SMS Blasters Briefing Paper
Version 2.0
25 March 2026

Security Classification: Confidential to

- GSMA Operator, Rapporteur, Industry & Sector members
- Law Enforcement Agencies, Telecom Regulatory Agencies and/or Radio Frequency Agencies

Copyright Notice

Disclaimer

Compliance Notice

The information contained herein is in full compliance with the GSMA Antitrust Compliance Policy.

This Permanent Reference Document has been developed and is maintained by GSMA in accordance with the provisions set out in GSMA AA.34 - Policy and Procedures for Official Documents.

Table of Contents

Executive Summary

Mobile network operators (MNOs) across the globe have reported smishing attacks where fraudsters use false base stations to send SMSs directly to mobile users, bypassing network-side SMS filtering. These attacks use a particular type of false base station called an SMS Blaster, which is off-the-shelf equipment dedicated to and optimised to deliver SMSs to large volumes of mobile users. SMS Blasters are openly advertised for sale on the internet. They auto-configure themselves to the surrounding network and require no technical expertise to operate. SMS Blasters are portable, and fraudsters typically load them into vehicles and drive through cities to reach large volumes of victims. They work by simulating legitimate 4G networks to capture the user equipment (UE) of victims and once captured, downgrade their network connection to a less secure 2G connection, which allows the Blaster to send the phishing SMS to the victim's UE. The victim's UE is then released back to the legitimate network. The phishing SMS typically tricks the victim into providing credentials to a fake website, making a call or downloading malware that the fraudsters will exploit, often for banking fraud.

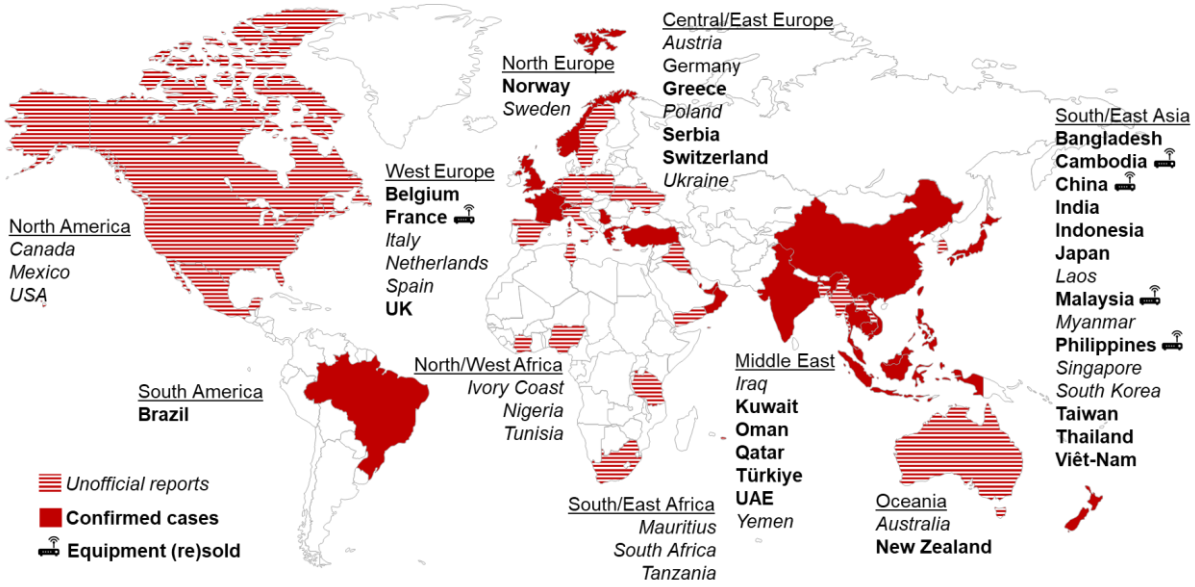

Figure 1 – Countries where SMS Blasters have been confirmed in the news [7] or where unofficial reports suggest their presence and/or use [6]

1 Introduction

The purpose of this document is to educate MNOs about a new threat and drive implementation of recommendations across the mobile ecosystem. GSMA has been made aware, through its Fraud and Security Group (FASG), of the fraudulent use of false base stations to send phishing SMS to mobile customers, usually for financial fraud, user equipment compromise or credential theft [1-4]. These false base stations, called SMS Blasters, are sold on the internet and do not require technical expertise to configure or operate. They mostly auto-configure themselves, and their configuration can be adjusted using a mobile app [5], [6]. SMS Blasters are based on software-defined radio and capture UEs in a similar way to other false base stations, such as International Mobile Subscriber Identity (IMSI) catchers and StingRays. SMS Blasters are optimised, however, to send SMS to as many mobiles as possible within their radio range and are usually placed in a vehicle driven across busy areas of a city, see Figure 2. SMS Blasters come in different sizes and models, as seen in [1], and can operate in different ways. This document is based on a model that started operating in France in 2021, see [2]. The mode of operation of the French model matches recent reports [7].

SMS Blasters exploit security weaknesses in the 2G standard, which is still supported by UEs, independently of whether operators still support this legacy protocol. SMS Blasters have been reported in several countries, including countries where 2G was already sunset.

MNOs in impacted countries worked together with the local authorities to capture the equipment and arrest the fraudsters [7]. Section 2 describes how the attack works. Section 3 provides an impact assessment. Section 4 provides some actions that MNOs can take to detect and mitigate this attack, and Section 4.3 provides some references for further reading.

Figure 2 – SMS Blasters are usually placed in a car or in a backpack on a motorcycle driven across different busy areas of a city. (Images from Dan Tri News Agency, dantri.com.vn)

1.1 References

Ref	Description
[1]	GSMA FSAG 121 SMS Blaster Investigation, available on Member Gateway at FSAG Doc 121_021 Huawei SMS Blaster Investigation.pdf
[2]	GSMA FASG 25 Smishing via False Base Station, available on Member Gateway at FASG25_43 Orange Smishing via False Base Station.pdf
[3]	GSMA FASG 25 Smishing and False Base Station: Signatures and Detection. Available on Member Gateway at FASG25_52 False Base Station signatures and detection Orange
[4]	Example of a fraudster using an SMS to try to steal cryptocurrency from a journalist BBC News Video Crypto Thieves Dec 31 2024 (on threads.net) BBC News Video Crypto Thieves Dec 31 2024 (archived on Member Gateway)
[5]	Examples of websites selling SMS Blasters https://www.smsbroadcaster.com/sms-broadcast-machine https://www.septier.com/portfolio-item/sms-blaster/ https://kkcsms.com https://ptcjammer.en.made-in-china.com/product-group/IbxEGWNVYLkh/SMS-Blaster-SMS-Broadcaster-catalog-1.html https://www.addstore88.com/sms-broadcaster/ https://mactro.com/web/
[6]	Unofficial reports of countries where SMS Blasters are being demonstrated, used, or sold, according to vendors' websites or social media channels: France: demonstration of an SMS Blaster and its Mobile App, available on Member Gateway at

Ref	Description
	Vendor Video SMS Blaster Demo in France Vendor Video SMS Blaster Configuration App Australia, Austria, Bangladesh, Belgium, Cambodia, Canada, China, France, Germany, Hong Kong, India, Indonesia, Iraq, Italy, Ivory Coast, Japan, Kuwait, Laos, Malaysia, Myanmar, Netherlands, Nigeria, Pakistan, Philippines, Poland, Singapore, South Korea, Spain, Sweden, Switzerland, Tanzania, Tunisia, UK, Ukraine, USA, Vietnam and Yemen are available at: https://t.me/kkcsms Dubai, Malaysia, Mexico, Indonesia, Italy, Mauritius, Philippines, South Africa and United Kingdom available at: https://www.smsbroadcaster.com
[7]	Press articles about confirmed SMS Blasters around the world in: **Brazil** - Polícia descobre central do golpe via SMS que funcionava em apartamento na região da Avenida Paulista **Cambodia** - អាជ្ញាធរខេត្តព្រះសីហនុរកឃើញឧបករណ៍ Fake BTS បំពាក់លើរថយន្តចល័ត ល្បចទិន្នន័យទូរសព្ទពលរដ្ឋ **China** - 23歲男子用「偽基站」發送過萬條假「#」SMS　涉串謀詐騙被捕 **France** - SMS frauduleux et Imsi-catchers : les dessous d'une escroquerie dernier cri – Libération (liberation.fr) **Greece** - Τι είναι η μέθοδος «SMS blaster» -Έτσι οι δύο Κινέζοι άρπαζαν τραπεζικά δεδομένα από κινητά πολιτών στην Αττική - iefimerida.gr **India** - बिना इंटरनेट के भी ऐसे हैक हो रहा है आपका फोन! 5G से अचानक हो जाता है 2G और फिर शुरू होता है 'खतरनाक खेल' **Indonesia** - SMS Tipu-Tipu Bikin Boncos, Modus Phising Dibongkar Polda Metro! - Suar News **Japan** – "偽基地局"の餌食になったとしても「絶対にやってはいけないこと」　総務省が注意喚起 - ITmedia Mobile **Kuwait** - https://x.com/moi_kuw/status/1889962485496557904 **Malaysia** - PDRM-MCMC Tumpaskan Sindiket SMS Scam 📠 MCMC **New Zealand** - Teen arrested for 'smishing scam' using technology never before seen in New Zealand | RNZ News **Norway** - Nytt bedragerimodus avdekket i Norge - Økokrim advarer - Økokrim **Oman:** https://x.com/RoyalOmanPolice/status/1943369135477657693 **Philippines** - Globe moves to stop 8080 'spoofing' messages - Daily Guardian **Qatar** - https://x.com/MOI_Qatar/status/1914354918690889827 **Serbia** - Uhapšeni prevaranti iz Kine koji su krali podatke građana Srbije preko lažnih SMS poruka: Policija u gepeku našla i improvizovanu opremu FOTO **Switzerland** - New risk from "SMS blasters" **Taiwan** - Man fined NT$4 million for setting up fake base station - Focus Taiwan **Thailand** - ธปท.เตือน "ปลากระเบน" ภัยรูปแบบใหม่ หลอกดูดเงินเสียหาย 200 ล้าน **Türkiye** - MİT'in sahte baz istasyonu operasyonunda Bursa da var! | Bursa Haber **United Arab Emirates** - Scammers caught transmitting fake mobile network in Dubai **United Kingdom** - Man jailed for spamming commuters with phishing attempts - London | British Transport Police **Vietnam** - Nở rộ thủ đoạn lừa đảo thông qua tin nhắn ngân hàng

Ref	Description
[8]	Singapore Guidelines on Shared Responsibility, available on the web at draft-guidelines-on-shared-responsibility-framework.pdf (mas.gov.sg)
[9]	EU Considering Shared Responsibility, available on the web at Revision of EU Rules related to Payment Services (New Regulation)
[10]	Network support and clarification of redirection to 3G, available on the 3GPP website at 3GPP CR to TS 24.301 (C1-236303) 3GPP CR to TS 36.331 (R2-2312806)
[11]	Protection against improper reselection to GERAN/UTRAN, available on the 3GPP website at 3GPP CR to TS 36.306 (R2-2313928) 3GPP CR to TS 36.304 (R2-2313929) 3GPP CR to TS 36.331 (R2-2313930)
[12]	Android 12 and Android 12L release notes, Toggle to disable 2G
[13]	Android Enterprise – Android 14 business features for your distributed teams
[14]	Android 14 and Android 14-QPR1 release notes, Disable cellular null cipher/integrity mode
[15]	Mandatory requirements for cellular cipher visibility for the user, available at 3GPP TS 33.501 Rel 17
[16]	Google Keyword – How Android protects you from scams and phishing attacks.
[17]	Google Safe Browsing
[18]	Federal Trade Commission – Report Fraud, available on the web at https://reportfraud.ftc.gov/
[19]	Information Commissioner's Office – Report spam texts and nuisance sales calls, available on the web at https://ico.org.uk/make-a-complaint/nuisance-calls-and-messages/spam-texts-and-nuisance-calls/
[20]	CTIA – Protecting yourself from spam text messages, available on the web at https://www.ctia.org/consumer-resources/protecting-yourself-from-spam-text-messages
[21]	3GPP TR 33.809, Study on 5G security enhancements against False Base Stations (FBS)
[22]	GSMA FS.42 “Binary SMS Filtering Guidelines”
[23]	“What are SMS Blasters”, BBC, available on the web at https://www.bbc.co.uk/videos/ce3ngk22qdno
[24]	Examples of honeypots that can be used or adapted to detect SMS Blasters: • Android-IMSI-Catcher-Detector (AIMSICD) • Cellguard • Crocodile Hunter • Darshark • Eagle Security • Rayhunter • SeaGlass • SnoopSnitch • Wiretap Detector

Ref	Description
	• XDetect
[25]	Altaf Shaik et al. “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems”, available on the web at https://www.ndss-symposium.org/wp-content/uploads/2017/09/practical-attacks-against-privacy-availability-4g-lte-mobile-communication-systems.pdf
[26]	Guidelines on 2G Sunset: GSMA Best Practices for Technology Lifecycle, available on Member Gateway at WAS WA.01 Best Practices for Technology Lifecycle v3.0 GSMA 2G-3G Sunset Guidelines, available on the web at https://www.gsma.com/newsroom/wp-content/uploads/NG.121-v3.0.pdf

2 The Attack

2.1 Attack Overview

This section describes the overall mechanisms used by SMS Blasters to send an SMS to a victim’s mobile. This description is based on an SMS Blaster model used in France and other models may work differently. The SMS Blaster is made of two false base stations: the first false base station uses 4G and tricks the UEs in its vicinity to attach to its radio interface by emitting the radio signal typically of up to 4 different MNO networks. The second false base station uses 2G and is used to send the fraudulent SMS to the devices initially captured by the 4G false base station. This is done by exploiting the lack of mutual authentication in 2G and skipping the use of a cipher, see Figure 3. SMS Blasters use at least two different methods to downgrade the radio connection of the device captured on its 4G interface to its 2G interface, see section 2.2. The SMS Blaster skips the use of ciphering in the 2G connection so it can inject payloads into the device, see section 2.3. The SMS Blaster pushes the device back to the legitimate network after sending it an SMS and avoids recapturing it to ensure it captures as many different devices as possible, see section 2.4.

2.2 UE Capture

This section describes two methods used by the SMS Blaster to capture the UE on 4G and downgrade it to 2G. The 4G or 5G-NSA UE selects the 4G radio signal of the SMS Blaster because that signal is stronger than those of the legitimate networks[1]. The SMS Blaster broadcasts a Tracking Area Identity (TAI) either equal or different to that used by the legitimate MNO in the Blaster’s vicinity, depending on the method used to downgrade the UE to 2G. The SMS Blaster broadcasts a TAI different to that used by the legitimate network in the Blaster’s vicinity if it redirects the UE to its 2G radio interface, as described in section 2.2.1. The SMS Blaster broadcasts a TAI equal to that used by the legitimate MNO in the Blaster’s vicinity if it forces the UE to reselect its 2G radio interface, as described in section 2.2.2.

[1] Capture and downgrade techniques described in this section apply equally to SMS Blasters operating in 4G or 5G-NSA as both technologies use the same 4G signaling.

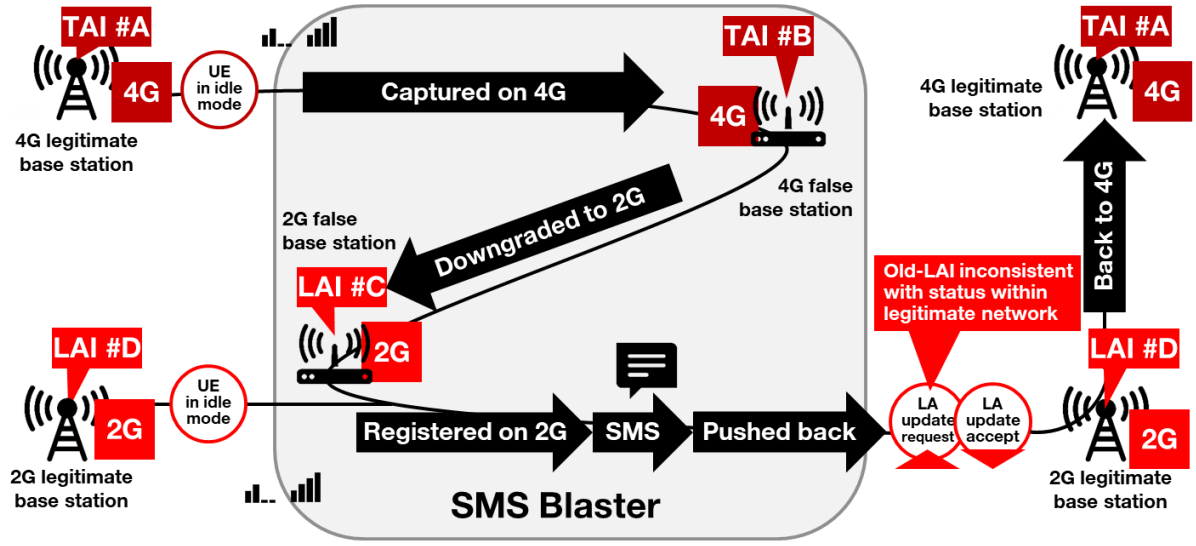

Figure 3 – SMS Blaster Attack Steps

2.2.1 Downgrade by Unsecured RRC Redirection

This section describes the method used by SMS Blasters to downgrade the radio connection of a captured device to 2G by redirecting it directly to its 2G radio interface. The SMS Blaster broadcasts a TAI different to that used by the legitimate MNO in the Blaster's vicinity. This tricks the UE into entering a different part of the network, and the UE initiates a Tracking Area Update. During that update, the SMS Blaster uses a radio optimisation technique which allows Radio Resource Control (RRC) Redirection to redirect the captured UE to 2G without establishing 4G security first. In particular, the SMS Blaster releases the 4G radio connection by sending to the captured device the message "RRC Connection Release" with cause "EPS services not allowed", which indicates the 2G radio frequencies (absolute radio-frequency channel numbers / ARFCNs) that the UE should immediately use. This message triggers the UE to attach to the 2G interface of the SMS Blaster, where it receives the SMS in the clear without any authentication procedure, as illustrated in Figure 4 and described in section 2.3.

2.2.2 Downgrade by Cell Reselection

This section describes an alternative downgrade mechanism where SMS Blasters force the captured UE to reselect the 2G radio interface of the SMS Blaster [11]. This mechanism requires a different configuration of the Blaster and is used if RRC redirection doesn't work. The SMS Blaster broadcasts a TAI equal to that used by the legitimate network in the Blaster's vicinity. This tricks the UE into thinking that the 2G radio frequencies in the System Information Block Type 7 (SIB7) messages broadcast with the highest priority by the Blaster are from a network that previously established 4G security with the UE. Once the UE is attached to the 2G interface of the SMS Blaster, it receives the SMS in the clear without any authentication procedure, as described in section 2.3.

2.3 Injection of SMS Payload

This section describes how SMS Blasters inject an SMS once the UE is downgraded to their 2G radio interface. The SMS Blaster broadcasts on its 2G radio interface a Location Area Identity (LAI) different to that previously received by the UE from the legitimate network

during the last Tracking Area Update. This triggers the captured UE to perform a location update procedure just after attaching to the 2G interface of the SMS Blaster.

During the location update, the SMS Blaster requests the IMSI and International Mobile Equipment Identity (IMEI) of the captured device and completes the procedure by skipping authentication and ciphering, which are optional in 2G. The SMS Blaster then delivers the fraudulent SMS to the UE. The Blaster's user interface offers the ability to configure any SMS origin number in alphabetic or numeric format, as well as the SMS content.

The SMS Blaster then pushes the UE back to the 2G legitimate network, as described in section 2.4.

2.4 Push Back to the Legitimate Network

This section describes how the SMS Blaster pushes a captured UE back to the legitimate network after sending it an SMS.

The SMS Blaster sends the UE a new Temporary Mobile Subscriber Identity (TMSI) in a message indicating a different LAI than the one broadcast by the SMS Blaster. The LAI mismatch triggers the UE to perform a new location area procedure that the SMS Blaster rejects using a special cause, "No Suitable Cells in Location Area", and thus achieves a double goal. First, the SMS Blaster ensures a UE that received the SMS is pushed back to the legitimate network, where victims will be able to click on possible fraudulent links in the SMS. Second, the SMS Blaster ensures a UE does not receive the same SMS multiple times by not reselecting its 2G interface for 12 to 24 hours, thanks to the error code "No Suitable Cells In Location Area", see Figure 4.

The time during which a 4G capable UE is captured by an SMS Blaster can be as high as 5 minutes or as low as 15 seconds. However, some 2G only devices, including machine-to-machine (M2M) and Internet of Things (IoT) devices, can have a shorter capture time because the downgrade from 4G is not needed.

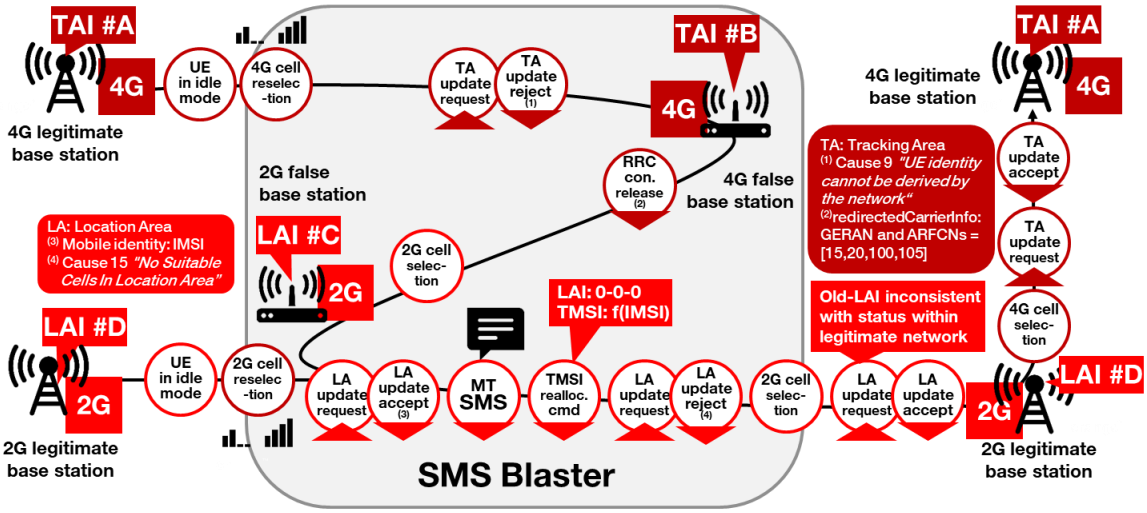

Figure 4 – SMS Blaster attack steps for RRC re-direction case

3 Impact assessment

3.1 Customer Impact

This section describes the impact of SMS Blasters on mobile customers. We first differentiate the following types of impact:

1. **Mobile service disruption and degradation** are likely to impact customers who are in the vicinity of an SMS Blaster or, in some cases, customers who are visiting an area where an SMS Blaster previously operated.

    a) **Service unavailability**, including voice calls and emergency calls, will impact UEs that are captured by the SMS Blaster, which can last up to five minutes or even longer depending on the type of SMS Blasters, see section 2.4 [25].
    b) **Call drop and degraded data throughput** will impact UEs that are captured by the SMS Blaster and UEs that are visiting an area where the SMS Blaster operated due to radio interference and/or handover failure, see 3.c) in section 3.2.

2. **Sending harmful SMS messages targeting the customer or their UE** is likely to impact customers who are tricked by the SMS they receive from the SMS Blaster and can have one or several of the following consequences:

    a) **Banking, cryptocurrency and payment fraud** will impact customers who fall for the scam. They may contact fraudsters who can use social engineering to approve money transfers from their bank account, cryptocurrency transfers from their crypto wallet or purchases at their expense.
    b) **Private information loss** can impact customers who are tricked by the SMS received from the SMS Blaster to make a call to a false customer service centre, access a fake website or install a malicious application.
    c) **Mobile malware** can impact customers who are tricked into installing a malicious application in their UE, which can be used for fraud, including banking and payment fraud. These customers may require guidance and assistance to disinfect their UE, see [7].
    d) **Panic or disinformation messages** sent by SMS Blasters can impact the population in their vicinity.
    e) **Malicious binary SMS messages** sent by SMS Blasters can lead to a variety of threats, including UEs being temporarily unavailable or even bricked (see also FS.42 [22]).
    f) **New fraud or information loss scenarios** could impact customers if SMS Blasters are reprogrammed to implement them, for example spear-phising or Wangiri. Captured information such as IMSIs and IMEIs can be used in other scenarios for example location tracking or signalling attacks.

We also distinguish the following three types of customers that can become victims of SMS Blasters:

3. **Home network users** through their mobile and IoT devices, including smartphones and smartwatches. These victims are usually the primary target of the SMS Blaster and are the ones who are most likely to fall for the scam and experience financial and

private information loss. They are likely to contact their financial institutions, their MNO, and their national authorities.

4. **Roamers** through their UEs. SMS Blasters are operated in busy city areas where tourists are likely to be present. Roamers are usually collateral victims and are less likely to fall for scams in a foreign language or specific to the visited country, but they may complain to their home network about receiving unsolicited SMS and service loss, which will be transmitted between the roaming teams of the home and serving networks. However, roamers from certain countries can also be targeted by scams that take advantage of their presence abroad, making them more vulnerable to specific social engineering tactics. SMS Blasters can be configured to selectively target roamers.

5. **Machine device users** through their M2M devices. These customers are usually collateral victims but could become a primary or secondary target. They are less likely to fall for scams that require human intervention, but they can issue some complaints about service disruption, which will be received by the business team contact within the MNO.

3.2 Operator Impact

This section describes the impact of SMS Blasters on MNOs. We distinguish the following types of MNO impacts:

1. **Increase of complaints from customers** who may report service unavailability, receiving some phishing SMS and suffering financial losses due to such SMS. The increasing number of complaints can trigger national authorities to get involved. National authorities may also detect and report the SMS Blaster equipment to the MNOs, see [7].
2. **Financial impact** on MNO revenues and costs:

    a) **Increase in costs** due to the increase in customer complaints and the introduction of new controls, for example to detect or mitigate the impact of SMS Blasters, see section 4.
    b) **Reduced A2P SMS revenues** due to the loss of confidence in SMS as a delivery channel.
    c) **Lower return on investment in network-side SMS filtering** due to its reduced effectiveness in the presence of SMS Blasters.
    d) **Liability for customer losses** due to legislation in preparation in Singapore and Europe, which proposes that MNOs share financial liability in case of financial services fraud involving mobile services, see [8], [9].

3. **Reduced network performance** in the areas where the SMS Blaster is operating or has operated due to the following issues:

    a) **Radio jamming** caused by the frequencies used by the SMS Blaster to capture the UEs. The SMS Blaster uses the same 4G frequencies as the legitimate network it impersonates. An SMS Blaster could also jam the MNO 4G and 3G cells to cause the UE to perform normal reselection toward the SMS Blaster 2G radio; this is a variant of a downgrade by cell reselection.

b) **Radio interference** caused by frequencies used by SMS Blasters that can conflict with the ones used by the legitimate network for a different technology, such as 3G or 5G. The SMS Blaster can thus create interference in the legitimate networks beyond 2G and 4G.
c) **Radio network misconfiguration** caused by the false base station being automatically added by mistake to a legitimate network that uses the Automatic Neighbour Relation (ANR) feature. The MNO performance indicators will show a high number of handover preparation failures from UEs in CONNECTED mode while the Blaster is in the area. Depending on the radio access network (RAN) vendor, the ANR configuration, the Self-Organising Network (SON) configuration and the physical cell ID (PCI) allocation scheme, this misconfiguration can lead to an increase in handover failures after an SMS Blaster leaves an area. For further information, see the discussion on SON poisoning attacks by false base stations in 3GPP TR 33.809 [21].

4. **Unauthorised use of network resources** by SMS Blasters, which include the following types:

    a) **Radio spectrum** including 2G and 4G frequencies, which are selected by the SMS Blaster to increase the number of captured mobiles by ensuring a smooth intra-frequency cell reselection. The use of mobile radio frequencies is illegal without authorisation from the national authorities in most countries.
    b) **Mobile network identifiers** including the MCC and MNC used to impersonate the MNOs to capture devices already attached to their network and the TAI and LAI selected to trigger nearby devices to attach to the false base stations of the SMS Blaster.
    c) **Base station identifiers** including the Cell ID and E-UTRAN Cell Identity (ECI), are used to identify the 2G and 4G false base stations of the SMS Blaster, which are sent to the legitimate network by nearby mobiles in their measurement reports and can cause misconfiguration, see 3.c.
    d) **User equipment identifiers** including the collection of IMSI and IMEI of captured UEs, which is illegal without authorisation in several countries. There are no reports to date of MSISDNs being collected by the SMS Blasters because the IMSI to MSISDN translation is performed in the home network to which an SMS Blaster doesn't have access.

5. **Potential impact on 3G and 5G.** SMS Blasters exploit unsecured downgrades from 4G/5G-NSA to 2G where they can send an SMS to the UE. However, SMS Blasters could be modified to exploit other downgrade paths to 2G from:

    a) **5G-SA** to 4G/5G-NSA followed by either a direct downgrade from 4G/5G-NSA to 2G or an indirect one from 4G/5G-NSA to 3G followed by a downgrade from 3G to 2G.
    b) **4G/5G-NSA** to 3G followed by a downgrade from 3G to 2G.
    c) **3G** to 2G directly.

3.3 Other Stakeholders Impact

This section describes the impact of SMS Blasters on other stakeholders.

1. **Organisation System Intrusion:** SMS Blasters can be used to specifically target an organisation staff, around offices or data centers, aiming to steal credentials and gain unauthorized access to the organisation systems, including MNO's network. This poses a significant security threat, potentially leading to system compromise, data breaches, and operational disruptions. Addressing this risk is crucial to safeguarding the integrity and security of an organisation infrastructure and that of its partners.

4 Required Actions

4.1 Mobile Network Operators

4.1.1 Detecting SMS Blasters

This section describes methods MNOs can use to detect SMS Blasters by combining subscriber feedback, network telemetry, and targeted sensing. The following subsections detail indicators that, when combined, improve detection accuracy and timeliness. Because any single signal can be ambiguous, MNOs should cross-validate detections across the following subsections before escalation. Active engagement with national authorities is essential to further reduce false positives and accelerate enforcement. Close collaboration between MNOs in the same country and sharing of indicators, strengthens confidence in detections using these techniques.

4.1.1.1 Customer spam reports

MNOs can detect SMS Blasters by identifying SMS messages that have been reported by their customers as spam for which there are no call details records (CDRs) [18], [19], [20]. MNOs can use the timestamp, length, origin and destination addresses, and possibly the location of the SMS reported as spam to verify there are no matches with existing CDRs. MNOs can also leverage the one-click spam reports functionality in the device that provide meta-data including the exact date and time the SMS was received. For example, Android users can opt-in to on-device SMS spam protection and Safe Browsing features [16].

SMS spam protection is built into Google Messages. With spam protection for messages, Android warns users about suspected spam and unsafe websites. Users can help improve the spam detection mechanisms by reporting if the message is spam or not. The user can report spam texts in messages at any time and block the conversation to avoid receiving future messages. The Safe Browsing feature offers broad protection on Chrome and other browsers and warns users about potentially risky sites, downloads and extensions [17]. Google Safe Browsing can detect both phishing and malware-based websites. Safe Browsing is built into Android and therefore applies for any app that uses Chrome custom tabs (CCT) or WebView (Facebook, WhatsApp, etc.). Safe Browsing as part of Chrome also supports the ability to raise the level of protection (Enhanced Safe Browsing).

4.1.1.2 Core signalling patterns

MNOs can analyse core network signalling on the S1 interface to detect SMS Blasters as follows:

1. **Handover storms with unknown TargetID**: monitor S1AP "HandoverRequired" messages carrying cause values such as "Handover Desirable for Radio Reasons" or

"Resource Optimisation Handover", followed by message "HandoverPreparationFailure" from the MME with cause "Unknown TargetID".

2. **Bogus Global eNB ID**: flag "HandoverRequired" messages with TargetID (Global eNB ID) embedding MCC, MNC values that do not belong to the operator serving that site or where the Global eNB ID is absent from operator's inventory.
3. **Reuse of static network identifiers across locations**: track repeated use of identical or near-identical tuples (TAC, eNB ID, Cell ID) seen in signalling across different locations.
4. **Visible downgrade artefacts**: detect UEs whose NAS contexts after 2G fallback show an old LAI/LAC equal to the local LTE TAC (OLD_LAC = TAC), and/or an old TMSI that appears derived from the IMSI rather than randomly assigned.

4.1.1.3 Radio Signalling Signatures

MNOs can analyse radio network signalling to detect SMS Blasters as follows:

1. **Static or rotating PCI patterns**: detect a single static PCI reused across many bands, rotation among a small, repeating set of PCIs or simultaneous duplication of the same PCI across different frequency layers.

2. **RAN-sharing anomalies**: Flag cells advertising multiple PLMN IDs where the operator does not deploy RAN-sharing, or where RAN-sharing would normally use different bandwidths and frequencies

3. **Unusual LTE carrier bandwidth usage**: Flag cells that broadcast 5 MHz LTE carriers across bands where the operator normally uses 10/15/20 MHz. This anomaly does not show in UE reports and requires a radio scanner.

4. **2G carrier collision with legitimate 3G or 4G networks**: Flag 2G radio signal, for example at 900 or 1800 MHz, that sits on the same frequency as, or on the edge of, a live 3G or 4G carrier. Confirm by looking for local increases in interference and dropped calls on 3G/4G

4.1.1.4 Network Services Monitoring

MNOs can also detect Blasters by identifying if a high number of mobile users establish connections to the same domain, or initiate calls to the same B-number, from the same geographical area in the same timeframe. Legitimate location specific messaging campaigns (via SMS or other channels) might generate false positive detections when this method is used, but analysis of the domain or B-number might help minimise false positives.

4.1.1.5 Honeypots

MNOs can detect SMS Blasters by deploying honeypots in high-traffic areas of a major city, such as in their retail outlets or inside busy train stations, where honeypots could be targeted by SMS Blasters. The honeypot can distinguish between SMS traffic delivered by an SMS Blaster and legitimate SMS traffic by ensuring it cannot receive any SMS routed through the legitimate MNO network. This can be achieved by configuring a UE as a honeypot and reporting any SMS delivery through an automated mobile application. For example, MNOs can prevent the honeypot UE from receiving SMS routed via their own network by applying an Operator Determined Barring (ODB) on incoming SMS to the UE subscription. It is

important to protect any honeypot UE placed in a public location against fraudulent use and theft.

4.1.2 Enhancing SMS Blasters Detection

MNOs can enhance their initial SMS Blaster detection by combining the following techniques:

1. **Extending core and radio network detection** to the whole network by deploying a false base station detection feature from network vendors, see Sections 4.1.1.2 and 4.1.1.3.

2. **Detecting devices receiving an SMS by an SMS Blaster** by deploying an application in some customer UEs, for example, as a specific smartphone app for MNO employees. The application can send suspicious events to a server that analyses these events and determines whether they were caused by an SMS Blaster or not. The application can report suspicious SMS reception, for example, after detecting a change of radio access technology from 4G to 2G, followed by the reception of only one SMS and followed by another change of radio technology from 2G to 4G. MNOs can search for a match between the suspicious SMS reception event reported by the application and the corresponding customer CDR to identify false positives.

3. **Identifying mobile phones traveling with the SMS Blaster** by correlating device mobility patterns with SMS Blaster movements. This could be used to identify mobile phones (roaming or non-roaming) that belong to the driver or in vehicle SMS Blaster operator accompanying the SMS Blaster. The remote-control data link and the communications between the driver and the remote-control operator will most likely utilise roaming SIMs. The reason for using roaming SIMs is that the SMS Blaster could attack more than one network at a time, and roaming SIMs can be more easily switched between networks to avoid the SMS Blaster disrupting the data link and driver comms links.

4.1.3 Mitigating the Impact of SMS Blasters

MNOs can prohibit insecure RRC redirection, described in 2.2.1, in mobiles attached to the mobile network to avoid the SMS Blaster downgrading these devices to 2G without any security procedures. The redir-policy bit can be used to protect 3GPP Release-15 and later UEs from insecure RRC redirection to 2G and Release-18 UEs conformant to TS 24.301 v18.4.0 (and later) from insecure RRC redirection to both 2G and 3G. From Release 18 onwards, UEs will prohibit insecure RRC redirection even if the redir-policy bit is not sent by the network. Despite the fact that 3GPP specifies that this redirection policy control feature does not prohibit CSFB (see 3GPP TS 24.301 section 5.6.1.6 abnormal case b), it is recommended that 2G and 3G capable networks disable any CSFB optimization solutions in the radio network that use insecure RRC redirection before prohibiting insecure redirection using the redir-policy bit and before Release 18 UEs enter the field. This avoids redirection policy control interfering with CSFB in the case of non-compliant UEs.

Improper reselection, described in 2.2.2, can be mitigated with new cell reselection behaviour defined in 3GPP Rel-18 (TS 36.304 and TS 36.306) [11], which are optional for UE to support. Operators are encouraged to require their terminal suppliers to implement this new cell reselection behaviour.

MNOs can also maintain lists of malicious domains and phone numbers and then take steps in their fixed and mobile networks to block users from contacting those domains or phone numbers. MNOs would benefit from having access to malicious domains and phone numbers determined from spam reports that are reported to mobile OS vendors, see section 4.1.1, so that these can also be blocked in their networks.

See section 4.3 for other actions MNO can take with the industry to mitigate the impact of SMS Blasters.

4.1.4 Use of Secure MFA for IT Operations

Employ a multi-factor authentication method that is not exposed to vulnerability exploitation by compromised devices or SMS interceptions, such as hardware token generated one-time passwords.

4.1.5 SMS Blasters Forensic Analysis

Lawful forensic examination of seized SMS Blasters provides evidence for prosecution and yields indicators that strengthen detection and mitigation across operators. Findings should be shared with GSMA members to reduce global risk. Key aspects of forensic analysis include:

1. **Target and SMS Volume Data:** Collect details on the number of targeted users, the nature of the SMS messages sent, and the geographic or demographic profiles of victims. This information can assist law enforcement in prosecuting perpetrators and understanding attack scope.

2. **Downgrade Technique Identification:** Analyse the methods used by the Blaster to downgrade UEs (e.g. RRC redirection, cell reselection). Identifying new or evolving downgrade techniques can inform network defences and mitigation strategies.

3. **Radio Signature Profiling:** Extract radio signatures such as PCI rotation algorithms, TMSI derivation methods, and other unique radio frequency characteristics. These signatures can enhance future detection and classification of SMS Blasters.

4. **Type Approval Codes (TACs)** of any modem / routers that may be visible on the cellular networks which are travelling with the SMS Blaster. This also provides intelligence about the device models purchased and built into the SMS Blaster to understand the supply chain.

5. **Manufacturer and Seller Identification:** Determine the origin of the equipment, including the manufacturer and distributor. This intelligence can provide reports on countries where these devices have been shipped for demonstration or operational purposes.

6. **Management Infrastructure Analysis:** Investigate the backend control systems and cloud management infrastructure associated with the Blaster. This can reveal broader criminal networks, facilitate disruption of command-and-control channels, and identify signatures for proactive detection.

4.2 Device Original Equipment Manufacturers

4.2.1 Improved Device Features

Device original equipment manufacturers (OEMs) are recommended to:

1. **Improve the processing of the redir-policy bit** in the UEs to prevent SMS Blasters from downgrading these devices to 3G in addition to 2G by insecure redirection [10]; see section 2.2.1 for background on the attack this mitigates.
2. **Enhance the cell selection procedures** in the UEs to prevent SMS Blasters from tampering with system information to downgrade UEs to 2G by cell reselection [11]; see section 2.2.2 for background on the attack this mitigates.

4.2.2 Presentation of Insecure SMS

Device OEMs can provide better visibility on SMS Blaster fraud to users, e.g., by highlighting and/or warning those messages received over an insecure or unencrypted connection [14]. Fraudulent SMS messages from SMS Blasters are always strictly sent over an unciphered connection and could therefore be flagged as insecure.

4.2.3 Options to Disable 2G and/or Enforce Encryption

Providing configurable options to disable 2G and/or enforce SMS/MMS encryption in the UEs can protect users from 2G weaknesses such as those exploited by SMS Blasters on their home network or while roaming abroad. These configurations could be provided to the users or be automated based on, e.g., the device location.

Android devices support disabling 2G at the modem level (2G toggle) without impacting emergency calls [12]. Devices must be running Android 12 or above and implement Radio 1.6 Hardware Abstraction Layer (HAL) or above.

For those enterprises and corporations with high security requirements, it is also recommended to disable 2G to protect from this type of fraud. Android Enterprise introduced the ability for IT administrators to disable 2G in Android 14 [13]. The same hardware requirements apply.

Android 14 and above also supports disabling null ciphered connections or situations where the ciphering procedure is skipped (user encryption toggle) [14], which prevents receiving fraudulent plain text SMS payloads from SMS Blasters. Devices must adopt Radio 2.0 HAL or above.

4.3 Industry-wide

4.3.1 Raising National Operators' Awareness

MNOs are encouraged to discuss the issue of SMS Blasters together with other national MNOs as this equipment has been found to impact all MNOs in a given country. Efficient coordination and intelligence sharing among national MNOs can contribute to improving the detection of SMS Blasters and motivate national authorities to address the issue.

4.3.2 Raising National Authorities' Awareness

MNOs are recommended to brief their national authorities about the risk of SMS Blasters, particularly in geographical regions where SMS Blasters have already been detected, to request the support of the different competent authorities, including the following public bodies and agencies:

1. **Telecom regulatory agency** should be aware of the methods used by SMS Blasters to use without authorisation the radio spectrum allocated by the regulator.
2. **Radio frequency agency** can perform radio measurements to provide formal proof of the exploitation of the radio spectrum by SMS Blasters and their geographical location.
3. **Law enforcement agency** can process the legal complaints of the MNOs, lead the investigation, arrest the detected SMS Blasters and take legal action if such equipment is sold illegally in their jurisdictions.
4. **Customs and market-surveillance authorities** can enforce import and sale restrictions of SMS Blasters by forbidding e-commerce and postal shipments, seizing and disposing of equipment, and sharing intelligence with MNOs and law enforcement.

4.3.3 Raising Customer Awareness

It is desirable to raise customer awareness about the risks of SMS Blasters in countries where they have been detected and to encourage the use of available mobile features that provide protection, such as the 2G and encryption toggles available in major operating systems [18], [19], [20], [23].

4.3.4 2G Sunset

MNOs are recommended to plan and communicate their 2G network sunset to ensure device suppliers can consequently plan to remove support for 2G in UEs and prevent fraudsters from exploiting 2G security weaknesses in the future. Guidance on best practices for legacy network sunsets and MNO responsibilities can be found in [26].

4.3.5 Industry-wide Efforts

It is critical that MNOs worldwide support the ecosystem in developing further cellular privacy features for their subscribers. For example, the security specifications for 5G state that the device must provide transparency to the user with respect to the confidentiality and integrity algorithms in use, which would allow flagging messages received over an insecure connection, as described in section 4.2.2.

MNOs are also recommended to reach out to their OEM suppliers and modem system on chip (SoC) counterparts endorsing cellular privacy features and requesting support and adoption of both existing and new cellular privacy features.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	31 Jul 2024	First approved version	TG	Eric Gauthier, Orange
1.1	25 Oct 2024	Updated security classification and template.	FASG	David Maxwell, GSMA
1.2	12 May 2025	Updated impacted countries map, added example voice call scam, added cryptocurrency theft as a new threat, added voice call as a new detection technique, added risk of false positives through cell broadcast and added two new mitigations.	FASG	Eric Gauthier, Orange
2.0	25 Mar 2026	Updated list of SMS Blaster offerings, impacted countries and added relevant references. Detection advice updated to add core signalling and radio signatures, honeypots identification of devices travelling with SMS Blasters. Recommendations on forensic analysis also added.	ISAG	James Moran, GSMA

A.2 Other Information

Type	Description
Document Owner	Fraud and Security Architecture Group
Editor / Company	Eric Gauthier, Orange

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.