International Conference on Combating Online Scams

Phnom Penh, Cambodia, 23 September 2026

REMARKS for the High-Level Session: Online Scams as a Global Emergency

Prepared for H.E. Dr. Kao Kim Hourn, Secretary-General of ASEAN

Your Excellency Abhisantibindit, Deputy Prime Minister and Minister of Interior of the Kingdom of Cambodia;

Your Excellencies Ministers, Vice Ministers, Heads of Delegations and Representatives of International Organisations,

Excellencies, Distinguished Participants, Ladies and Gentlemen,

Good Morning !

1. First, I would very much like to express my appreciation to the Royal Government Cambodia for the kind invitation to speak at this Conference. I would also like to congratulate the Royal Government of Cambodia for convening this important initiative, and for its all-out efforts and commitment to tackle and eradicate online scams.

2. These efforts are not only important for Cambodia, but also contribute to the safety, security, prosperity and well-being of ASEAN and the wider region. The continued growth and increasing sophistication of online scams make this Conference particularly relevant. These activities are posing increasingly serious threats to our people, economies, communities and societies, both within our region and beyond.

3. The theme of this Conference, *"Acting Together towards Breaking the Chain and Eradication of Online Scams,"* captures the nature of the challenges we face. Online scams are rarely isolated acts. They increasingly operate through sophisticated networks that cross borders, exploit digital technologies, move illicit proceeds across jurisdictions and, in some cases, are linked to other forms of transnational crime. Breaking this chain therefore requires us to look beyond individual incidents and address the wider ecosystem that allows these activities to operate and expand.

Excellencies, Ladies and Gentlemen,

4. The growing sophistication of online scams also presents significant challenges for law enforcement. It undermines the safety, security and trust that are essential to ASEAN's expanding digital ecosystem and economy. Cambodia, like several other ASEAN Member States, has itself been affected by this transnational crime. Cambodia's own experience, together with its determined efforts to address the problem, reminds us that no country is immune and safe from this threat. The scale of the challenge is substantial. According to the Global Anti Scam Alliance (GASA) State of Scams in Southeast Asia 2025 report, losses from scams in the region reached 23.6 billion US dollars in 2024, and the report highlights that many cases remain unreported.

5. The issue has received attention at the highest political level. Online scams were raised by the Leaders of ASEAN and its external partners during the ASEAN Summits and related Summits held last year, and were further discussed at the ASEAN Summit held in May this year. This reflects ASEAN's continued recognition of the evolving nature of the threat and our commitment to strengthening collective action against it.

6. For ASEAN, this means that no single agency, sector or Community pillar can address the challenge on its own. We need a whole-of-government approach within each ASEAN Member State, and a whole-of-ASEAN approach at the regional level. Our response must bring together law enforcement agencies, prosecutors and judicial authorities, digital and telecommunications authorities, financial institutions, technology providers and other relevant stakeholders.

7. Importantly, while ASEAN does not have a specific treaty dedicated solely to online scams, we already have a range of legal instruments, mechanisms and sectoral bodies that can support our response. What we need is to collectively make better use of these existing instruments and mechanisms, and strengthen the links between them.

8. Under the ASEAN Political-Security Community, the ASEAN Treaty on Mutual Legal Assistance in Criminal Matters – signed in 2006 - provides an established basis for ASEAN Member States to assist one another in investigations and prosecutions of criminal offences. This is particularly relevant when online scam investigations require evidence, information or other forms of legal assistance across jurisdictions. We now also have the ASEAN Treaty on Extradition, signed in 2025. Once in force, it will provide another important legal basis for ASEAN Member States to cooperate in the extradition of persons for prosecution or for the imposition or enforcement of sentences in respect of criminal offences. Together with mutual legal assistance, extradition can strengthen our ability to ensure that perpetrators cannot evade justice simply by operating across borders. The newly established ASEAN Prosecutors/Attorneys-General Meeting, or APAGM, also provides an important avenue for strengthening cooperation on prosecutorial matters among ASEAN Member States. Its establishment reflects ASEAN's recognition that closer prosecutorial cooperation is an important part of addressing transnational crime and strengthening the rule of law.

9. These legal instruments and mechanisms should therefore be seen as part of the broader ASEAN architecture for combating online scams. The challenge is to ensure that law enforcement agencies, central authorities, prosecutors and other relevant authorities can work together more closely and effectively, so that information can translate into investigations, prosecutions, asset recovery and, where appropriate, extradition.

Excellencies, Ladies and Gentlemen,

10. Let me also turn to the work under the ASEAN Political-Security Community, particularly in the law enforcement sector. Cybercrime and online scams constitute one of the eight priority areas under the ASEAN Plan of Action in Combatting Transnational Crime for 2026–2035. The Plan guides cooperation under the ASEAN Ministerial Meeting on Transnational Crime and its subsidiary mechanisms. To put this cooperation into practice, the ASEAN Senior Officials' Meeting on Transnational Crime Working Group on Cybercrime and Online Scams provides a platform for exchanging information and advancing practical responses.

11. We should continue to strengthen cooperation among our law enforcement agencies, including through timely information-sharing, coordinated investigations and operations, mutual legal assistance, and the tracing and recovery of illicit proceeds. Scam networks do not operate according to national boundaries. Our law enforcement cooperation therefore needs to be equally capable of crossing those boundaries as well.

12. ASEAN also recognises that online scams cannot be addressed purely as a cybercrime or fraud issue. The growth of industrial-scale scam operations has demonstrated their convergence with other forms of transnational crime, particularly trafficking in persons and forced criminality. In some cases, victims are recruited and exploited to participate in scam operations.

13. This link between technology-facilitated crime and trafficking in persons has also received the attention of ASEAN Leaders. During Indonesia's ASEAN Chairmanship in 2023, ASEAN Leaders adopted the *ASEAN Leaders' Declaration on Combating Trafficking in Persons Caused by the Abuse of Technology*, underscoring the need for stronger regional cooperation to address the abuse of technology in facilitating trafficking and related transnational criminal activities. In this context, SOMTC also plays a cross-sectoral role as the Lead Body for ASEAN cooperation against trafficking in persons, including through the implementation of the ASEAN Multi-Sectoral Work Plan Against Trafficking in Persons 2023–2028 (Bohol TIP Work Plan 2.0).To date, SOMTC has also been collaborating with Australia, China, Japan, the Republic of Korea, the Plus Three, the United Kingdom, Italy and UN agencies to build regional capacity in combating cybercrime and online scams and in addressing the convergence between trafficking in persons and online scams.

14. Beyond law enforcement, other ASEAN sectoral bodies also have relevant roles to play as well. The ASEAN Defence Ministers' Meeting, or ADMM, through the ASEAN Cyber Defence Network, contributes to strengthening cyber resilience and cooperation among ASEAN defence establishments as well. Online scams have

also been taken up within the ASEAN Regional Forum, whose Manila Plan of Action 2026–2036 supports national and regional strategies and legal frameworks, practical cooperation and information-sharing, as well as capacity-building on emerging ICT-related threats, including AI. A seminar and workshop on combating online scams is also in the pipeline now.

15. The ASEAN finance sector has also taken steps. Under the Roadmap for Instant Payment Connectivity (RIPC), ASEAN is holding policy dialogues to manage cross-border payment risks, align oversight practices and build capacity for resilience against scams and fraud. ASEAN Central Banks are also convening cybersecurity knowledge exchanges through the ASEAN Cybersecurity Resilience and Information Sharing Platform (CRISP), while the ASEAN Capital Market Forum (ACMF) is preparing a white paper on regulatory and supervisory technologies against cybersecurity threats and online scams.

Excellencies, Ladies and Gentlemen,

16. While law enforcement and legal cooperation remain indispensable, an effective response must also address the digital environment in which online scams are increasingly enabled, facilitated and perpetrated. Let me now turn to the efforts being advanced under ASEAN's digital sector.

17. The ASEAN Digital Masterplan 2030 provides a framework for strengthening regional cooperation and building digital trust. It also promotes ethical and responsible digital behaviour, while supporting greater public awareness and consumer protection against scams, fraud and other harmful practices across digital and telecommunications channels.

18. Building on this broader framework, the ASEAN Working Group on Anti-Online Scams was established in 2024 by the ASEAN Digital Ministers' Meeting (ADGMIN) as a dedicated platform for collaboration. Its work focuses on identifying technical measures, building capacity and sharing information to address online scams across digital and telecommunications channels. Since its establishment, the Working Group has delivered two key outputs: the Report on Online Scam Activities in ASEAN (2023–2024) and the ASEAN Recommendations on Anti-Online Scams. It subsequently developed the ASEAN Guide on Anti-Scam Policies and Best Practices. It provides practical recommendations for governments, telecommunications regulators and industry stakeholders to strengthen anti-scam measures. In 2026, the Working Group continued to explore potential approaches for developing a public-private anti-scam information-sharing initiative, as well as capacity-building support for Call Traceback Mechanisms or CTM.

19. These efforts reflect ASEAN's recognition that online scams require a whole-of-ecosystem response across the digital and telecommunications sectors. They also highlight the need to address different stages of the scam kill chain through coordinated interventions. This means acting not only after a scam has occurred, but also further upstream: strengthening the resilience of digital and telecommunications networks, improving information sharing and cooperation, and supporting preventive measures that can disrupt scam activities before they reach potential victims.

20. ASEAN is also moving towards a stronger region-wide legal framework for the digital economy. The negotiations for the ASEAN Digital Economy Framework Agreement, or DEFA, has been successfully concluded with signing expected later this year. The Agreement can provide an important framework for deeper regional cooperation in areas relevant to combating online scams, including online consumer protection, digital identity and authentication, electronic payments, and cybersecurity.

21. Taken together, these efforts demonstrate that ASEAN already has multiple pieces of the architecture needed to address online scams: legal cooperation through the MLAT and the Treaty on Extradition; prosecutorial cooperation through APAGM; law enforcement cooperation through AMMTC and SOMTC; digital cooperation through ADGMIN and the Working Group on Anti-Online Scams; and cyber resilience cooperation through ADMM and the ACDN.

22. The task before us is therefore to connect and make better use of the mechanisms we already have.

Excellencies, Ladies and Gentlemen,

23. Online scams transcend borders, jurisdictions and sectors, and our response must do the same. This is where the ASEAN spirit can make a difference. We need to unite in both the spirit and action of ASEAN to address this common threat. Every Member State has an interest in ensuring that our region does not become a safe operating environment for transnational criminal networks engaged in online scams.

24. At the same time, we should guard against politicising or weaponising the issue of online scams by targeting any particular country. Online scams are a transnational criminal challenge, and no ASEAN Member State is immune from its effects. Our focus should remain on strengthening cooperation, identifying criminal networks, disrupting their operations, protecting victims and bringing those responsible to justice. This requires trust among Member States and a willingness to share information and work together effectively.

Excellencies, Ladies and Gentlemen,

25. Building on ASEAN's existing efforts, I would like to highlight three potential avenues for further exploration.

26. First, strengthening digital trust and leveraging technology for scam prevention. This could include exploring interoperable digital identity and authentication mechanisms, secure-by-design measures, and the responsible use of artificial intelligence (AI) and other advanced technologies. These tools and capabilities can help strengthen user verification, detect emerging scam patterns, and prevent and respond to evolving scam tactics across digital services. Equally important is closer cooperation with technology companies and digital service providers, whose systems and platforms are often at the frontline of efforts to detect, prevent and disrupt scam activities.

27. AI and other emerging technologies are also important for the law enforcement sector. They can support the detection and investigation of scams, enable more expedient responses to reports from scam victims, and help trace illicit financial flows for the timely identification, freezing, seizure and recovery of assets. They can also support efforts to disrupt the transnational criminal networks behind online scams. AI, however, can also be exploited by criminals to make online scams, fraud and cybercrime more sophisticated and harder to detect. Generative AI can be used to create convincing messages, impersonate individuals, manipulate images and audio, and automate fraudulent activities at greater scale and speed. This makes it increasingly important for ASEAN to strengthen safeguards, detection capabilities and cooperation as the technology continues to evolve.

28. Second, building secure regional anti-scam information-sharing platforms. These platforms could facilitate the timely exchange of real-time alerts, scam typologies and threat intelligence across digital and telecommunications channels, as well as among law enforcement authorities, particularly anti-online scams command or control centres.

29. Third, adopting a whole-of-ecosystem approach by strengthening public-private partnerships among relevant stakeholders. This includes law enforcement agencies, prosecutors, financial institutions, telecommunications providers, digital platforms and civil society. Such partnerships can help identify and implement coordinated measures across the scam lifecycle, from prevention and detection to response.

30. More broadly, if ASEAN is to be more effective in addressing this challenge, we need both a whole-of-government approach within our Member States and a whole-of-ASEAN approach at the regional level. Within governments, agencies responsible for law enforcement, justice, digitalisation, telecommunications, finance and other relevant areas need to work together. At the ASEAN level, our different sectoral bodies need to strengthen coordination and ensure that their respective efforts reinforce one another.

Excellencies, Ladies and Gentlemen,

31. Behind every statistic on online scams is a person, a family or a business that has been affected. For those who fall victim, the consequences can extend well beyond financial loss. There can be lasting effects on their sense of security and trust in the digital environment. This reminds us that our efforts are ultimately about protecting people and businesses, and preserving the trust on which our digital societies depend.

32. Cambodia’s concerted efforts clearly demonstrate the importance of sustained national action. At the same time, Cambodia’s experience, like all other ASEAN Member States, demonstrates why national efforts alone cannot fully address a crime that operates across borders. We therefore need to strengthen the links between national action, ASEAN cooperation and international collaboration.

33. To conclude, ASEAN’s existing commitments, legal instruments and institutional mechanisms provide a strong basis for practical cooperation against online scams.

The priority now is to make better use of these mechanisms, strengthen coordination among our law enforcement agencies and prosecutors, and deepen cooperation across the digital, telecommunications, financial and technology sectors.

34. Above all, let us continue to act in the ASEAN spirit; collectively, constructively and with a shared determination to protect our peoples and businesses. By taking a whole-of-government and whole-of-ASEAN approach, we can better strengthen our collective resilience, help break the chain of online scams, and create a digital environment that is safe, secure and trusted, while ensuring that the benefits of digitalisation can be enjoyed by all.

I wish this International Conference a resounding success. Thank You.

***