GSMA
Services Showcase
LIVE

#18 Tackling mobile theft and fraud: How GSMA is collaborating with the mobile industry to provide innovative solutions

Tuesday 1 April 2025
14:00 BST

Agenda

Time	Segment	Speaker
14:00	Welcome and housekeeping	Chris Sumner-Smith **GSMA**
14:03	Fraud and Security Group Update	James Moran **GSMA**
14:13	How the industry is taking action on Device Theft	Natliya Stanestky **Google**
14:23	Introduction to GSMA Mobile Device Crime Data	Hugo Saboia **GSMA**
14:38	Why we contribute to the Device Registry	Steve Schwed **Verizon**
14:48	eSIM Expansion of Device Registry	James Moran **GSMA**
14:50 – 15.00	Q&A and closing remarks	Chris Sumner-Smith **GSMA**

Fraud and Security Group Update

James Moran, GSMA

April 1, 2025

GSMA™

FASG Mission

Securing the global mobile ecosystem

Centre Of Expertise

Drive industry management of mobile fraud and security

Trusted Environment

Provide a trusted environment for discussing fraud and security matters.

Increase Protection

Mobile operator technology & infrastructure

Customer identity security and privacy

Reputation

Maintain industry reputation and trust in mobile operators and services

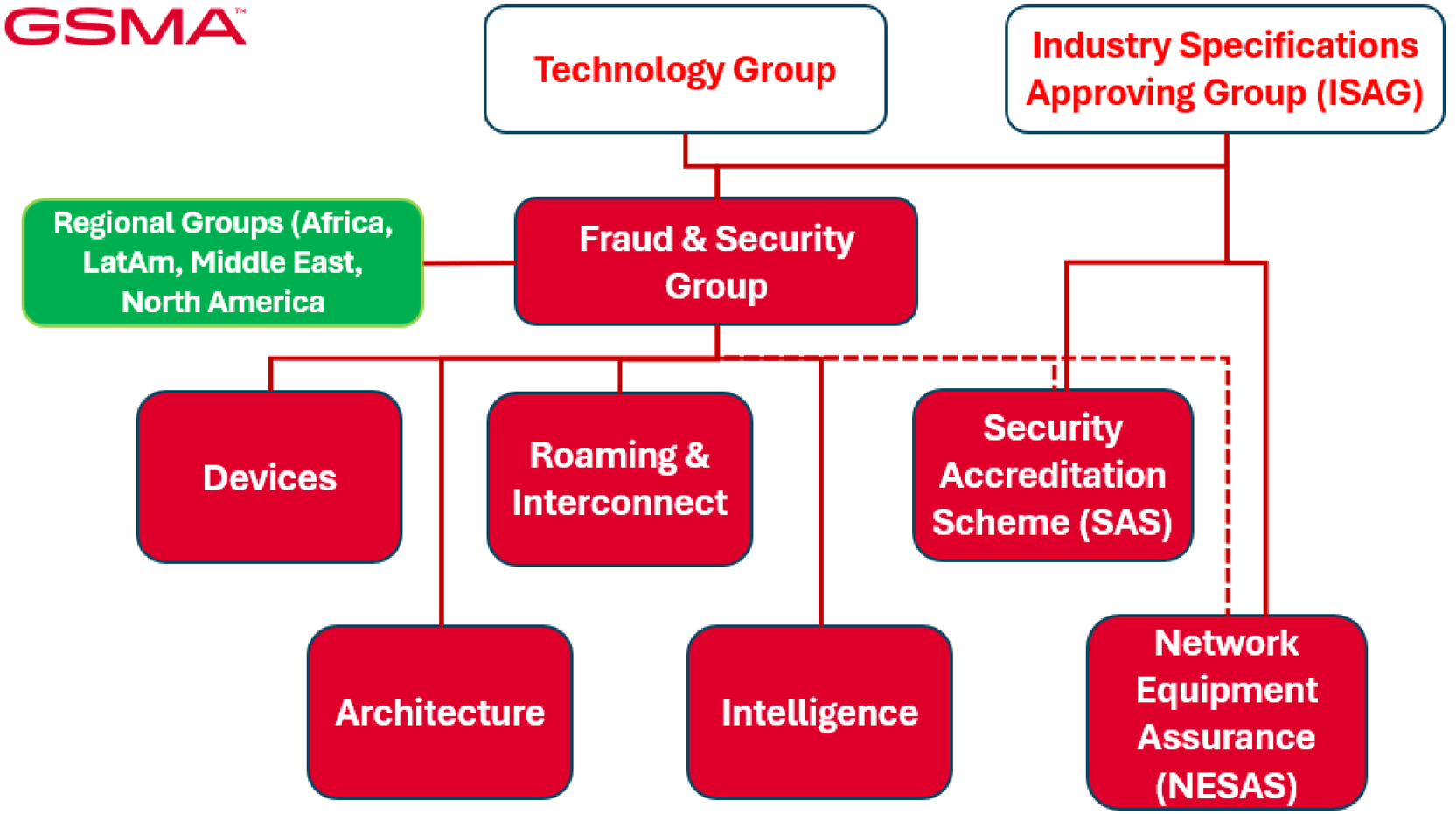
GSMA™

Fraud and Security Group

Terms of reference

- Assess the global fraud and security threat landscape
- Define and prioritize appropriate mitigating actions
- Assess and report threats and actual implementation across the globe
- Specify technical fraud solutions and security enablers and drive adoption
- Review new and existing architectures, services and solutions
- Define fraud and security requirements and baseline controls
- Promote fraud and security awareness across the industry
- Provide guidance and support for GSMA's service offerings
- Assist members with the investigation of fraud and security incidents
- Liaise with regional fraud and security groups on topics of concern
- Collaborate to improve industry and consumer protection

Fraud and Security Group Structure



SAS and NESAS are Industry Specification Issuing Groups (ISIGs) formally reporting to ISAG that operate within the FASG domain.

FASG Work Items

Increasing Security Together

Device Security

5G Security

Security Architecture

Security Assurance

Roaming & Interconnect

Intelligence

Device Security Issues Increasing and Multifaceted

Browser

Phishing
Pharming
Clickjacking
Man-in-the-Middle
Buffer Overflow
Data Caching

Phone/SMS

Baseband Attacks
SMishing

Apps

Sensitive Data Storage
No Encryption/Weak Encryption
Improper SSL Validation
Config Manipulation
Dynamic Runtime Injection
Unintended Permissions
Escalated Privileges

System

No Passcode/Weak Passcode
IOS Jailbreaking
Android Rooting
OS Data Caching
Passwords & Data Accessible
Carrier-Loaded Software
No Encryption/Weak Encryption
User-Initiated Code

Malware

Device Security Group

Terms of reference

- Be the centre of expertise on device security
- Identify, classify and work to address common device security issues
- Tackle cross-platform and cross-sector security issues
- Address end-to-end device ecosystem aspects
- Monitor and respond to reported emerging threats
- Build relationships with device security experts and key stakeholders
- Maintain and develop materials on mobile device security
- Liaise with relevant external standards bodies
- Promote and communicate the importance of device security
- Promote the use of the IMEI Database to share stolen device data

IMEI Integrity

Preserving IMEI integrity is critical for the identifier's various uses	• **IMEI differentiates genuine & black/grey market devices** • **Legitimate ranges ensures spurious IMEI identification** • **Integrity provides confidence in barring stolen devices**
Industry initiatives to enhance the integrity of IMEI implementations	• **Industry agreed technical security design principles** • **Ecosystem wide security weakness reporting and correction process established**

IMEI Technical Design Principles

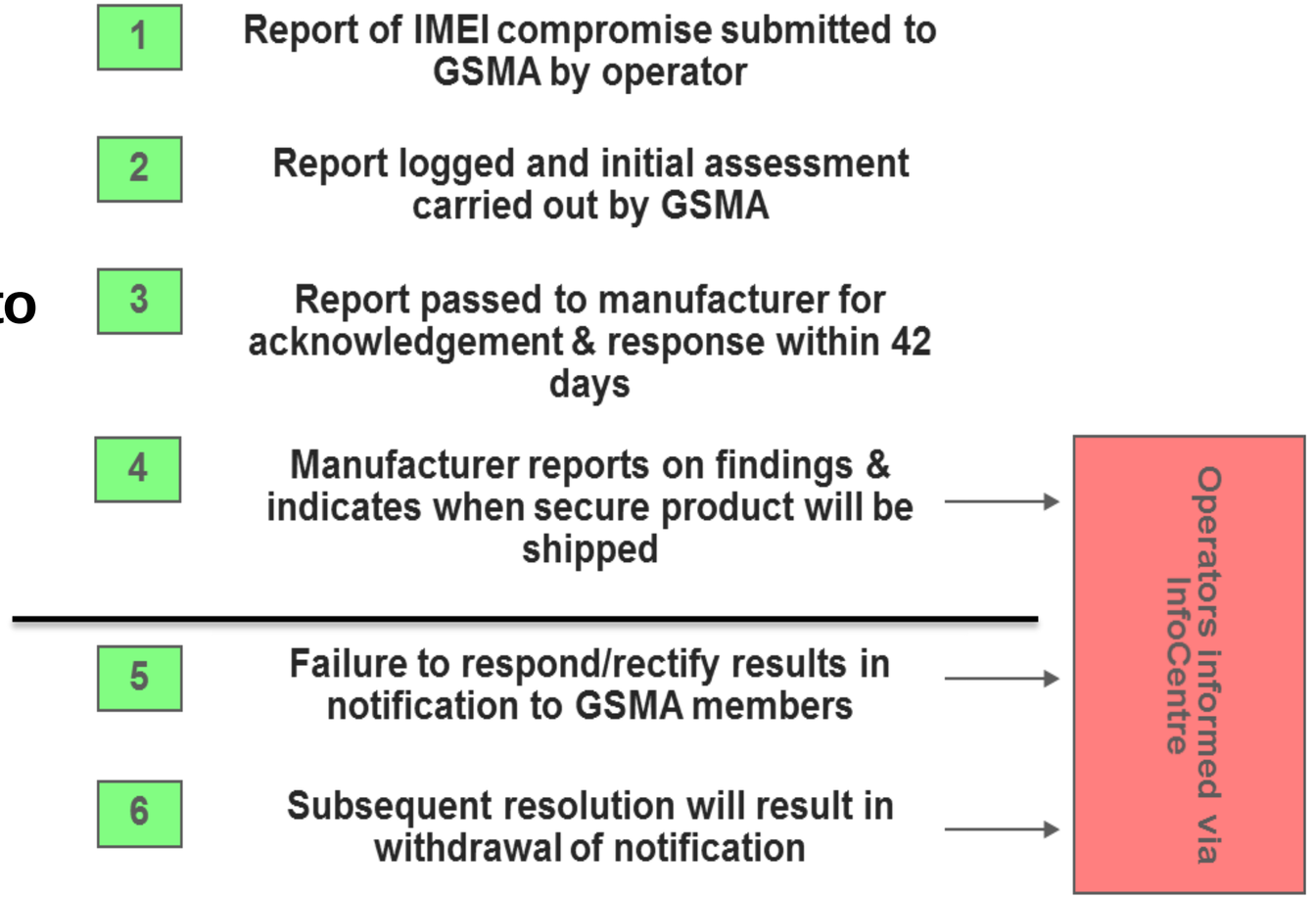
Technical security design principles agreed with manufacturers

- Uploading, downloading and storage of executable code and sensitive data
- Protection of components' executable code and sensitive data
- Protection against exchange of data/ software between devices
- Protection of executable code and sensitive data from external attacks
- Prevention of download of a previous software version
- Detection of, and response to, unauthorised tampering
- Software quality measures
- Hidden menus
- Prevention of hardware substitution

IMEI Security Weakness Reporting and Correction Process

Report device models/ manufacturers where IMEI tampering has been detected to GSMA

GSMA will address the issue with the manufacturer



Device Theft Related Publications

- Mobile device theft whitepaper
- SG.18 – Device Registry Specification and Access Policy
- FS.44 – Mobile Device Crime Data Third Party Access Policy
- FS.45 – Device Blocking and Data Sharing Recommended Practice
- SG.24 – Anti-Theft Device Feature Requirements

GSMA White Paper: Phone Theft

Nataliya Stanetsky, Google

April 1, 2025

GSMA™

Mobile device theft is becoming a global safety crisis

BBC

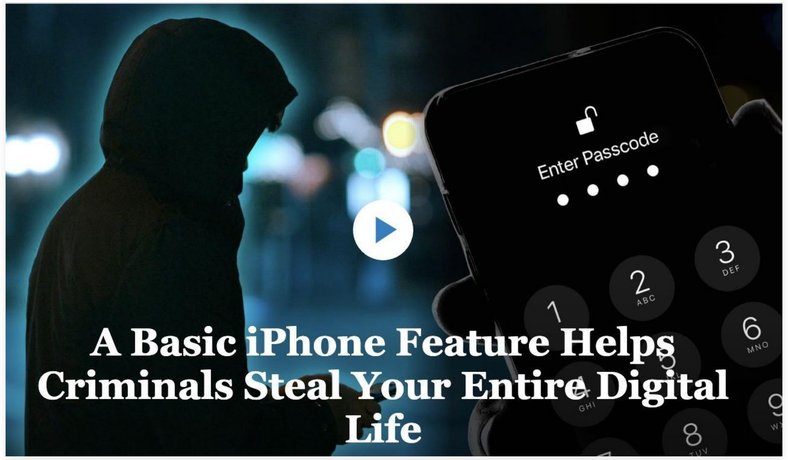
Register Sign In

London mayor and Met boss urge phone firms to help tackle theft of mobiles

17 October 2023

Share

THE WALL STREET JOURNAL.



GSMA

Background and motivation

Importance and Implications of mobile theft has become far greater due to the nature of information it holds

- Mobile Theft has become more sophisticated over last decade
- Despite anti-theft measures theft rate remains steady at 1% of active subscribers. With increment in subscribers, the number of theft respectively grows.
- Mobile phones hold sensitive user data and information that upon compromise may lead to security breaches and safety risks

Impacts of device theft

Customer Experience

Negatively impacts customer trust and satisfaction
Personal safety and security risk

Financial Impact

Financial loss for device owners, MNOs, OEMs, retailers and insurance companies
Increases prices

Security & Privacy

Risk of identity theft, and access to unauthorized data e.g., wallet, media, PII, etc, may impact safety and security

Reputational risk

Negative impact on reputation of mobile network operators, manufacturers and product developers

Reasons for mobile theft

Financial gain

Flagship mobile devices are highly valued locally or internationally

Steal phone and break them into parts to sell it

Laundering phones for cash commonly via thrift-shops, second-hand electronic store, online auctions, etc.

Identity Theft and Extortion

Identity theft by unauthorized access to personal financial accounts

Money Laundering

Launder funds by funding trafficking and distribution of stolen devices

Organized Crime and Systematic Fraud

Swapping IMEI numbers to with someone in another country

Organized phone snatching from tourists to use it against MNOs for fraud

Tax avoidance

Stolen devices can mean a discount of 10% - 30% of VAT

Theft for Services

Use access to bank accounts and contactless payments to buy goods for sale

Personal usage

Steal and use

GSMA™

Deterrence features offered in the mobile ecosystem

Deterrence capabilities today primarily falling into the categories of physical and software-related protection

Physical Protection Solutions

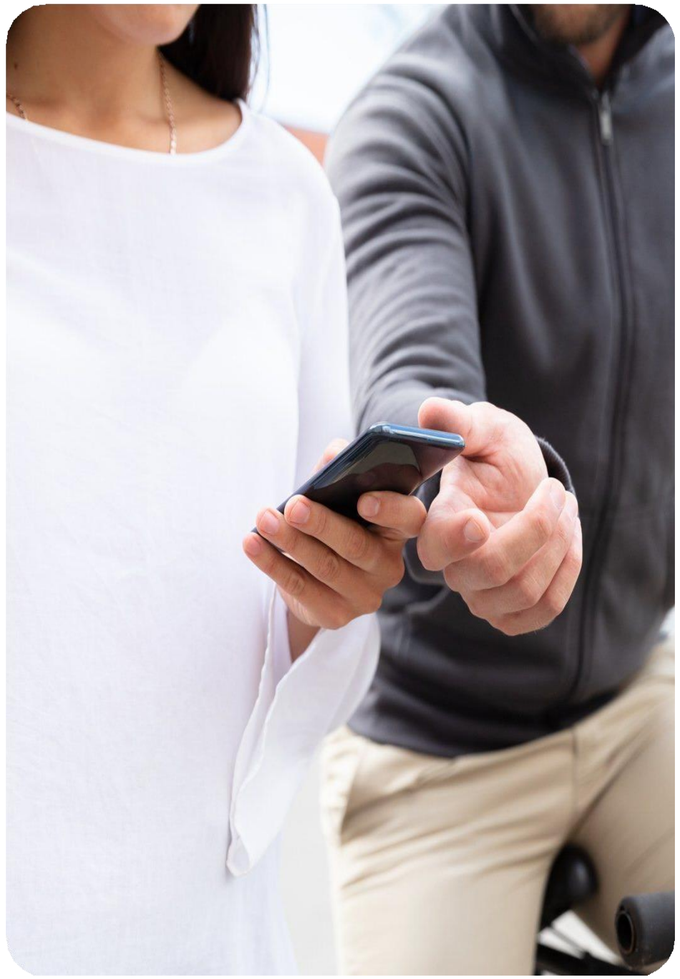
are commonly used in retail to prevent device theft:

- Cable retention solutions are often used to "lock down" devices in a store.
- Some devices use geofencing software to set an alarm when moved from their intended location (e.g., a storefront).
- Tethering mechanisms can "brick" a device if the alarm is not silenced within a set time or after exceeding the geofence area.

Software Level Solutions

can occur at the device level, network level or both

- Stolen devices can be "bricked" (made unusable) by the victim or Mobile Operator.
- Success is ensured by “Persistent locks” ensuring the device remains unusable / unsellable even after a factory reset.
- All modern mobile operating systems offer hardware backed lockscreen protection (e.g., PIN or Passcode) and file-based encryption.



GSMA™

OS

Deterrence features offered in the mobile ecosystem

Android OS features

Find My Device

Android phones allow owners to find, secure, or erase device data remotely.

Trusted friends or family members can help locate, secure, or erase the owner's device.

Multi-user mode

Allows trusted users (e.g., family members) to share a device such as automobile using digital key.

Primary member can remove, disable, lock or perform remote factory reset on the device.

Locating the device

Find My Device uses GPS, Wi-Fi, and cell towers to locate the device and can play a sound if it's nearby.

Screen lock options

Disabling Find My Device or extending screen timeout now requires user auth.

Locking a device remotely using verified phone number and challenge on any device

OS

Deterrence features offered in the mobile ecosystem

Android OS features (continued)

Private Space

New feature lets a user create a separate secure area in the phone that can be hidden and locked with a separate PIN.

Biometric Authentication

Allows users to have biometric authentication such as facial recognition or fingerprints. Additionally, mandatory biometric authentication will be required for changing critical settings or apps.

Google Files Safe Folder

Provides encrypted, password-protected storage for sensitive files, inaccessible without authentication.

Theft Detection Lock, Offline Device Lock, and Failed Authentication lock

Locking the phone when detecting unusual movements of the phone (using AI), e.g., snatch, wireless connectivity is disabled, or after consecutive authentication failure.

OS

Deterrence features offered in the mobile ecosystem

Apple iOS features

Find My App

Helps users locate Apple devices like iPhone, tracks them in the map and inform user if left in unfamiliar places.

Stolen Device Protection feature requires sensitive actions in a stolen device to undergo Security Delay, biometric verification, hour wait, and re-authentication.

Hardware Security and Biometrics

Uses the principle of limited functions to support only specific functions to minimize hacking risks, ensures device starts securely, encrypts user data and allows only authorized users.

Uses **Secure Enclave,** an isolated part of the hardware to store and process biometric data, manage encryption, etc.

Users can remotely lock lost devices via **Lost Mode** and erase permanently lost devices either in **Find Devices** on iCloud.com/find or in Find My of another trusted Apple device.

Marking an Apple device as lost disables Face ID and Touch ID being used to unlock the Apple device.

Face ID data—including mathematical representations of one’s face—is encrypted and protected by the Secure Enclave.

OEM

Deterrence features offered in the mobile ecosystem

HMD Global

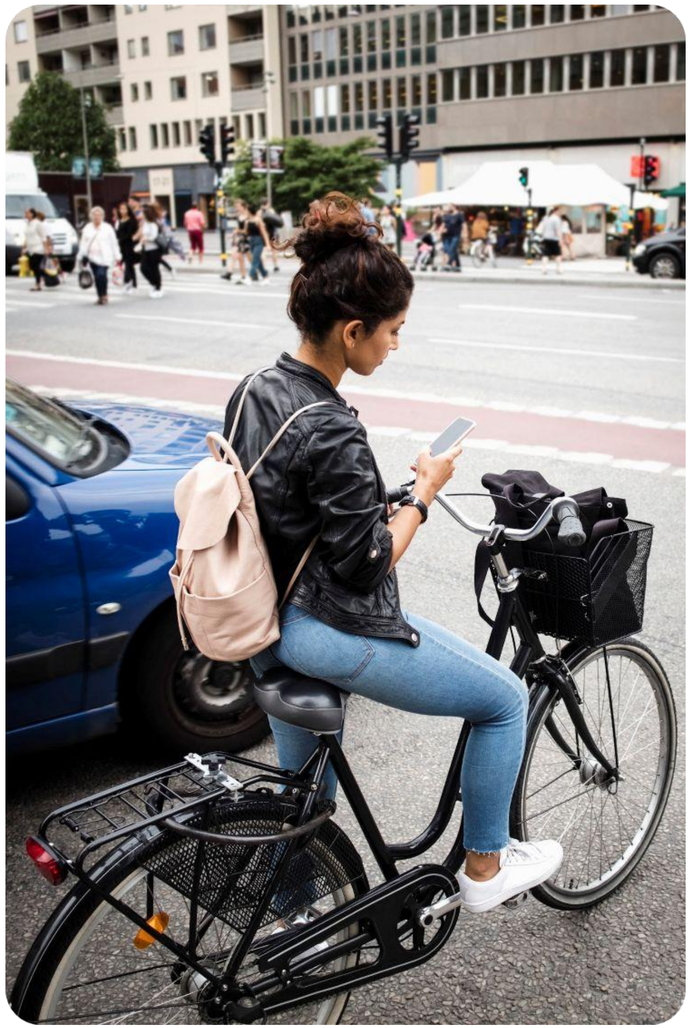
HMD Global offers remote device locking of assets such as mobile devices to prevent theft/fraud

Feature allows owners to:

Lock the network on the enabled devices

Enable specific operator's network instead of manual SIM lock

Prevent device use on certain networks



GSMA

OEM

Deterrence features offered in the mobile ecosystem

Huawei

Locate, lock or erase data

Huawei allows users to locate the device in a map using Huawei cloud with Huawei identifier.

Once the device is located, an authorized user can lock it. If the device doesn’t have a password, then a new lock screen password can be set.

Once the device is located, all the data can be erased from the device, enforcing its factory setting.

Biometric Protection

Users can unlock and authenticate their device using biometric data (fingerprints, faces, voiceprints).

The pre-processing, entry, and authentication of biometric data are performed and stored in a highly secure part of the device.

The data is turned into a secure code and stored safely on the device and not shared anywhere else outside of the device.

OEM

Deterrence features offered in the mobile ecosystem

Samsung

Locate, lock or wipe registered Samsung devices.

Locate the device, showing an approximate location on a map.

Lock the device remotely, by entering a PIN.

Lock power off feature prevents unauthorized users from powering off the device.

Wipe feature allows remote data deletion by the authorized user.

Extended battery maximum power saving mode with Lock power off to locate device.

Samsung Padlock (Galaxy Lock) Frictionless remote lock, available in Brazil only.

Samsung Knox A comprehensive mobile security platform for hardware and software threats.

Knox Vault Keeps biometrics data in the secure processor and isolated memory, which includes hardware-based protection.

Offline finding Offline Finding will find the device even when it is disconnected.

Secure Folder Isolated encrypted space on the device for storing data.

OEM

Deterrence features offered in the mobile ecosystem

Motorola

Secure Folder

Motorola Secure Folder protects sensitive apps and media, keeping work and personal information hidden.

It can be customized with a fake name and icon to deceive device thieves.

Lock Screen Security

Users can enable a function to keep network and security features locked when the screen is locked.

Enabling this setting randomizes
the PIN pad configuration on the lock screen.

Auto lock detection

Enabling this feature locks the phone outside of trusted places or when disconnected from trusted devices.

Privacy Dashboard

One can view apps accessing data, their permissions, and usage times.

OEM

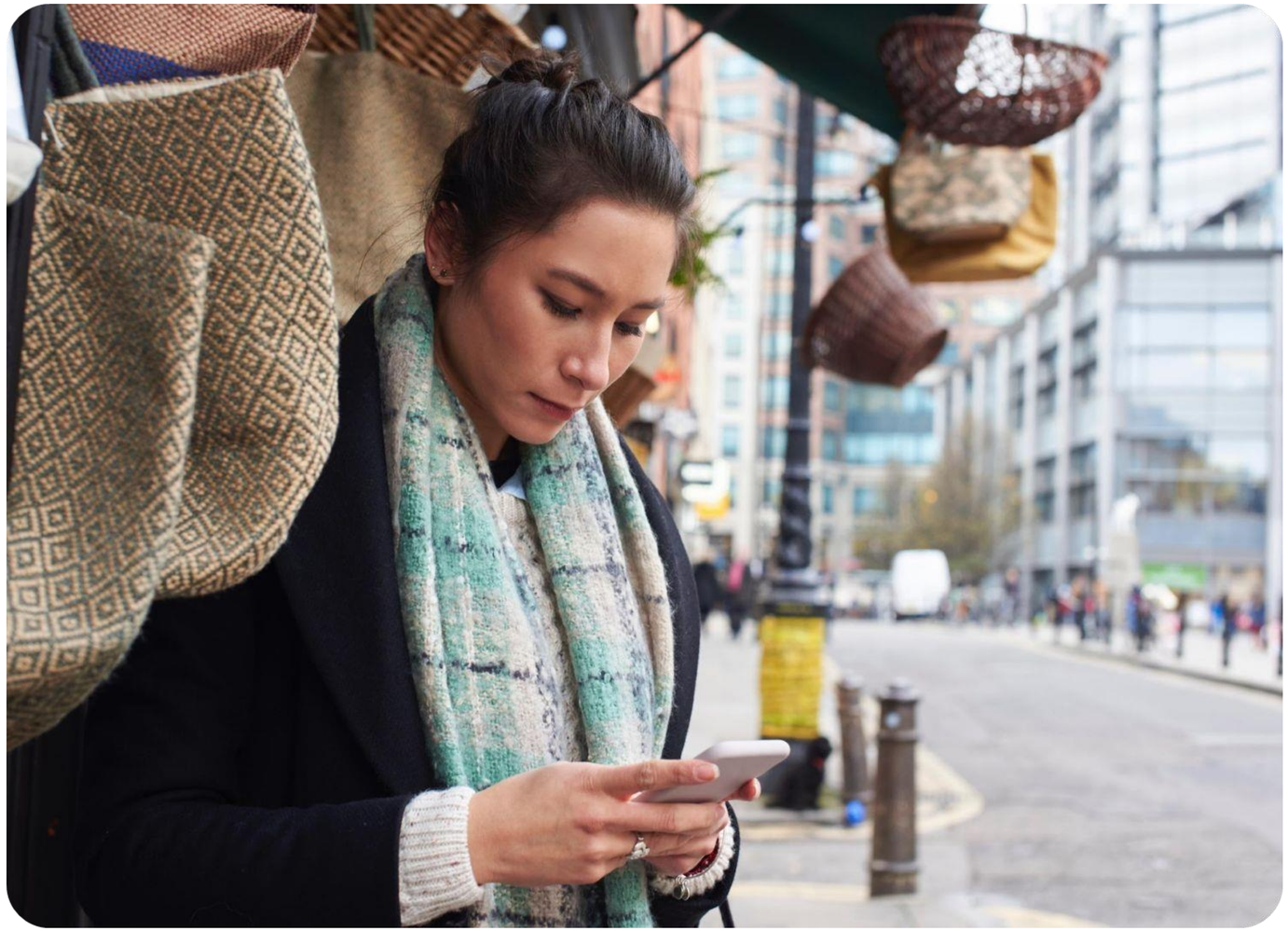
Additional Enterprise Control and Deterrences

Enterprise and Government Usage

All modern mobile operating systems/mobile devices offer special enterprise management capabilities and controls that could further protect the enterprise data on a lost or stolen device.

Each of the following OS vendors provide additional enterprise-specific deterrence capabilities.

- **Google Android**
- **Apple iOS**
- **Samsung Knox**
- **Huawei Harmony OS**



GSMA

For consumers

Recommendations for device theft prevention

- Use a strong PIN or password
- Use biometrics authentication
- Write down your phone’s IMEI number
- Pin a screen to lock your device to one app that remains in view until you un-pin using your PIN, pattern of password
- Enable additional security for your apps
- Use passkeys to log-in to websites and apps
- Backup and restore your data
- Set a SIM PIN
- Hide notification content from the lock screen

GSMA

GOV'T

Government interventions

UK Mobile Telephone Reprogramming Act 2002 declared re-programming of unique identifier as illegal and adopted Recyclers Code of Practice

Colombia's CRC, ICT Ministry, and mobile operators set up a system to register and block stolen devices.

Ecuador's regulator implemented a positive list of Type Allocation Codes to block invalid IMEIs.

Kenya's Communication Authority proposed a DMS targeting counterfeit devices and whitelist IMEIs in 2020.

Uganda's Communication Commission adopted a central equipment registry to block counterfeit devices in 2019.

Ukraine operates a national registry of IMEI numbers.

USA working on an update to Federal Law to make it illegal to advertise restricted devices on digital marketplaces

GSMA

OTHER

Deterrence features offered in the mobile ecosystem

Other/Third Party Protection

Multiple third-parties offer device lock solutions that can "brick" a mobile device.

Trustonic provides a SaaS platform consolidating Android OS and OEM solutions for improved security.

Trustonic's platform enhances payment behavior, deters theft, and integrates seamlessly via APIs.

Device financing involves third-party providers offering locking or bricking solutions.

Non-payment of weekly or monthly fees results in device locking.

Payment via online portal enables quick unlocking. Locking persists through factory resets

Police operations have been deployed to discover techniques and to gather information.

TV advertising, posters and online campaigns to raise awareness.

Recyclers Code of Practice established requirements for incoming phones.

.

GSMA™

Conclusion and Result

- Increase awareness of device theft risks and prevention techniques
- Potential measurable reduction in device theft rates over time
- Reduce losses and increased revenue for mobile operators, manufacturers and insurance companies
- Improve customer experience and enhance trust in the ecosystem
- Reduce identity theft and better data protection for users
- Positive brand image for operators, manufacturers and entire mobile industry

GSMA

Hugo Saboia,
Senior Product Director,
GSMA

Agenda

Overview

Stakeholders and Roles

Where and How Used

Device Check and look ups

There are nearly 9 billion smartphones globally. ~1% of smartphones are stolen annually globally.

With 80-90 million stolen devices, organizations need to protect their customers, their assets and their reputations.

Deliver **peace of mind** across the global secondary device market.

Lead the way to **effective device crime prevention.**

GSMA™

GSMA's role in combatting mobile device fraud and theft

Contributors

Insurer

Retailer

Distributor

OEM

MNO / MVNO

Network Operator Access

Device Status Exchange

- Mobile Network Operators globally help protect **1+ billion** users

GSMA Device Registry

Multiple data sets and use cases to help prevent device crime

Safer Device handling

GSMA Device Check™

- Trade ins / recycle / repair / insure
- Law Enforcement & customs investigations

GSMA's role in combatting mobile device fraud and theft

Contributors

Insurer

Retailer

Distributor

OEM

MNO / MVNO

Network Operator Access

Device Status Exchange

- Mobile Network Operators globally help protect **1+ billion** users

GSMA
Device Registry

Multiple data sets and use cases to help prevent device crime

Safer Device handling

GSMA Device Check™

- Trade ins / recycle / repair / insure
- Law Enforcement & customs investigations

Device Registry Contributors

Contributors

- **> 170+ accounts in all 6 Continents**
- **Must directly own devices, *provide inventory tracking and management solutions* and/or operate mobile networks**
- **Examples are device manufacturers, retailers, insurers, MNOs/MVNOs, asset/inventory managers and device re-sellers**
- **CNOs (Contributor Network Operator) are uniquely permitted to download data from the Device Registry to facilitate ongoing network-based checking and blocking.**

Use Cases

Stolen or Lost	Fraudulently Obtained	Broken or Faulty	Duplicated IMEI	Court Ordered Block	Ownership Claim	Financial Claim
• Not with rightful owner	• Obtained with no intent to pay • Sufficient evidence to file a police complaint	• Technical and/or safety issue	• IMEI is known to be duplicated • Suggests counterfeiting or tampering	• MNO use only • Legal obligation	• Assert ownership • Prevent unapproved trade • Flag devices in transit or inventory	• Assert financial claim • Prevent premature trade

Block trade and use (Block List)

Consider further investigation before trade or use (General List)

GSMA's role in combatting mobile device fraud and theft

Contributors

Insurer

Retailer

Distributor

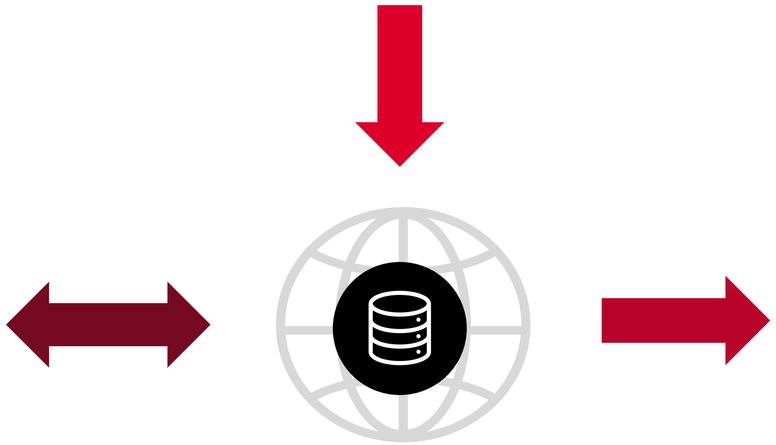
OEM

MNO / MVNO

Network Operator Access

Device Status Exchange

- Mobile Network Operators globally help protect **1+ billion** users



GSMA
Device Registry

Multiple data sets and use cases to help prevent device crime

Safer Device handling

GSMA Device Check™

- Trade ins / recycle / repair / insure
- Law Enforcement & customs investigations

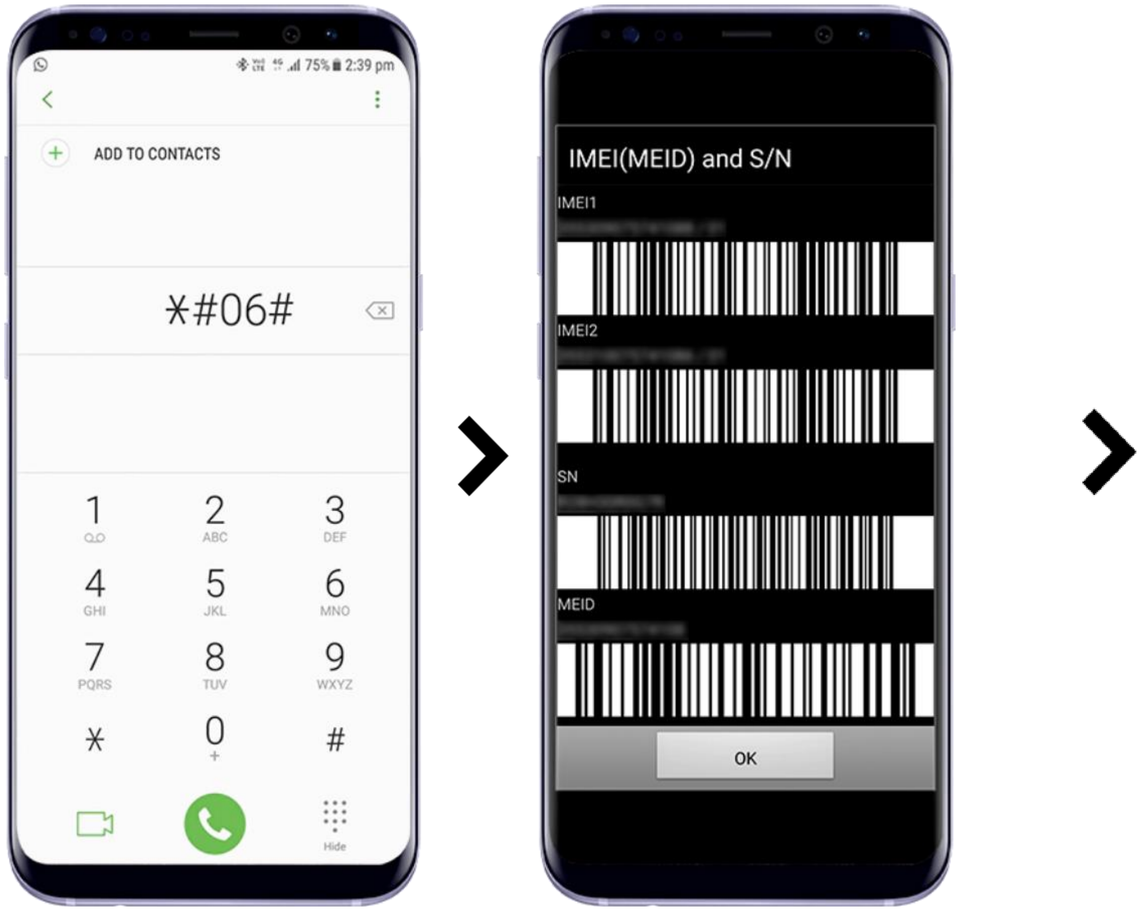
Who uses GSMA Device Check?

Device Trade In / Device Recyclers / Device Repairers / Device Retailers/ Insurance Companies / Law Enforcement investigations / MNOs / MVNOs

- 1000+ organizations
- 50+ countries
- 150+ million devices queried per year

GSMA™

What does a look up show?



Device Status:

Block List

General List

Device History

Previous reports to the GSMA Device Status Lists

Device Details

Manufacturer

Model

Band Name

Device Type

Bluetooth

WLAN

& more

How can GSMA Device Check™ help the ecosystem?

	Identify and eliminate devices (via IMEI) reported as lost or stolen before you acquire, engage or activate them	Confirm model for authenticity and to help calculate value and/or ensure appropriate tax duties are paid	Reduction in financial losses from device crime, fraud and increases the chance of recovering stolen assets	Establish whether a device is valid and not fraudulent	Provide fast and accurate point of sale information	Helps prevent lost and stolen devices re-entering the supply chain	Deters criminals by making theft and fraud less rewarding	Monitor your device inventory for ongoing lost/stolen/ownership status changes	Helps police investigate lost/stolen devices, including repatriation of devices and identifying criminals linked to robberies
Device Insurers	✓	✓	✓	✓		✓	✓	✓	
Device Recyclers	✓	✓	✓	✓	✓	✓	✓	✓	
Device Retailers	✓	✓	✓	✓	✓	✓	✓	✓	
Government and Law Enforcement Agencies		✓		✓		✓	✓		✓
MNOs/MVNOs	✓	✓	✓	✓	✓	✓	✓	✓	

GSMA™

Blocklisting and SIM Locking

Steve Schwed
Fraud Strategy
April 1, 2025

verizon

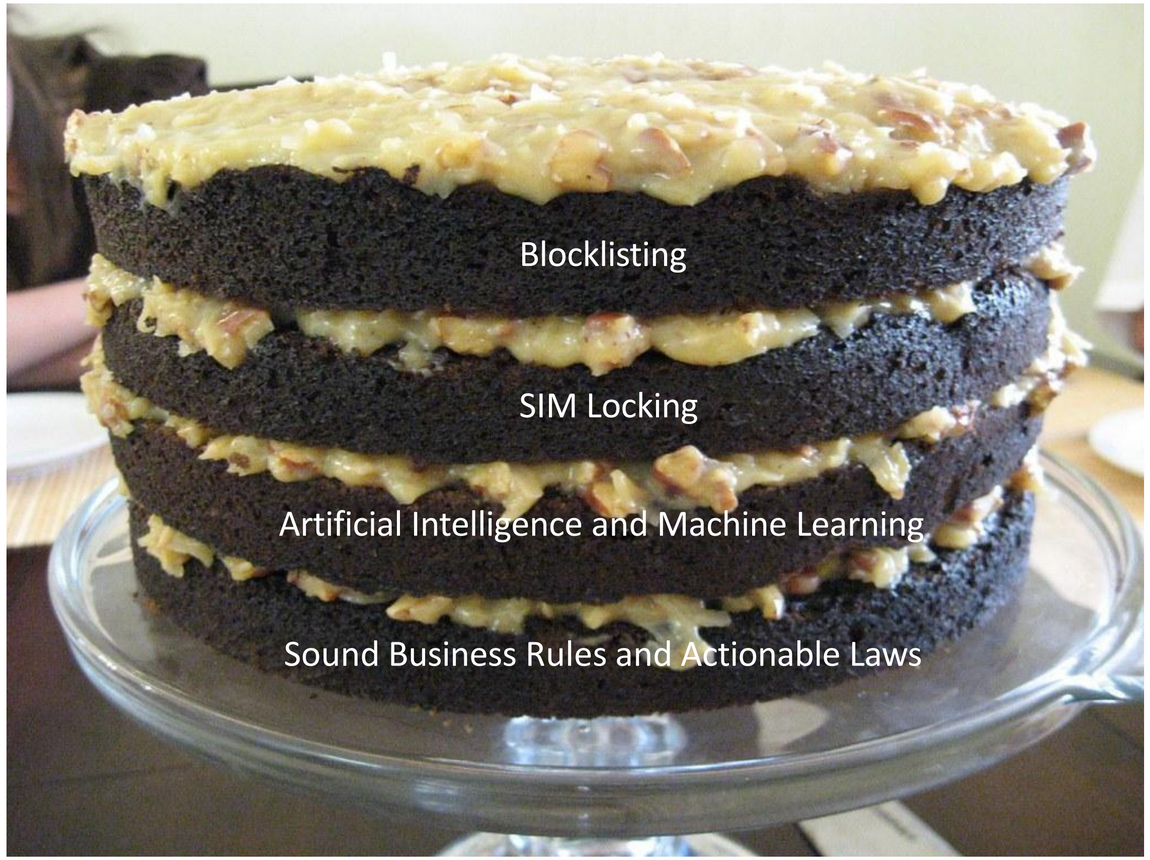
About the Speaker …

Steve Schwed

Vice President | CFCA
Verizon | Fraud Strategy Manager

Steve began his career in telecommunications in 1997 with Bell Atlantic Mobile in their Customer Financial Services group before assuming responsibility for the Executive Relations group for the Philadelphia Region in 2000 followed by managing the Verizon Wireless National Executive Relations Team from 2005 until 2013.
In addition, Steve was responsible for maintaining the relationship and service level commitments for responses to consumer complaints for the various Attorneys General, The FCC and other regulatory and consumer advocacy groups.
Steve's involvement with Telecommunications Fraud began in 2013 while working as a Process Manager in the VZW Customer Service Groupand was tasked with addressing issues related to Loss and Policy. Steve officially joined Verizon's Fraud Strategy Team in 2015. He is a member of various GSMA Forums and member of the CFCA and co- chairs the CFCA Handset Trafficking Taskforce.
Steve holds a bachelor's degree in Economics and speaks frequently regarding handset Fraud Losses .

A Comprehensive Strategy for Device Assurance



GSMA Blocklisting Objectives

GSMA Centralized Electronic Identification Register (CEIR)

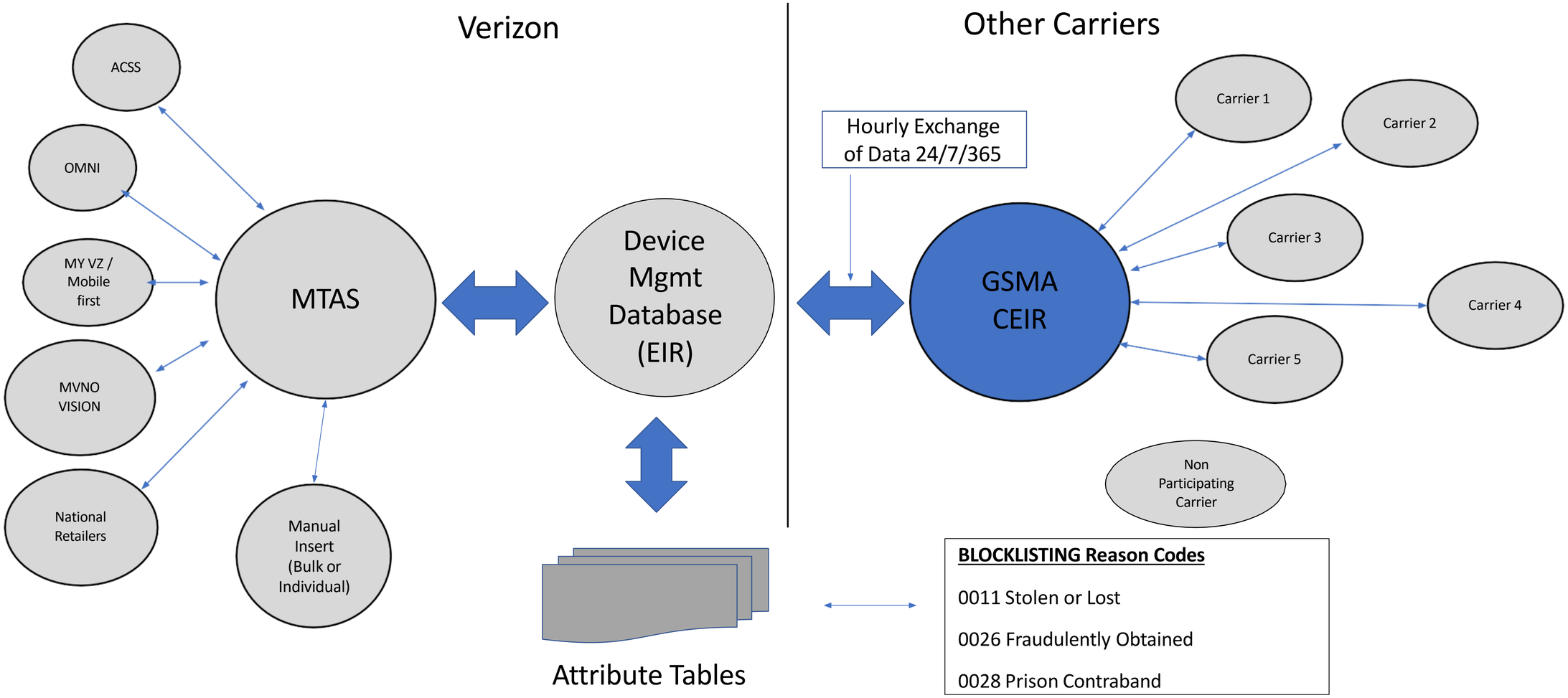
1. **Homogenous Process Across Carriers**
   - Engage all carriers possible
   - Ensure treatment methods are clearly defined

2. **Create a Better Barrier from Fraudsters**
   - Devalue Devices
   - Make device activation more challenging.

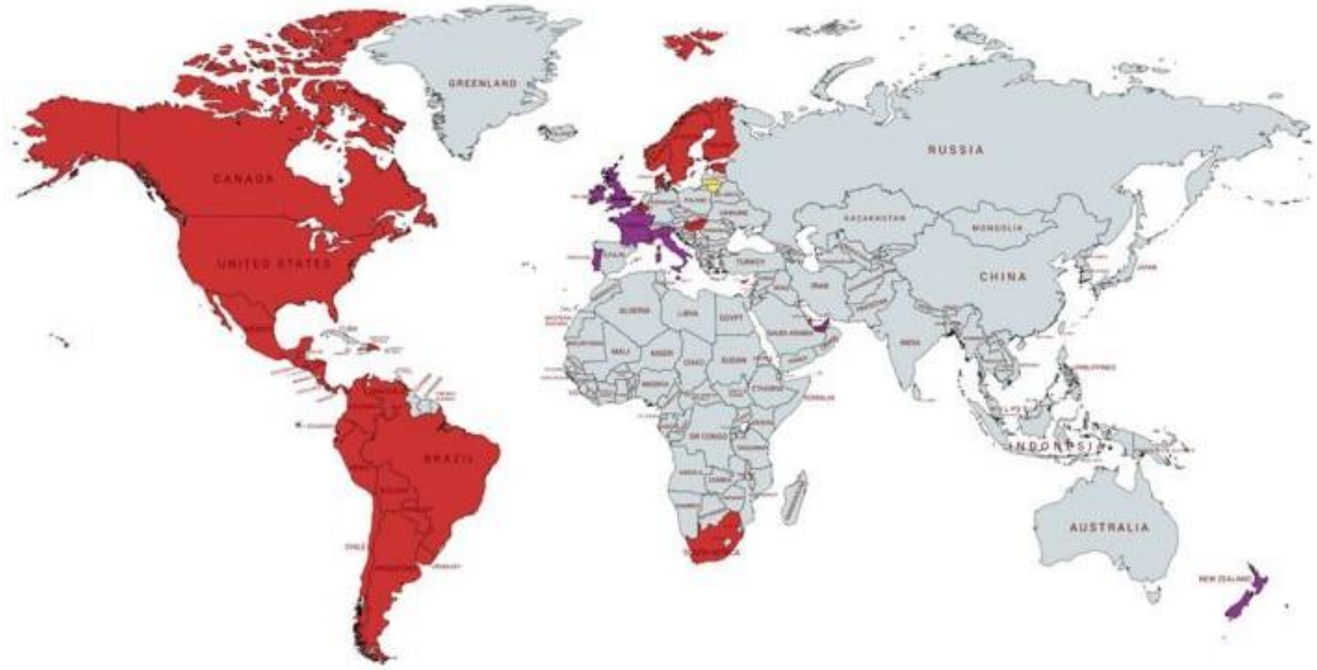
3. **Third Party Inclusion**
   - Widen the net
   - Protect all partners in the business
   - Prevent the Spread of Losses

4. **Encourage Compliance and Benefits**
   - Leverage relationships to encourage compliance
   - Engage OEM’s to participate

Connectivity to the GSMA …..



Global coverage and Participation of GSMA CEIR



This map depicts the countries where operator networks are currently connected to the IMEI Database to utilize the GSMA Blocklisting service. The red shaded countries are those where there is some level of Global or Regional data utilization, whereas the purple shading indicates countries where there is primarily only national blocking of lost or stolen devices. Yellow shading indicates a country where there is initial Blocklisting activity by an operator in the test phase. An increasing number of operators and countries are interested in joining the global IMEI Blocklisting effort and such activity will be reflected in future reports

Further resources

Check these out for more information

Landscape report: https://www.gsma.com/solutions-and-impact/technologies/security/gsma-mobile-telecommunications-security-landscape-2025/?utm_source=LinkedIn&utm_medium=webpage&utm_campaign=gsma_security_Device_Security_Webinar

Ensure you register for the upcoming Linkedin Live

https://www.gsma.com/solutions-and-impact/technologies/security/gsma_events/gsma-security-and-fraud-linkedin-live-security-landscape-2025/?utm_source=LinkedIn&utm_medium=webpage&utm_campaign=gsma_security_Device_Security_Webinar

Thank you for joining, any questions?