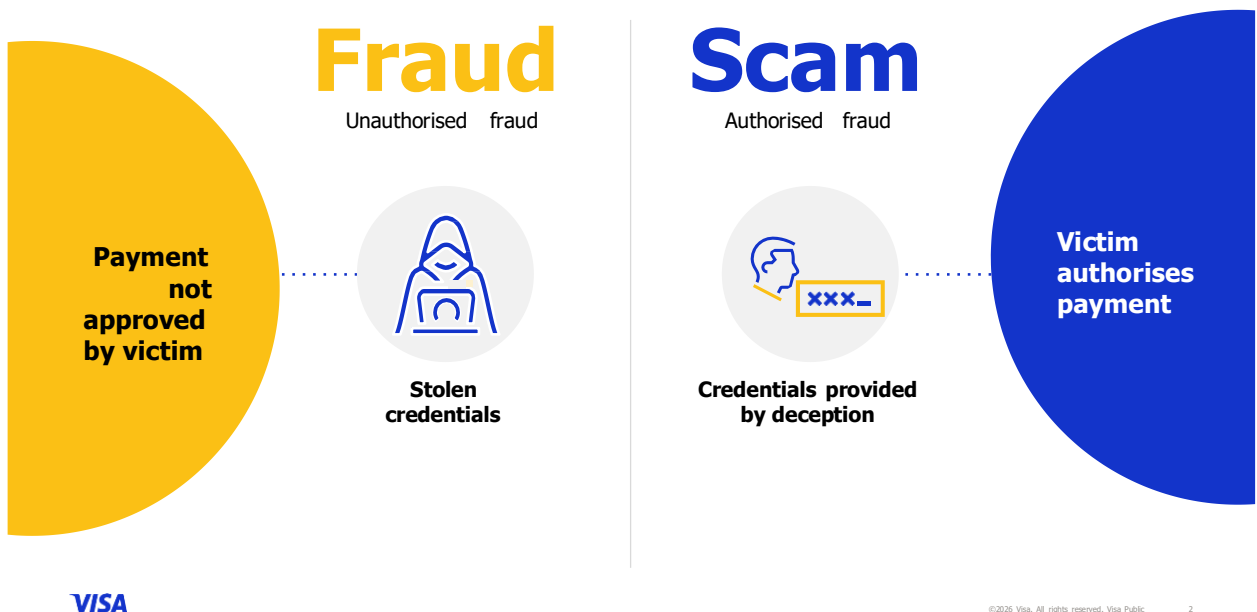
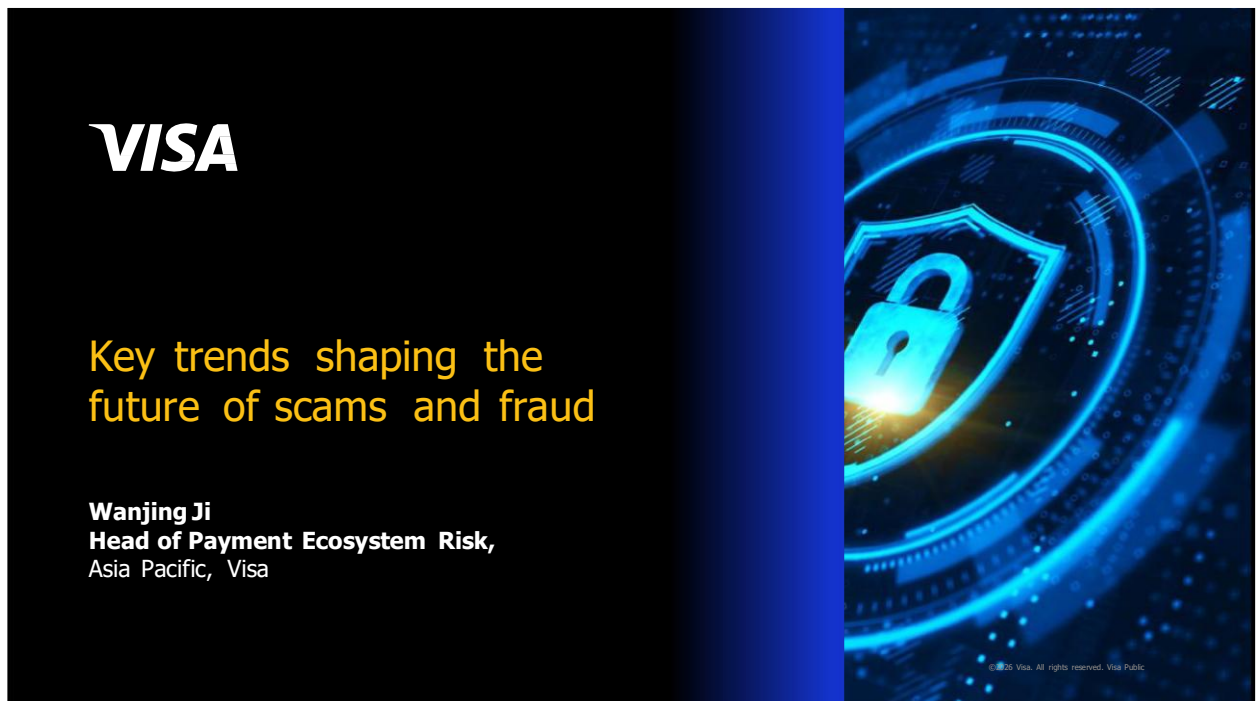
Several overarching themes emerged. Scams are increasingly cross-border in nature, requiring stronger international cooperation to address jurisdictional challenges and enforcement gaps. Artificial intelligence is reshaping both the threat landscape and the tools available for detection and prevention, necessitating continuous adaptation. At the same time, efforts to combat scams must remain proportionate, ensuring that protective measures preserve trust, protect privacy, and support innovation within the digital economy.

In light of these findings, two priority recommendations emerged. First, strengthening regional information-sharing frameworks and cross-sector coordination mechanisms is essential to improving the ability to detect and disrupt evolving scam typologies, and criminal scam networks. More timely, structured, and trusted data exchange, both within and across economies, will be critical to addressing the speed and scale of modern scam operations.

Second, promoting balanced, proportionate, and scalable anti-scam tools and policy approaches can help close cross-border enforcement gaps while maintaining an enabling environment for digital trade and innovation. Alignment across sectors and jurisdictions will be key to ensuring that these measures are both effective and sustainable.

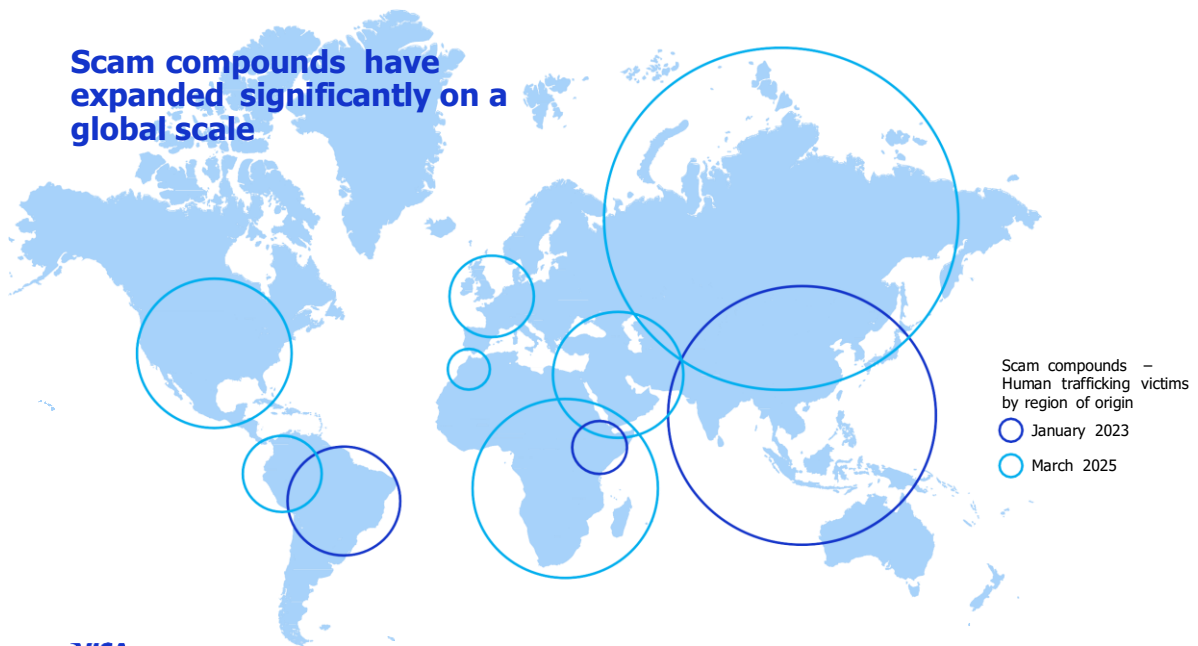
Looking ahead, continued engagement within APEC and ABAC can play an important role in advancing these priorities. By supporting the development of practical good-practice frameworks, capacity-building initiatives, and public–private cooperation models, APEC economies can strengthen their collective response to online fraud and scams. Sustained collaboration will be essential not only to mitigate current risks but also to reinforce trust and ensure the long-term resilience of the digital economy.

**Annex A – “Key Trends Shaping the Future of Scams and Fraud” Presentation by
Wanjing Ji, Head of Payment Ecosystem Risk, Asia Pacific, Visa**





Scam compounds have expanded significantly on a global scale



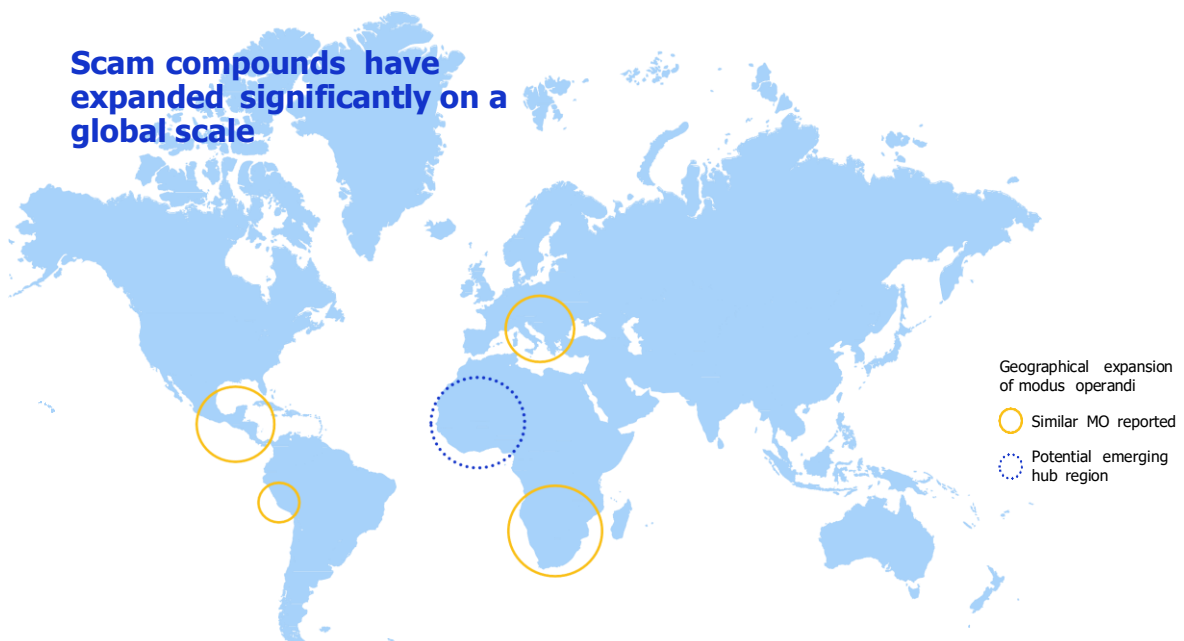
VISA

Source: Adapted from [Interpol](#), [United Nations Office on Drugs and Crime](#).

©2025 Visa. All rights reserved. Visa Public

5

Scam compounds have expanded significantly on a global scale



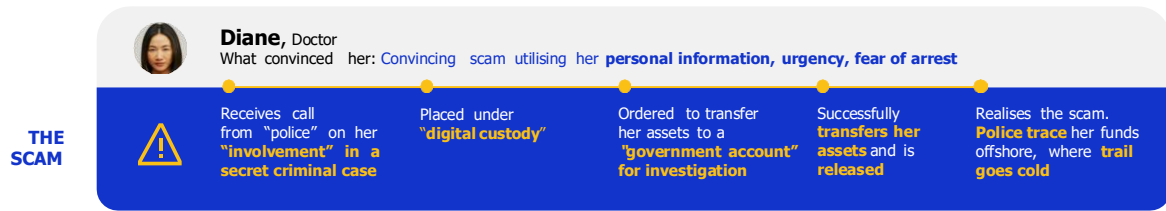
VISA

Source: Adapted from [Interpol](#), [United Nations Office on Drugs and Crime](#).

©2025 Visa. All rights reserved. Visa Public

6

Layered, complex and creates victims on both sides



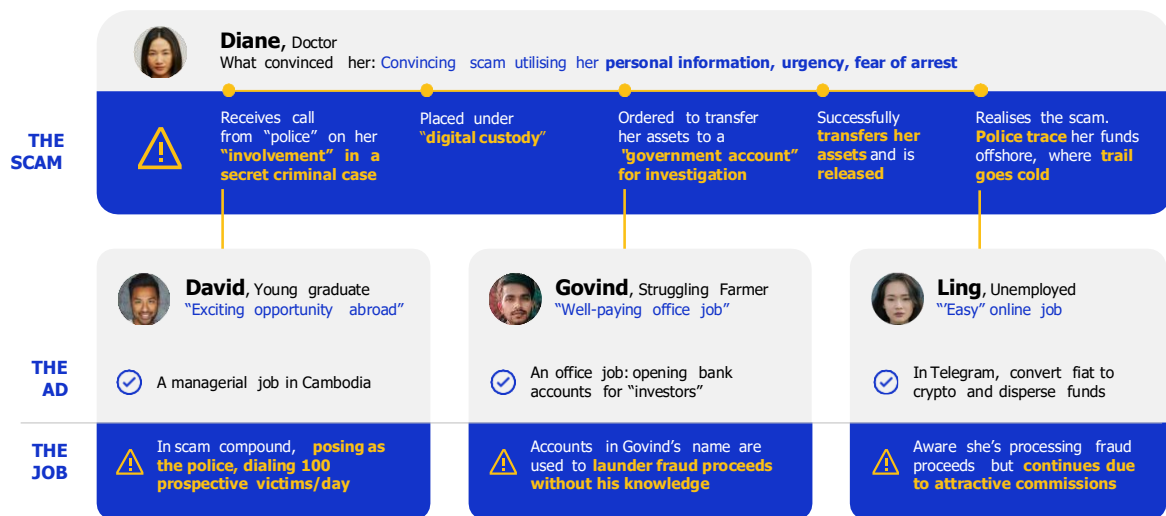
VISA

Sources: Adapted from Bloomberg, 'Digital Arrests: India's Billion Online IDs Sparked Criminal Scam' Bonanar, Image credits: Unsplash

©2026 Visa. All rights reserved. Visa Public

7

Layered, complex and creates victims on both sides



VISA

Sources: Adapted from Bloomberg, 'Digital Arrests: India's Billion Online IDs Sparked Criminal Scam' Bonanar, Image credits: Unsplash

©2026 Visa. All rights reserved. Visa Public

8

Layered, complex and creates victims on both sides



Call to Action



Combatting fraud & scams require an ecosystem response



Drive shared responsibility and end-to-end consumer protection across the ecosystem



Strengthen public-private collaboration to outpace increasingly sophisticated fraudsters



©2025 Visa. All rights reserved. Visa Public

11

**Annex B – “AI-based Voice Phishing Prevention Policy” Presentation by Sunup Park,
Deputy Director at the Personal Information Protection Commission (PIPC) of the
Republic of Korea**



2026 APEC Workshop
: Combatting Online Scams and Fraud

AI-based Voice Phishing Prevention Policy

4th February

 PERSONAL INFORMATION
PROTECTION COMMISSION
Republic of Korea

Contents

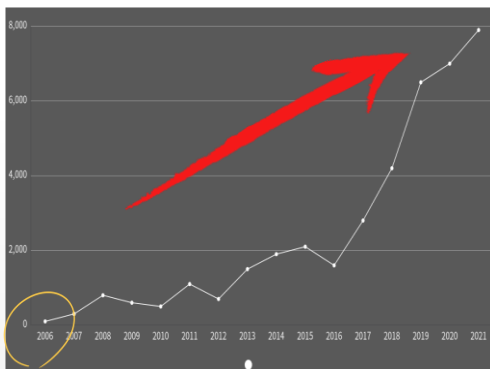
- 01 Background
- 02 Best Practices for Public-Private Collaboration
 - (1) Inter-agency MoU
 - (2) Regulatory Sandbox
 - (3) Prior adequacy Review
- 03 International Cooperation

2

01 Background

01 Background

Backgrounds — Increase in Voice Phishing Related Financial Losses in Korea



01 Background

Backgrounds — Challenges related to AI-based Voice Phishing Prevention

- **Legal Basis**

for collecting and
using personal
information

- **De-identification**

(e.g. pseudonymization)

Privacy
Issue

Obtain
High-quality
Data

- Suspect's Voice
- Call Context and
Patterns Data



개인정보보호위원회

PERSONAL INFORMATION
PROTECTION COMMISSION

05



PERSONAL INFORMATION
PROTECTION COMMISSION

02

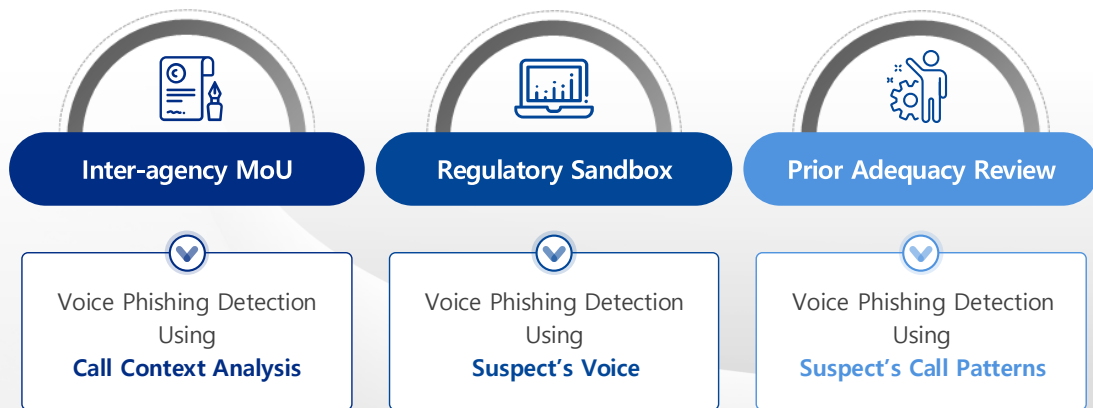
Best Practices for Public-Private Collaboration

6

02 Best Practices for Public-Private Collaboration

3 Directions — Inter-agency MoU / Regulatory Sandbox / Prior Adequacy Review

Overview



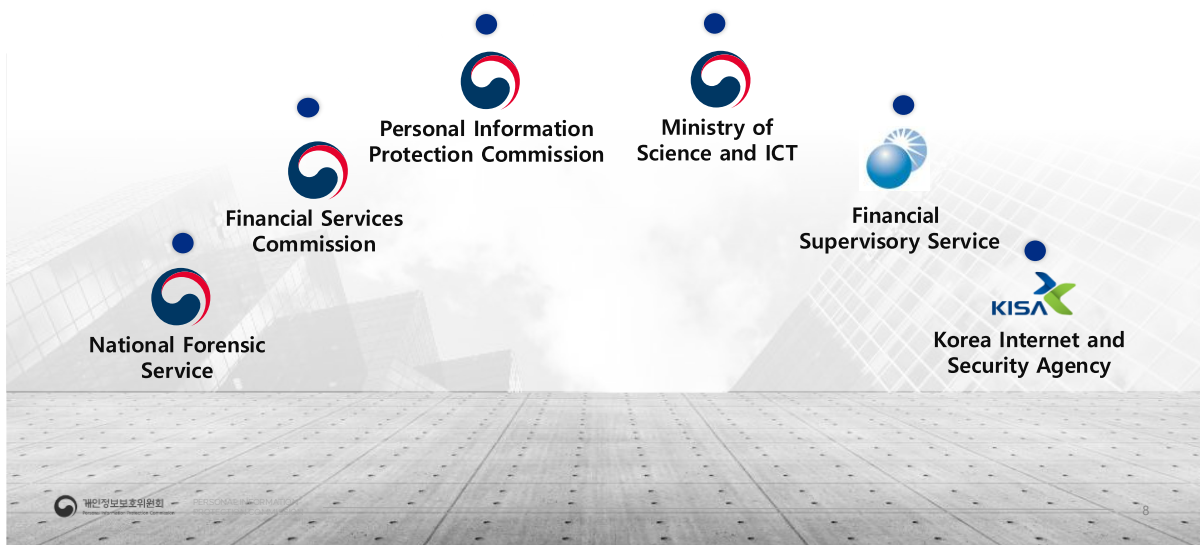
개인정보보호위원회

PERSONAL INFORMATION
PROTECTION COMMISSION

07

02 Best Practices for Public-Private Collaboration

(1) MoU on AI-based Voice Phishing Prevention (June 2024)



개인정보보호위원회

PERSONAL INFORMATION
PROTECTION COMMISSION

08

02 Best Practices for Public-Private Collaboration

(1) MoU on AI-based Voice Phishing Prevention (June 2024) - AI Model for 'Call Context Analysis'

Mechanism

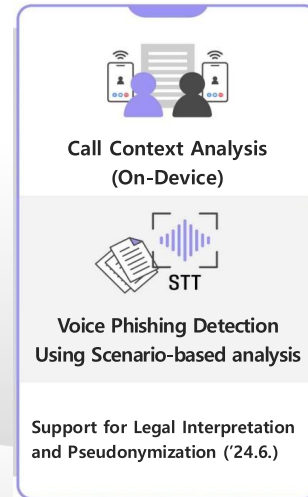
- ① Voice-to-Text Conversion (National Forensic Service)



- ② Support for Legal Interpretation and Pseudonymization
Share de-identified call data related to voice phishing
(National Forensic Service > Telecom Companies)



- ③ Development of an AI Model for 'Call Context Analysis'
(Telecom Companies)



02 Best Practices for Public-Private Collaboration

(2) Regulatory Sandbox Approval for Using Suspected Scammers' Voice

Mechanism

- ① Extraction of Suspect's Original Audio
(National Forensic Service > Telecom Companies)

Regulatory Sandbox PIPC Collaborated with Ministry of Science and ICT

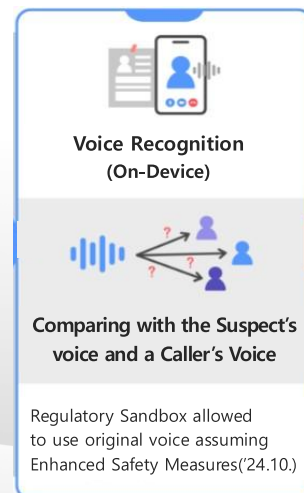


- ② AI Model for 'Context-Analysis' (Telecom Companies)
+
'Speaker-Recognition' Technology Embedded (On-Device)



- ③ Detected by Comparing with a Caller's Voice and Notified
(Mobile Device)

Detection Accuracy 91.6%



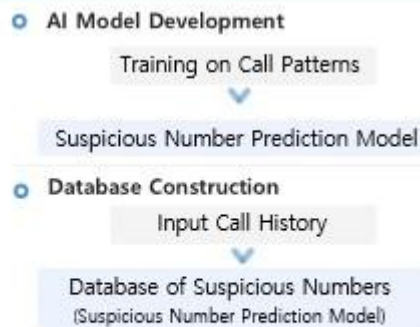
02 Best Practices for Public-Private Collaboration

(3) Prior Adequacy Review

- AI-Based Voice Phishing Detection Using Call Patterns Analysis

Mechanism

Suspicious Number Prediction Stage (Telecom Companies)



Prediction Result Utilization Stage (Telecom Companies + Financial Institutions)



02 Best Practices for Public-Private Collaboration

(3) Prior Adequacy Review

- AI-Based Voice Phishing Detection Using Call Patterns Analysis

Recommendations on safeguards

Purpose Specification

- Operate the service solely for voice phishing prevention

Transparency

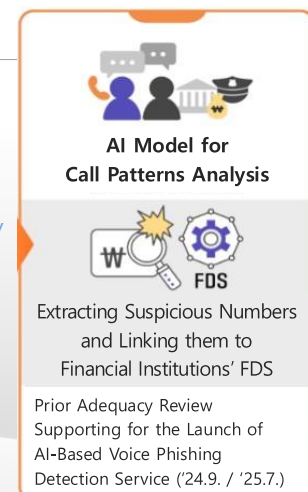
- Disclose the purpose and processing mechanisms in the privacy policy

Accountability

- Outsource a data processing only under a contract
- Processor(intermediary) is subject to supervision and oversight

Use Limitation

- Financial institutions shall query the voice phishing suspect database only when it is necessary to assess the risk of financial fraud



03

International Cooperation

13

03 International Cooperation



The illicit trading and circulation of
personal information across borders



Secondary crimes occurring across borders
including Voice phishing, Scams, and Fraud



Need for a collaborative response network

03 International Cooperation

Launch of APPA(Asia-Pacific Privacy Authorities) Working Group

Share and learn from emerging trends in combatting illicit personal information trading and circulation



Promote the global dissemination of best policy practices



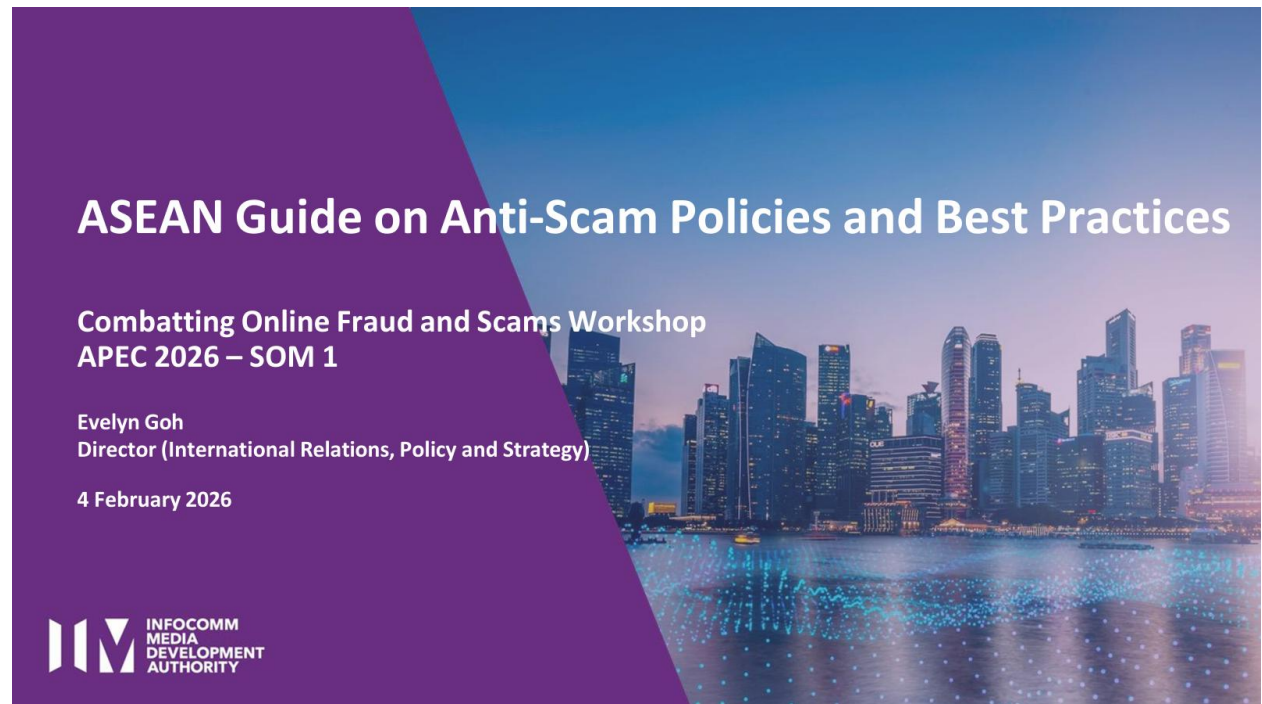
Establish a hotline to coordinate the detection and removal of illicitly circulated personal data



Thank you



Annex C – “ASEAN Guide on Anti-Scam Policies and Best Practices” by Evelyn Goh, Director, International Relations, Policy and Strategy, Infocomm Media Development Authority, Singapore



4 February 2026

ASEAN Guide on Anti-Scam Policies and Best Practices (“Guide”)

- The Guide is the region's first comprehensive framework for combatting scam calls and SMS.
- Developed with ASEAN Members (AMS), the Guide reviews regional and global anti-scam measures and recommends actions AMS can adopt according to their technical readiness and regulatory contexts.
- The Guide supports policymakers, regulators and telcos in harmonising safeguards and boosting regional collaboration against cross-border scam threats.
- The Guide can be accessed via the ASEAN Main Portal.



Overview of Guide's Recommendations

- The Guide proposes a framework for best practice anti-scam measures that could be adopted within AMS, structured around two core recommendations.

Recommendation (A) Strengthen Anti-Scam Measures



AMS are encouraged to implement a **set of best practice measures** based on a **tiered framework**, including:

- SIM Card and Equipment Controls
 - Network-Based Measures
 - Wider Information Sharing

Recommendation (B) Collaboration within ASEAN



AMS and telcos operating in ASEAN can **work together to strengthen anti-scam information sharing mechanisms**, including implementing a comprehensive **regional traceback** procedure

3

Recommendation (A) Strengthen Anti-Scam Measures

Categories of Recommendations

A total of **10 recommendations** across the following categories:

-  SIM Card and Equipment Controls
-  Network Anti-Scam Call Measures
-  Network Anti-Scam SMS Measures
-  Information Sharing

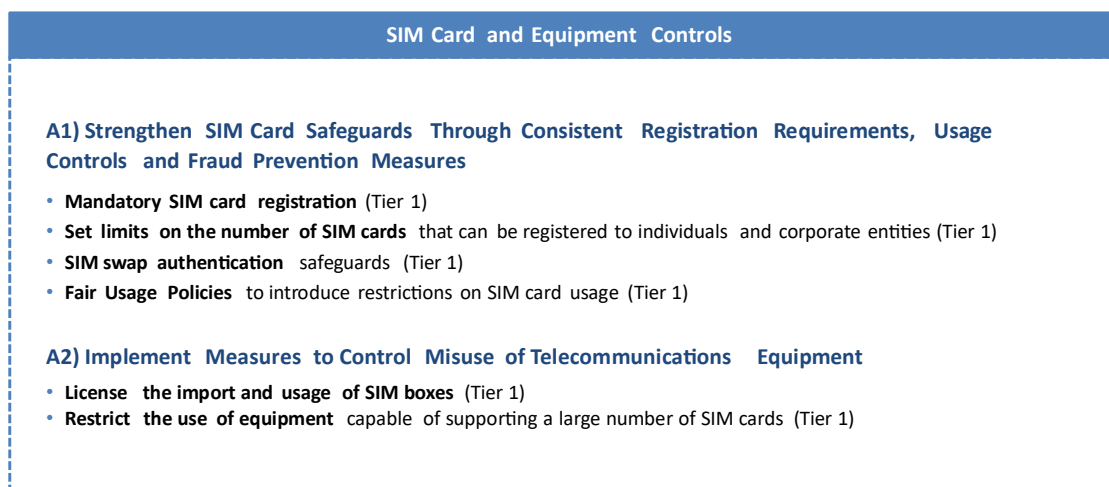
Tiering of Proposed Measures

Measures to achieve these recommendations are divided into **three tiers**.

Tier 1 – Baseline Protection – Foundational Measures
Foundational measures of an anti-scam strategy, focusing on limiting scammers' access to telecommunications infrastructure and enable basic validation of traffic
Tier 2 – Enhanced Protection – Proactive Filtering and Increased Reliance on Intelligence
Rule based and analytical measures that identify and reduce scam based on patterns and predictive intelligence
Tier 3 – Advanced Protection – Real-Time Blocking & Proactive Intelligence
Sophisticated measures involving advanced analytics, potentially in real-time, for prompt scam detection, intervention and prevention

4

Limit scammers' access to telecommunications infrastructure

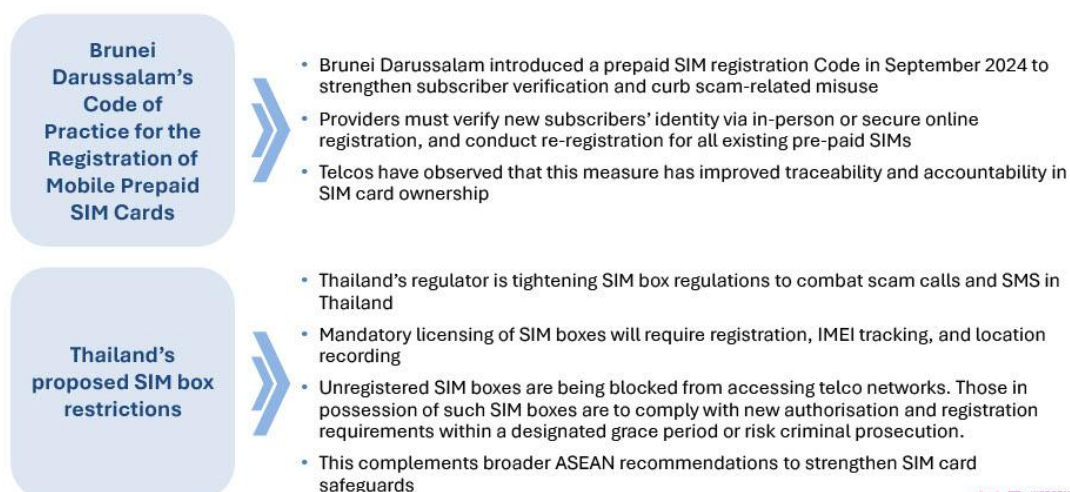


5



4 February 2026

SIM card registration and SIM box regulations in the region



6



Baseline and enhanced protections against scam calls

Network Anti-Scam Call Measures	
A3. Implement Measures to Block Calls from Scammers - Block calls with invalid economy codes (Tier 1) - Add prefix to international incoming calls without an economy code (Tier 1) - Allow user-initiated international call blocking (Tier 1) - Detect scam calls using analytics / Artificial Intelligence (AI) (Tier 2/3)	EXAMPLE 1  EXAMPLE 2 
A4. Prevent Calling Line ID (CLI) Impersonation - Basic CLI/phone number validation methods (Tier 1) - Advanced call authentication and caller name ID display (Tier 3)	
A5. Block Reply Calls to Identified Scam Numbers - Block reply calls to scam numbers identified using AI / Machine Learning (ML) (Tier 2/3) - Divert calls to identified scam numbers to a consumer warning (Tier 3)	

7

Image originally retrieved from: <https://www.channelnewsasia.com/singapore/scam-call-overseas-plus-65-businesses-ima-2663341>. Graphic was edited for presentation.



4 February 2026

Baseline and enhanced protections against scam SMS

Network Anti-Scam SMS Measures	
A6. Implement Measures to Block SMS from Scammers - User-initiated international SMS blocking (Tier 1) - SMS firewalls for scam content filtering (Tier 2) - Advanced firewalls using data analytics / ML (Tier 3)	
A7. Measures to Prevent SMS Sender ID Spoofing - Sender ID checks by SMS originators (Tier 1) - Implement SMS Sender ID registries (Tier 2)	

8



Regional practices that prevent impersonation over calls and SMS

Displaying caller names for government agency calls in Viet Nam



- Viet Nam issued a directive in May 2024 to enhance caller ID for government calls
- By November 2024, telcos implemented Branded Caller ID for 732 official government numbers
- The Ministry of Science and Technology manages a central portal for approved agency names as a trusted source
- Citizens are advised to confirm caller identity on a screen-enabled device for verification

Singapore's SMS Sender ID Registry



- Singapore launched the SMS Sender ID Registry as a voluntary scheme in March 2022, enabling organisations to register their alphanumeric Sender IDs on a first-come, first-served basis
- The scheme became mandatory in January 2023 for all organisations sending Application-to-Person (A2P) SMS using Sender IDs
- Today, all SMS from unregistered Sender IDs are flagged as "Likely-SCAM" to alert consumers
- The mandatory scheme reduced scam cases by 70% within three months of its implementation and covers 96% of commercial SMS traffic today

9

Conclusion

- The Guide reflects ASEAN's commitment to regional cooperation against scam calls and SMS and serves as a best-practice reference for policymakers, regulators, enforcement agencies, and industry stakeholders.
- While the Guide was developed for the ASEAN region, the tiered anti-scam measures are highly impactful and practical for adoption across jurisdictions, based on their technical capabilities and regulatory maturity.
- As scam tactics evolve, ASEAN and the wider APEC community must stay agile, strengthen capabilities, and deepen regional cooperation to protect citizens, build trust in telecommunications, and lead the fight against scams.

10

Thank You



To access the ASEAN Guide, please scan this gov.sg code:

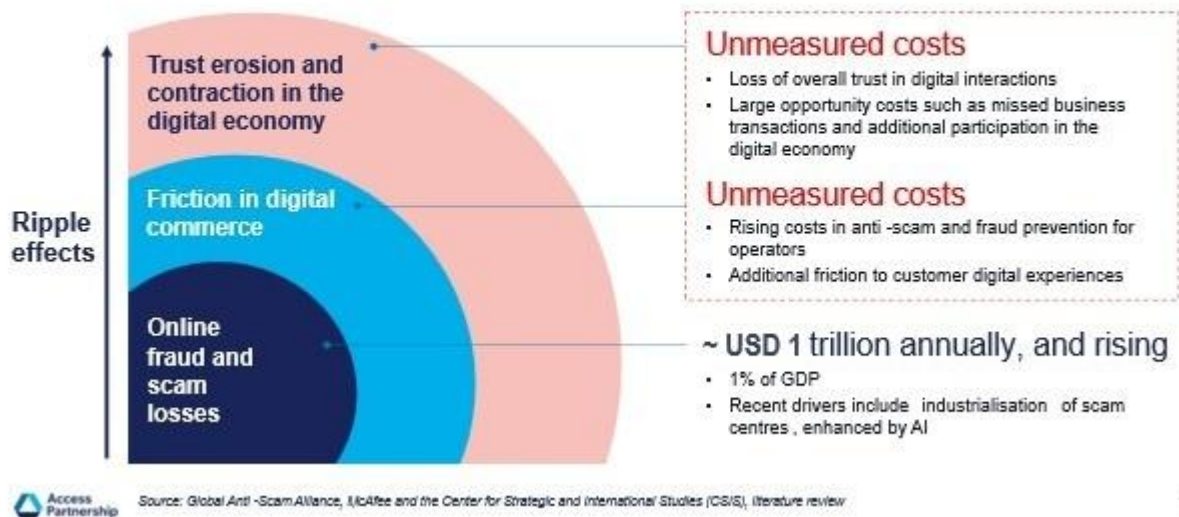


<https://go.gov.sg/g4wix7>

**Annex D – “Combatting Scams and Fraud in Telecommunications” by Daryl Teo,
Manager, Economics Strategy, Access Partnership**

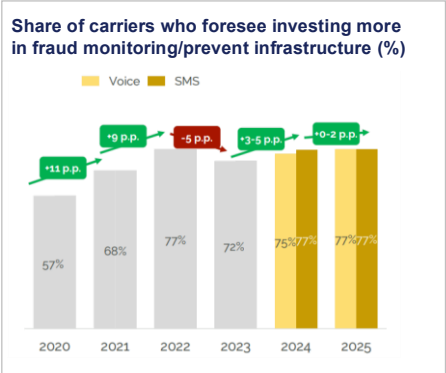


The true societal cost of fraud and scams are likely much greater than USD 1 trillion



Incentives are misaligned – Fraud and scam prevention measures are an ever enlarging expense for telcos, with little revenue recourse

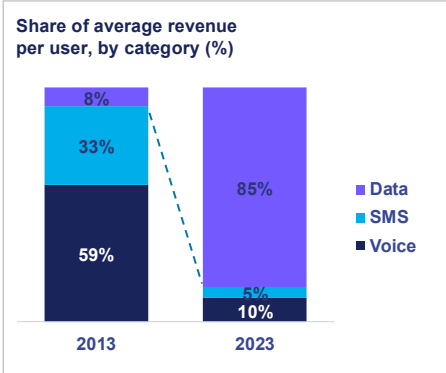
Operators foresee greater investments in antifraud systems for voice/SMS...



Source: Global Leaders Forum Fraud Report 2025



... but are combating falling revenue contributions from voice and SMS itself



Source: TRAI Consultation Paper 2023



Scams remain a key priority for Singapore

- Online scams continue to challenge Singapore and remain an urgent priority. We are especially susceptible due to high levels of digitalisation and social trust.
- Scam reports and losses in Singapore worsened over the past five years.
- Trust, whether of digital security/services or public-private partnerships, is hard-won but easily lost.

We take a whole-of-society approach to fight scams

- Singapore adopts a whole-of-society approach to tackling scams.
- The Government collaborates closely with industry, community and the public to pursue scam disruption, enforcement, and uplift measures to secure digital channels/platforms.
- Our protective measures target the scam chain and are implemented in collaboration with online platforms.
 - We introduced the Online Criminal Harms Act in 2023. It enables the Police to disrupt online scam content and require online platforms to implement safeguards against scams.
 - We launched the E-commerce Marketplace Transaction Safety Ratings in 2022, which rates major e-commerce platforms on their anti-scam measures.

3



We implement upstream defences where possible

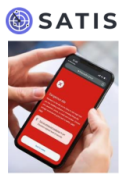
- To prevent and block scammers from reaching victims, we work with telcos and online platforms to secure communication channels.
- We enhance device protection against scams:
 - In Feb 2024, the Cyber Security Agency of Singapore (CSA) partnered with Google on a pilot for Enhanced Fraud Protection (EFP) within Google Play Protect in Singapore.
 - In 2024, CSA published a new Safe App Standard to set out best practices that reduce the risk of malicious actors exploiting weaknesses in the app design.



4



We accelerate scam disruption through technology



- To more effectively detect and disrupt scam activity at scale, we leverage technology:
 - Scam Analytics and Tactical Intervention System (SATIS) was co-developed by the Government Technology Agency of Singapore (GovTech Singapore) and the Singapore Police Force (SPF) to disrupt scam sites at scale. SATIS leverages artificial intelligence to monitor and evaluate potential scam websites for blocking.
- We strongly support public-private partnerships in combatting scams:
 - GovTech Singapore is the first government agency to join the Global Signal Exchange (GSE), a platform that allows member organisations to rapidly share information for scam disruption. In partnership with the SPF, GovTech Singapore sends scam signals, including scam-tainted websites, through the GSE to strengthen overall scam detection and disruption efforts.

A vigilant public is our best defence

- We continue to invest in public education efforts:
 - Emphasise personal vigilance and agency through the anti-scam campaign “I can ACT against scams”
 - **ADD** – Add security features (e.g. enable International Call Blocking on mobile devices, enable two-factor authentication (2FA) or multi-factor authentication for online accounts)
 - **CHECK** – Check for scam signs with official sources
 - **TELL** – Tell the authorities, family and friends if you encounter scams. Report and block any suspected scam accounts, chat groups, and any fraudulent transactions.
 - Amplify anti-scam messages through nationwide roadshows. The latest roadshow held in Nov 2025 saw over 15,000 visitors over two days.
 - Strengthen scam prevention awareness with the ScamShield suite, which comprises the ScamShield app, the 1799 helpline, website, and WhatsApp and Telegram alert channels.
 - Reinforce resilience through simulated training exercises.

Fighting scams is tough, but we can ACT together

- Scam syndicates are highly organised and agile. They constantly innovate and exploit new technologies and vulnerabilities to reach out to victims and scam them for monies.
- Our efforts prove that they can be disrupted, and the harms they cause can be limited. We must continue our fight against scams by smarter prevention, robust enforcement, and ongoing education.
- No single economy or entity can tackle this scourge alone. By committed partnership across public and private sectors, we can ACT together and prevail.

Thank you!



MINISTRY OF
DIGITAL DEVELOPMENT
AND INFORMATION

☎ 1800 837 9655

🌐 www.mddi.gov.sg

📘📱 SingaporeMDDI