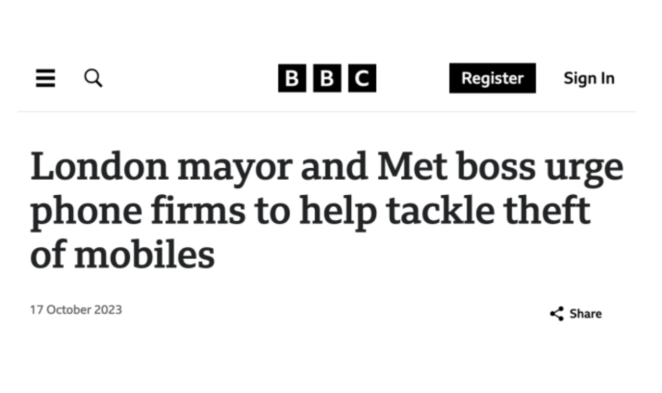
GSMA White Paper: Phone Theft

Nataliya Stanetsky, Senior Program Manager, Google
Jason Smith, Senior Director, GSMA

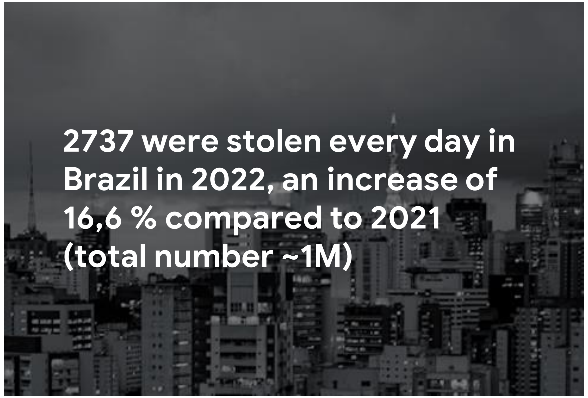
MWC Las Vegas
October 9, 2024

Mobile device theft is becoming a global safety crisis



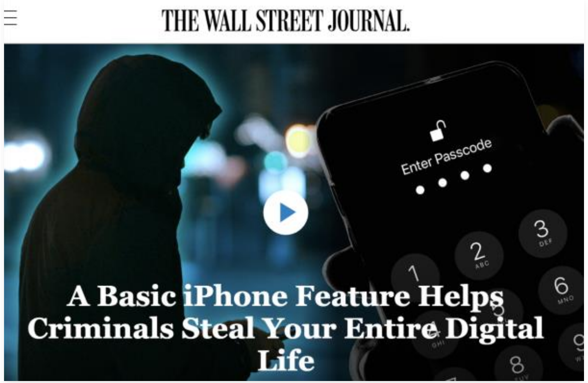
London mayor and Met boss urge phone firms to help tackle theft of mobiles

17 October 2023



2737 were stolen every day in Brazil in 2022, an increase of 16,6 % compared to 2021 (total number ~1M)

1 phone reported stolen every 6 minutes in London (over 91,000 in 2022), alone



THE WALL STREET JOURNAL.

A Basic iPhone Feature Helps Criminals Steal Your Entire Digital Life

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

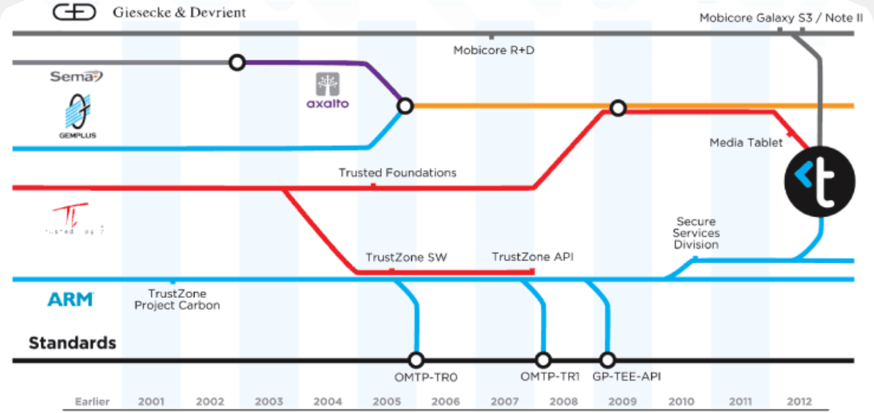
Personal usage

Steal and use

History of mobile device theft

- Theft of personal items was reported as early as 2nd to 4th century CA with the Bath ‘curse tablets’
- Mobile phone theft rose in late 1990s as devices spread across general population in Europe.
- Only after 2001 policy initiative in the UK extended into Europe and the US as they faced their own problems
- Reporting stolen devices required tedious steps like crime report numbers and evidence for OEMs and insurers
- The purpose of mobile theft has shifted from device value to data value

History of Technical Measures Taken by Industry



2001 - 2006

Work took place to reduce the incentive for theft

GSMA/EICTA IMEI Security Technical Design Principles

Mobile Industry IMEI Security Weaknesses Reporting and Correction Process

Enhancement of GSMA Device Registry as a multi-national Central Equipment Identity Register (CEIR)

2006 - 2010

Work was conducted on root technical causes of device compromise

OMTP Trusted Environment: TR0

OMTP Advanced Trusted Environment: TR1

2012

New hardware and software measure for iOS and Android Phone

(See image from here)

2013 onwards

Politicians in big cities across the world started

to raise the issue

Stolen Device Tracking Solutions and Apps made available

GSMA SG.24 Anti-theft Device Feature Requirements

Point of sale registration of devices in retail

GSMA registry

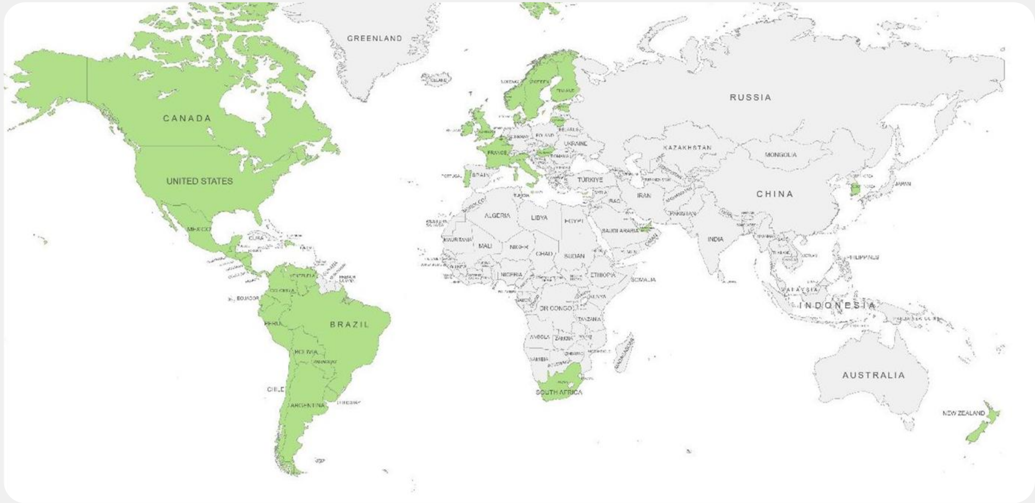
Limiting device theft and sale

Stolen devices retain value when sold in countries without GSMA Device Registry.

130 of the approximate 800 operators globally participate in the Device Registry, with more than 30 device insurers, retailers and MVNOs.

Operators welcome OEMs using block list data to deny service to theft devices, enhancing Device Registry compliance and reducing the theft device’s value.

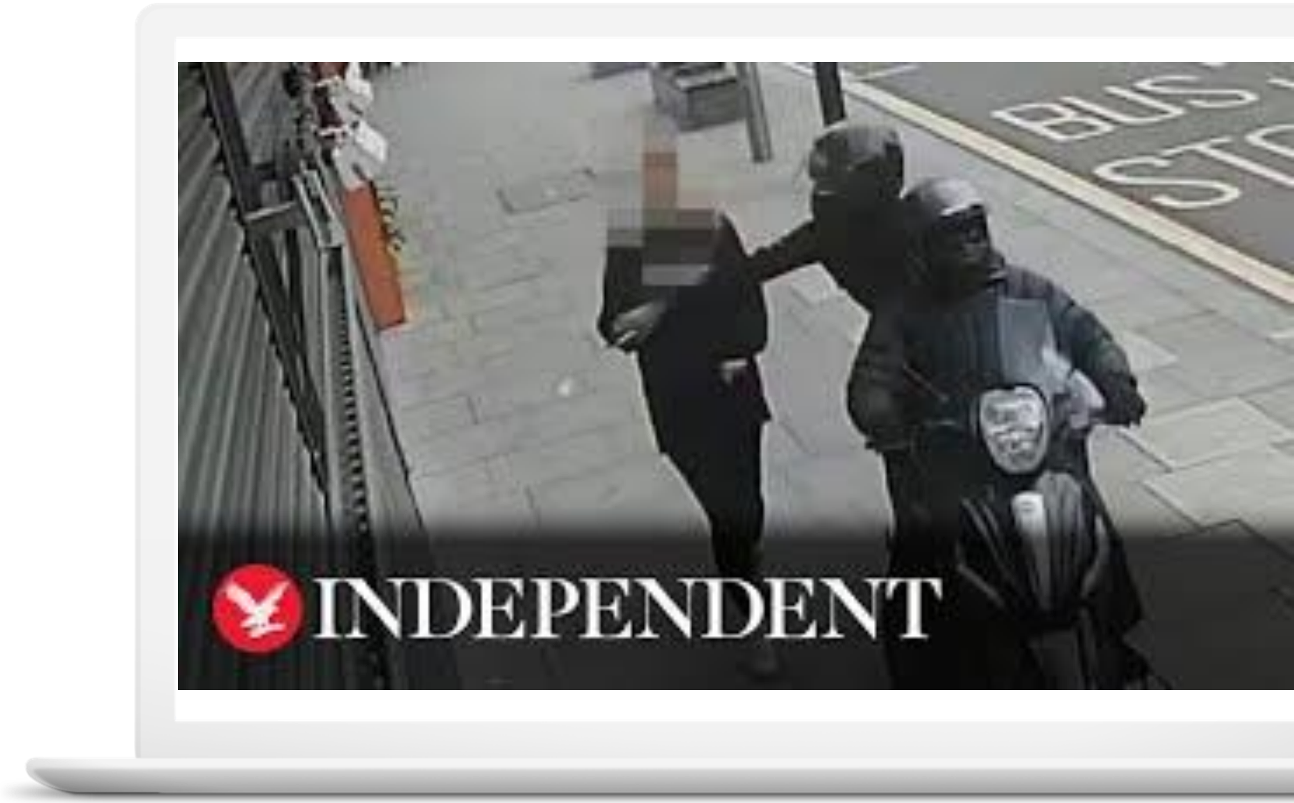
Countries with Operators using GSMA Device Registry as of April 2024



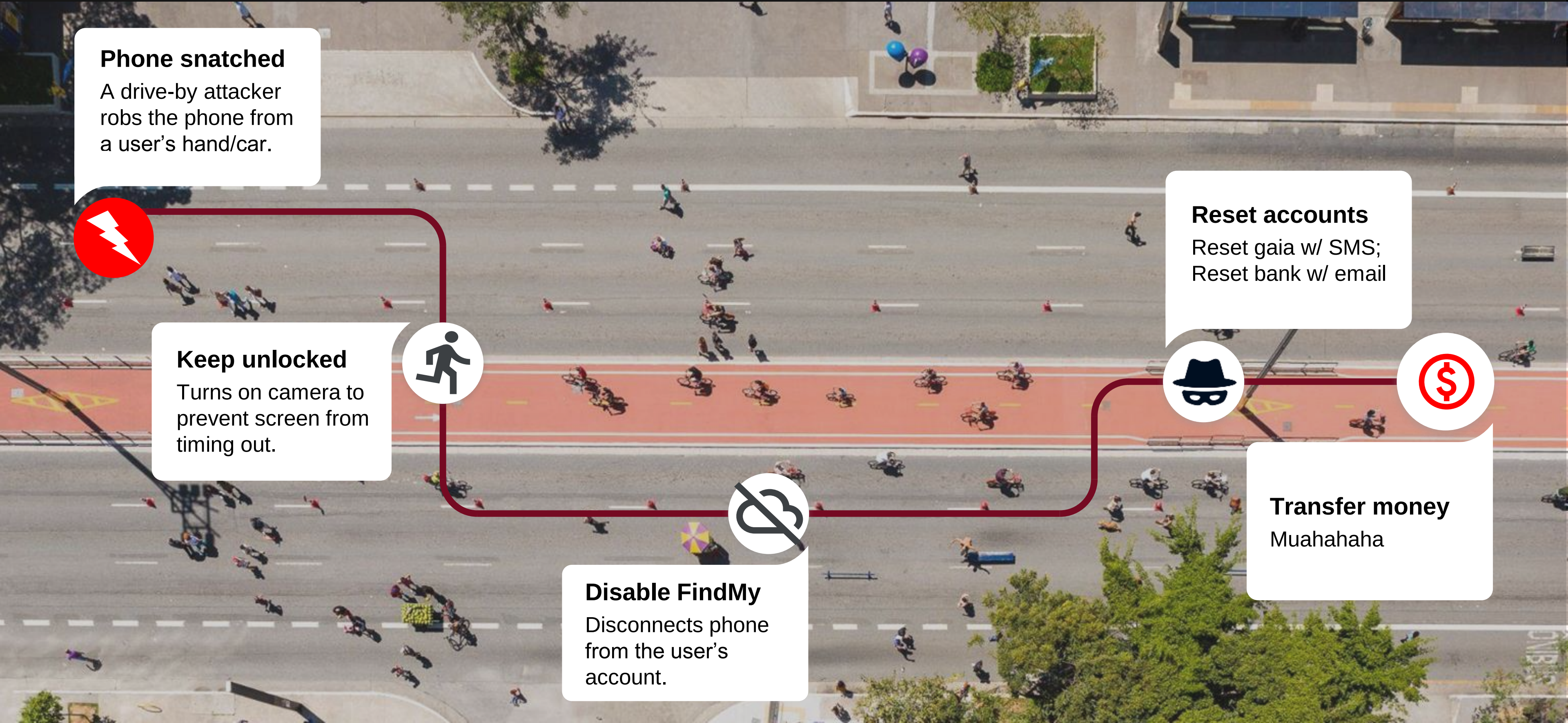
Key methods of mobile device theft

- Fraud
- Snatch and grab
- Pickpocketing
- Burglary or Forceful robbery
- “Steaming” or “Smash and grab” from retailers
- Trade in kiosk robbery
- Unattended phones
- Theft of inventory
- Supply chain and bulk theft

Key methods of mobile device theft →



How does it happen?



Phone snatched

A drive-by attacker robs the phone from a user’s hand/car.

Keep unlocked

Turns on camera to prevent screen from timing out.

Disable FindMy

Disconnects phone from the user’s account.

Reset accounts

Reset gaia w/ SMS;
Reset bank w/ email

Transfer money

Muahahaha

Fraud

A method of obtaining devices without paying for them is by committing fraud.

New devices sold by operators are obvious targets

The CFCA Global Fraud Loss Survey estimates over $10.8bn devices were lost by operators globally to fraud in 2021

A proportion of fraud is expected to be undetected as Never Pay Fraud

Fraud types

Subscription Fraud

Dishonest application for subscription or mobile device.

Uses stolen genuine documents with no intention to pay

First party fraud: Fraud committed against a company

Second party fraud: Fraud by an individual trusted by the victim

Third party fraud: Identity theft

Account Takeover

Devices shipped to locations for delivery can be stolen by the fraudster

Unauthorized access account through social engineering or online credentials from dark web

Muling (Proxy fraud)

Criminals exploit vulnerable victims as "mules" to obtain devices using their credit

Synthetic Identity Fraud

Create fake credit profiles using borrowed or fictitious inform

Fraud

A method of obtaining devices without paying for them is by committing fraud.

New devices sold by operators are obvious targets

The CFCA Global Fraud Loss Survey estimates over $10.8bn devices were lost by operators globally to fraud in 2021

A proportion of fraud is expected to be undetected as Never Pay Fraud

Fraud types (continued)

Skip/Gone Away Customer knowingly takes out credit for devices and moves around frequently to evade debt.

Bust Out Fraud

Fraudster builds credibility, then maxes out credit and defaults

Never Pay Fraud

Debtor nonpayment of any their instalments for devices taken on credit

Credit Card Fraud

Fraudster uses stolen or counterfeit credit card to obtain devices by impersonating the card owner.

Romance Scams (Lonely Hearts)

Fraudster romances victim in online dating scam to obtain mobile devices, then disappears, leaving victim with debt.

Business "Respawning"

Business identity theft to obtain financing and devices, exploiting dormant businesses' good credit.

Deterrence features offered in the mobile ecosystem

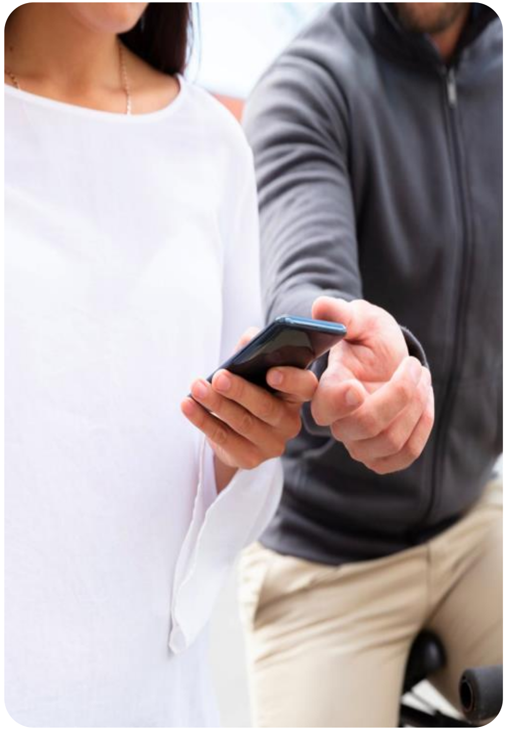
Deterrence capabilities today primarily falling into the categories of physical and software-related protection

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.



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

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.

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

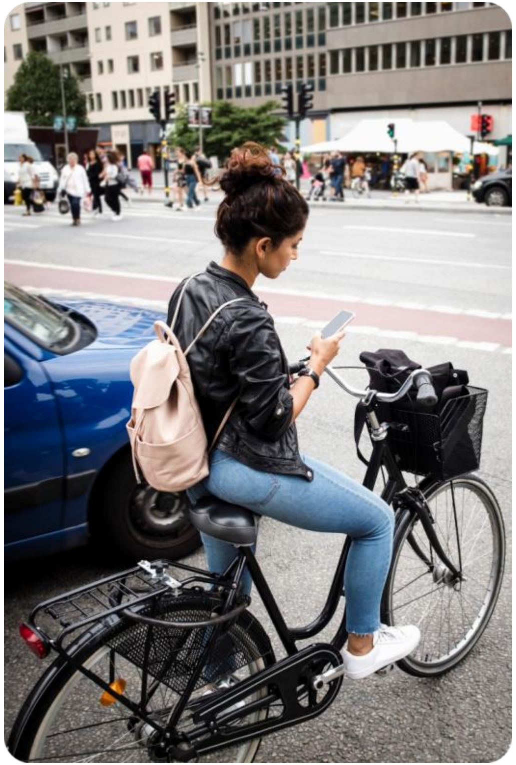
HMD Global offers remote device locking of assets such as mobile devices to prevent theft/fraud

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



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.

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 password, PIN, or pattern.

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

Backup: SmartThings Find allows to remotely backup phone to Samsung Cloud.

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.

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**

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

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

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.

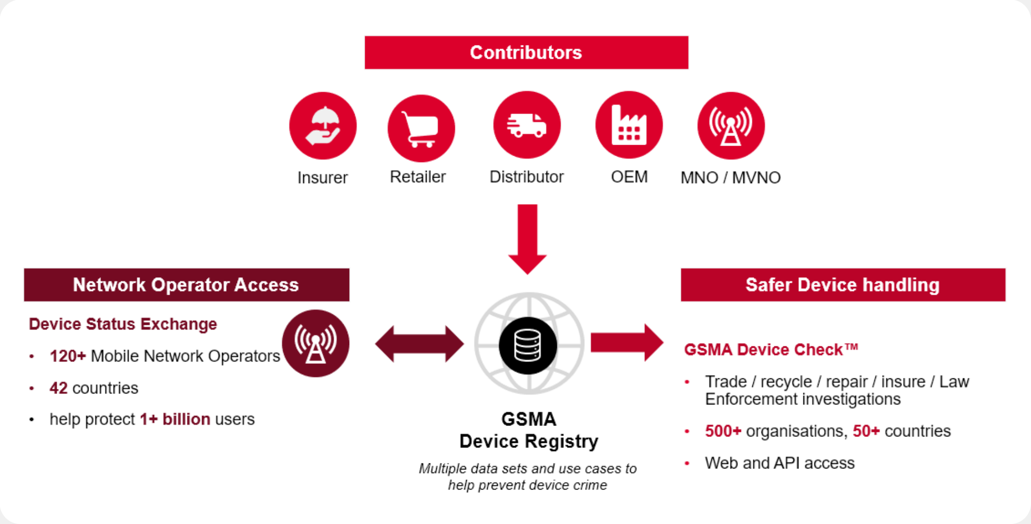
.

Recommendation

GSMA manages Device Registry and Check services globally to combat device crime and fraud.

- Stakeholders report device losses, fraud, faults, court blocks, and duplicated IMEIs
- Device Check service offers industry and public access to query Device Registry
- Informs industry to avoid certain devices for transactions and law enforcement.
- Operators should globally exchange data for effective device crime prevention.

For consumers



Contributors

Insurer

Retailer

Distributor

OEM

MNO / MVNO

Network Operator Access

Device Status Exchange

- **120+** Mobile Network Operators
- **42** countries
- 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 / recycle / repair / insure / Law Enforcement investigations
- **500+** organisations, **50+** countries
- Web and API access

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

Q&A

GSMA™