GSMA White Paper February 2025

Mobile Device Theft - State of Affairs Report

About the GSMA

The GSMA is a global organisation unifying the mobile ecosystem to unlock the full power of connectivity so that people, industry and society thrive.

Led by our members, we represent the interests of over 1,100 operators and businesses in the broader ecosystem. The GSMA also unities the industry at world-leading events, such as MWC (in Barcelona, Kigali, Las Vegas and Shanghai) and the M360 Series.

Unlock the benefits of GSMA membership

As a member of the GSMA, you join a vibrant community of industry leaders and visionaries – helping to shape the future of mobile technology and its transformative impact on societies worldwide.

Our unique position at the heart of the mobile industry means you get exclusive access to our technical experts, data and analysis – as well as unrivalled opportunities for networking, innovation support and skills acceleration.

For more information, please visit:
http://www.gsma.com/membership/

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Antitrust Notice

The information contained herein is in full compliance with the GSM Association's antitrust compliance policy.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Contents

Executive Summary

This paper explores some of the history around mobile device theft, particularly over the twenty-five years up to 2024. It explores solutions and highlights insights and experience gained, all contributed from a broad range of industry experts and cyber security professionals so that readers can learn about the true challenges faced by all trying to tackle this very complex societal issue.

Many different approaches to the problem have been attempted, by a diverse range of stakeholders, from government to industry. Technical security measures have been implemented in devices which have also had a complimentary, beneficial effect to overall device and therefore user security. Industry and national schemes for blocking stolen device identities have been implemented, as have tools for preventing the re-activation of stolen devices. Awareness campaigns and educational material have been produced by government organisations and industry alike; to aid user understanding of the value of the devices they have in their hands. Educating users on how they can take action if a device is stolen has also been key, in terms of enabling tools that operate on devices, but also in taking specific actions post-theft. Law enforcement agencies around the world have tried different approaches to tackle street thieves and their methods and some have taken collaborative action against organised crime groups. Governments and law enforcement agencies, through intelligence gathering and information sharing, have also identified procedural loopholes that can be addressed, such as abuse of the re-sale and recycling supply chain.

Criminals have continued to target mobile devices as their value has gradually increased, both in the physical object itself and the services and personal data that are accessible once the device is accessed. Industry has been in a global 'cat-and-mouse' battle to ensure that mobile devices remain secure against an increasingly organised and transnational set of adversaries that facilitate and act as an accelerant to everything from snatch thefts in the street to the theft of bulk shipments of mobile devices.

This document sets out the current situation in 2024 but does not seek to set new technical requirements or recommendations for action. It does however show the need for collaborative intelligence sharing of information on the techniques and tactics employed by criminals whether it be technical or practical methods. Only then can action be taken by the correct stakeholders.

Throughout this paper there is a clear message for the need for continued industry engagement and collaboration, highlighting where governments, law enforcement agencies, GSMA members and other stakeholders across the world are leading impactful change.

Scope

The scope of this paper is to provide an overview of mobile device theft in 2024, documenting the history of the many efforts to tackle the problem by different stakeholders across the world, the types of criminal activity being engaged in, the range of solutions that have been created to address the issue and to provide consolidated reference material for those interested in the subject.

Purpose

This paper reviews the landscape of mobile device theft, aiming to both inform and discuss the security, privacy, financial, and reputational risks that this type of theft represents. It is also intended as a consolidated reference document for those who are new to the topic in order to facilitate study into what efforts have worked and to avoid repeating mistakes where those efforts have not had the desired effect.

Introduction

In today's interconnected world, the pervasiveness of mobile device theft significantly threatens individuals, businesses, and societies at large. Although this crime problem is not of the industry's making it is recognised that a range of industry stakeholders have key roles to play to better protect mobile users from the effects of device theft and related crime. While people have traditionally perceived device theft as an opportunistic and somewhat random personal robbery, it has become more sophisticated over the last 10 years. This shift is due in part to the success of anti-theft measures, but the adoption and evolution of more sophisticated criminal activity has kept the relative rate of device crime unchanged. The annual rate of mobile device theft reported to the GSMA by network operators that use the Device Registry Block List to report and share stolen device data remains steady at around 1%[1] of active subscribers. While this theft rate holds constant as a percentage of all active subscriptions, the absolute number of thefts continues to grow with the continuous growth of mobile device sales. The importance of device theft has become far greater due to the nature of the information and data stored in devices over the value of the device itself. This underscores the urgent need for continued innovation in prevention strategies and robust measures to protect devices and the sensitive data on them.

For this paper, the focus is on the 6.8 billion smartphone devices[2] (which is expected to grow in the future) as the main theft target. The paper does not discuss the theft of wearables, such as watches, fitness trackers, tablets or any other small IoT devices. Additionally, the paper focuses on the physical aspects of device stealing.

Those directly affected by device theft are diverse. Stakeholders range across the full spectrum of the mobile ecosystem:

- Mobile users
- Mobile network operators
- Device manufacturers
- Device retailers / issuers / traders
- Device insurers
- Operating System developers (for example Android, iOS, HarmonyOS)
- Law enforcement agencies

Device theft is a pervasive problem with far-reaching consequences. The impact of device theft is detrimental to the ecosystem in various ways:

- **Customer Experience:** Theft negatively impacts customer trust and satisfaction, as mobile users are the ultimate victims of device theft with higher costs and risk to personal safety. In many cases, digital wallets stored on smartphones hold an individual's digital identity, which can be onerous to replace or reset.
- **Financial Impact:** Device theft leads to significant losses for device owners, mobile network operators, device manufacturers and retailers, and insurance companies.
- **Security and Privacy:** Stolen devices present risks for identity theft, and unauthorised data access.
- **Reputational Risk:** High device theft rates can damage the reputation of specific network operators, manufacturers, or even entire regions.

1 GSMA: derived from participating Operator device theft reporting as a percentage of their subscribers
2 GSMA Intelligence statistics from Q1 2024

History of Device Theft & Previous Solutions

Since their introduction, mobile devices have been targeted by thieves. They remain an attractive target as users consolidate more of their personal information onto a single mobile device. This section covers a non-exhaustive history of initiatives and efforts by industry and authorities around the world to tackle the problem of device theft. New initiatives often overlook previous work, whether they resulted in failure or success. This section serves as a reference to assist with any historical information gap.

A key turning point and acknowledgment by authorities of the growing problem of mobile device theft emerged towards the end of the 1990s as devices began to proliferate across Europe in the general population. By 2001, a UK Home Office study estimated 710,000 mobile devices were being stolen each year in the UK. This kicked off several policy initiatives in the country, including the introduction of new legislation and industry initiatives to further secure devices and to block stolen device identities. This work extended into Europe, Latin America and the US over time as other countries faced their own problems with device theft.

Telecommunications

Criminals have targeted telecommunications services and devices throughout their existence and there is a long history of embedded systems hacking against mobile devices. The introduction of GSM, as the second generation digital mobile standard, dealt with the problem of weaknesses in electronics security by introducing the SIM card as a secure token for subscriber access which helped address historic subscription and cloning fraud and provided a basis for subscriber authentication and call confidentiality. The advent of the concept of subsidised devices led to the introduction of SIM and service provider locks, which were introduced by mobile network operators to protect subsidy investments by preventing those devices from being re-used on other networks before the subsidy was recovered or the subsidy period had expired. These controls could be unlocked legitimately by the user at the end of the subsidy period. A grey market emerged to remove the SIM lock which had been implemented on subsidised devices and this drove a lot of embedded systems hacking. Many of these original hackers came from the car radio hacking community, moving into SIM lock removal and other hacks for mobile devices, which were extremely lucrative from the late 1990s.

With the introduction of GSM, the device was separated from the subscription and had a separate dedicated identifier known as the International Mobile Equipment Identity (IMEI). ETSI standards required that this identity be secured against change after the point of manufacture, but this was a difficult task given that the technology simply wasn't then available to do this in a meaningful way. Compounding the challenge, servicing needs for devices and legislation in some countries such as Turkey and China required that devices retain their original identifier meaning that authorised repair of devices required re-programming of the IMEI. Manufacturers controlled these tools and, in some cases, had secure regional repair centres that were the only places where this IMEI programming was permitted.

There was heavy targeting of devices for SIM lock removal and research by embedded systems hackers often led to other breaks, such as being able to re-program IMEI numbers. In some cases 'dirty hacks' were created that would reset IMEI numbers (for example, set all to zero) and, in some cases, this may have been enough to circumvent an operator's equipment identity register (EIR), which is used to control which devices can obtain network access. Other hacks included adding new language packs to devices and other features that may be region specific, often to enable the export of stolen devices. Some of these were funded and facilitated by highly sophisticated criminal operations across multiple countries, producing hardware boxes and software protection to protect the hacks themselves and make them easy to use at mobile device repair shops and stalls at markets.

The battle between the embedded systems hacking world and the device manufacturers continued for many years evolving from SIM lock removal into jailbreaking and rooting. The mobile industry was heavily targeted by organised criminals, from mobile service centres and device manufacturer sites to design centres in order to steal tools and private encryption keys for signing software builds. Over the years, this situation led to massive improvements and advances in hardware and software security such as the Trusted Execution Environment (TEE), much of which has become the state of the art across many types of devices, not just in the mobile device world. It also led to the employment of some very impressive hacking breakthroughs and techniques such as Return Oriented Programming (ROP) in order to circumvent software defences that had been developed such as Address Space Layout Randomisation (ASLR).

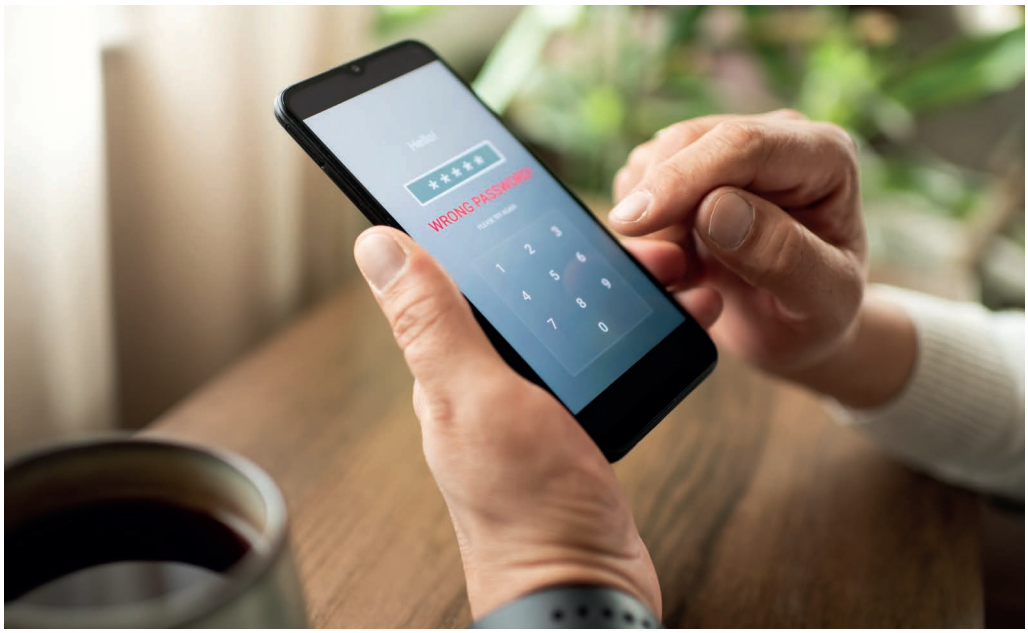
Reporting Stolen Devices

An early solution that was widely adopted by the telecommunications industry allowed users to report stolen devices directly to their mobile network operator. The telecoms standards defined the concept of an Equipment Identity Register (EIR), which enables the network operator to block device identifiers on their network if reported stolen by their owners. Reports helped but didn't give any real insight into the problem of device theft due to false reporting of devices that had been lost rather than stolen and fraudulent reports to claim insurance benefits. Some operators and insurance companies mitigate this by requiring a crime report to be filed with law enforcement agencies who can then contact the relevant network operator to block the device that has been reported stolen. Theft victims are generally advised to contact their network operator as soon as they realise their mobile has been lost or stolen to ensure the operator can block the device, block the subscription to avoid fraudulent use and provide advice on how to protect their personal data.

Device Access

In the past, devices had limited features for protecting access. Personal Identification Number (PIN) locks were available on both devices and SIMs but were rarely enabled by users because they were considered inconvenient. This meant that if a device was stolen, it could easily be unlocked. At the time, criminals were rarely interested in the contents of mobile devices and instead intended to sell the devices. The amount and sensitivity of user data was minimal on devices, mainly confined to phonebook and SMS messages, but that has massively changed since the advent of smartphones, increasing the value of the data on the device and the functions that enable access to high-value services such as banking or even crypto-currency wallet storage.

The requirement for user access control has grown to the point where it is essential for all users. Newer technologies (such as face unlock and other biometric based solutions) have been employed to assist users in protecting access to their devices. These solutions are more convenient and easier to use which has led to an increase in uptake of access control mechanisms.



This combined with the encouragement of usage of access control features through the device's initial start-up process means that most users now use some sort of device access control.

Early adopted biometric solutions could be bypassed using different technical and non-technical techniques in the past but these have substantially matured and improved. There has been an ever-present concern that pushing users to 'become the key' could lead to personal risk as the users themselves become the target of thieves. There has been evidence in extreme cases of individuals being tortured for PIN numbers (in the case of bank cards)[3], threatened, or beaten for access. Duress codes and techniques may be a future solution for such issues but are in no way a panacea to this issue. The very nature and purpose of devices means that legitimate access is always needed, and this will continue to be a point of weakness.

Work has been undertaken over the years to close the procedural loopholes that facilitate theft, whether it be around insurance fraud, recycling, or password resets. It's important to note that early intelligence sharing of exploitation of procedural flaws by the police, insurers, and others in the industry can help mitigate these problems.

Technical Measures Taken by Industry

Device manufacturers, mobile network operators, and operating system platform providers have long fought against embedded systems hacking and criminality to protect users of mobile devices. The following is a brief timeline of key initiatives over the years.

2001 - 2006

Work took place to reduce the incentive for theft, with the rationale being that if the device cannot be unlocked or re-enabled, it has no value. GSMA and EICTA (now known as DigitalEurope) developed nine security principles in IMEI Security Technical Design Principles - Enhancing Device Identifier Integrity to Combat Device Theft[4] to act as guidelines for all device manufacturers to follow to protect device identifiers against unauthorised change. The principles provide technical design guidance to mobile device manufacturers and provide operators with a set of criteria against which device security levels can be assessed. The design principles complement the 3GPP technical standards that require IMEIs to be non-reprogrammable but do not contain specific details or guidance as to how the IMEI should be protected.

The mobile industry introduced IMEI Security Weakness Reporting and Correction Process[5] where reports could be made to the GSMA about security weaknesses to IMEI implementations in specific device models that lead to the IMEIs in those devices being vulnerable to change. This initiative's overall objective was to improve device security during the manufacturing lifecycle of current and future products by reporting security issues to the relevant device manufacturers to have the IMEI compromise reports investigated and mitigated. Positive engagement from some leading device manufacturers, and their willingness to fix reported security issues, resulted in an overall improvement in IMEI and device security levels. Regular reports by EICTA and GSMA were provided to the European Commission and the progress made by, and attributable to, the industry initiatives was recognised. Complementary to industry efforts EU member states were invited to indicate their progress at a national level in terms of tackling theft through legislation and policing initiatives.

The 2006 UK Mobile Phone Industry Crime Reduction Charter represented a first of its kind national commitment, led by industry, to combat mobile device theft. It consisted of a number of elements including the establishment of a UKSEIR (Shared Equipment Identity Register), hosted by GSMA, that committed the UK mobile network operators to block stolen devices, across all UK networks, within 48 hours of them being reported to their service providers[6].

While progress was made on securing device identifiers through implementation of security requirements, monitoring and reverse engineering hacks, national governments, with a tiny number of exceptions, failed to complement and support industry efforts with legislation or promises of increased law enforcement activity. Similarly, the uptake of the blocklisting capabilities by network operators was not universal and most chose not to deploy EIRs to control device access to their networks, which allowed stolen devices to be resold and reconnected to networks without impediment.

3 https://www.theguardian.com/uk/2008/jul/05/knifecrime.ukcrime

4 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wpcontent/uploads/2017/06/IMEI_Security_Technical_Design_Principles_v4.0.pdf

5 https://www.gsma.com/publicpolicy/wpcontent/uploads/2017/06/IMEI_Security_Weakness_Reporting_and_Correction_Process_v4.0.pdf

6 https://www.theregister.com/2006/07/28/mobile_crime_charter/

2006 - 2010

Further industry work was conducted on root technical causes of device compromise, resulting in the creation of the OMTP Trusted Environment: OMTP TR0[7] and the OMTP Advanced Trusted Environment: OMTP TR1[8] recommendations, which led to a leap in hardware security, forming the basis of device hardware security implementations that exist today.

Regional Theft Guard

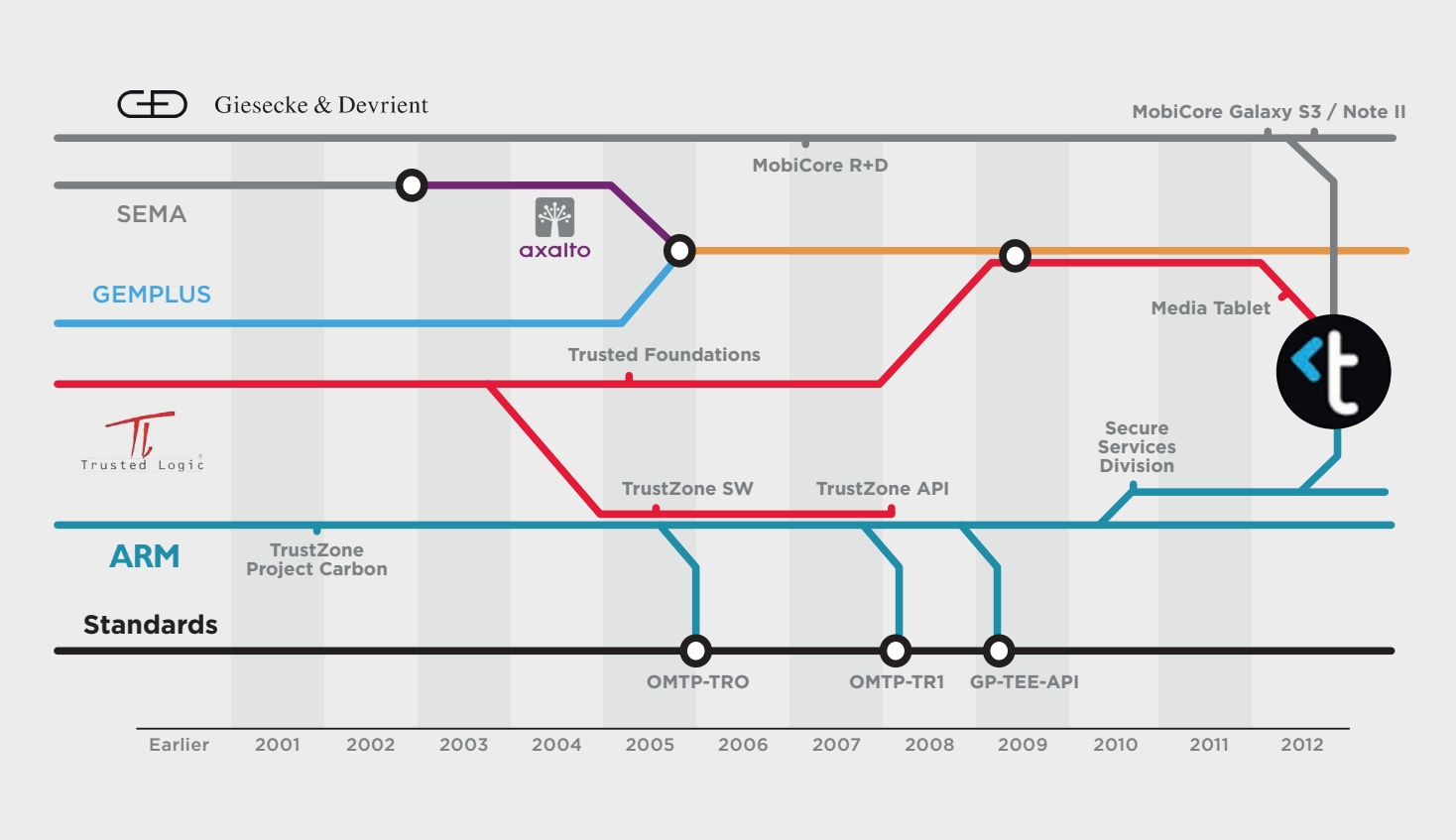
Approximately between 2005 and 2008, to address the gap that is inevitable in device blocking solutions – recognising that whole-world coverage is not possible and that not all mobile network operators were using the GSMA Device Registry, the mobile industry investigated the concept of 'Regional Theft Guard' at length. A number of different potential solutions were discussed and three of them were fully explored in terms of their technical ability to address the defined problem and the practicality of introducing them.
It was eventually concluded that the potential to subvert any solution, because of the need for backdoors, would prevent it from being a panacea to the problem of mobile device theft. The solutions proposed could also be subverted by other means once in place; there was a high threat of collusion at a low level, for example between thieves and staff in a shop and it was also found to be difficult to prove the originating operator / owner and therefore whether a device was stolen. At the time, most mobile devices were not connected to the internet, there were very few over-the-air update capabilities and, as such, the options were much more limited than presently.

7 http://www.omtp.org/OMTP_Trusted_Environment_OMTP_TR0_v1_2.pdf
8 https://www.gsma.com/newsroom/gsma_resources/omtp-documents-1-1-omtp-advanced-trusted-environment-omtp-tr1-v1-1/

This work is referenced in the GSMA's Security Principles Related to Theft paper[9].

2012

New smartphones, based on different operating systems and approaches from Google and Apple, began to adopt hardware and software security measures as they started to be targeted.



Source: Trustonic[10]

Figure 1, Mobile hardware security standards evolution timeline

2013 and onwards

Politicians in some major cities across the world raised the issue of smartphones being stolen and the need for a 'kill switch' to disable stolen devices. This led to further industry work on preventing re-activation and re-use of devices post-theft, particularly where devices were using alternative connectivity beyond the mobile network such as Wi-Fi, which meant that devices retained value for thieves.

In 2014, GSMA's Device Security Group produced the SG.24 'Anti-theft Device Feature Requirements' document[11] which sought to harmonise the requirements necessary to enable remote device disablement post-theft across the industry and the world. The paper warns against centralised 'kill switch' solutions (such as those proposed by politicians in different countries), as these could create an even greater cyber security risk to users but it, usefully, defined a benchmark set of features that can be used and enabled by industry stakeholders to allow users to protect, track, disable and re-enable stolen devices in a consistent way.

9 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2012/10/Security-Principles-Related-to-Handset-Theft-3.0.0.pdf
10 http://www.trustonic.com/about-us/who-we-are
11 https://www.gsma.com/newsroom/gsma_resources/sg-24-anti-theft-device-feature-requirements-v3-0/

A range of other technical solutions were created by a range of diverse stakeholders to help address the problem of mobile device theft. These have ranged from devices that make noise when stolen, to point-of-sale registration of devices to help the police find their owners if stolen devices were recovered (shown below), to detecting snatches using the accelerometers of devices. Services that allow those engaged in the legitimate repair and trading of mobile devices to check if devices they are handling have been reported stolen were also introduced. The diverse range of approaches and solutions illustrate there is no single panacea to device theft and criminals will always seek to subvert these countermeasures or find new approaches to ensure their criminal enterprises remain lucrative.

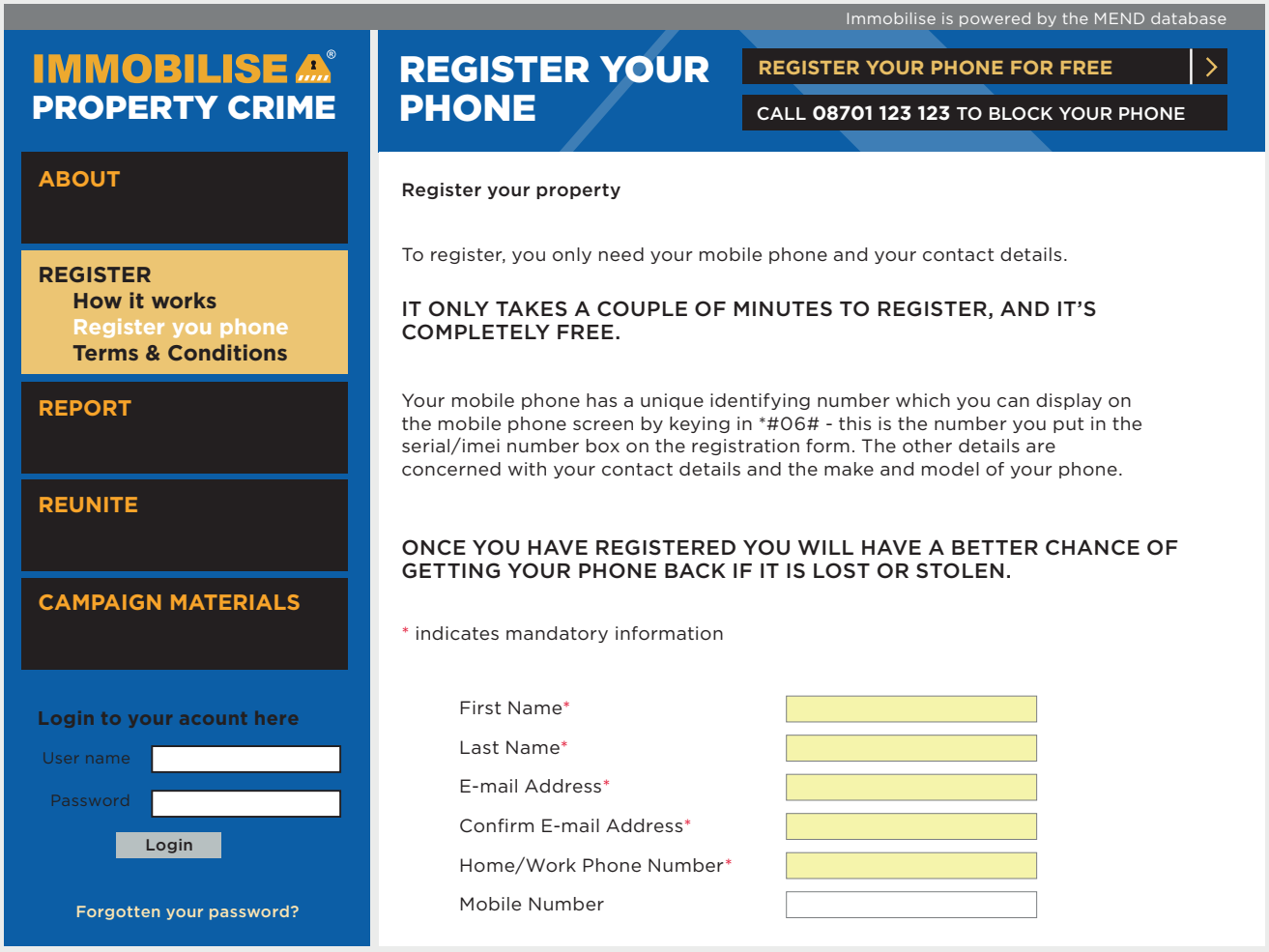


Figure 2, Screenshot of a point-of-sale registration for devices.

Source: immobilise.com

Methods and Motives

The actions of criminals are continually evolving in response to new defences being deployed in products as well as the introduction of new technology features. Their capability and motivation are most often driven by the ability to resell a stolen device. While there are many different actors involved in mobile device theft, the primary reason why most are involved has been the relatively high value of the stolen product and the relative ease with which it can be turned into cash. This section identifies three device theft categories: those relating to the end user, those that are undertaken in the supply chain and fraudulent acquisition.

Methods: End User

Burglary

In most jurisdictions this is defined as the unlawful entry to a premises to commit a theft. Usually, it is the broad contents of the premises which are being targeted, and the theft of mobile device is a byproduct of a larger theft.

Forceful Robbery

One of the most common mobile device theft methods on the street is through forceful robbery. In many countries in Western Europe as well as North and South America, there is an increasing trend in mobile device theft incidents that directly target mobile device users. In New York City, London and Rio de Janeiro crime related to consumer thefts via snatching has risen significantly. In the United Kingdom, published estimates from the Crime Survey for England and Wales show that 36% of theft from the person offences involved the theft of a mobile device phone in the past year[12]. On average, a mobile device is reported stolen approximately every 6 minutes and a 2022 report from the Metropolitan Police revealed that more than 90,000 mobile devices were stolen in London[13].

In New York City, in February 2024, Mayor Eric Adams announced that mobile device robberies have increased and described a recent wave of 64 thefts as follows:

"The crimes in this pattern involved multiple thieves on mopeds, snatching cell phones and purses from their victims. These thieves would ride up behind their victims on the sidewalk, steal their property and then make their getaway. Most of the victims are women simply just walking alone. We have seen that the mopeds used in these crimes are also stolen as well."[14]

It is clear, therefore, that those responsible for mobile device theft are also involved in other areas of criminality. Sadly, some of the thefts result in bodily harm to the victims as they are dragged along the street until they release the mobile device or they are otherwise physically assaulted and frequently left with traumatic memories.

Pickpocketing

Pickpocketing mostly relies on the art of diverting the victim's attention to facilitate the theft of their mobile device. Perpetrators often use distraction techniques such as bumping into victims, asking for directions, or even stopping in front of victims abruptly. Some pickpockets work in teams of two or more, where one will distract and the other will pick the pocket, before fleeing and potentially handing off the device to accomplices. By the time the victim realises what has happened the perpetrators are nowhere to be found.

Snatch and Grab

This is common on some streets because of its opportunistic nature and often takes place in urban areas, where crowded spaces are an advantage for thieves to blend in, snatch devices and escape unnoticed. The speed with which these incidents happen often gives the victim little to no reaction time to prevent it from happening. Usually, the victim is inattentive or distracted and the perpetrator or perpetrators simply use this to their advantage to grab a device from the victim.

12 https://www.gov.uk/government/news/crackdown-to-halt-rise-in-phone-thefts
13 https://www.bbc.com/news/uk-england-london-65105199
14 https://www.nyc.gov/office-of-the-mayor/news/100-24/transcript-mayor-adams-makes-public-safety-related-announcement

Opportunistic thieves take mobile devices which are left unattended in public spaces, such as cafés, restaurants, parks or beaches. This type of theft needs minimal effort from the perpetrators, and they simply rely on the opportunistic nature of it where victims are negligent by leaving their devices unattended.

Methods: Supply Chain

Bulk Theft and Theft in Transit

The movement of stock from one location to another (e.g. from the manufacturer to an operator's distribution center) may be a target of criminals, facilitating the theft of a significant volume and value of devices in one go. This hijacking is perpetrated by more sophisticated criminals who will plan and execute the theft of shipments of both new and used devices. In some cases, the coordination of the hijacking has relied upon internal participants who have access to privileged information relating to stock movement.

Manufacturer sites have been targeted by gangs in 'ram raids' and many devices have been stolen from lorries leading to losses in the multiple millions of dollars. Intelligence sharing by police and industry through forums such as the Transported Asset Protection Association (TAPA)[15] and adoption of enhanced security measures such as the provision of approved secured parking facilities for shipments in transit have helped to address this issue, but it remains an attractive proposition for thieves. One example from 2024 was the theft and recovery of a €19.3 million shipment of mobile devices and tablets from a warehouse at Amsterdam Schiphol airport. "Another 11 suspects were arrested for reportedly stealing phones worth €18.5 million from Schiphol in February 2021, while in July 2020 a Polish truck driver was arrested after allegedly using false documents to collect a €3 million consignment of phones at the airport."[16]

Due to the sheer volume and to avoid prosecution for possession of stolen property, these devices are generally exported. Whilst importing a shipping container of stolen merchandise may seem complex, it is not uncommon to hear of corrupt Port employees who facilitate entry to markets. The shipper accepts the risk of detection may be low as not every container can be inspected.

Couriers delivering devices to end users may also be targeted for witting or unwitting participation in device theft schemes which could involve box tampering or the substitution of genuine devices with fake alternates. Enhancements to packaging (e.g. to flag tampering) and strong security of goods in transit (e.g. weighing parcels at checkpoints) are common controls.

15 https://tapaemea.org/

16 https://tapaemea.org/intelligence/dutch-police-recover-e19-3m-of-stolen-phones-within-hours-of-amsterdam-schiphol-theft/

Burglary

The unlawful entry to business premises, for example warehouses, shops, repair centres and logistics facilities, to undertake device theft.

“Steaming” or “Smash and grab”

A technique for targeting mobile device stores and electronics retailers. This can involve gangs running into shops and raiding the storerooms (sometimes left open or unlocked due to shop staff not following procedure) and devices on display. Special locks to prevent devices being stolen from displays and operational procedures have been tightened in response to this activity. This also led to some measures being implemented by operating system providers such that device IMEIs are not active until they have been through the shipping process and sold.

Thieves (who may work in gangs) mostly capitalise on the element of surprise to grab as many devices as they can before fleeing the scene. While display devices are generally associated with product demonstrations running on a “loop”, they are perfectly capable of being used as fully functioning devices, hence they are targeted by the thieves. This is known as ‘steaming’ in some countries.

Theft of Inventory

Thieves also steal devices from stock rooms and locked cabinets and may spend time observing stores and staff activity to identify those who exhibit poor general security practices (e.g. leaving keys unattended, doors unlocked or propped open, or tailgating into stock rooms).

Customers (such as businesses) who may retain volumes of devices on their own premises for issuing to employees may become the target of burglaries, especially if they do not maintain strong stock management and security practices. Inventory may also be stolen by employees of the store/operator and may involve the modification of inventory records to try and delay the identification of such an embezzlement.

Trade in Kiosk Robbery

In this age of self service, customers in some markets may trade in devices for gift cards at automated kiosks. Thieves have been known to vandalise the kiosks and remove the deposits of multiple devices for aggregation and export.

Methods: Fraudulent Acquisition

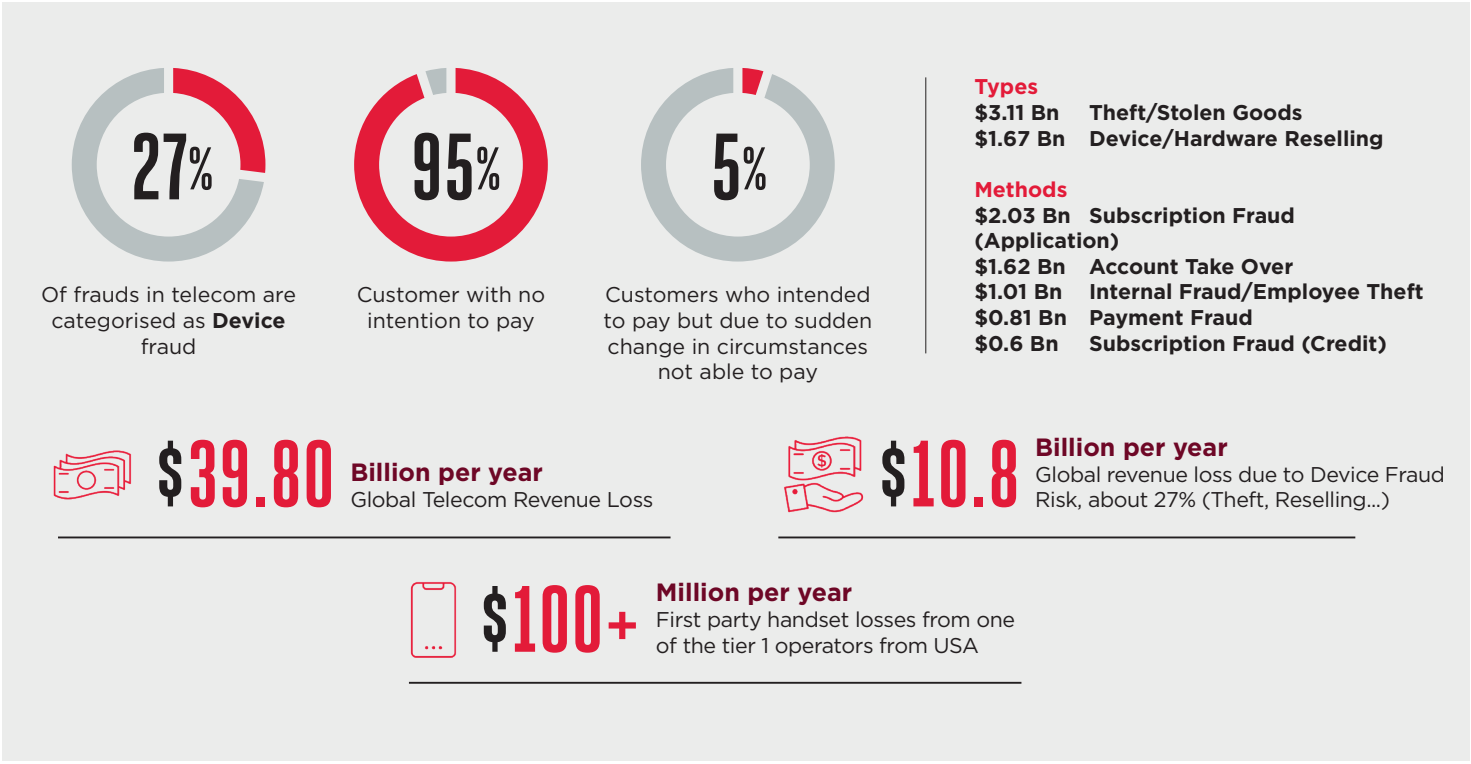
Another method of obtaining devices without paying for them, is through committing fraud. New devices sold by carriers are obvious targets for the many varieties of fraud that have been identified. The CFCA Global Fraud Loss Survey[17] estimated more than $10.8bn was lost by carriers globally due to device fraud in 2021. A proportion of fraud is expected to be undetected and hidden in bad debt or what may be referred to as Never Pay Fraud and is simply treated as Bad Debt. Incidentally, the same survey noted an estimated $3.11bn of losses due to Theft/Stolen Goods (7.8% of all frauds), which put it in the top five fraud types in 2021. By 2023, theft had dropped out of the top five fraud types[18].

Account Takeover

This occurs when unauthorised access to an account is obtained, usually through social engineering or the acquisition of online credentials from the dark web. Once an account is accessed, new devices are purchased with devices shipped to locations where the delivery can be stolen or accessed by the fraudster without the genuine customer ever being aware of the shipment or delivery. Some 'porch pirates' will lay in wait at the delivery location and meet the courier at their vehicle to 'save them the steps' in delivering to the front door or official delivery point. In more complex scenarios, shipments are redirected either through the carrier or delivery service to a vacant home or business or rerouted to a temporary rental office or similar location. This fraud can impact both consumer and business accounts. Other forms of account takeover also include adding account managers to a business or personal account who, with proper credentials, can verify account passwords and provide an ID (counterfeit or genuine) to support their identity and their story.

Business "Respawning"

Business respawning is effectively the identity theft of a business that may have been dormant or paused trading for a period of time. It may involve the use of business documents which are generated or created by government offices in efforts to re-establish the business's credibility. Bad actors then obtain financing and acquire mobile devices, even more so if the business was operating and genuinely had a good credit history prior to ceasing or pausing operations. Since business accounts generally utilise larger numbers of devices, the credit lines offered are typically more generous and therefore cause greater losses to the carrier.



Source: CFCA Survey 2021

Figure 3, Losses due to fraud.

17 https://cfca.org/document/2021-fraud-loss-survey/
18 https://cfca.org/document/global-fraud-loss-survey-2023/

Bust Out Fraud

A fraudster will pose as a good customer and maintain on time and in full payment performance for a period, so that they build up goodwill and credibility, before 'busting out' and acquiring as many mobile devices and as much credit as possible before defaulting on their debts.

Credit Card Fraud

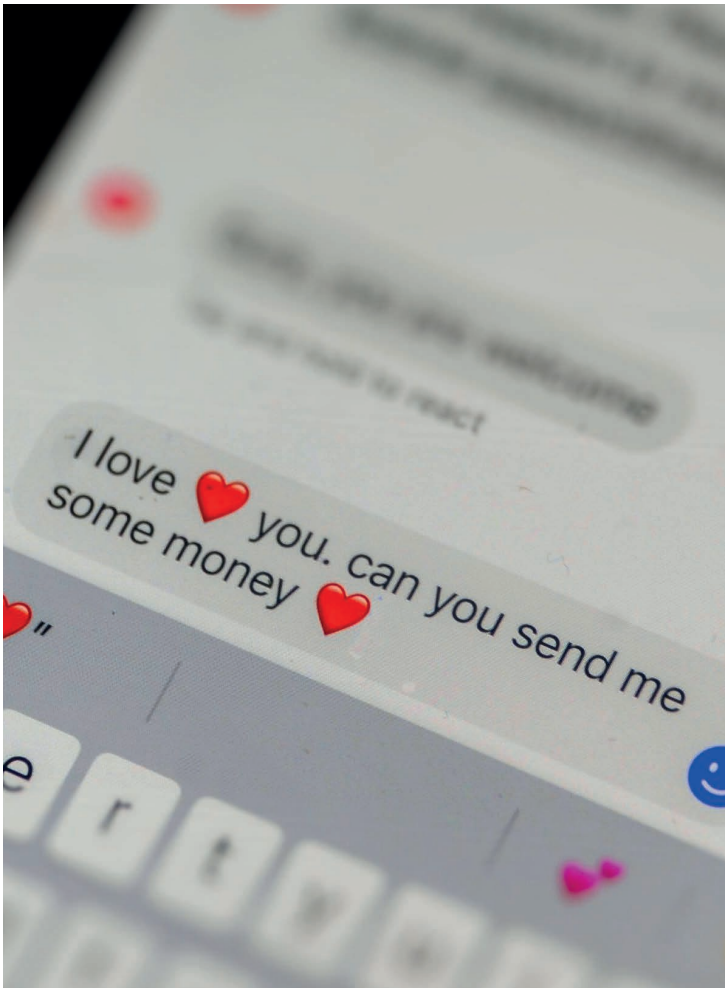
Using a physical (or virtual) credit card to pay for mobile devices without the authorisation of the legitimate card owner (either through stealing the card/its details or by using a counterfeit card/details). The user will typically fraudulently impersonate the genuine account holder and either receive devices in person or have them delivered to an address under their control or to which they have easy access.

First Party Fraud

Fraud committed against a company by one of its own, genuine customers. The perpetrator is in fact who they represent themselves to be, it is just that they have no intent of ever paying for acquired mobile devices. Typically, these devices will be acquired through finance, or chargeback claims will be raised to their card issuer suggesting that they did not purchase the devices in the first instance.

Muling

Also known as 'proxy fraud', criminals typically target more vulnerable victims (e.g. students) to become 'mules' who use their own access to credit facilities to obtain mobile devices before handing them over to their 'handler'. This is usually in exchange for a payment for the devices, but often the promised reward may not be forthcoming (the victim gets ripped off). Otherwise, victims can be convinced they're taking part in a mystery shopping exercise, or they (or family members) may be threatened with violence if they don't participate in the scheme. They could even involve insiders from retail stores who knowingly process and coach the applicants through the process. The handler consolidates the acquired mobile devices for distribution/resale elsewhere and will often offer guidance to the individual to deny the purchase in an attempt to avoid remaining responsible for the debt.



Never Pay Fraud

Defined through the debtor's nonpayment of any of their instalments for mobile devices taken on credit. The perpetrator could be an actual person, a mule or someone abusing a synthetic identity. This fraud may go undetected as they may appear as instances of poor lending decisions leading to an inflation of written off bad debt balances because there is no victim and therefore no complaint ever reaches the carrier about unauthorised accounts or charges.

Romance Scams (Lonely Hearts)

A consumer is deceived by a fraudster to use their good credit rating to obtain mobile devices fraudulently. Usually, the victim is lured into an online dating scam where the fraudster convinces a lonely widower of their need for assistance for a charitable purpose and a promise to repay the loan for them as they are awaiting some form of funding, coupled with promises of romantic involvement. The victim is romanced over time until the fraudster is convinced that he can persuade the victim to help them and once the acquired mobile devices are shipped to an overseas location or delivered to a person who is trusted to deliver or forward the devices, the romance is broken off and the victim left heartbroken, with a large balance owed for devices that they do not have and cannot return for refund or credit. Victims will typically reach out to carriers for assistance as they may not be able to afford the device payments and associated costs of service linked to the purchases. Some consumers may try to continue making repayments to avoid perceived additional embarrassment or judgement from their families or law enforcement.

Second Party Fraud

Fraud committed by someone in a position of power or by an individual trusted by the victim. This could be someone like a caregiver, or a housemate. The perpetrator abuses their position (e.g. by having access to data and/or documentation) to commit fraud in the victim's name, leaving them liable for mobile devices they obtain fraudulently on credit.

Skip Away or Gone Away

A customer knowingly takes out credit for mobile devices and moves around frequently to evade debt. They may also simply take no action and ignore collection attempts. Perpetrators who "skip" or move around will fail to quote their full or accurate residential history in their efforts to access more credit for new and additional devices (which wouldn't be approved had the applicant's full credit history been known). As the delivery of bills and financial statements has moved to become more digital, the detection of this fraud (previously through returned mail) has become more difficult.

Subscription Fraud

Subscription fraud can take many forms, but in essence involves making a dishonest application using false information, or genuine but stolen information (identify theft) together with forged or stolen documentation to obtain a post-paid subscription(s) to an operator's services and/or a mobile device with no intention to pay for the device at the time of application. Variations of subscription fraud are included below.

Synthetic Identity Fraud

The compilation of information about a fictional individual to seed a credit file or similar credit application that creates the appearance of a genuine creditor; however, it may be formed from borrowed credit histories, fictitious addresses and Personal Identification Numbers (e.g. social security numbers etc.) and self-reported trade and credit lines. Upon the creation of a synthetic identity an application for credit is utilised in many ways to obtain mobile devices. It is expected that advances in Generative Artificial Intelligence will make the prevalence of synthetic identity fraud more common, and the effects ultimately more profound.

Third Party Fraud

Commonly referred to as identity theft, this is a form of fraud where someone assumes the identity of a victim for the purpose of accessing their credit to obtain mobile devices and services. The fraudster benefits from receiving the device(s) and the debt is left as a liability of the victim. The victim's personal and financial information used to commit the fraud is often obtained from the Dark Web (having been gathered from data breaches) and used by bad actors to exploit in as many ways as possible, including fraud. This fraud can be perpetrated across all channels but may target those where controls are perceived to be weaker (e.g. via telephone sales channels where the information is provided verbally where personal identification and verification may be more problematic). More elaborate schemes may involve the creation of identity verification documents such as counterfeit identity documents. Identity theft is constantly evolving to counter identity verification methods and other methods of detection.

Motives

Mobile device theft is driven by a variety of motives, with financial gain being the most significant. Over recent years, the trafficking of devices to various territories has become more prevalent, particularly to countries that offer opportunities for uninhibited distribution and resale. These locations tend not to use the GSMA or other Negative Device Blocking Lists, and sometimes lack official distribution channels for certain original equipment manufacturer (OEM) devices, leading to increased demand and inflated prices. Additionally, organised crime and systematic fraud, including device swaps and exploitation of international blocklist weaknesses, contribute to the problem. Identity theft and extortion have also become alarming trends, with criminals exploiting personal data stored on smartphones. Other motives include tax avoidance, money laundering, and personal usage, highlighting the diverse and complex nature of mobile device theft.

Device swaps

A method has emerged to circumvent national blocklists of IMEI numbers whereby users swap their stolen device (that has been disabled) with someone in another country where no reciprocal device blocking takes place. This peer-to-peer method of re-enabling stolen devices demonstrates the weakness of blocking when countries do not receive or action stolen IMEI data between them or via the GSMA's global Device Registry.

Direct Exploitation

Mobile devices are stolen to gain access to bank accounts and contactless payment systems, which means that there is inherently a method for buying 'clean' goods, disposing of the stolen device and then being able to sell those goods on.

Example Case: In one well-known case, a victim had their mobile device stolen from a locker at a gym and found that the thief had exploited the fact that the device would display incoming messages while the device was locked. This facilitated the thief gaining access to the victim's bank account, because the 2FA (two factor authentication) message was displayed on the lock screen[19].

Exploitation of markets without distribution

In locations where a particular manufacturer may not offer distribution of a device or product line, there may be exploitation of the economic demand and lack of supply for various reasons including arbitrage, inflated gross margins or similar economic benefits.

Extortion and Blackmail

A particularly alarming and disturbing trend is sextortion. In this practice, thieves threaten to send sexually explicit content stored in victim's mobile devices to their loved ones, usually to their friends and families with the aim of extorting money from the victim. This category of crime is not just about stealing devices, but also about instilling fear in people so they give in to the demands of the criminal[20].

19 See https://www.bbc.co.uk/news/uk-england-london-6276765 and https://www.bbc.co.uk/news/uk-england-london-62809151

20 https://assured.co.uk/2024/the-stolen-iphone-epidemic/

Identity Theft

In today's digital world, mobile devices store a wealth of personal information, including credentials, banking details, and private photos, among others. Thieves who intend to commit identity theft usually exploit this sensitive data to gain unauthorised access to the user's personal accounts, make fraudulent transactions, apply for credit cards or loans under the user's name, and even sometimes engage in other illicit activities without the user's knowledge. Victims of this category mostly experience a significant threat to their privacy and security, as the thieves misuse their personal information for malicious purposes, leading to financial losses and potential reputational damage.

Parts / Laundering

It can be profitable for thieves to steal mobile devices and break them down into parts to sell. Thieves engaged in this activity do not care about the victim's personal information on the device, instead they just want to make money through an organised disassembly and distribution channel. They mostly sell the parts separately, either domestically or abroad. These thefts require a strong technical understanding as those involved need to know exactly how to take different makes and models of devices apart and, once dismantled, to identify where and who is best placed to sell the parts. There are various organised groups involved in this activity, each with a specific set of duties for them to perform.

Personal usage

This motive applies to thieves who have no intention of making a profit or committing fraud but rather a desire to use the stolen mobile device for their own personal use without having to pay the full retail price of the new device themselves. Thieves in this category often target brand new high-end models of device.

Resale

Flagship mobile devices are expensive and highly valued by most people, resulting in strong demand for both legitimately and illegitimately obtained devices. This demand facilitates the resale of stolen devices, both locally and internationally. A common reason for stealing devices is to sell them for a 'quick buck'. If the device has been recently released, it is easier for thieves to find buyers at a good price. These stolen devices are commonly sold in underground markets where people bid on them based on the make, model and age of the device. Some thieves sell stolen devices to pawn shops who then resell them to other buyers.

Tax Avoidance

In countries where mobile devices are subject to high levels of import duties and/or taxes such as Value Added Taxes, stolen devices are offered for sale at prices significantly lower than devices sourced from legitimate sources as the stolen devices are not subject to these taxes. These devices can represent a significant cost discount for consumers of 10% - 30% and make the purchasing of stolen goods much more attractive to cost conscious users.

Theft for Services

Some street thieves steal mobile devices specifically to exploit access to bank accounts and other services that may be running on the stolen devices that can be monetised.

Mitigations

A variety of theft mitigation capabilities exist today, ranging from mobile industry schemes, device manufacturer solutions, law enforcement intervention, and government policies and legislation.

Device Registry

Many operators in North America, South America and Western Europe participate in the GSMA Device Registry[21] where details of blocklisted devices are shared across network operators to enable their blocking to ensure they have limited value, other than for parts.

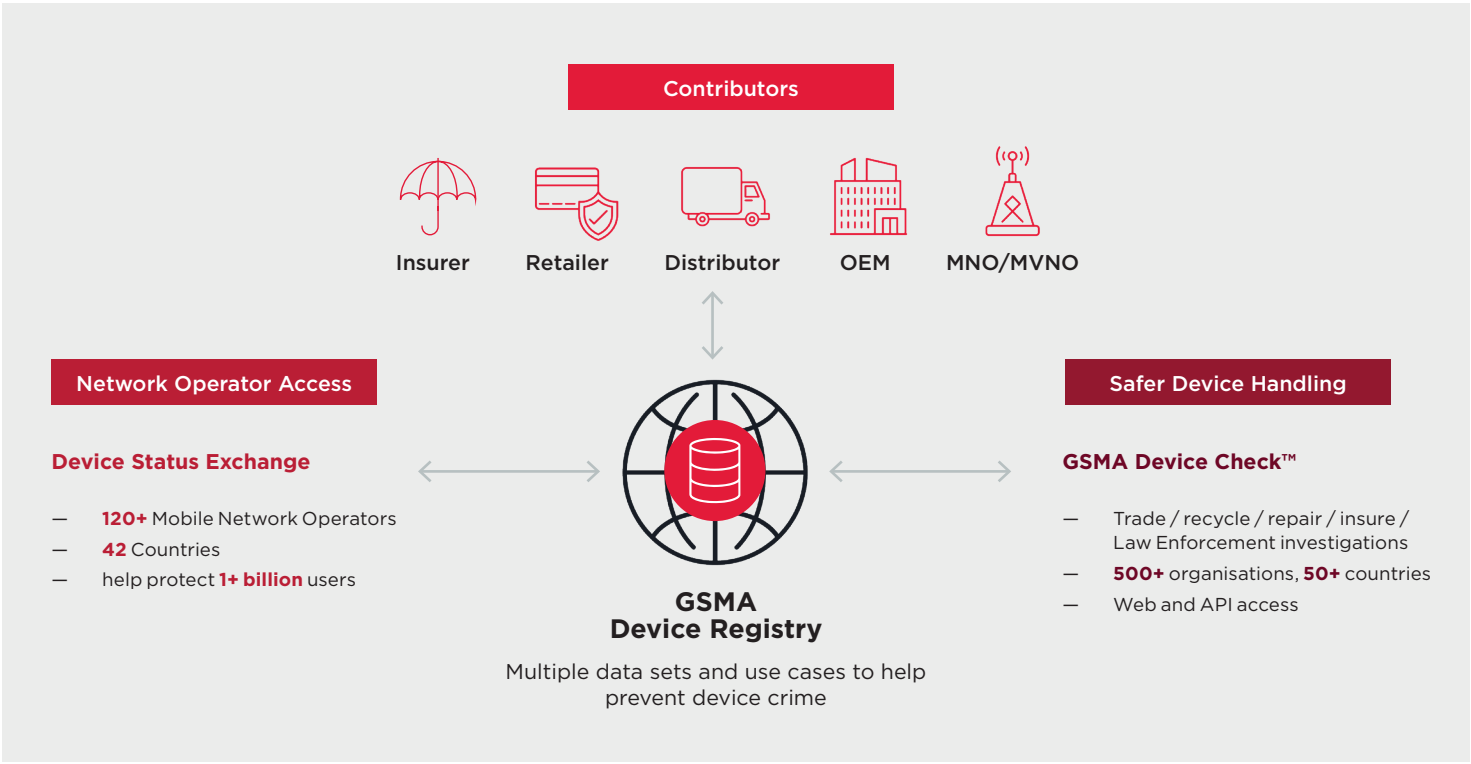
In most cases, for a stolen device to have any significant value outside a country that uses the GSMA Device Registry, it must be transported and sold in a country that does not use the GSMA Device Registry where it can be used unrestricted on local mobile networks. Currently, 130 of the approximate 800 mobile network operators globally participate in the Device Registry, reflecting a poor level of commitment on the part of operators to block stolen devices and the absence of encouragement from governments for operators to take action. Additionally, there is an inconsistent approach across some network operators that do not fully harness the capabilities and the data of the Device Registry by selectively allowing devices stolen from a particular country to be permitted on their networks. "Cherry-picking" of lost and stolen data and failing to block devices that have been reported stolen creates inconsistency and significant gaps in the global marketplace.

Figure 4, Countries with Operators using GSMA Device Registry (31st December 2024)

21 https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-registry

Recognising that many network operators are resistant to device blocking, greater participation of device manufacturers and OS developers in utilising block list data to deny service to stolen devices could reduce the existing reliance on network operators to take action. This has the potential to significantly help prevent stolen devices from operating in countries where Device Registry use is poor or non-existent. Additionally, blocking by device manufacturers and OS developers is of benefit where Wi-Fi usage could otherwise circumvent the mobile network-based blocking protections. Ultimately, this could reduce the resale value of these devices and in turn the incentive for their theft. In some countries where no official product distribution is available and no blocking is in place, these stolen devices are sold at a premium and disruption of that market is essential to reduce the attractiveness of stolen devices.

The GSMA operates the Device Registry[22] and Device Check[23] services on behalf of the mobile industry and related organisations worldwide to help exchange device information for the common good in the collective fight against device crime. Operators and other ecosystem stakeholders can report device loss and theft to their peers via the Device Registry, and the platform also supports other use cases such as fraud, broken/faulty, court ordered blocking, and known duplicated IMEIs. The Device Check service allows widespread industry and other stakeholders, including mobile users, access to query the Device Registry database. This helps to inform those querying the database about devices they should avoid using, buying, selling, insuring, or repairing and supports a variety of law enforcement activities.



Source: CFCA Survey 2021

Figure 5, GSMA Device Registry

22 https://gsma.com/deviceregistry

23 https://www.gsma.com/solutions-and-impact/industry-services/device-services/gsma-device-check

Physical Protection Solutions

Physical protection solutions are most often used in a retail setting. Often, cable retention solutions are used in a retail store to lock down devices to a location. However, these can be forcefully circumvented and, as such, are not guaranteed to prevent theft.

Related to physical protections, but actually a software protection, some devices employ a geo-fencing solution that sets an alarm when a device moves out of proximity from its intended location (in a storefront). These tethering mechanisms may also work to disable a device if the alarm is not silenced (after a period of time or after exceeding a preset geofence area).

Software Level Solutions

Related to software threat prevention techniques, software level solutions can be accomplished at the device level, the network level, or both. At the device level, a mobile device can potentially be disabled (made unusable) by the owner of a stolen device or by the relevant mobile network operator. Key to the success and effectiveness of such a technique is that the device remains persistently disabled. In the past, organised crime groups would steal mobile devices in bulk (e.g. pallets of devices stolen from a warehouse in the UK used to store items from Heathrow[9]) and these devices would be reset to factory settings and then shipped and sold within days in other countries. The people purchasing these devices would not necessarily know that they had been stolen. If a solution is persistent, the lock will survive a reset to factory settings, and the device will remain useless. If all devices stolen could be locked persistently, this would potentially help to curb device theft, as the device could not be resold, and its value is reduced. However, a residual market exists as stolen devices can often be broken up into parts and sold for a reasonable profit. Software versions change over time and future versions may have very different functionality that could be harnessed to reduce the utility of stolen devices.

Operating Systems

All modern mobile operating systems offer theft deterrence capabilities starting with hardware backed lockscreen protection (i.e. PIN or Passcode) as well as the utilisation of file-based encryption. Both Android and iOS platforms offer data encryption, ensuring all user data are protected and accessed only with correct credentials. Additionally, both platforms prevent unauthorised use of the device and ensuring the device cannot be re-activated without proper authentication after a factory reset.

Android

Android offers a comprehensive set of theft deterrence capabilities that provide users with multiple layers of protection and options to secure their devices in case of loss or theft. Additionally, in 2024 Android introduced a new suite of advanced theft protection features. These features have been rolled out through Google Play services updates in late 2024 to the billions of devices running Android 10+, with some features available in Android 15. Learn more here[24].

Theft Detection Lock

Theft Detection Lock is a powerful new feature that uses Google AI to continuously monitor device motion patterns to identify actions commonly associated with theft, such as sudden acceleration or forceful removal from a user's grasp. When a suspicious motion pattern is detected, Theft Detection Lock automatically and quickly locks the device. This proactive measure reduces the window of opportunity for a thief to gain access to personal data on the device. This feature is available to Android 10+ devices through a Google Play services update in late 2024.

Remote Lock

With Remote Lock, users are able to quickly lock their devices with just their verified phone number using any device by going to android.com/lock. It allows for a quick response in the event of device theft when users don't remember their Find My Device password immediately. This feature is available to Android 10+ devices through a Google Play services update in late 2024

Offline Device Lock

A common strategy for thieves to avoid remote locks is to disable cellular connectivity and Wi-Fi connectivity. To mitigate this strategy, Offline Device Lock detects when cellular and Wi-Fi connectivity have been disabled and automatically locks the device. This feature is available to Android 10+ devices through a Google Play services update in late 2024.

Multi-user Mode

Android supports multiple users on a single Android device by separating user accounts and application data. For instance, parents may allow their children to use the family tablet, a family can share an automobile, or a critical response team might share a mobile device for on-call duty. Learn more here[25].

Private Space

Private space is a new feature that lets a user create a separate area in the device that can be hidden and locked with a separate PIN, giving additional security for applications that might contain sensitive data, like health or financial information. This feature is available as part of the Android 15 update.

24 https://support.google.com/android/answer/15146908?hl=en
25 https://source.android.com/docs/devices/admin/multi-user

Google Files Safe Folder

Allows users to save files in a password protected area using the Google Files App. Learn more here[26].

Protect Sensitive Settings

Protect sensitive settings helps deter thieves and protect users' data in the event of a theft, requiring authentication (PIN, password or biometrics) when making changes to sensitive settings often abused by thieves. This covers: disabling Find My Device, extending screen time-out, turning off Remote Lock, erasing an eSim, turning phone number verification on or off for Remote Lock. This feature is available as part of the Android 15 update.

Identity Check

Android incorporates biometric authentication to enhance device security and user convenience. This includes fingerprint recognition, facial recognition, and iris scanning, depending on the specific device and Android version. Biometric authentication serves as an alternative or supplement to traditional PINs, passwords, and patterns. Identity Check keeps the device secure even if the PIN is known by a thief. The new feature requires biometrics for accessing and changing critical settings and apps, like Google account, changing PIN, disabling theft protection, or accessing Passkeys from an untrusted location. This feature will be released to select devices in late 2024.

Failed Authentication Lock

Failed Authentication Lock locks the device's screen after consecutive failed authentication attempts across the device. This prevents thieves from attempting to brute force or simply guess the login. This feature is available as part of the Android 15 update.

Find My Device (formerly Android Device Manager)

Find My Device is a feature that helps users to locate a lost or misplaced Android device. It can show the device's location on a map, lock the device, erase data, or make the device ring at full volume even if it's set to silent.

Apple (iOS)

iPhone has pioneered a range of theft deterrence and protection mechanisms that span the threat spectrum from basic monetisation strategies that seek to resell stolen hardware to the most sophisticated attackers that obtain a user's passcode and then steal the device to engage in identity theft and other attacks such as draining money from banking and crypto apps. Further reading for the latest on Apple platform security can be found here[27].

Find My

The Find My app helps users locate and find their Apple devices, such as an iPhone, even if they're offline and it can be used to remotely lock a device if it is lost or stolen. The application allows for tracking devices on a map, finding devices with an audible tone, and the Find My app can even let you know if you leave your devices in an unfamiliar location. Learn more here[28].

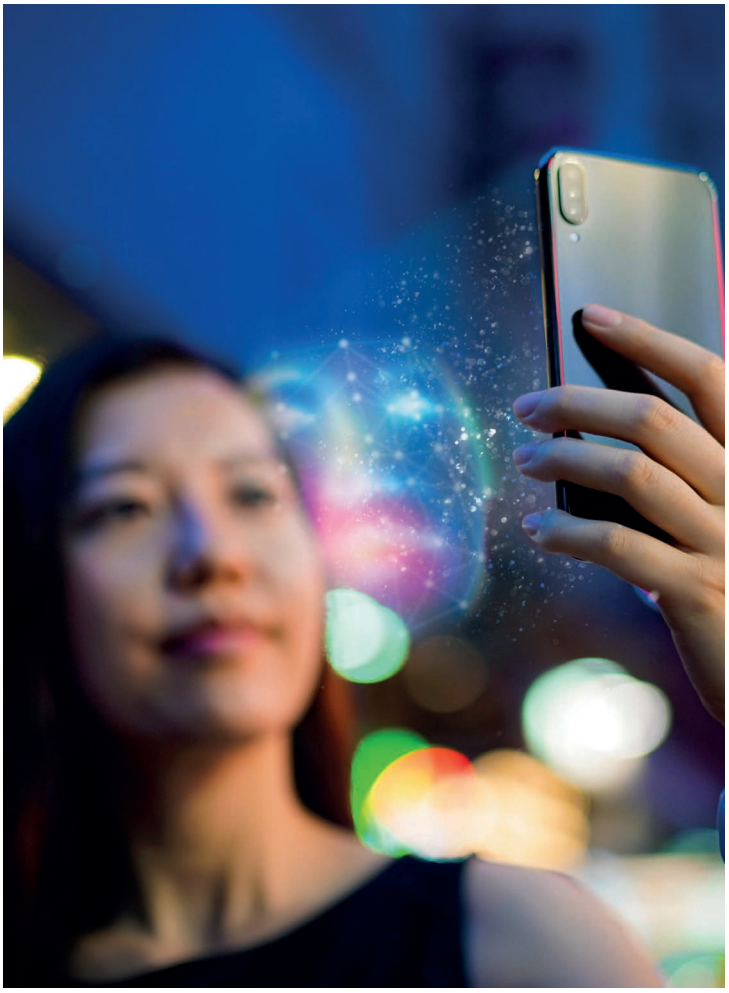
Activation Lock

Activation Lock[29] helps users keep their devices secure, even if those devices are in the wrong hands, and can improve their chances of recovering them. Even if the user erases the device remotely, Activation Lock can continue to deter anyone from reactivating the device without permission. It is automatically enabled when Find My is turned on.

Lost Mode

Users can turn on Lost Mode (or Mark as Lost) to lock a lost or stolen Apple device and can erase the Apple device remotely if it is permanently lost or stolen, either in Find Devices on iCloud.com/find or in the Find My app of another Apple device. Learn more here[30].

26 https://support.google.com/files/answer/9935264
27 https://support.apple.com/en-gb/guide/security/welcome/web
28 https://support.apple.com/find-my
29 https://support.apple.com/en-us/108794
30 https://support.apple.com/en-us/101593



Stolen Device Protection

Stolen Device Protection[31] for iPhone enhances security when a device is away from familiar locations like home or work. It requires Face ID or Touch ID—with no passcode alternative or fallback—so that only the authorised user can access sensitive features such as stored passwords or credit cards. A security delay helps prevent immediate changes to critical settings if the device is stolen. This protection helps prevent critical account or device changes when thieves have obtained both the iPhone and the user's passcode, a sophisticated but rare attack.

Hardware security and biometrics

For software to be secure, it must rest on hardware that has security built in. That's why iPhone—running iOS—has security capabilities designed into silicon. These capabilities include a CPU that powers system security features, as well as additional silicon that's dedicated to security functions. Security-focused hardware follows the principle of supporting limited and discretely defined functions to minimise the attack surface. Such components include a boot ROM, which forms a hardware root of trust for secure boot, dedicated AES engines for efficient and secure encryption and decryption, and a Secure Enclave. The Secure Enclave also provides the foundation for the secure generation and storage of the keys necessary for encrypting data at rest, and it protects and evaluates the biometric data for Face ID and Touch ID.

The technology that enables Face ID is some of the most advanced hardware and software available in any consumer device. The TrueDepth camera captures accurate face data by projecting and analysing thousands of invisible dots to create a depth map of the user's face and also captures an infrared image of their face. A portion of the neural engine of the chip—protected within the Secure Enclave—transforms the depth map and infrared image into a mathematical representation and compares that representation to the enrolled facial data to help ensure a proper match.

31 https://support.apple.com/en-us/120340

Device Manufacturers

Device manufacturers have also implemented their own solutions separate from those created by the OS developers.

HMD Global

HMD Global is a device manufacturing company that provides service for remote locking of assets such as mobile devices to protect them from anyone attempting to steal or commit fraud. An additional feature allows device owners to lock the network on the enabled devices, only enabling a specific network operator's network instead of manual SIM lock, in case of fraud or device theft, preventing the device from being used in certain networks.

Huawei

Huawei, with its Harmony Operating System, protects user data privacy and security with several mechanisms[32]. The local protection of device data allows the user's data protection from the device startup until the end of life of the device.

Huawei's Find My Phone[33]

Huawei allows users to locate the device in a map using Huawei cloud with Huawei identifier. Once the device is located, an authorised 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. This means that the device will enforce its factory setting.

File Safe

Users can store pictures, audio and video, and files on the device in the "File Safe" to prevent others from peeping or accessing them in the event that the device is lost or stolen. After saving user data or files in the safe, the user will need to verify their identity when they access them again.

Notepad Lock

Locking notes in Notepad gives users another level of protection, by ensuring that no one else can view them without the user's authorisation. Locked notes cannot be screenshotted or recorded. The user can even apply a lock screen password, fingerprint, or facial recognition protection to locked notes, for added convenience.

App Lock

When the user sets an application lock for chat, payment and other applications, the user must enter a password or perform biometric authentication to use these applications even if the device is unlocked, so that these applications are protected in an unlocked device, preventing others from accessing the applications without permission. In case of a stolen device, access to these applications is protected.

Biometric protection

Users can use biometric data (fingerprints, faces, and voiceprints) to unlock and authenticate the device. The pre-processing, entry, and authentication of biometrics are all performed in a highly secure part of the device and are never saved as they originally appear. Instead, biometric data is turned into a secure code and stored safely on the device, not shared anywhere else outside the cloud server or device.

Samsung

The Samsung Knox Platform, starting from the hardware layer and encompassing software components, offers protection against diverse security threats. By ensuring the security of each Samsung Galaxy device from activation onwards, Knox's multi-layered defence mechanism effectively isolates and protects data such as passwords, biometric information, and cryptographic keys, rendering the device highly resilient against unauthorised access and other cyber threats. Samsung Galaxy devices are equipped with comprehensive theft deterrence features to prevent unauthorised access, data theft and loss.

32 https://consumer.huawei.com/en/privacy/privacy-control/

33 https://consumer.huawei.com/en/support/article/en-us15770794/

Samsung Find

Samsung Find (application and web-based service) helps users locate and find their Samsung Galaxy devices. Samsung Find will attempt to locate the device with an approximate location indicated by a marker in a map. The owner can wipe and lock the device remotely, with a PIN. Samsung also introduced a feature that allows the owner to lock the device so that it cannot be powered off. Additionally, Samsung Find allows the authorised users to extend the battery life by remotely turning on Maximum power saving mode. In addition, Samsung Find includes Offline finding – a feature that allows the device to be found even when it is not connected to the network. It will also allow the mobile device to be used to scan for lost devices that may be nearby. (This does not work when the device is turned off.)

Secure Folder

Secure Folder is a personal secure space that allows users to securely separate their applications and data. Applications and data inside Secure Folder are sandboxed separately on the device and gain an additional layer of security and privacy. Secure Folder helps with privacy by separating sensitive data and normal data. Sensitive data is not accessible outside of Secure Folder.

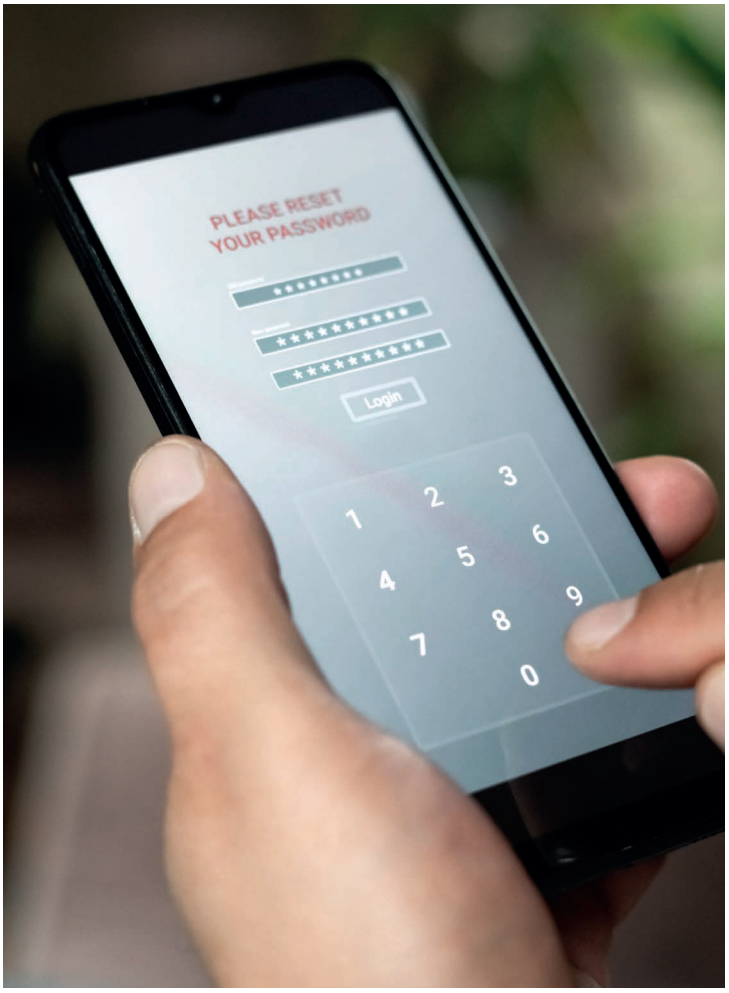
Knox Vault and Biometrics

Samsung Knox Vault is a hardware-based security platform which protects the most critical data on a device such as lock screen credentials including PIN/passwords/patterns and biometric data (fingerprints and facial recognition information) and sensitive cryptographic keys. Based on security processors and isolated secure memory, powerful security protection is provided by Samsung Knox Vault against various types of attacks such as physical tampering, side-channel attacks and reverse engineering to ensure that sensitive data is stored and managed securely, reducing the risk of identity theft or unauthorised access.

Motorola

Secure Folder

Motorola secure folder allows the device user to protect their most sensitive applications and media separately. Secure Folder keeps the user's work and personal information safely hidden, which would otherwise require a separate PIN for access. The folder can be customised with a fake name and icon to fool the device thief.



Network Lock

Motorola devices give users an option to lock the network and security related functions while the device is locked.

Pin Pad Scramble

When this setting is enabled, the lock screen displays a different PIN pad configuration each time when attempting to unlock the device.

Auto Lock Detection Mechanism

With this feature enabled, the mobile device can be configured with trusted scenarios, (that is, trusted places and trusted devices). The device automatically locks when outside of trusted places or when the mobile device is disconnected from trusted devices.

Additional Enterprise Controls and Deterrence

For enterprise and government use, all modern mobile operating systems/mobile devices offer additional enterprise management capabilities and controls that could further protect the enterprise data on a stolen device. You can learn more about each vendors enterprise capabilities below:

- Google Android[34]
- Apple iOS[35]
- Samsung KNOX[36]
- Huawei Harmony OS[37]

34 https://www.android.com/enterprise/security/
35 https://support.apple.com/en-gb/118102
36 https://docs.samsungknox.com/admin/fundamentals/whitepaper/samsung-knox-for-android/the-samsung-knox-platform/
37 https://medium.com/huawei-developers/huawei-mdm-engine-empowering-mobile-device-management-cb087652f1c1

Government Interventions

Many governments around the world have recognised mobile device theft as a problem and have taken a variety of approaches. A few countries have legislated to make reprogramming unique identifiers (such as the IMEI number) illegal. Some countries have sought to have some form of 'approved' or 'allowed / positive' list of devices which have led to unintended consequences. Proposals for 'kill switches' have repeatedly been made, however such a capability represents a significant risk to a country's cyber security if abused or broken. Other actions have been aimed at preventing counterfeit or 'substandard' devices which represent a large percentage of the market in some economically disadvantaged areas of the world. These devices contain invalid or misused IMEI ranges which create barriers to block listing when stolen.

GSMA's Mobile Policy Handbook has further information on the role of national authorities[38].

The following is a non-exhaustive list of different government interventions in a number of countries:

Colombia

In Colombia, the telecommunications authority Communications Regulation Commission (CRC), in collaboration with the ICT Ministry and mobile operators, implemented a system to identify, register and manage device access to the country's mobile networks, and to establish a process for blocking those reported as stolen. This IMEI-based approach, first implemented in 2011, was a regional forerunner that aimed to ensure only legal and legitimate mobile devices could be used.

To lay the regulatory groundwork, the CRC passed a series of resolutions addressing issues such as the sharing of data between the mobile operators and assigning the legal and financial responsibility for a centralised database to the operators. This database consisted of a 'positive list' of all legally imported and acquired mobile devices approved for use in the country, together with the names of the registered owners of each device, and a negative list of devices that should be denied network access.

Unfortunately, in addition to the data protection risk this approach introduced, collection and reporting of such information imposed a significant compliance burden and created a barrier to selling or transferring handsets. Consequently, the government's admirable goal of addressing a serious societal problem failed to make a meaningful difference, while imposing costly obligations on the mobile ecosystem. Over a decade later, with the results failing to justify the costs, Colombia is re-evaluating and may eliminate device registration requirements altogether, as part of a wider regulatory simplification scheme[39].

Ecuador

In Ecuador, the regulator chose to implement a positive list including the Type Allocation Codes (TACs) of legitimate, approved mobile devices, hence blocking invalid IMEIs. However, during the COVID-19 quarantine in 2019-20, the government decided to ease the restriction, acknowledging that the restriction was a potential barrier to citizens' adoption of mobile communication services.

Kenya

In 2020, the Communication Authority of Kenya proposed the introduction of a Device Management System (DMS) which attempted to address a number of different abuse cases including counterfeit devices and a 'whitelist' of allowed IMEI numbers[40].

Pakistan

In 2019, the Pakistan Telecommunication Authority (PTA) introduced its Device Identification, Registration and Blocking System (DIRBS) which functions as a centralised Equipment Identity Register (EIR) that aggregates and shares device data with individual network EIRs, local tax authority, device manufacturers and law enforcement.

38 https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/mobile-policy-handbook/consumer-protection/#mobile-device-theft
39 https://www.crcom.gov.co/es/proyectos-regulatorios/2000-71-17
40 https://cipit.strathmore.edu/unpacking-the-device-management-system-dms-judgement-2/

The approach taken by the PTA requires subscribers to register their devices, along with proof that relevant taxes have been paid, in a national allow list. Network operators must submit to DIRBS, on a daily basis, details of all devices and related subscriber credentials, active on their networks. DIRBS generates and makes available to the local network, on an hourly basis, a block list that contains IMEIs of devices reported lost/stolen, devices for which custom duties/taxes have not been paid and non-compliant devices with invalid IMEIs. An allow list that contains IMEIs of all devices to which network access can be granted is also made available to the network operators.

For lost and stolen devices, victims can file a request to the PTA to have the IMEI of their device blocked to prevent it from potential misuse. Devices are blocked within 24 hours of reporting, after necessary verification.

DIRBS involves the compulsory registration of mobile devices by users and the provision and sharing of personal information across a range of platforms. It is a cumbersome and expensive approach but has the potential to help consumers check the status of devices that they intend to purchase by submitting IMEIs to a centralised verification system that reports back whether a device is on the block list or the allow list.

Uganda

In order to block the high number of counterfeit devices, which is a distinct problem from device theft, in the country, in 2019 Uganda's Communication Commission adopted a central equipment registry[41].

Ukraine

The country operates a national registry of IMEI numbers. A government Bill in 2019 intended to block so-called 'grey' devices (i.e. those not on the permitted list) was withdrawn[42].

United Kingdom

Legislation was enacted under the Mobile Telephones (Re-Programming) Act (2002) which was subsequently modified to cover the offering of services to change a unique identifier.[43] The offenses include changing or offering to change a unique identifier, interfering with the operation of a unique identifier, and possession (with intent) of tools which change unique identifiers. The offenses carry a maximum of 5 years imprisonment. It is understood that only two other European countries enacted similar legislation: Lithuania and Latvia.
The country also introduced a police unit within the London Metropolitan Police dedicated to device theft matters called the National Mobile Phone Crime Unit (NMPCU) which has since been disbanded. It has also engaged extensively with the mobile industry on various solutions such as preventing re-activation of stolen devices.

41 https://www.telecompaper.com/news/uganda-adopts-central-imei-phone-registry-to-block-counterfeit-devices--1321103
42 https://archive.kyivpost.com/ukraine-politics/fedorov-withdraws-bill-permitting-blocking-grey-phones-using-imei-code.html
43 https://www.legislation.gov.uk/ukpga/2002/31

Police Operations

A number of different tactics have been deployed by police forces around the world. In 2003, the UK established the National Mobile Phone Crime Unit (NMPCU) as a dedicated intelligence unit to combat theft and the subsequent re-programming and sale of stolen devices. The group observed many different criminal activities and methods including the export of stolen devices by individuals when travelling on holiday to pay for their trips to visit family. This was gradually disbanded in the mid-2010s. On average the cost of the unit was £2 million a year to maintain[44].

In 2014, Europol worked with police forces in the EU and took action in 'Operation Ringtone' together with a number of other countries against 213 individuals and organised criminal gangs demonstrating that international collaborative action is possible, and that organised crime is heavily involved with mobile device theft [45].

Young offender interviews have proven to be useful as is the discovery of techniques and information following police action against thieves[46]. If this intelligence is shared with the mobile industry it can help shine a light on methods and new technical breaches that may not have been seen before.

Education

User education by industry, governments and police organisations is one part of addressing the mobile device theft crime puzzle. TV advertising, posters, online campaigns, and leaflets at the point of sale have all proven useful in helping to raise awareness of robbery and other crimes against mobile device users.

Recyclers Charter and Code of Practice

The secondary market for used mobile devices has become an exciting and very active exchange with carriers offering incentives to encourage trade in activity. Increased device trade in and reuse has introduced new challenges to the industry which could lead to the laundering of stolen and fraudulently obtained devices. Today, many carriers and other device traders evaluate the status of a device in the GSMA Device Registry to ensure it has not been reported to the GSMA Block List. This helps to avoid

Figure 7, UK Home Office advertising campaign (early 2000s)

financial losses, legal claims and reputational harm from handling devices that are not with their rightful owner. Unfortunately, some bad actors continue to openly trade these devices and export to countries that do not participate in the GSMA Device Registry.

It has also been very difficult to establish exactly how many stolen mobile devices are exported to non-participating markets as they just disappear from networks. However mobile operating system providers are now in a much better position to discover this information due to the level of connectivity of modern devices. There is evidence to suggest that stolen mobile devices are exported to shipment hubs overseas, including from individual users who have been able to track their stolen devices while they were being exported around the world.

In the UK, the Telecommunications Fraud Forum (TUFF) adopted a Recyclers' Code of Practice[47] which sought to establish that incoming mobile devices to recyclers were not stolen and in 2010 published the following Compliance Requirements[48]:

44 https://hansard.parliament.uk/Commons/2010-01-26/debates/10012685000041/NationalMobilePhoneCrimeUnit
45 https://www.europol.europa.eu/media-press/newsroom/news/international-action-against-mobile-phone-thieves
46 https://image.guardian.co.uk/sys-files/Guardian/documents/2002/01/08/mobilephone.pdf
47 https://www.gov.uk/government/news/new-code-of-practice-to-close-multi-million-pound-stolen-phones-loop
48 https://www.stoprecycledstolenphones.com/cop

In the United States, there are efforts being put forth by the CTIA Stolen Phone Working Group to update Federal Law to make it illegal to advertise restricted devices on digital marketplaces for sale, solicit sales, and in general make it illegal to distribute equipment to obfuscate an IMEI to avoid detection of a stolen or fraudulently obtained device.

While there is no formal industry code of practice for recyclers or secondary marketers in the United States, general law dictates adherence to stolen property statutes. Most reputable traders will query devices against the GSMA Device Registry even though they are not bound by industry agreements.

- Be a TUFF member.
- Use a compliant status checking service.
- Check phone status as soon as you obtain the IMEI(s).
- For in-person transactions, reject those with adverse status.
- For seller-not-present transactions
  - Quarantine those with adverse status.
  - Hold for up to 28 days to allow the rightful owner to recover, or the seller to clear the adverse status.
  - After 28 days, dispose of the device in a way to ensure it cannot re-enter the market or return to the seller.
- Store seller details in case of change in status or investigation.
- In your terms and conditions make it clear and obvious to sellers that:
  - If they send you a stolen phone they won't get paid and may not get it back.
  - Their details will be shared with other parties for the prevention and detection of crime.

Figure 7, Code of Practice Compliance Requirements for the TUFF Recyclers' Code of Practice[49]

Other Protections Including Third Party Solutions

In addition to device lock solutions from device manufacturers, multiple third parties provide solutions that can effectively disable a mobile device, one solution being that from Trustonic[50]. Trustonic offers a SaaS platform that acts as a single pane of glass to consolidate Android OS and device manufacturer solutions in one space, ensuring the best security is applied. It aims to improve payment behaviour through device financing and deter supply chain and end user theft. The platform can be seamlessly integrated into business processes via APIs for an automated operation.

National blocking systems / databases have been implemented[51] by government agencies to combat counterfeiting and theft which often require pre-registration of devices with IMEI and IMSI pairing. Some of the solutions deployed are at odds with the global mobile standards and have had significant negative impact on local markets and legitimate users while achieving little in the way of success against device theft levels. Done properly and comprehensively, device blocking and data sharing via the GSMA Device Registry, can be effective as part of a portfolio of measures to reduce the impact of device theft.

The device financing space has multiple 3rd party providers for locking / 'bricking' a solution. If a user does not pay their weekly or monthly device ("rental") fee, then it can be locked and disabled. If a consumer pays the bill (via online portal, etc.), the device can be unlocked in seconds. A key to these solutions is that the lock is somewhat persistent (survives a factory reset, etc.) and these solutions could be used to combat device theft.

As with many cybersecurity solutions, a layered approach can be effective – i.e. employ software solutions both at the device and network levels. Mobile device manufacturers can leverage any capabilities that are provided by the OS provider, and device manufacturers may layer their own solutions on top of this (e.g. Samsung, HMD Global, etc.).

49 from: https://www.stoprecycledstolenphones.com/cop

50 https://www.trustonic.com/device-locking

51 Example: India – CDOT https://www.ceir.gov.in/

Advice For Consumers

Use a strong PIN or password

Make sure to use a strong, complex PIN, pattern, or password. Preferably it should be six-digits or more that doesn't repeat digits or create a simple sequence, pattern, word, or phrase that's recognisable or easily associated with consumers. This ensures that criminals won't have easy access to your data and information. Even if consumers use biometrics, they are still advised to set up a strong password in case an attacker tries to override biometric protections. Android users can learn more about setting a screen lock[52]. For iOS users, learn more about setting a passcode here[53].

Use biometric authentication

Biometric authentication offers a balance of security and convenience. On devices with a robust fingerprint or facial recognition, biometric authentication can be hard to fake since it's unique to the user, thus making it harder for an attacker to access their device. Learn more about setting Touch ID[54] and Face ID[55] on iOS.

Write down the device's IMEI number

Each device has a unique serial number, most often an IMEI number. This can be helpful for your mobile operator to mark this as a missing device. Some police departments also ask for the IMEI number to report a stolen device. The IMEI can typically be found under Settings, on the device packaging, or by dialing *#06#.

Pin and unpin screens

Users can pin a screen to lock their device to one app that remains in view until they un-pin using the PIN or pattern of password. This can be useful in times when sharing a device or in a public place where one may worry about theft. Pinning a screen ensures that the customer can use the device but only for a select app. For Android users, learn more about pinning and unpinning screens here[56]. For iOS users, learn more about Guided Access here[57].

Enable additional security for applications

Many applications provide additional security by allowing the customer to add a PIN or password, use biometrics, or two-step verification to unlock the device. Especially for applications with sensitive or valuable information, like finance, payment or social apps, look for options to add. Customers can look for additional options in their applications under the security or privacy settings.

Use passkeys to log-in to websites and applications

For websites that support them, passkeys are a secure way to sign-in without using a password. Android customers can learn more about passkeys here[58]. iOS customers can learn more about passkeys here[59].

Back-up and restore your data

Some people who lose their device to theft hesitate to erase their data remotely if they have valuable data. By learning how to back-up your data, the customer can move quickly to factory reset their device without worrying about lost data. Android users can learn how to use back-up and restore here[60]. iOS users can learn how to back up their products here[61].

Set a SIM PIN

When a device is lost or stolen, an attacker might take out the SIM card and insert it into another device to receive one-time passwords and account reset links by SMS, which is a way that many companies offer to recover lost passwords. As this can be a source of attacks, protecting the device SIM card with a PIN prevents it from being used for this purpose, as at every new boot or when it is inserted on another device, the SIM PIN will be required. Please, be mindful that some network operators have a default PIN and it is advisable to change it, as this information might be public.

Hide notification content from the lock screen

Information from notifications in the lock screen might give attackers enough data to initiate scams. To prevent this, it is possible to hide notification content from the lock screen[62] and avoid the inclusion of any personally identifiable information (for example personal telephone numbers).

52 https://support.google.com/android/answer/9079129
53 https://support.apple.com/en-us/119586
54 https://support.apple.com/en-us/102528
55 https://support.apple.com/en-us/108411
56 https://support.google.com/android/answer/9455138
57 https://support.apple.com/en-us/111795
58 https://support.google.com/android/answer/14124480?hl=en
59 https://support.apple.com/guide/iphone/use-passkeys-to-sign-in-to-apps-and-websites-iphf538ea8d0/ios
60 https://support.google.com/android/answer/2819582?hl=en&sjid=14342968453930799020-NA
61 https://support.apple.com/en-us/118426
62 https://www.gsma.com/security/mobile-device-theft/

Conclusions

The persistent, increasingly sophisticated and orchestrated challenge that device theft poses, casts a long shadow across the mobile ecosystem, affecting consumers, network operators, device manufacturers, OS developers and society as a whole. As smartphones continue to evolve into indispensable tools for communication, commerce, and personal expression, the stakes associated with their theft have risen exponentially.

Continually addressing such a multifaceted challenge demands a concerted effort from all stakeholders, from industry to law enforcement, governments and individual device users and it is critical that the lessons from the past and the journey that all stakeholders have undertaken are understood, in order to recognise what works and what doesn't work to better protect future consumers.

There is also an ever-present need to promote consumer awareness and education, and individuals should be encouraged to make full use of the capabilities both built-in and more widely available to safeguard their privacy and protect their valuable data.

This paper has shown that proactive measures, encompassing enhanced device security, industry schemes, robust and easily accessible anti-theft technologies, and government initiatives, all play their part in the fight against mobile device theft. However, it is acknowledged that criminal techniques and tactics will always evolve and, as such, this will be an ongoing battle to protect the individual users of mobile technology.

This report has been produced by the GSMA Device Security Group.

Further Reading

It should be noted that there has been extensive research work over many years into the issues of theft and robbery, and these serve as useful references to the rationale and motivations behind types of theft whether it stems from societal issues, poverty or profit. Some papers also explore potential technical solutions. A small illustrative sample is provided below:

Ronald V. Clarke (1999) **'Hot Products: understanding, anticipating and reducing demand for stolen goods'.** This paper introduced the concept of 'CRAVED' - six elements that make products attractive to thieves, that they are: Concealable, Removable, Available, Valuable, Enjoyable and Disposable.

Jen Mailley (2011) '**The prevention of mobile phone theft: a case study of crime as pollution; rational choices and consumer demand**'. This thesis looks at rational choice event modelling by device thieves, based on interviews with 40 device thieves.

Lookout (2014) **PHONE THEFT IN AMERICA Breaking down the phone theft epidemic**. Lookout's Phone Theft in America report, a survey of smartphone theft victims conducted by IDG Research, examines the smartphone theft epidemic in the U.S.

Graham Farrell (2015) '**Preventing phone theft and robbery: the need for government action and international coordination**'. This paper looks at technical mechanisms to prevent theft and how international coordination is necessary.

Zhiling Tu, Ofir Turel, Yufei Yuan, Norm Archer (2015) 'Learning to cope with information security risks regarding **mobile device loss or theft: An empirical examination**'. This paper considers social influence, coping and threat appraisal by users using protection-motivation and social learning theories.

Xinyu Liu, David Wagner, Serge Egelman (2018) '**Detecting Phone Theft Using Machine Learning**' This paper explores a technical solution to detect 'grab and run' thefts, using machine learning techniques.

Camille Vanier (2019) **Phone Theft: Characteristics of Incidents and Victim Profiles**. This paper (written in French) provides the result of a survey of 113,000 individuals aged 14 and older owning a mobile device between 2009 and 2015 together the National Institute of Statistics and Economic Studies.

GSMA Head Office
1 Angel Lane
London
EC4R 3AB
UK

Email: info@gsma.com