Gulistan Ladha
Director, Consumer Policy
GSMA

Industry perspective: Challenges for mobile operators

17 April 2024

GSMA™

GSMA - who we are

- Unite 1000+ mobile operators and organisations across the ecosystem and related industries
- Advance innovation and reduce inequalities around the world
- Three broad pillars:
  - Connectivity for Good
  - Industry Services
  - Solutions and Outreach

Website: www.gsma.com
Follow: @GSMA

We provide the world's largest platform to convene the mobile ecosystem at the MWC and M360 series of events

In the Media

Top Data Breaches in 2022 and 2023 Point to Increases in Phishing and Ransomware

December 30, 2023

Africa grapples with surge in digital fraud

Scam alert: Beware of phishing emails that impersonate CBUAE

A fresh round of scam messages were sent to residents in the UAE, mpersonating the Central Bank of the UAE

Does Customer Data Privacy Actually Matter? It Should.

8 JUN 2023 NEWS

Cyber Extortionists Seek Out Fresh Victims in LatAm and Asia

The growing costs of cybercrime – a data breach can impact a business for many years to come

berattacks: You could be the next target

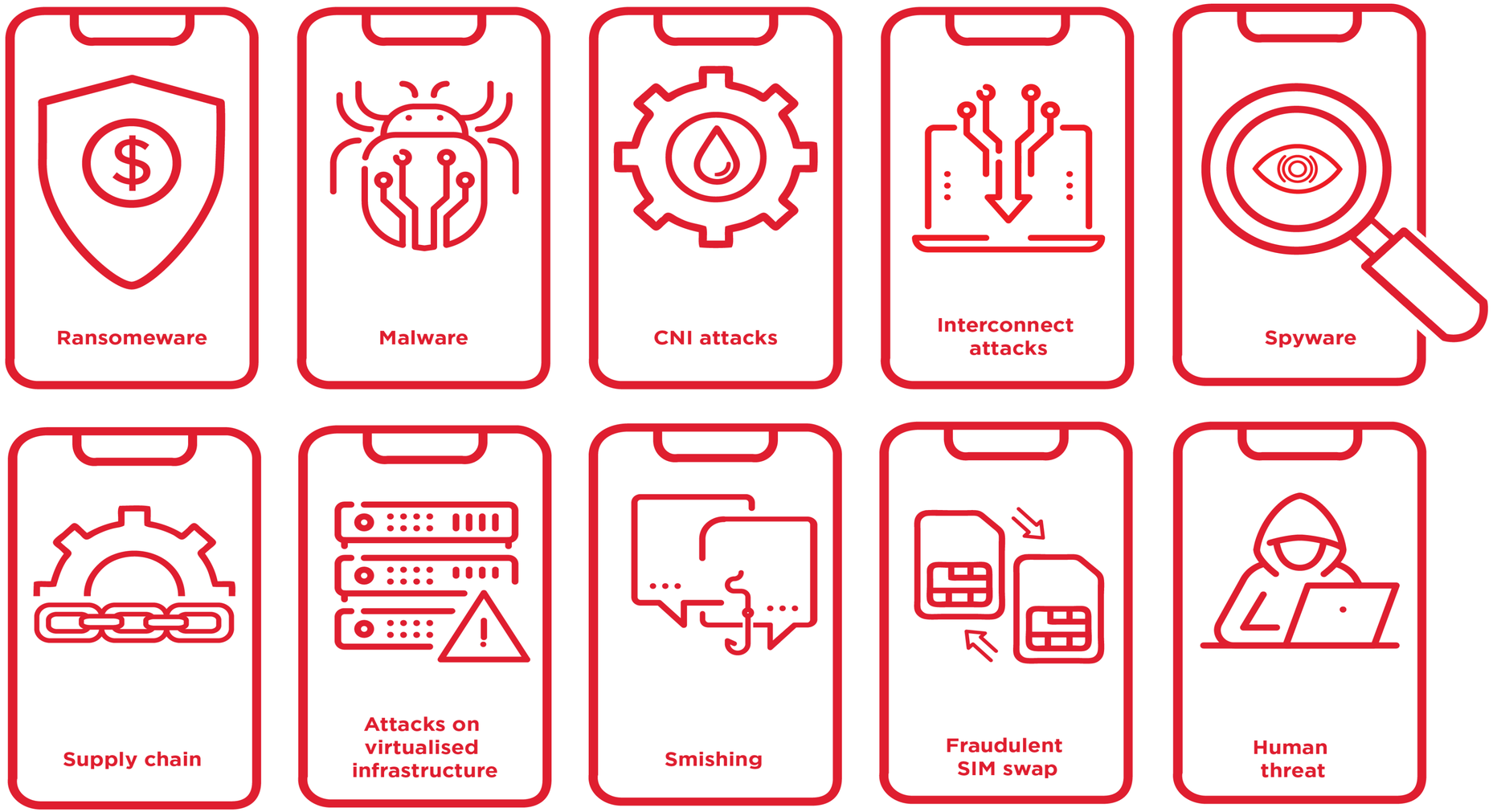
The surge of cybersecurity breaches in India has raised concerns, inviting calls for overhauling weak preventive systems, greater awareness and a stringent legal and regulatory framework

Eastern European Governments Urge Tech Firms To Fight Disinformation

Is ChatGPT a cybersecurity threat?

GSMA

Global Mobile Security Threats



Source: GSMA report: 'Mobile Telecommunications Security Landscape 2023'

GSMA

Key Priorities for the Mobile Industry

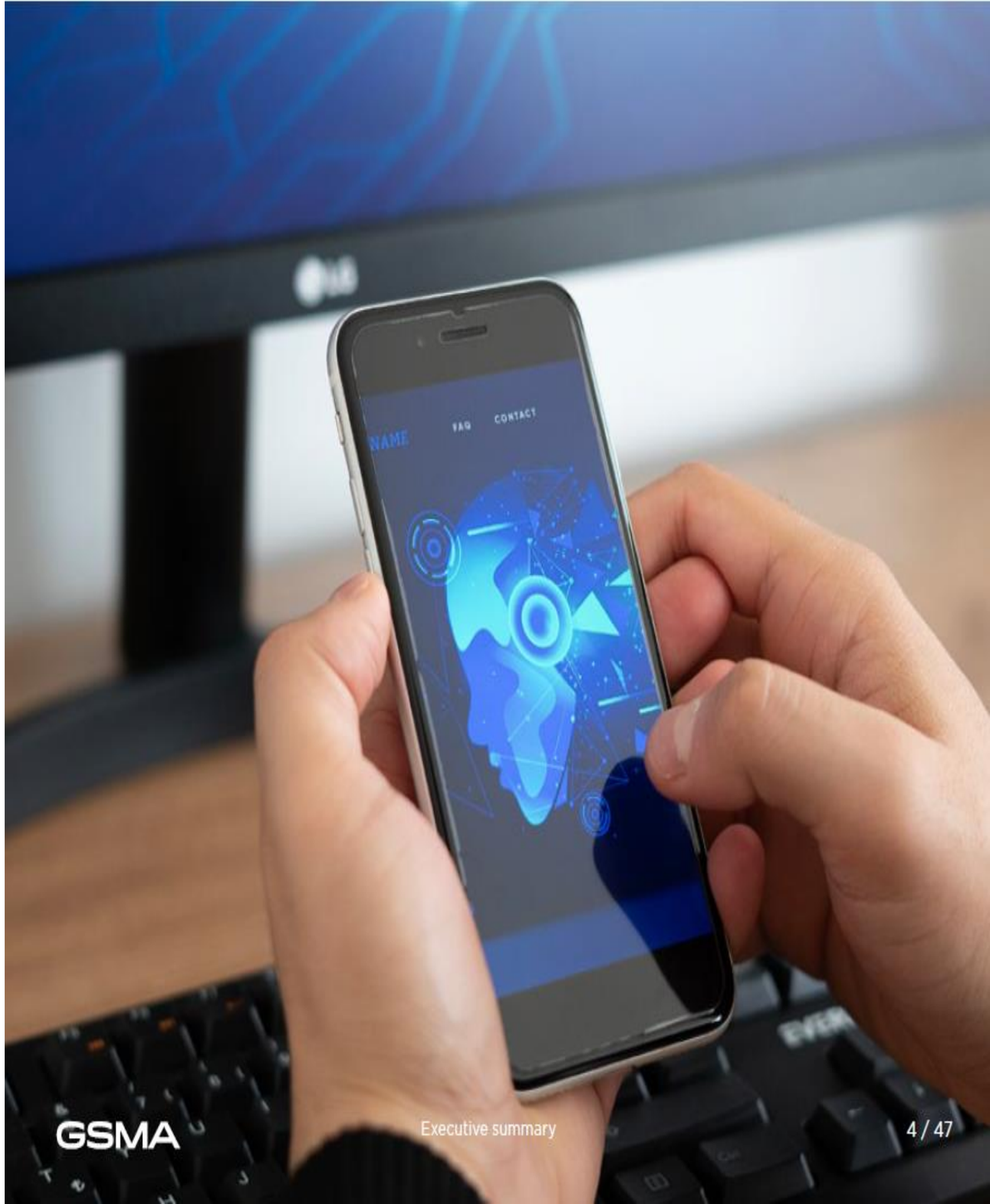
- Enable safe and secure use of products and services
- Test for vulnerabilities and deploy latest technology
- Comply with laws and regulations
- Educate customers and raise awareness
- Share best practice and threat intelligence
- Collaborate with stakeholders in the wider mobile ecosystem

GSMA Framework

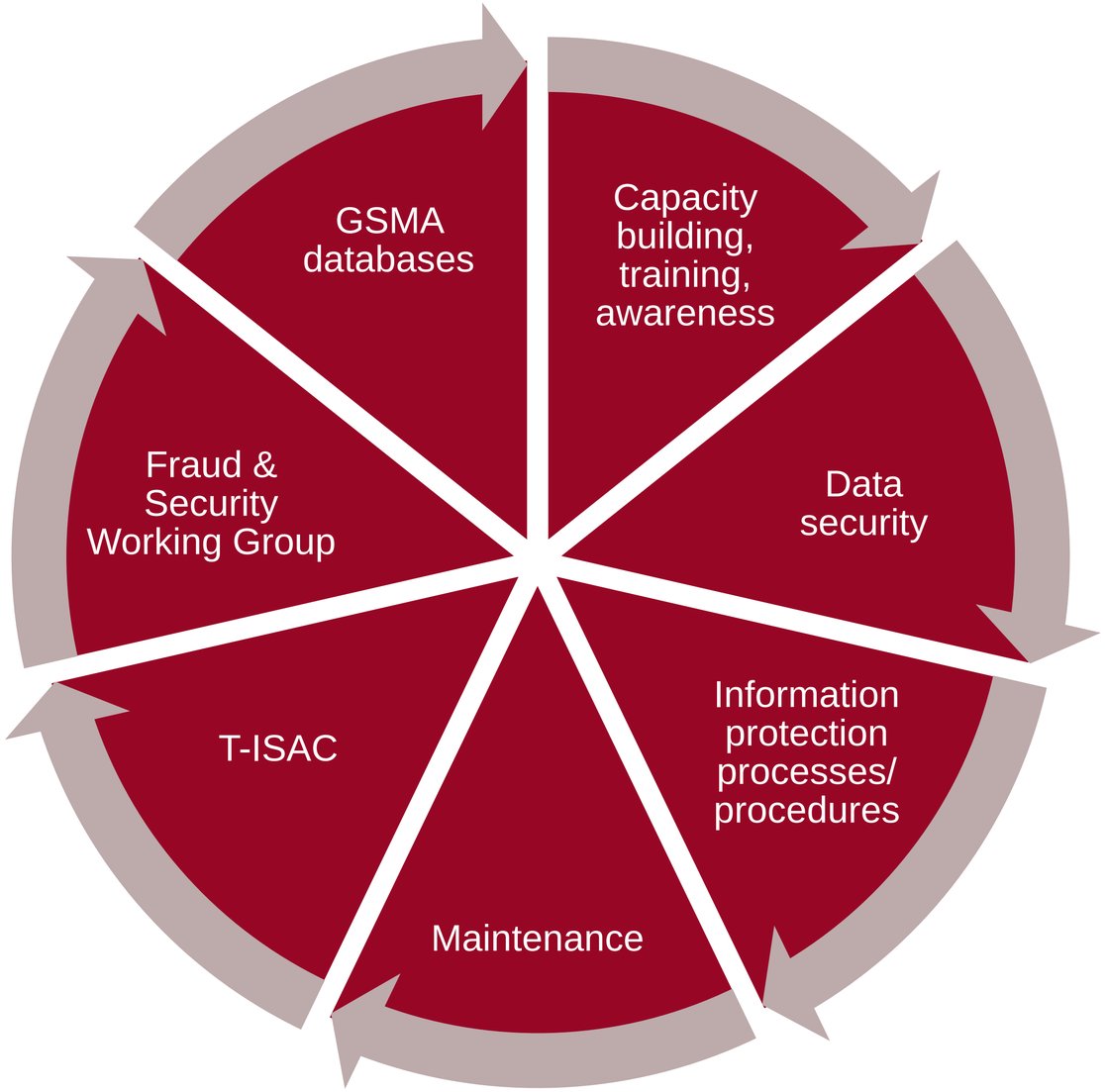
GSMA

Protect against fraud

- Incorporate ‘privacy by design’ and ‘secure by design’
- Implement best practice cybersecurity frameworks
- Collaborate with industry players to share intelligence
- Proactively educate customers
- Report data breaches and identity theft incidents



GSMA Intelligence Sharing



GSMA Fraud and Security Services

Device Check Device Registry	Coordinated Vulnerability Disclosure (CVD)	Type Allocation Code system (TAC)
eUICC Security Assurance (eSA)	Network Equipment Security Assurance Scheme (NESAS)	Security Accreditation Scheme (SAS)

GSMA Member Initiatives

Telecommunication Information Sharing and Analysis Center (T-ISAC)

- A central hub of information sharing for the telecommunication industry

Fraud and Security Group (FASG)

- Fraud and security intelligence-sharing for mobile operators

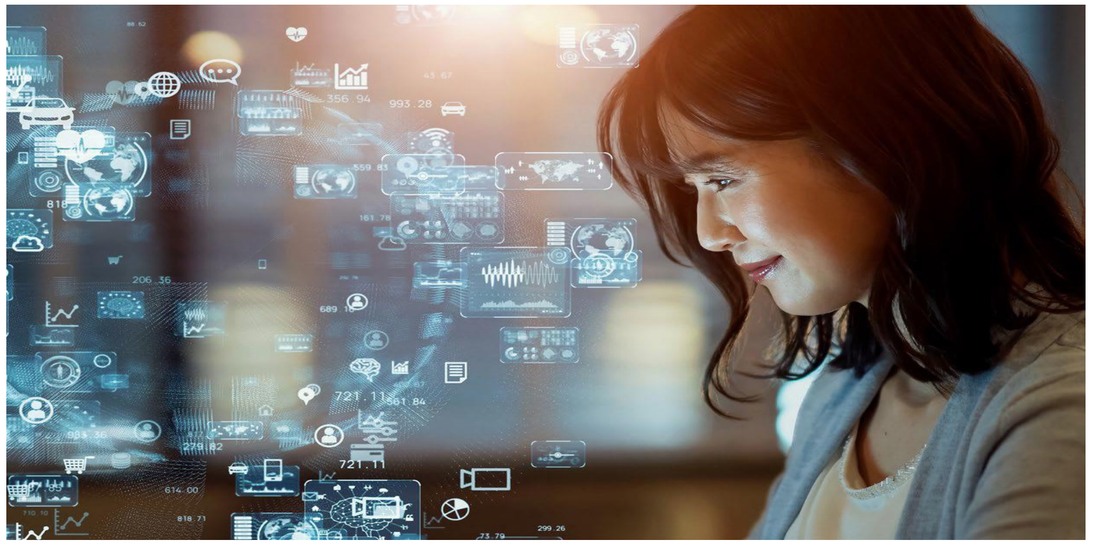
Industry can’t do it alone

Promote skills training

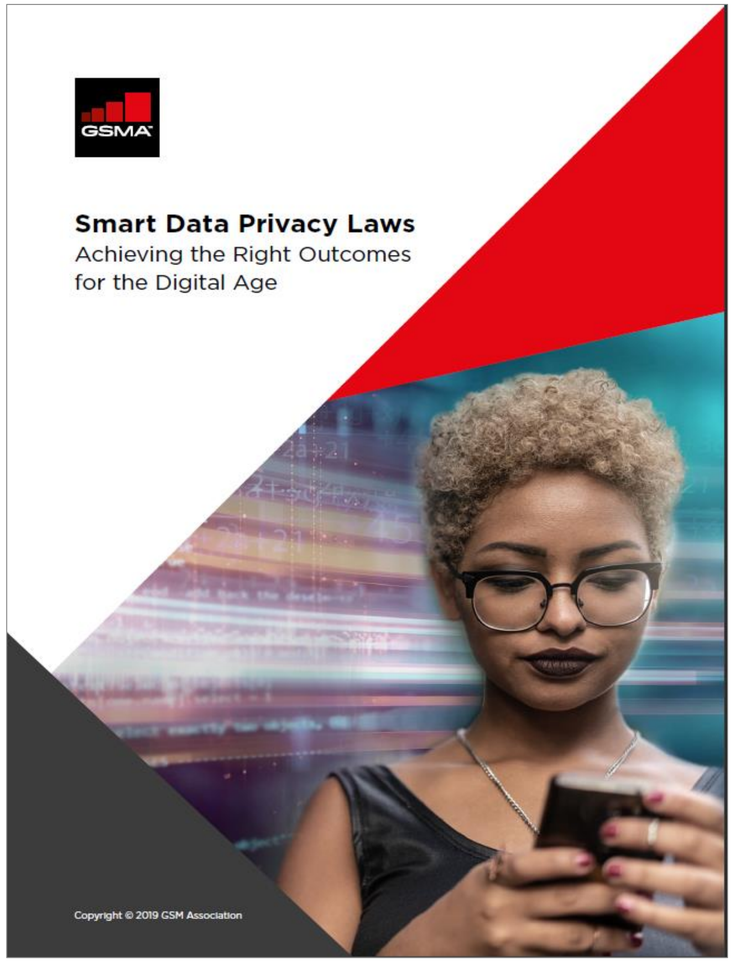
- Increasing awareness among mobile customers
- Building digital skills by including cyber skills and Internet safety considerations

Protect the public from online harms

- Multi-stakeholder efforts needed to encourage safe and responsible use of mobile-based online services and devices
- Legal frameworks, resources and processes should be targeted at criminal behaviour



Smart data privacy laws and Implementation



Resource for Policymakers

When drafting, reviewing
*Or **Implementing***
data privacy laws

*Cuts through **complexity***

GSMA Smart Privacy Laws – full version

Latin America

Challenges

- Social engineering - phishing and malware (Argentina, Brazil, Chile, Colombia, Mexico, Peru)
- In Mexico and Guatemala - over 70% of mobile owners not using mobile internet reported safety and security concerns as an important barrier
- 38% in Mexico reporting it as the top barrier

Latin America

- Anatel’s website contains information on the most common scams and how to prevent them

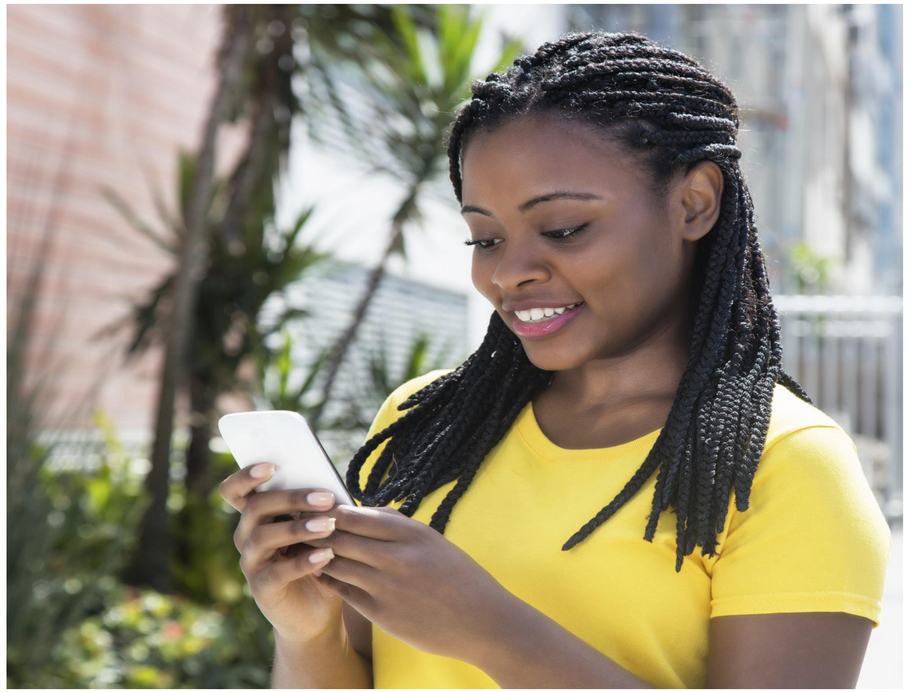
- FTC cooperation agreement with consumer protection authorities of Chile, Colombia, Mexico and Peru to combat unfair, deceptive and fraudulent practices

- Telefonica: Global Security Regulatory Framework and ISO22301 or ISO27001 certification in Argentina, Brazil, Ecuador and Peru (Colombia has SGI de Movistar)

Sub-Saharan Africa

Challenges

- M-Pesa fraud through social engineering
- Low consumer financial literacy rates
- 31% of mobile money account holders cannot use their account without help
- In 2022 South Africa saw 24% surge in reported digital banking fraud incidents (SABRIC)
- Theft of over R740 million from victims attributed to increasing fraud cases related to banking applications and online banking



Sub-Saharan Africa

Mozambique

- Collaboration between government authorities, mobile operators, internet service providers and financial institutions
- Standardised procedures for subscriber registration
- Central database for subscriber identification
- Risk centre to detect fraudulent activities
- Signatory to Malabo Convention

Operator Gateway Initiative

- Launched in 2023
- Standardises APIs by Mobile Network Operators
- Enhances security measures within banking applications and online banking platforms
- Implements robust fraud detection and prevention mechanisms
- Increases overall resilience of digital banking systems against cyber threats

Latin America

Brazil

- Claro, TIM and Vivo became the pioneer for GSMA Open Gateway
- Launched three anti-fraud network services: Number Verify / SIM Swap / Device Location.
- In March Claro recorded 3 million requests/month for the SIM Swap API

Sub-Saharan Africa

- Number Verify and SIM Swap APIs available in South Africa
- Help combat fraud and digital identity theft in sectors including banking / finance / insurance / retail
- Mobile operators are strategically placed to work with developers to help banks, financial institutions and commerce providers mitigate the risk and protect their customers

Thank you