CRC Mongolia Innovation Workshop

Fraud and Scams: Staying Safe in the Mobile World

Natasha Nayak
Senior Policy Manager, GSMA

GSMA™

WHY THIS MATTERS

Online fraud and scams: Problem & Impact

- In 2023 criminals stole over approx. USD 1 trillion from victims. (Global Anti-Scam Alliance)
- Individuals in the US experienced the highest losses, with an average of $3,520 per victim.
- In India, more than INR11,000 crore ($1.5 billion) was lost to online scams during the first nine months of 2024, with stock trading and investment scams the most frequently reported cases.
- In Thailand, the Anti-Online Scam Operation Centre recorded five significant scam cases within one week in January 2025, resulting in a total loss of THB21 million ($610,000).
- The global financial cost of cybercrime, including fraud, is projected to be USD 15.63 trillion by 2029.

Hypothetical scenario

Emma is reasonably familiar with technology and has a social media profile that her relative Stephen helped her set up so she could stay connected with family and friends.

One day, Emma receives a call from someone claiming to be a bank representative. This "representative" informs her that a number of bank accounts have been compromised by fraudsters, and her account is one of them.

To secure her funds, the representative explains that a new account has been created and asks her to quickly transfer her money into this account to protect it from being stolen. Concerned and wanting to secure her finances, Emma follows the instructions and authorises the transfer.

Later, when Emma contacted the Bank to inquire about the new account, the bank had no knowledge of the call or any such account, revealing that Emma had fallen victim to a fraudulent scam, and the money had been transferred to the fraudster's account.
The bank is now working to trace the funds.

Impact on Consumers

Financial loss

Emotional Distress

Digital Distrust

Some of the common types of frauds

- Smishing and Vishing
- SIM swap fraud
- Phishing
- Spoofing
- Impersonation
- Identity theft
- Others

Need for a multistakeholder effort

Social media platforms, MNOs, banking institutions, consumer organisations, regulators, policy-makers etc. all need to come together to address this growing menace

Governments and regulators (through a WGA) can foster a collaborative approach by:

- **establishing frameworks to facilitate cross-sector and cross-border data sharing**
- **introducing regulatory sandboxes to pilot new fraud prevention technologies and services**

Mobile operators can protect their customers by:

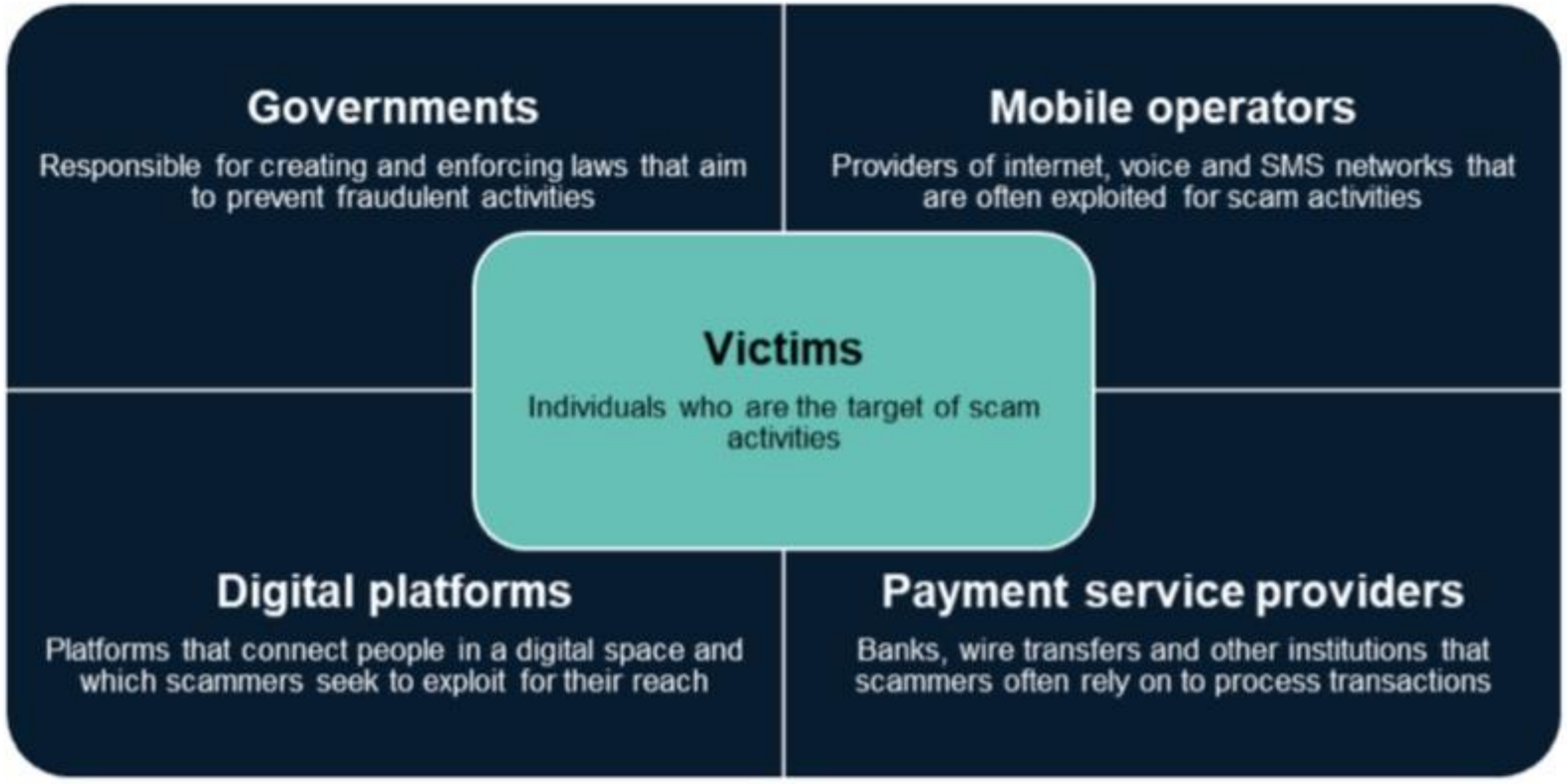
- **swiftly acting on fraud threats and sharing intelligence with industry and other sectors**
- **providing regular employee training on security, fraud and scams and developing innovative technologies**
- **publishing helpful information for consumers**

Continued..

<u>Consumers</u> can protect themselves by exercising awareness and caution, and by:

- **being vigilant and recognising warning signs**
- **learning about types of frauds and scams**
- **implementing two-factor authentication and employing strong, unique passwords**

Individuals and entities entangled in a scam economy



INDUSTRY ACTIONS

GSMA APAC Cross-Sector Anti-Scam Taskforce (ACAST)

Recognising the critical importance of cross-sector collaboration to tackle the scam economy, members joined forces to launch the ACAST initiative.

Purpose: To foster cross-industry collaboration between MNOs and digital platforms to combat the growing threat of online scams across the Asia-Pacific region. Through collaborative sharing and best practices, the Taskforce seeks to enhance user protection and rebuild trust in the digital ecosystem.

Key Deliverables:

APAC Compendium of Anti-scam Initiatives	**Engagement Roadmap**	**Common Repository of APAC Awareness Resources**	**Development of Collaboration Tools**	**Examination of Anti-scam Frameworks**

31 Organisations across 16 countries in the region

GSMA Open Gateway APIs

Some of the Asia Pacific region's mobile operators are collaborating through the GSMA Open Gateway framework to tackle online fraud and help increase consumer trust in new digital services across various countries such as Malaysia, Singapore, and Thailand.

A number of APIs are aimed at improving digital security by addressing online fraud and protecting the digital identities of mobile customers.

Globally, mobile operators from across all regions (Asia Pacific region, Europe, Latin America, Sub-Saharan Africa, Middle East and North Africa and North America) are committed to deploying APIs to reduce risk of fraud

Examples of GSMA OGW APIs

- **Number Verify checks that the user is interacting with a service from a device with the mobile phone number that has been registered and paired with the device.**
- **SIM Swap checks the last time the SIM card associated with a mobile number was changed**
- **Device Location Verification provides security in location-dependent transactions**

Operator led initiatives and technical solutions

Source: GSMA Intelligence

Operator	Solution
Airtel	In September 2024, Airtel introduced a network-based solution that uses AI to detect spam calls and messages in India. It analyses 250 parameters, such as a caller or sender usage patterns, call/SMS frequency and call duration, in real-time. By cross-referencing the information against known spam patterns, the system identifies suspected spam calls and SMS.
Axiata	Axiata has implemented its Helios platform across its operations in Asia Pacific, including Malaysia (CelcomDigi), Indonesia (XL Axiata) and Sri Lanka (Dialog Axiata). The Helios platform conducts real-time analysis to identify and prevent fraudulent activities, such as unauthorised network access and scam attempts, within its networks.
NTT Docomo	NTT Docomo uses an advanced machine-learning system to address subscription fraud and premium-rate scams. Its analytical tools process extensive datasets to identify irregular usage patterns, such as sudden increases in international calls. The system is aligned with Japan's national initiatives to combat telecoms fraud through improved KYC processes.
SK Telecom	SK Telecom has implemented AI-powered fraud detection, which includes real-time network monitoring and voice biometrics. The systems analyse call data and user behaviour to identify anomalies, such as SIM box fraud or account takeovers. Additionally, SK Telecom's approach incorporates predictive analytics to anticipate AI-enabled deepfake and phishing scams.
Telstra	Telstra has implemented a solution in accordance with Australia's Reducing Scam Calls Code, using network-level blocking and AI analytics to identify and prevent scam calls, including those using spoofed numbers. In 2024, Telstra reported blocking millions of scam calls in compliance with ACMA regulations. The company employs behavioural analytics to detect unusual traffic patterns indicative of fraud, such as Wangiri or PBX hacking.
True Corporation	In December 2024, True Corporation launched True CyberSafe – a cyber-protection system designed to safeguard against online fraudulent activities in Thailand. This system offers protection from phishing links and scam SMS, and includes call filtering. By the end of January 2025, True Corporation reported that True CyberSafe successfully blocked more than 370 million suspicious link clicks, protecting its customers from potential scams.

BEST PRACTICES

Best Practices: Regulatory Actions (Some examples)

In December 2024, the Department of Telecommunications in India announced the deactivation of more than 8.5 million mobile connections that were either registered with fake documents or linked to fraudulent activities. This action followed the introduction of ASTR – an AI-powered facial recognition tool that aids in detecting SIM cards obtained under multiple names by the same individual.

- In January 2023, Singapore implemented the Singapore SMS Sender ID Registry (SSIR) and the Decision on the Implementation of Anti-Scam Filter Solutions within mobile networks. These require organisations that use SMS Sender IDs to register with the SSIR maintained by the Infocomm Media Development Authority (IMDA), and operators to implement systems that scan all SMS messages to cross-check URLs against a continuously updated database of known malicious links. In December 2024, the Monetary Authority of Singapore and IMDA jointly introduced a new Shared Responsibility Framework that assigns banks and operators relevant duties to mitigate phishing scams.

Best Practices: Legislation (Some examples)

- In February 2025, Australia passed the Scams Prevention Framework Bill. The Australian Communications and Media Authority and other regulators will enforce industry codes for banks, telecoms operators and social media firms.

- In January 2025, it was reported that the Malaysian government was reviewing proposals to amend digital-related laws to regulate social media platforms and address online scams and fraud. The proposed amendments would expand the scope of responsibility to include telecoms operators, with coordination led by Bank Negara Malaysia

Collaborative efforts and Data sharing (Some examples)

- In Singapore, the Anti-Scam Command (ASCom) collaborates with various stakeholders, including financial institutions and telecoms operators, to share data and intelligence on scam activities. This facilitates the prompt detection and disruption of scam operations. ASCom aims to achieve greater synergy between the various scam-fighting units within the Singapore Police Force

- The Philippines Anti-Financial Account Scamming Act, enacted in 2024, enhances data sharing between the Bangko Sentral ng Pilipinas, financial institutions and law enforcement agencies to monitor and freeze accounts associated with scams. Additionally, the Cyber and Forensics Division of the Philippine SEC collaborates with foreign regulators by providing evidence to combat cross-border fraud, including fraudulent loan applications.

- In 2023, the Australian government established the National Anti-Scam Centre (NASC) within the Australian Competition and Consumer Commission (ACCC). The NASC has been credited with contributing to a 13.1% reduction in reported losses in Australia during 2023.

Examples of Global Initiatives

- GSMA Fraud and Security Group
- GSMA Open Gateway APIs
- Global Anti Scam Alliance
- Interpol Cybercrime Units
- ITU Recommendations
- Others

Conclusion: Way Forward

Build	Enable	Advance	Protect and Educate
Fraud and scam is a shared responsibility : build a collaborative ecosystem with various stakeholders	Data and Intelligence Sharing .e.g. India's Digital Intelligence Platform	Innovative Technical Solutions	Spread awareness among Consumers

THANK YOU

For further discussion/queries, contact me at nnayak@gsma.com

GSMA™