



MEF

**FUTURE OF
MESSAGING
PROGRAMME**



BUSINESS SMS FRAUD FRAMEWORK VERSION 3.0



MEF

MOBILE ECOSYSTEM FORUM

 @MEF



INTRODUCTION

MEF's Future of Messaging Programme was established in 2015, uniting all stakeholders in the business messaging ecosystem to support the deployment of best practices to limit fraudulent behaviours as well as enable the development of new messaging technologies and business models. Its collaborative cross-ecosystem working group is represented by senior executives from across Commercial, Operator Relations, Product and Technical teams.

Business SMS (also known as Application to Person (A2P) SMS) is a trusted messaging channel for businesses to communicate with their customers. All kinds of businesses have come to rely on SMS as a key channel and annually they spend over \$17.9bn sending messages to their customers. As business communications evolve, SMS remains key due to its ubiquity across all mobile devices and networks worldwide as well as its reliability and effectiveness for driving customer engagement.

However, it is also imperative that across the entire ecosystem all necessary actions are taken to prevent and mitigate fraud attacks to ensure the

sustainability of SMS as a trusted communications channel. Common understanding and awareness across the messaging ecosystem is essential.

MEF's Fraud Management Working Group first developed its Business SMS Fraud Framework in 2016 to identify and map fraud types, their causes and impacts on different key stakeholder groups.

Version 1.0 of the framework (2016) set the foundations for the work of the Programme to develop best practice guidelines for both the messaging industry and buyers of messaging solutions. It was the basis of MEF's self-regulatory service Trust in Enterprise Messaging (TEM) service which launched in 2018 and includes MEF's Business SMS Code of Conduct.

As the Business SMS ecosystem continues to evolve, the working group regularly reviews the fraud framework to ensure that it remains current. This edition V3.0 has been fully aligned to V2 of MEF's Business SMS Code of Conduct (released December 2020). A 14th fraud type has been added (Message Trashing) and the latest information included to reflect changes in both regulation and the ever-evolving tactics of the fraudsters including app-initiated frauds such as crowdsourced SIM Farms.

The framework is recommended for anyone buying or delivering Business SMS, particularly those in the following business areas:

- Procurement
- Product, Marketing & Communications
- Logistics
- Sales & Business Development
- Compliance & Legal

The framework helps all stakeholders:

- Understand why fraud exists
- Recognise the fraud types which affect the ecosystem today
- Identify the different stakeholders within the ecosystem
- Consider the impact of fraud on the whole ecosystem
- Learn what steps can be taken to mitigate and protect against fraud



CONTENTS

THE BASICS

- Business SMS Ecosystem
- Why does fraud exist?
- Common fraud attacks
- Impact of fraud

FRAUD TYPES

- Identity Theft
 - 1. SMS Originator Spoofing
 - 2. SMS Phishing / Smishing
 - 3. Access Hacking
- Data Theft
 - 4. SIM Swap Fraud
 - 5. SMS Roaming Intercept Fraud
 - 6. SMS Malware (SMS Hacking)
- Commercial Exploitation
 - 7. Grey Routes, Bypass, Non-Interworked Off-Net Routes
 - 8. Message Trashing
 - 9. SIM Farms
 - 10. Spam
 - 11. Artificial Inflation of Traffic (AIT)
- Network / System Manipulation
 - 12. MAP Global Title Faking
 - 13. SCCP Global Title Faking
 - 14. SMSC Compromise Fraud

COMBATTING FRAUD

GLOSSARY

ABOUT



THE BASICS








BUSINESS SMS ECOSYSTEM



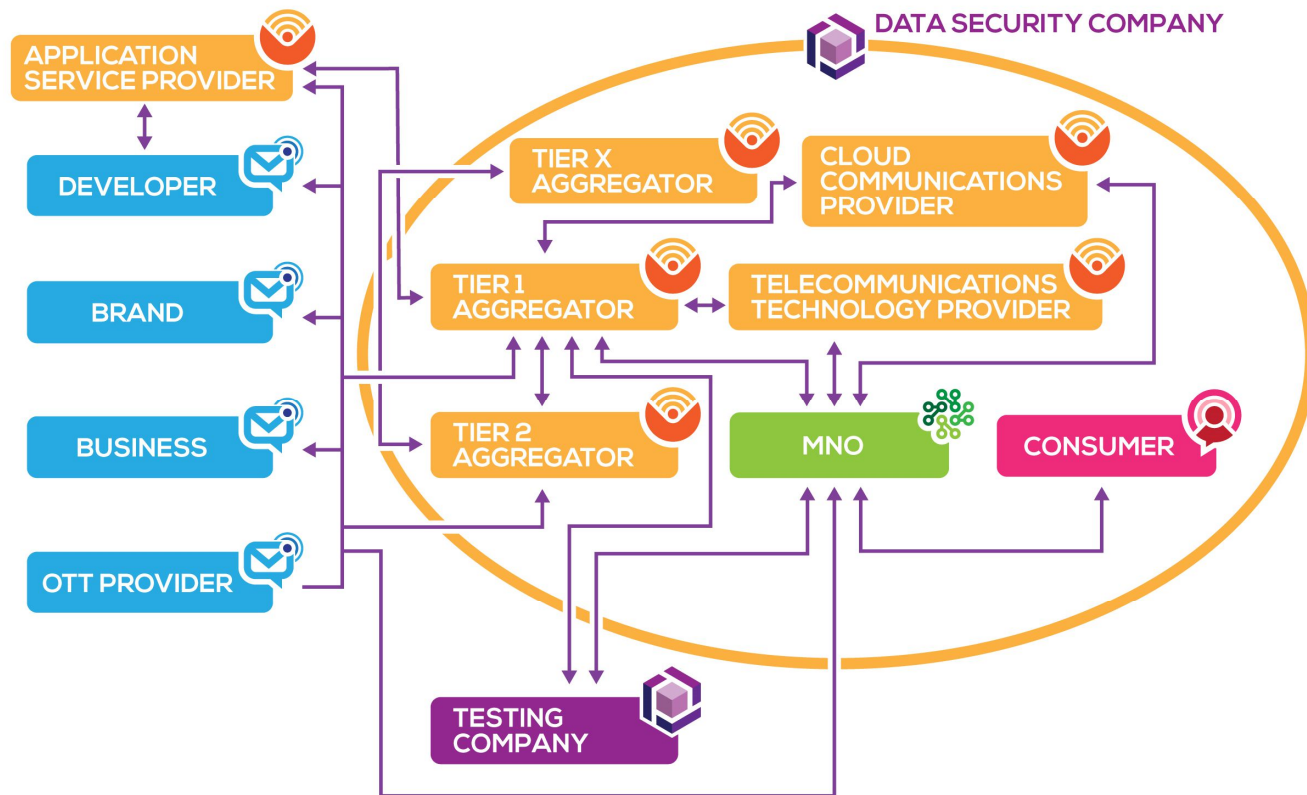
Business SMS has grown from the early days of person to person (P2P) messaging to offer a global and cost-effective means of connecting a business directly to their customers, irrespective of their location or technology. A mature technical and commercial infrastructure exists to enable and facilitate this relationship.

The ecosystem also contains parties which are not directly engaged within the end-to-end message delivery chain, but provide support services such as testing, reporting and data security companies.

 MNO	 MESSAGING PROVIDER	 BUSINESS	 CONSUMER	 SUPPORT SERVICE
MOBILE NETWORK OPERATOR (MNO)	TIER 1 AGGREGATOR TIER 2 AGGREGATOR TIER X AGGREGATOR TELECOMMUNICATIONS TECHNOLOGY PROVIDER COMMUNICATIONS PLATFORM AS A SERVICE PROVIDER APPLICATION SERVICE PROVIDER	BUSINESSES OTT PROVIDER DEVELOPER	CONSUMER: WHERE THE RELATIONSHIP IS WITH AN ENTERPRISE MOBILE SUBSCRIBER: WHERE THE RELATIONSHIP IS WITH AN MNO	DATA SECURITY COMPANY: ANTI-VIRUS, FIREWALL TESTING COMPANY



BUSINESS SMS ECOSYSTEM MAP





BUSINESS SMS ECOSYSTEM cont.

The complexity of the Business SMS ecosystem means that it is common and often necessary for individual messaging providers to partner with other companies to be able to offer a single solution which can reach a global customer base and offer a variety of effective and economically viable authorised solutions to the Business Messaging market. For example, different solutions enable messages to be sent in large volumes at the same time, to reach specific countries or to deliver messages to the subscribers of multiple MNOs.

The legitimacy, reliability and quality of a mobile messaging solution is assured through the establishment of back-to-back contracts along the length of the business messaging delivery chain. This is crucial to ensure that any route offered to a business is both legal and authorised from end-to-end and that all relevant parties in the chain are accountable for a message travelling from a business through to a consumer.

MEF's [Enterprise Mobile Messaging Guide](#) provides a comprehensive explanation of the six authorised ways available within the business messaging market to reach a terminating MNO to deliver mobile messages, both nationally and internationally, between a business and their customer.

As territories establish data protection legislation, such as the EU's General Data Protection Regulation, understanding who is in control of the message delivery chain is even more crucial for all stakeholders.

Also, as more parties join the message delivery chain, a business SMS solution becomes more exposed to the risks of using unauthorised or fraudulent routes. Transparency is key to knowing what will happen and what has happened after a message has left a business before it reaches the consumer.





WHY DOES FRAUD EXIST

By definition, fraud is wrongful or criminal deception, intended to result in financial or personal gain, against an individual or organisation.

The global Business Messaging ecosystem has grown and developed at different rates across different regions in order to meet demand, accommodate local requirements and to comply with legal and regulatory requirements. As such, the level of advancement and maturity of some countries compared to others means that the barriers to prevent fraud are lower in some countries than in others.

Fraud is indiscriminate. It can impact all parties within the business SMS ecosystem, either directly or indirectly and is carried out in order to achieve one or more of the following objectives:

- **IDENTITY THEFT:** obtaining information required to steal someone's identity
- **DATA THEFT:** obtaining information required to access personal and private banking or other financial accounts
- **COMMERCIAL EXPLOITATION:** to gain competitive advantage by exploiting gaps within the commercial structures of the ecosystem
- **NETWORK / SYSTEM MANIPULATION:** to gain competitive advantage or perform illegal activities via the deliberate manipulation of a message or the exploitation of system vulnerabilities to bypass protection measures intended to safeguard MNOs and consumers



COMMON FRAUD ATTACKS

The 14 fraud types identified within this framework are, in reality, often carried out in combination. For example, deliberate manipulation of a message to bypass an MNO's security systems to avoid termination fees and to enable the delivery of a smishing message which would otherwise be blocked from reaching a consumer. Below are some examples of fraudulent activities which can take place today:

Scenario 1: Spam and Spoofing

A perpetrator generates a distribution list of mobile numbers through brute force sequencing, changing the originator so that it appears to be sent from an MNO. The perpetrator uses the message to a) check whether each number is live and active, and b) as a sales opportunity by suggesting that the sender has an existing relationship with the consumer, e.g. "Your contract is coming to an end so please contact us to discuss an upgrade".

Scenario 2: Malware, Financial Theft & Spam

An alternative to Scenario 1 is the delivery of a message containing a URL which initiates the download and installation of malware which can be disguised and overlaid on top of a legitimate app. On the surface, an app would look normal, but it can be programmed to capture bank account login details, phish credentials, intercept two-factor authentication messages, or selectively forward communications to a different handset without the consumer's knowledge. Once installed, malware can also access a consumer's contact list and spread itself to devices via Spam which tricks recipients into thinking the message is from a trusted source, namely, the consumer.

Scenario 3: Spam, Spoofing & Smishing

A perpetrator buys a list of mobile subscriber numbers from a third party – the perpetrator does not have permission from the consumers to contact them by SMS. The perpetrator creates a message, setting the originator to look like the message is from a bank. The message content suggests that the 'bank' is contacting their own customer to alert them to a potential problem, setting the recipient up to reveal confidential information, e.g. "we have noticed unusual activity on your account so please log in <<here>> or call XXXXXXXXXX". The URL will divert the consumer to a fake website or the phone number will connect to the perpetrator, not the bank, who will attempt to gather the consumer's banking details.

Scenario 4: Identity & Financial Theft

In a secondary stage to Scenario 3, a perpetrator will search online for personal information which is publicly available, such as a full name, date of birth, address and maiden name. The perpetrator will then contact the consumer's MNO and pretend to be the consumer, using the personal information to clear security checks. The perpetrator can then ask the MNO to cancel and reissue a new SIM, for example, due to apparent loss or damage, which the perpetrator then links to a different handset. All SMS and voice calls will be diverted to the new handset. The perpetrator now has the consumer's banking details from Scenario 2, plus access to all communications directed to the consumer's mobile number. The perpetrator can now contact the consumer's bank, reset all online bank settings and authorise transactions, using the consumer's "phone" – namely, their mobile number - within a mobile banking authentication process as identity and One-Time Passwords (OTPs) are sent to the consumer's mobile number, which is now under the control of the perpetrator.



IMPACTS OF FRAUD

The impact and consequences of fraud are felt globally.

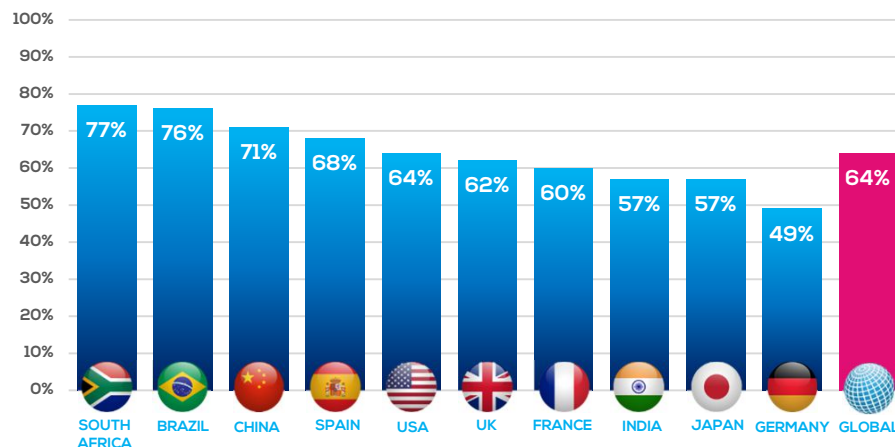
As the scenarios show, fraud within the Business SMS ecosystem can have a significant and direct detrimental impact on individuals, in addition to the wider financial implications and reputational damage caused to parties who have a genuine commercial relationship with a victim.

In MEF's annual global consumer study which looks at the attitudes and behaviours of smartphone users in 10 countries, 64% of consumers worldwide reported they were 'very or moderately concerned' that someone sending a mobile message would try to impersonate a company e.g. a bank, to try to steal money or login and password details.

The level of impact will vary by region and country because the global ecosystem operates within a complex set of legal, regulatory and commercial frameworks which differ by country and which may see a certain practice permitted in one country but not another. The enforcement of regulations or contracts can also influence how local markets operate and facilitate some types of fraud as parties seek to exploit gaps in these frameworks to bypass authorised and regulated routes to meet ill-advised demand for low-cost messaging, to gain commercial advantage or at worst, to commit theft.

As market opportunities grow within national and global enterprise communities, so does the significance and impact of fraud on the quality and reliability of services, on the ability for legitimate players to monetise services, and ultimately, on the continued growth of the sector.

PERCENTAGE 'MODERATELY' OR 'VERY' CONCERNED ABOUT MOBILE MESSAGE FRAUD



Base: n=650 per market, total 6,500



IMPACTS OF FRAUD cont.

The direct monetary losses being incurred by the industry through fraud are significant. However, the real impact of fraud on the global ecosystem extends beyond the direct financial losses incurred by MNOs.

FINANCIAL IMPACT

- Theft from or the unsuspecting disclosure of personal or confidential information and data by a consumer can result in:
 - unknowingly authorising financial transactions
 - bank accounts being taken over using diverted OTPs
 - damage to credit scores and personal financial status
 - bill shock as a result of high voice call, premium rate or data charges
- Charges incurred in countries where certain receivers pay for the receipt of messages e.g. USA, Canada
- A randomly-generated MSISDN used as an originator to commit fraud may belong to a mobile subscriber who would be invoiced for messages they never sent
- Resource and increased operational expenditure required to identify, investigate and rectify problems including consumer and enterprise complaints, interworking fee discrepancies, negotiation of incorrect fees with interworking partner(s), unofficial routes which need to be closed or made formal through a new commercial agreement
- Revenues lost internally within an MNO whereby:
 - an MNO's retail consumer offer can be leveraged at a more competitive rate than the official Business SMS mobile rate or interworking agreement rate
 - mobile business messages can be bought for a specific destination at a rate lower than an MNO's own official national rate
- Loss of revenue and profit by parties which may pay out revenue share only to have it withdrawn by an MNO which detects fraud



IMPACTS OF FRAUD cont.

REPUTATIONAL DAMAGE

- Brand damage caused by association to fraudulent activity
- Liability for compromised, delayed or lost messages

POOR OR UNRELIABLE QUALITY OF SERVICE

- There is limited functionality, flexibility and support available on unauthorised routes, such as for ported numbers, use of originators, alphanumeric support, provision of accurate data and reporting where delivery receipts and reporting information may be absent or fabricated
- Routes can be changed or terminated with little or no notice
- Messages can be altered, delayed, lost or deleted, including One Time Passwords or targeted permission-based advertising

LOSS OF TRUST IN BUSINESS SMS

- Legitimate messages may be ignored if consumers believe them to be annoying, irrelevant or even intrusive
- Increased uncertainty amongst businesses, consumers and regulatory agencies about Business SMS will affect adoption rates for new services, sectors and markets and the long-term growth of the sector

CUSTOMER DISSATISFACTION

- Customer complaints are directed at the party with which a consumer has a direct relationship, namely an MNO and the business
- Real or perceived blame about cause and responsibility can lead to high churn of subscribers from one MNO to another, particularly within the prepaid market
- Annoyance at the receipt of unwanted or irrelevant messages, including:
 - unsolicited 'prize draw' messages which claim that the recipient can claim a prize in exchange for calling a number, normally at a premium, or filling up a form-link provided within the message
 - overzealous marketing from an unknown sender or even a known brand innocuous messages masking something more sinister



IMPACTS OF FRAUD cont.

UNFAIR MARKET ENVIRONMENT

- Messaging providers who do not participate in fraudulent activity are placed at a disadvantage and may become less competitive - legitimate companies lose business to less ethical or rogue providers
- Unauthorised routes which are available below an official market rate cause confusion and volatile market prices
- Parties operating outside of regulatory controls which determine the availability of certain functionality only on unauthorised routes cause confusion and may in turn influence pricing

REGULATORY INTERVENTION

- Targeted regulatory controls introduced to address consumer harm can limit the flexibility of messaging solutions, for example, prohibiting the use of unauthorised originators or mandating short codes instead of alpha originators
- Strict regulation in some countries such as Japan, Australia and the USA, brings an associated perception that Business SMS is 'high risk' and may discourage its adoption and negatively impact the growth of the market

BREACH OF DATA PROTECTION LEGISLATION

- The controller of a consumer's personal identifiable information, typically the enterprise sending a mobile message to a consumer, is responsible for all sub-processors in the delivery chain of such a message. As such, the enterprise is running the risk of breaching local data privacy law if it does not have control over and has made sure all parties in the delivery chain adhere to the relevant data privacy legislation.
- Breach of data privacy law anywhere in the mobile enterprise delivery chain can lead to significant fines for the data controller i.e. the business.



FRAUD TYPES



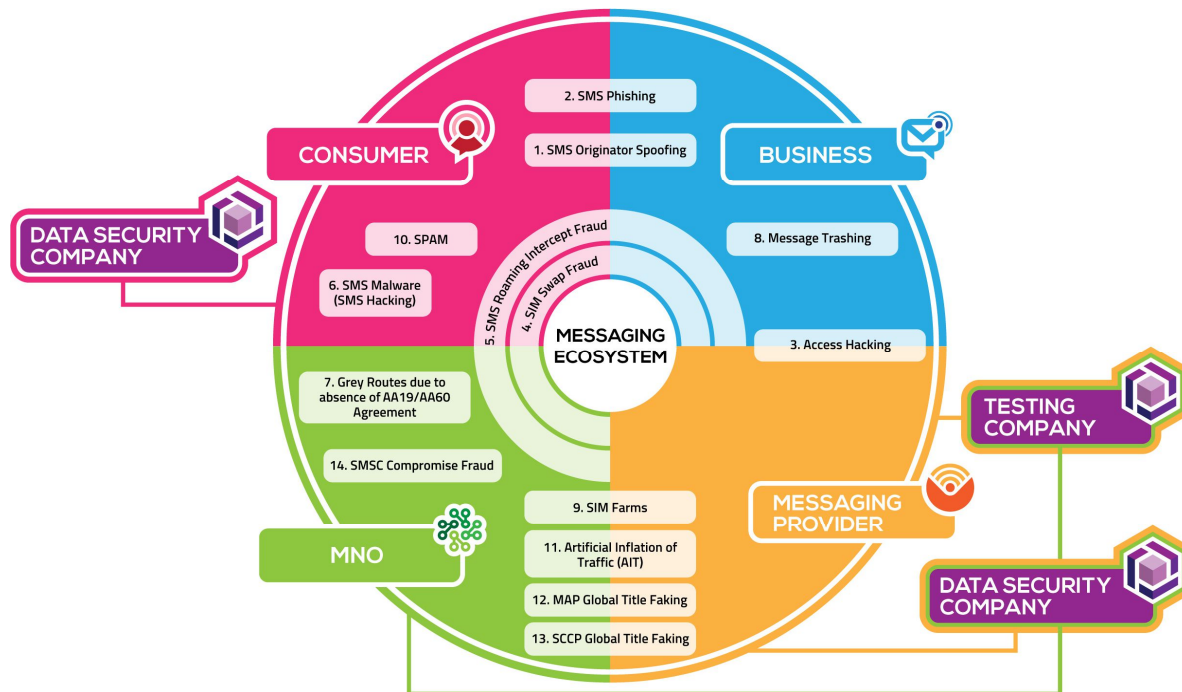
FRAUD MAPPING



This framework identifies 14 fraud types, each of which directly impacts on one or more of the four core communities within the Business SMS ecosystem.

Some of the fraud types are highly complex and cut across a large proportion of the Business SMS delivery chain.

The solutions identified to detect and protect against fraud include commercial, technical and process, compliance and legal requirements and will need continuous cross-ecosystem collaboration to fully address all aspects of fraud in the Business SMS ecosystem and be successfully implemented.





IDENTITY THEFT: #1 SMS ORIGINATOR SPOOFING



DEFINITION

SMS Originator Spoofing [Spoofing] is the act of changing an originator to hide a sender's true identity and trick a consumer into thinking a message is from someone they know or a legitimate commercial entity. For example, by spoofing a short code or falsely using the originator "Apple", or "HMRC" [UK Tax Office] or '[your family member].

Spoofing does not involve the use of random originators, which falls under SIM Farm Fraud.

This of particular concern because if the consumer has already received messages from the spoofed brand, the fraudulent message along with legitimate messages are shown within the same conversation thread."

EXAMPLE

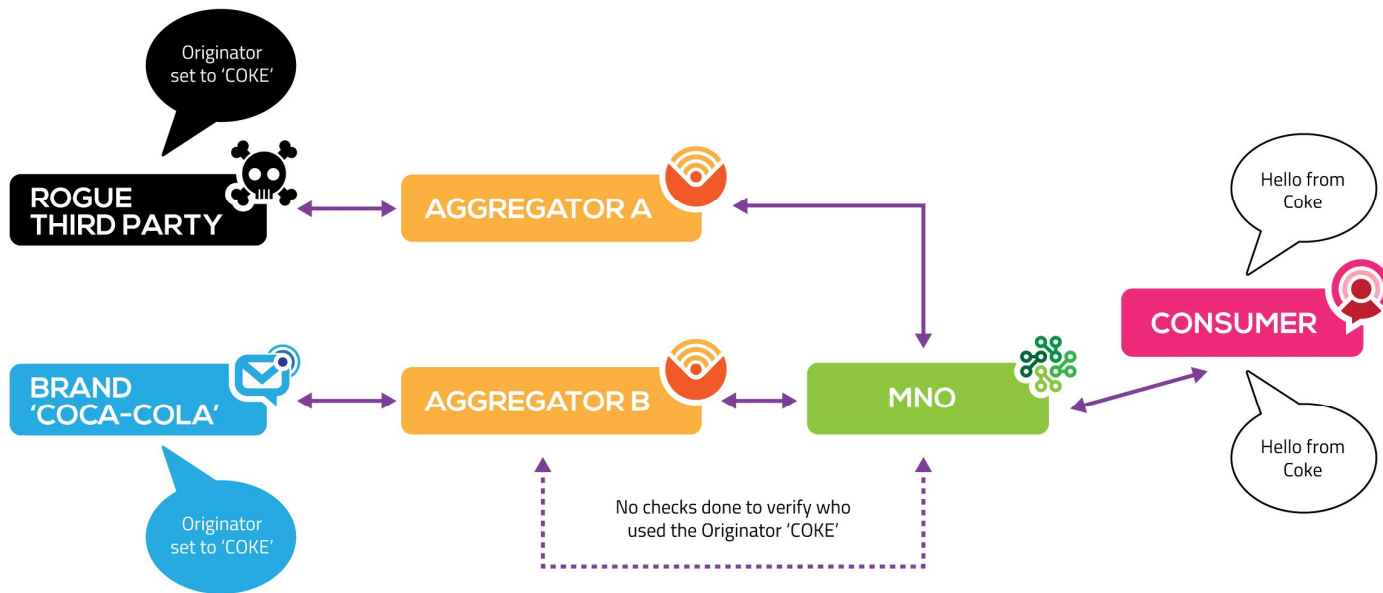
An example of an SMS Originator Spoofing message. Note the use of an alpha originator to masquerade as Vodafone in order to identify the status of the mobile number.



CAUSE

- Lead generation by pretending to be a known company to verify whether a MSISDN is live and active, or to generate new business, e.g., a sender pretending to be Vodafone to determine if a Vodafone customer's contract is due for renewal
- Using a short code which offers a two-way reply path to return a consumer's response to a rogue third party instead of a legitimate enterprise
- Sending unwelcome or abusive messages to an individual but pretending to be someone else
- SMS Phishing to extract sensitive personal and confidential financial information to try and steal from a mobile subscriber

#1 SMS ORIGINATOR SPOOFING





IDENTITY THEFT: #2 SMS PHISHING



DEFINITION

SMS Phishing, also known as Smishing, is a form of criminal activity combining Spam, SMS Originator Spoofing and social engineering techniques to pretend to be a trustworthy entity, in order to gain access to online systems, accounts or data such as credit card, banking information or passwords, for malicious reasons.

EXAMPLE

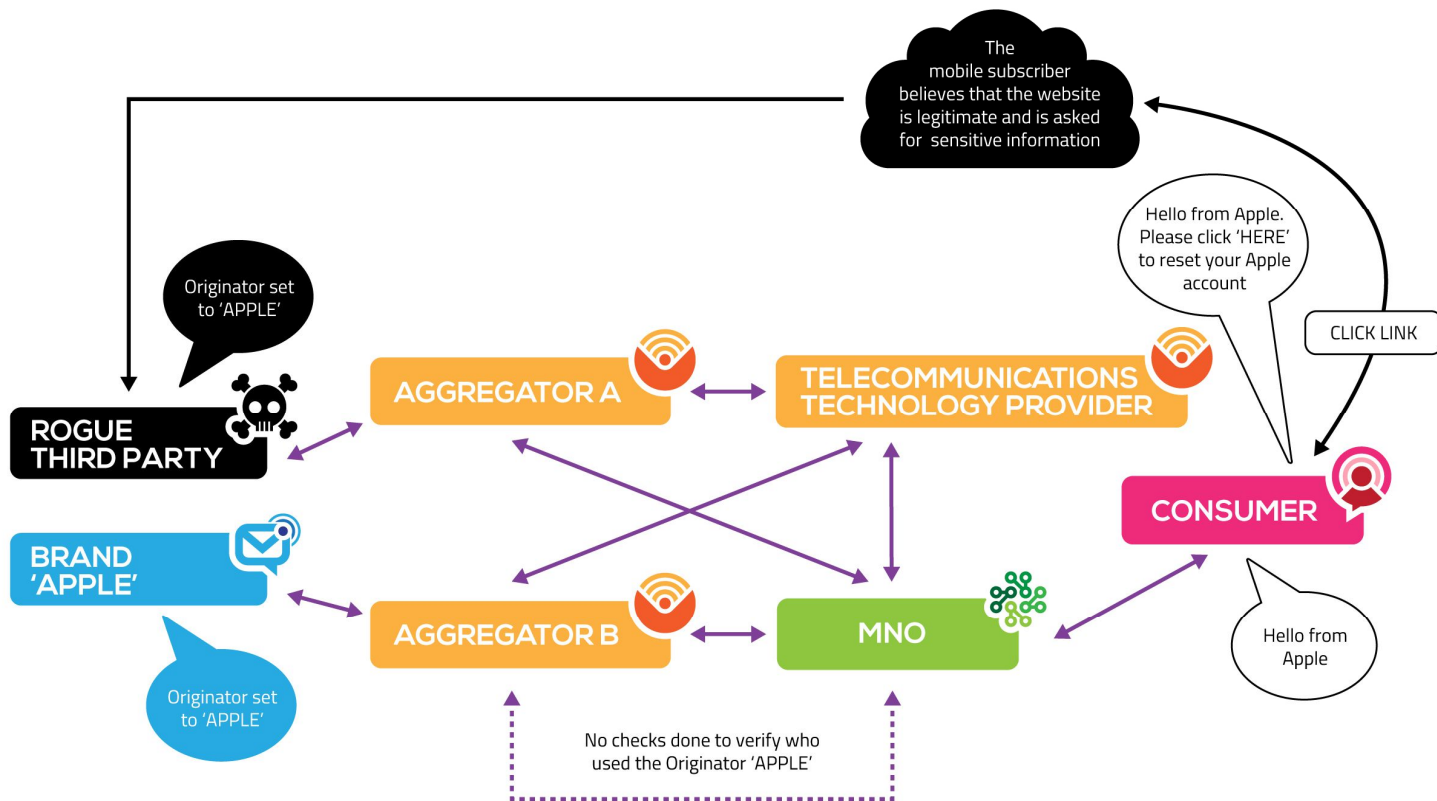
An example of an SMS Phishing message. Note the use of an alpha originator to masquerade as HMRC (UK Tax office).



CAUSE

- The promise of financial gain, either directly or indirectly through identity theft
- The ease with which consumers can be fooled through the use of basic social engineering and masquerading techniques to engender trust - consumers respond automatically to familiar situations and messages and may not be aware of or looking for potential risks
- Senders can use a percentage-based approach and so do not need to know whether a consumer has a relationship with the enterprise they are pretending to be, although having that information will increase their likelihood of success
- An enterprise not effectively managing their relationship with their customer, including proactively reiterating what channels they use to communicate with their customers and stating explicitly what information they will not ask for under any circumstances
- Poor regulation of the providers of business messaging solutions
- Other contributing causes include:
 - Use of Two Factor Authentication (2FA) codes creates a perceived layer of trust
 - Network support for "dynamic" alpha originators
 - Number harvesting tools which gather MSISDNs and associated personal information

#2 SMS PHISHING





IDENTITY THEFT: #3 ACCESS HACKING



DEFINITION

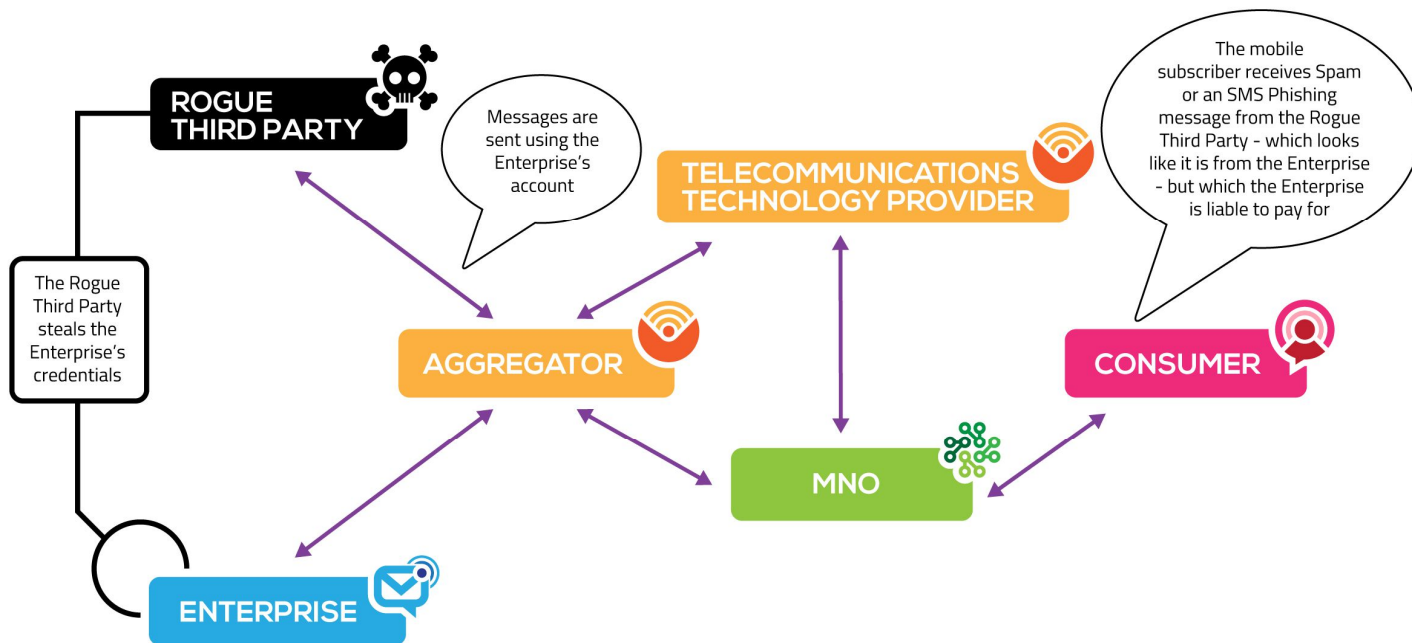
Access Hacking is the act of hijacking the credentials of a legitimate third party, using at least one of the following techniques and using those credentials to send messages:

- Hacking techniques, such as accessing a website which has the capability of sending SMS messages
- Providing inaccurate or false company information
- Using a stolen credit card or other payment method
- Buying messages using false credentials with no intention of paying for them

CAUSE

- The promise of financial gain, either directly or indirectly through identity theft
- The delivery of Spam or SMS Phishing messages to consumers anonymously to avoid any consequence or liability
- The opportunity to obtain messages on credit from MNOs or large messaging providers to resell
- The availability of free credit on SMS portals

#3 ACCESS HACKING





DATA THEFT: #4 SIM SWAP FRAUD



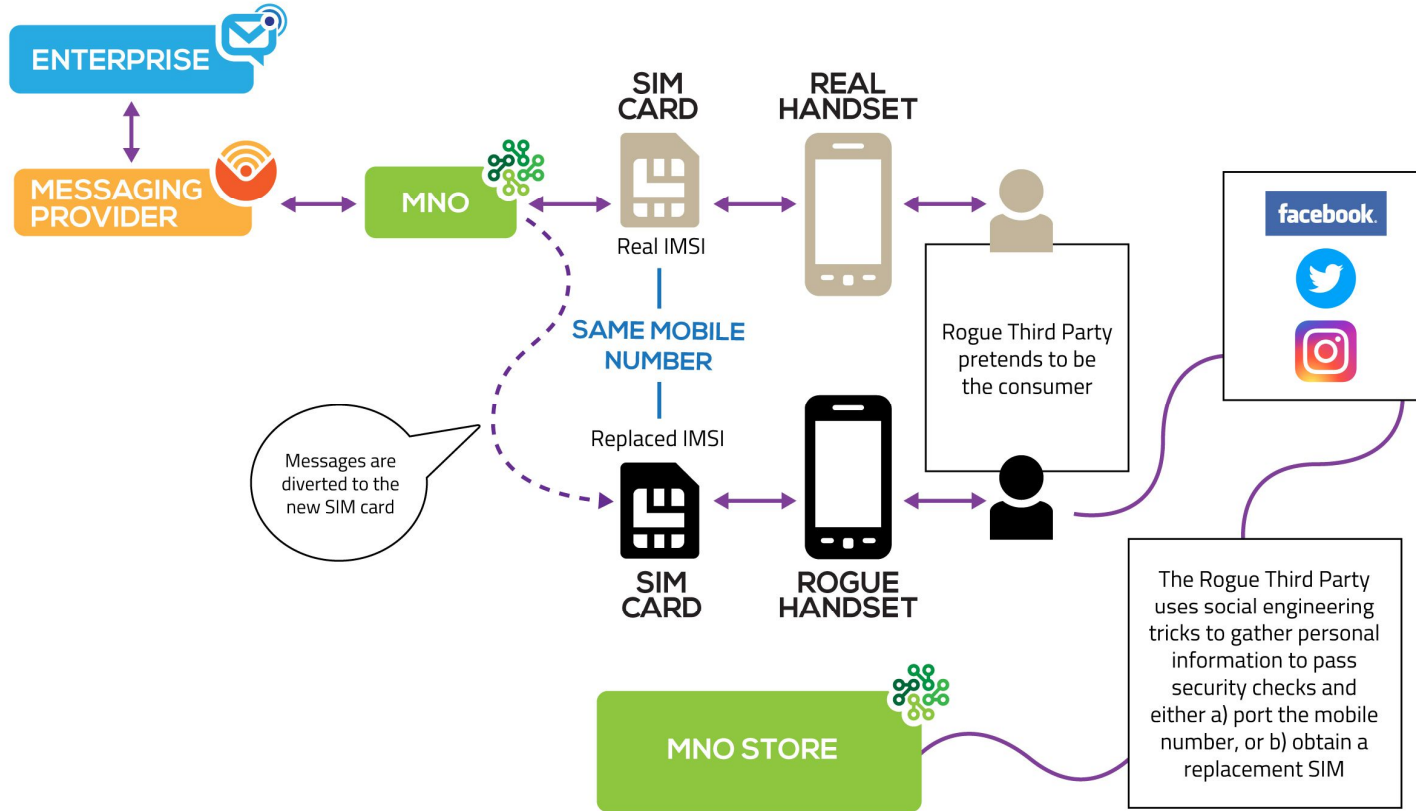
DEFINITION

SIM Swap Fraud is the act of obtaining control of a mobile number by cancelling the SIM linked to a consumer's handset and activating a new SIM with the same MSISDN linked to a different handset. All calls and texts to the victim's number are then routed to and from a different handset, outside of the control of the consumer.

CAUSE

- Financial gain, either by re-routing of SMS messages and calls to a new handset, including the diversion of activation codes or authorisations needed for online bank transfers, such as an OTP to a criminal's own handset – enabling the criminal to potentially access the customer's bank account and transfer funds or by generating voice calls, premium rate or data charges which are billed to the consumer
- SIM Swap is commonly associated with e-mail Phishing and SMS Phishing to gather confidential information and/or personal details from publically available social media, such as a full name, date of birth, address and maiden name – with key personal information, a criminal can contact the consumer's MNO, purporting to be the account holder, to request a replacement SIM

#4 SIM SWAP FRAUD





DATA THEFT: #5 SMS ROAMING INTERCEPT FRAUD



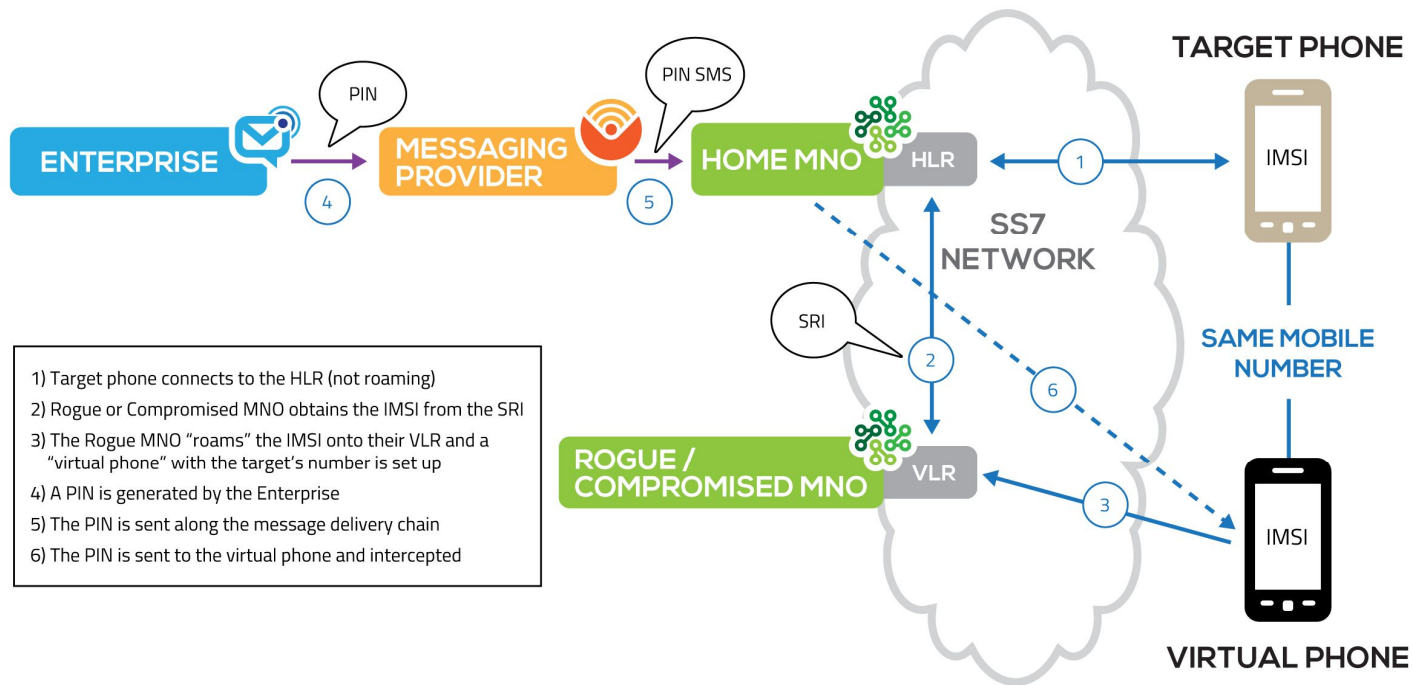
DEFINITION

SMS Roaming Intercept Fraud is the act of deliberately intercepting a message while a consumer is roaming. The message will generally contain sensitive or confidential information, for example an OTP, which would allow a rogue third party to gain access a consumer's bank account or to authorise a payment without the account-holder's knowledge or consent.

CAUSE

The promise of financial gain by accessing a consumer's bank account through the interception of private and confidential information, such as an OTP or 2FA message

#5 SMS ROAMING INTERCEPT FRAUD





DATA THEFT: #6 SMS MALWARE (SMS HACKING)



DEFINITION

SMS Malware is a form of criminal activity combining Spam, SMS Originator Spoofing and technical exploitation techniques such as Hacking to gain access to a consumer's MNO operating system and the information and data within it, including account or credit card details, banking information or passwords.

SMS Malware messages are used to direct a victim's smartphone browser to a malicious URL which initiates a software download and installation onto a handset without the consumer's knowledge, or which is disguised as an innocent app that acts silently in the background compromising sensitive data or exploiting the connectivity of the device, including:

- Re-configuring phone settings, applications or data,
- Sending messages or making calls to premium rate numbers,
- Accessing the message inbox to locate bank balance alerts or PIN codes etc.
- Accessing the contact list and other personal information, or,
- Using the contact list to spread the malware via a communication from a "trusted source", namely, the victim.

CAUSE

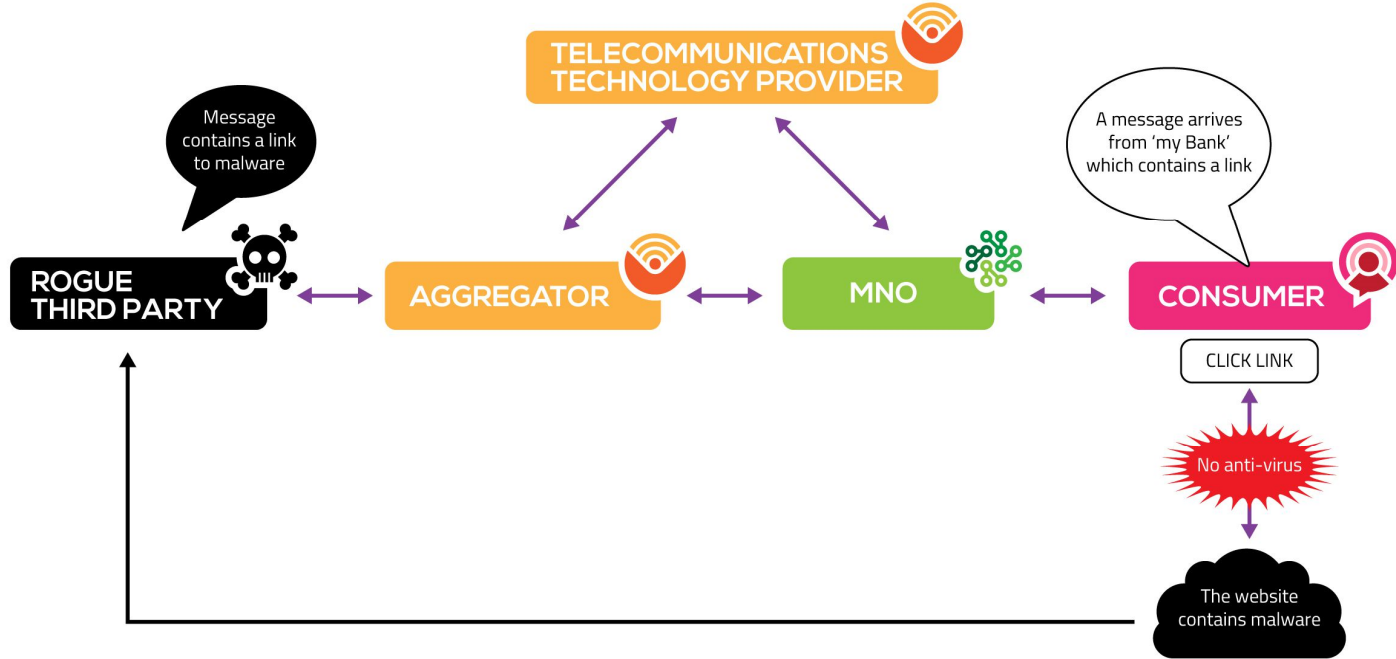
- The promise of financial gain, either directly or indirectly through data theft and through the ability to sell connectivity to third parties
- undetected until there is a direct financial or personal impact and can be difficult to recognise
- Consumers respond automatically to familiar situations and messages and may not be aware of or looking for potential risks due to the trusted and intimate nature of the situation which is created by the sender
- The ease with which consumers can be fooled through the use of basic social engineering and masquerading technique
- The relative openness and power of certain operating systems, combined with the fragmentation of versioning, and lack of security patching by mobile subscribers leaves many devices exposed to security vulnerabilities that can be exploited
- In the majority of cases, victims inadvertently install malware themselves - a simple click on a link in a message received by an unsuspecting mobile subscriber can direct a web browser to a SMiShing or Malicious URL

EXAMPLE

An example of an SMS Malware message. Note the use of an alpha originator to masquerade as a Supermarket. Clicking on the link may initiate a software download or it may take the consumer through to a fake site where a rogue third party could capture any log-in details entered there.



#6 SPAM MALWARE (SMS HACKING)





COMMERCIAL EXPLOITATION:

7 GREY ROUTES, BYPASS, NON-INTERWORKED OFF-NET ROUTES



DEFINITION

The use of open routes without a commercial agreement in place, i.e. a Grey Route, is not fraudulent, but rather, opportunistic. Grey Routes are however included in the Fraud Framework since it makes sense to provide a definition and context given the impact and proliferation of Grey Routes in the mobile messaging ecosystem.

A Grey Route is one which is used as a way to avoiding paying the correct charges, or to avoid paying any charge for message termination. For example, a) sending Business SMS messages via an MNO's P2P Hub or via a roaming signalling link, which are not authorised by an MNO to carry such traffic or b) the termination of international traffic via national routes designated only for delivery of domestic traffic, which has a lower SMS interworking fee than designated international routes or c) sending mobile enterprise traffic from one MNO to another where no agreement to monetize the traffic is in place, etc.

It is still not uncommon for Business SMS messages to be sent between MNOs without a commercial agreement in place, in the form of an AA.19 or AA.60 Agreement. This stems from a legacy 'sender keeps all' policy prior to the uptake of Business SMS messaging, when P2P traffic between MNOs was generally balanced and only small net amounts needing to be settled between the sending and receiving parties thus making the practice unnecessary.

Also, where there is no alternative way to send a Business SMS message, for example, if the sending MNO will not provide a commercial agreement for the termination of messages to any party, either directly via a Business SMS messaging agreement, through AA19 or SS7, or via a Hubbing connection, then sending a Business SMS message without a commercial agreement in place will be deemed legitimate and falls outside of this definition of a Grey Route.

To note: If a message is manipulated by changing the Global Title in the MAP layer to circumvent a firewall and avoid detection, then this is captured as a separate fraud type called **MAP Global Title Faking**.

CAUSE

- Messaging providers attempting to reduce the cost of sending a message to:
 - increase margins on existing traffic
 - attract more traffic by offering a competitive advantage
 - remain competitive against those already using grey routes within their messaging solutions
- A common acceptance of the commoditisation of Business SMS enables messaging providers to incorporate grey routes as part of a blended messaging solution ("It's just an SMS")
- A perceived one-size-fits-all view of Business SMS and its business applications

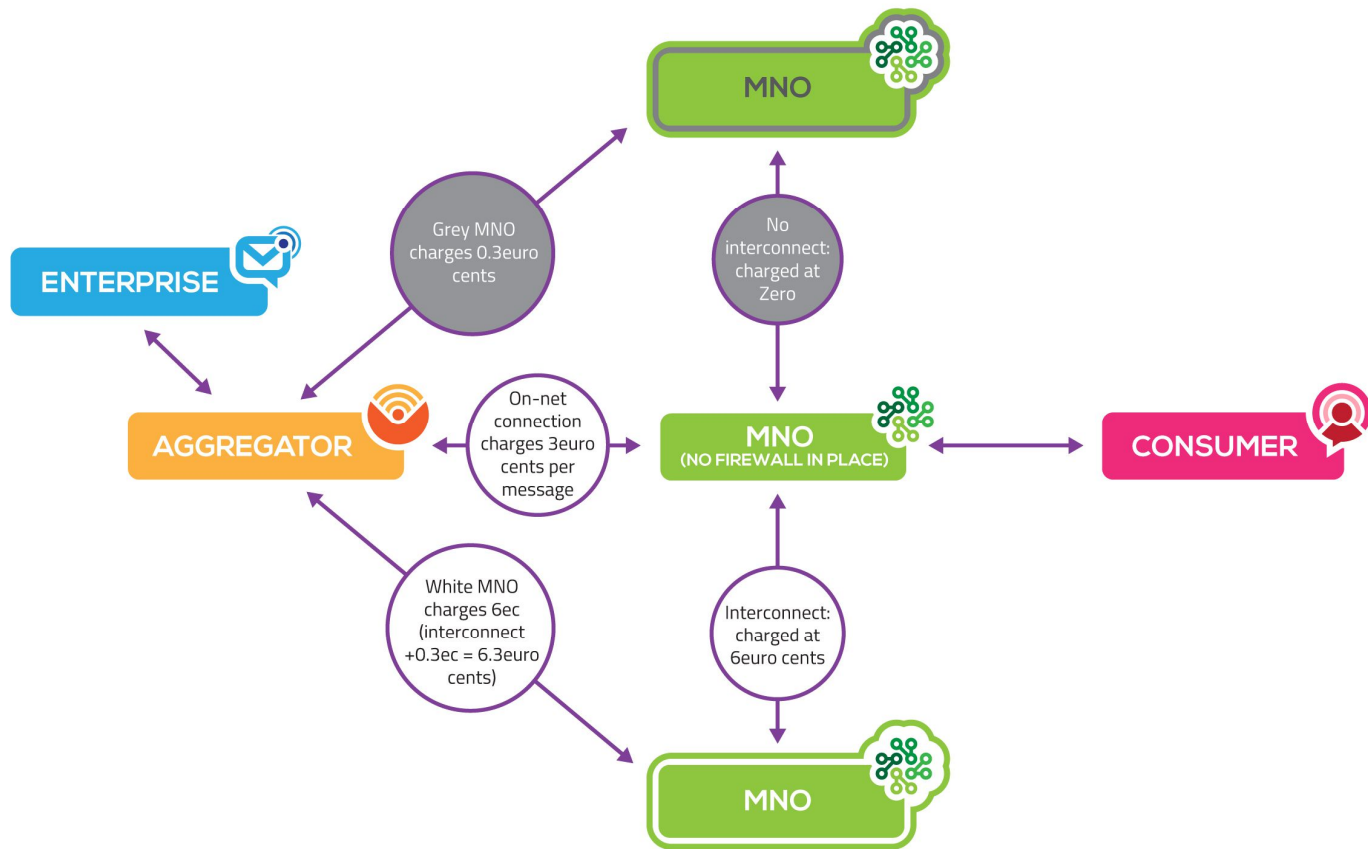
- Price-led procurement activities carried out by messaging providers and some OTT players via Business SMS messaging auctions
- The absence of a joined-up digital communications strategy within enterprise
- The ease with which parties can obtain Global Titles and point codes from certain regulators
- A disconnect within MNOs between P2P and Business SMS messaging teams, as well as between business stakeholders and procurement teams
- Insufficient controls in place by the MNOs to track, monitor and block traffic which is arriving from unauthorised/unmonetized routes

EXAMPLE

An example of a message sent via a Grey Route due to absence of AA19 / AA60 Agreement. The message has been sent from a business in Germany to a subscriber in the UK, via an SMSC in the USA, without being paid for.

```
Signature
+44: UK Sender ID
Source TON/NPI
1/1
Timestamp
Unix Time: 1440750831
28/08/2015 10:33:51 +0200
SMSC Timestamp
15/08/28 09:08:00 +0100
SMSC
+1( SMSC +1 region)
Data Coding Scheme
0
Encoding
0 (Default GSM)
Has UDHI
No
Concatenation
Group: 0 Count: 0 No.: 0
Flash/Alert
No
Message Text
Ihr Verifizierungscode lautet 837485
A2P Enterprise One time password SMS
```

#7 GREY ROUTES DUE TO ABSENCE OF AA19/AA60 AGREEMENT





NETWORK / SYSTEM MANIPULATION:

#8 MESSAGE TRASHING



DEFINITION

Message trashing is the act of deliberately not even trying to deliver a validly formatted Business SMS message with valid content intended to be sent to a valid MSISDN. The perpetrating party in the message delivery chain trashes the message instead of sending it to an MNO or messaging provider for onward delivery to the consumer.

To hide the fraud, the perpetrator often creates a fake delivery receipt which it sends to the enterprise or messaging provider earlier in the delivery chain.

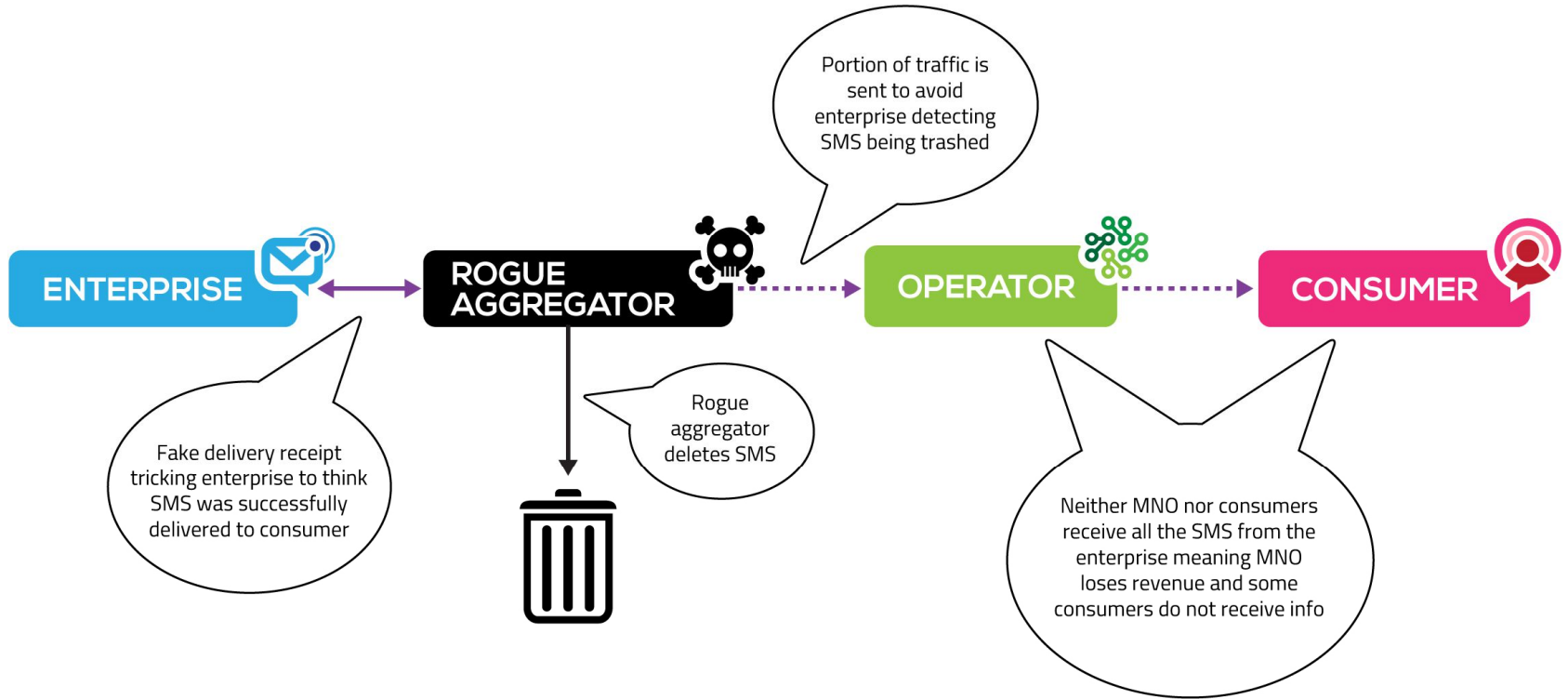
To further seek to avoid detection, the perpetrator typically only trashes a portion of the messages sent by a single sender.

Finally, trashing of messages is much more common for use cases like marketing where no direct action tied to the message is expected of the consumer whereas trashing of, e.g. messages containing one-time-passwords is typically avoided by perpetrators as low response rates would risk alarming the enterprise sending the messages.

CAUSE

- Messaging providers reducing their average cost of sending a message to:
 - increase margins on existing traffic
 - attract more traffic by seemingly offering a competitive advantage
- A common acceptance of the commoditisation of Business SMS enables messaging providers to get away with message trashing since the entity earlier in the delivery chain assumes the lower price point is achieved by means of SIM-farms or grey routes
- Price-led procurement activities carried out by messaging providers and some OTT players and some enterprises via Business SMS messaging auctions. This is especially true for Business SMS messages with perceived lower value by the sender such as for instance marketing.
- The complexity for the sender to know if a Business SMS has been delivered to the consumer when masked by a fake positive delivery receipt. This is especially true for traffic, like marketing, where no direct action tied to the message is expected of the consumer and where the quality of the sender's number database might be low.

#8 MESSAGE TRASHING





NETWORK / SYSTEM MANIPULATION:

#9 SIM FARMS



DEFINITION

A SIM Farm is a method of using a bank of SIM cards for the delivery of Business SMS, either from the destination or another domestic or foreign MNO, which are not intended for that use to avoid paying wholesale messaging rates, for example:

- Consumer SIM cards available through a specific retail offer, such as On-net or Off-net domestic bundles, which allow messages to be sent through P2P channels without a marginal cost per message
- Legitimate M2M or Enterprise SIMs which are sold without sufficient contractual protection to prevent them being used for mobile messaging

A variation of SIM Farming is the technique whereby a mobile subscriber acts as a "crowdsourced-SIM Farm" - a mobile subscriber downloads and installs an app provided by the perpetrator who then sells Business SMS messages that it subsequently sends to the destination number using the app on the mobile subscriber's handset.

This crowdsourced SIM Farm scenario requires a) active participation by the mobile subscriber and b) a consumer pricing plan with a zero marginal-to-low price for sending messages and c) data connectivity (WiFi or 4G).

In order for the use of SIM Farms (regardless of type) to be in breach of commercial contract and hence fraudulent, the MNO issuing the SIM cards must have terms & conditions in place that explicitly state how the SIM cards can and cannot be used.

Besides potentially being in breach with MNO terms & conditions, crowdsourced SIM-farms are in breach with certain data protection legislation, e.g. the GDPR in the EU, since the MSISDN of the subscriber who has installed the app is shared (in the form of being used as the originator of the messages sent) with the recipient of the messages.

To note, SIM Farms are not always used to commit fraud and it should not be assumed that all SIM cards are assigned for allocation to consumers.

CAUSE

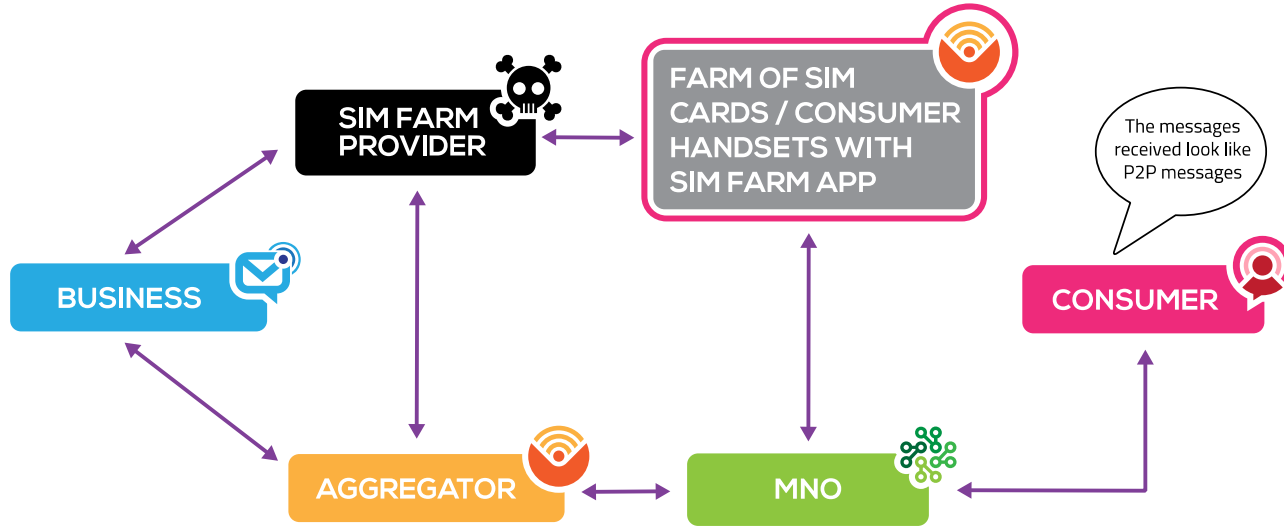
- Exploitation of an MNOs own retail, corporate or M2M SIM offers, bypassing official A2P SMS connectivity or interworking agreements and charges
- Insufficient controls in place by the MNOs to track, monitor and block Business SMS messages which is arriving from consumer, M2M or enterprise SIMs routes
- A disconnect within MNOs between retail and Business SMS messaging teams, where retail teams have incentives to sell SIM cards sometimes driving the sale of SIM cards for unauthorized uses
- A messaging provider can avoid all interworking costs thus improving margins and/or creating the ability to sell below market rates
- An enterprise can buy a Business SMS messaging solution at a cheaper rate than the official MNO rate

EXAMPLE

An example of a message sent using a SIM Farm.



#9 SIM FARMS





NETWORK / SYSTEM MANIPULATION:

#10 SPAM



DEFINITION

A Spam message is one which is sent to a consumer, which the sender does not have the permission of the recipient to send. Spam is commonly commercial in nature, and examples include:

- Payment Protection Insurance (PPI)
- Debt clearance firms
- Accident insurance helplines
- Competitions

Spam is a term commonly used but also misused to encompass a broad range of unwelcome or unsolicited messages, including messages which the recipient may have legitimately agreed to receive. It does also include non-commercial messages, such as political messages which a consumer may not want to receive, but are not Spam messages in the true sense.

In some cases, consumers may believe that they have received Spam simply because they do not remember giving permission to a sender. If a consumer has given consent to a particular enterprise to allow it to send specific mobile business messages and where those messages are all sent within the remit of a contractual agreement and national legislation, any such business SMS cannot be termed Spam for the purposes of this framework.

Typical ways to opt-in to and give permission for the receipt of Business SMS are:

- to agree as part of a sign-up process online
- on a physical form, or
- as part of an enquiry to purchase or an actual purchase

To note: Transactional messages are not included in the definition of Spam as they are requested through the course of a specific transaction and delivered on a one-time basis.

CAUSE

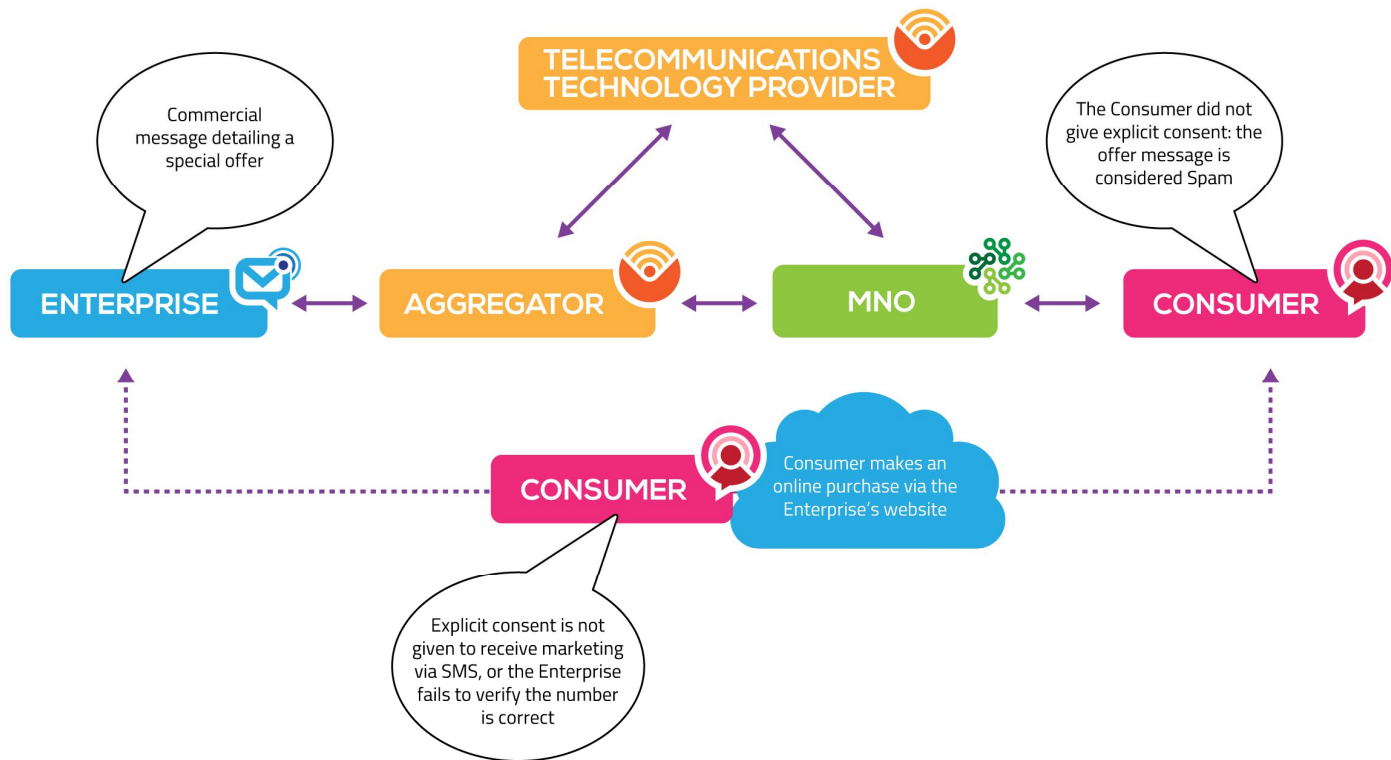
- Marketers who want to increase sales by sending promotional messages to MSISDNs which have been bought, farmed or automatically generated through brute force sequencing and then checked against a Home Location Register (HLR) to determine which numbers have been activated and are live
- Business SMS can be sent in large volumes - the more consumers who are made aware of a product, the more sales can be achieved
- Business SMS has significantly higher delivery and open rates compared to most other forms of marketing such as email, and consequently high conversion rates
- Low market pricing – either by design or due to pervasive fraudulent routes – combined with light regulation
- Poor data management by an enterprise, for example:
 - in countries where MNOs recycle MSISDN's, the previous owner of a mobile number may have agreed to the receipt of messages where the new owner has not
 - Sending messages to consumers who have removed their permission

EXAMPLE

This is a typical example of a SPAM message. The use of a numeric originator makes it likely that it was sent through a SIM Farm.



#10 SPAM





NETWORK / SYSTEM MANIPULATION:

#11 ARTIFICIAL INFLATION OF TRAFFIC (AIT)



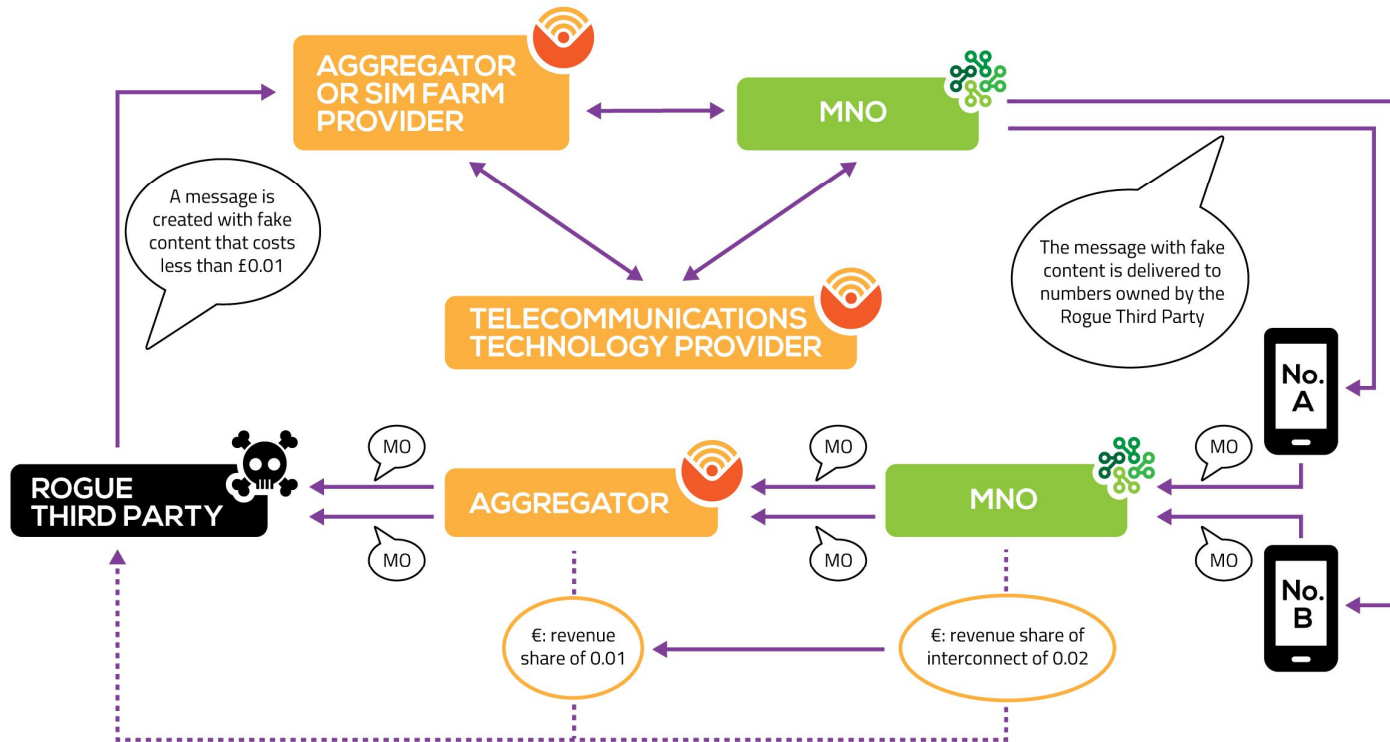
DEFINITION

Artificial Inflation of Traffic occurs when a party sends messages to numbers it controls to generate profit from the mobile originated (MO) interconnect revenue share.

CAUSE

- The promise of monetary gain by using very simple commercial and technical capabilities
- The cost of sending a message is lower than the revenue share return of an interconnect agreement

#11 ARTIFICIAL INFLATION OF TRAFFIC (AIT)





NETWORK / SYSTEM MANIPULATION:

#12 MAP GLOBAL TITLE FAKING



DEFINITION

MAP Global Title Faking is the act of an individual or company manipulating the Business SMS environment by:

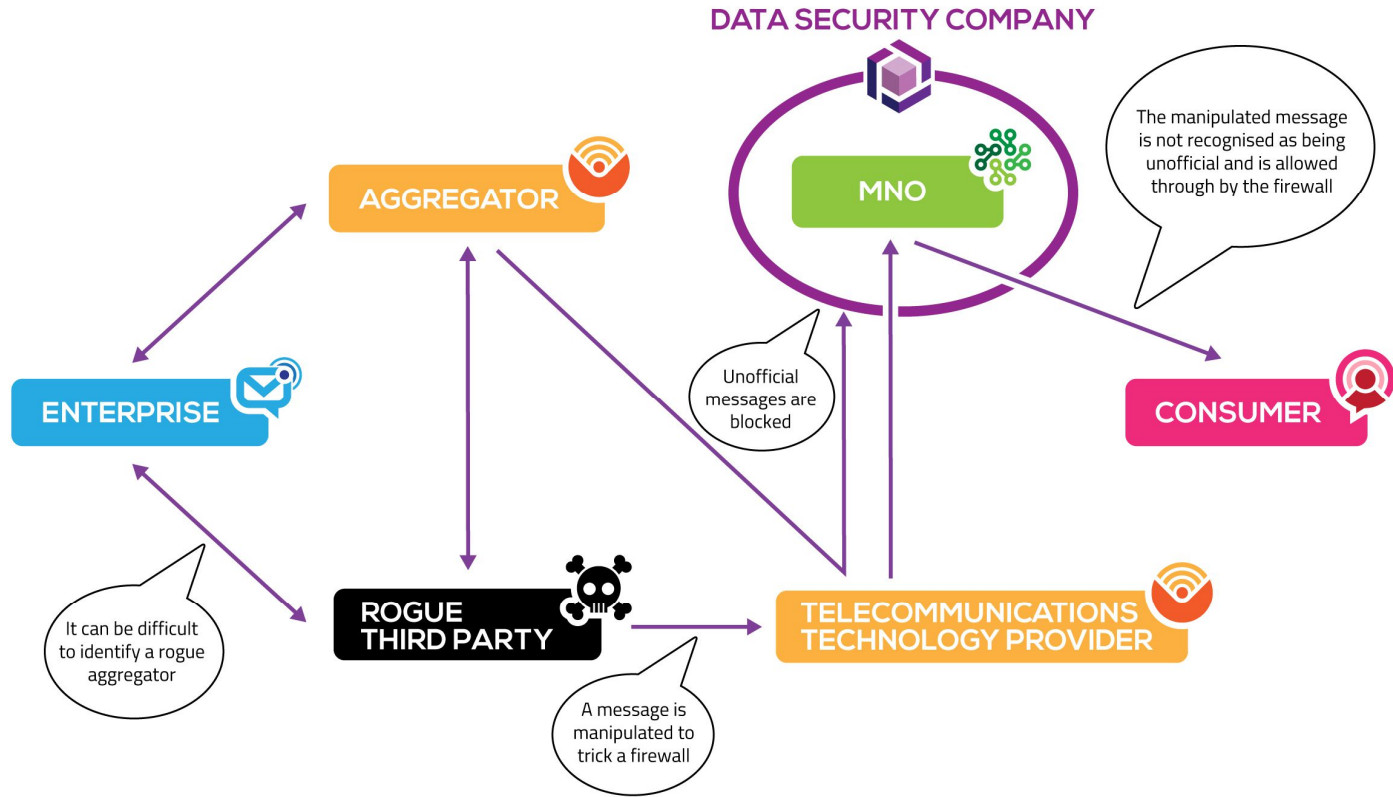
- manipulating a message by changing a MAP parameter to avoid SMS firewall blocking
- pretending to be an MNO by changing a MAP parameter which does not have a commercial agreement in place with the sender

The entity generating the fraud has access to the International SS7 Network and by circumventing or avoiding being blocked by an MNO's firewall, they can reach a MNO's SMSC at MTP level (signalling point code).

CAUSE

- Manipulation of a message to bypass an MNO's firewall which would otherwise be blocked enables a messaging provider to:
 - reduce the cost of sending a message
 - increase margins on existing traffic
 - attract more traffic by offering a competitive advantage
- A common acceptance of the commoditisation of Business SMS messaging providers to incorporate grey routes as part of a blended messaging solution - "It's just an SMS"
- A perceived one-size-fits-all view of Business SMS and its business applications
- Price-led procurement activities carried out by messaging providers and some OTT players via Business SMS auctions
- The absence of a joined-up digital communications strategy within enterprise
- The ease with which parties can obtain Global Titles and point codes from certain regulators
- A disconnect within MNOs between P2P and Business SMS teams, as well as between business stakeholders and procurement teams

#12 MAP GLOBAL TITLE FAKING (CREATED THROUGH MAP OR OTHER MANIPULATION)





NETWORK / SYSTEM MANIPULATION:

#13 SCCP GLOBAL TITLE FAKING



DEFINITION

SCCP Global Title Faking [Faking] is the act of sending a message to a handset originating from a Global Title that does not belong to the sender:

The entity generating the fraud has International SS7 capabilities at SMSC level. The manipulation of a Global Title within the routing environment allows the entity to initiate SMS MT (mobile terminated) call flows with the destination MNO which is unaware that the Global Title being used by the sender is not legitimate or has been subject to some manipulation.

This can happen in one of two ways:

1. The same Global Title is used to send both the SRI (send routing information) and FSM (forward short message) requests. The Messaging Provider uses the Global Title without authorization or knowledge of the MNO owning it and it is implemented on the messaging provider's side, so messages will be sent using this Global Title.
2. The Messaging Provider performs a SRI via some sort of legitimate or illegitimate access in order to obtain necessary information such as IMSI (international mobile subscriber identity) and VLR (visitor location register). The Messaging Provider then uses a Global Title without authorization or knowledge of the MNO owning it to send the FSM. As such in this scenario, a different Global Title is used to send the SRI and the FSM. Sending the FSM is purely unidirectional as a FSM confirmation is not needed.

In both cases, it will appear to the destination MNO as if the MNO whose Global Title is being misused was sending the message thus resulting in a) the destination MNO's firewall not blocking the messages which it might otherwise have done and b) the destination MNO charging an interconnection fee of the MNO whose Global Title is being misused if an AA.19 agreement is in place between the two MNOs. To reduce risk of getting caught using Global Title's of an MNO with an AA.19 agreement with the destination MNO is preferred by fraudsters as MNOs tend not to monitor this traffic as vigorously as non-paid for traffic. To reduce risk further fraudsters do faking in both directions leaving the traffic balance between the MNOs in question intact.

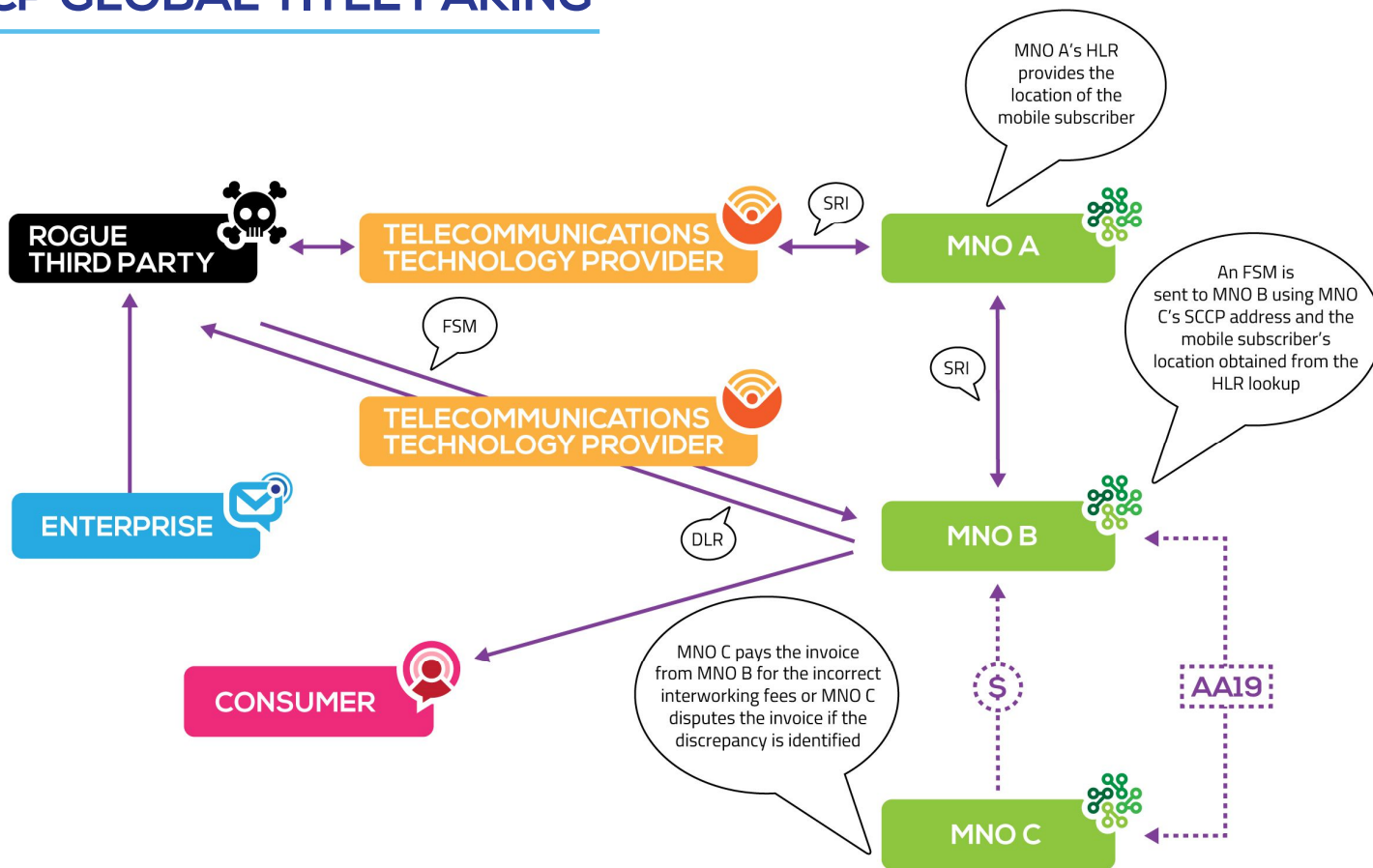
This definition does not cover IMSI Faking which is rare and difficult to carry out.

CAUSE

Faking enables a messaging provider to sell messages at below market rate – the sender will pay for the signalling costs but the termination cost will be close to zero. Faking is facilitated because:

- A messaging provider needs a full International Mobile Subscriber Identity (IMSI) in order to Fake messages
- MNOs will give out the full International Mobile Subscriber Identity (IMSI) when selling Sender Route Information (SRI)
- Telecommunications technology providers typically only check once if the sender owns the Global Title address space being used and can therefore be easily manipulated
- Telecommunications technology providers are not incentivised to proactively monitor the Global Title address spaces used by a sender as they make money on traffic by charging for Message Signal Units (MSUs)
- MNOs are not adequately protecting their own network by blocking any traffic where an FSM is not preceded by an SRI originating from the same MNO
- MNOs are not investigating interconnect charge discrepancies to the extent needed to discover past or still ongoing faking occurrences, neither on total level of traffic nor on traffic imbalances
- Although the vast majority of Faking comes from within the ecosystem, a lack of coherent end-to-end processes in place to identify unambiguously the fraudulent parties means that the fraudulent parties remain in plain sight without facing any consequences

#13 SCCP GLOBAL TITLE FAKING





NETWORK / SYSTEM MANIPULATION:

#14 SMSC COMPROMISE FRAUD



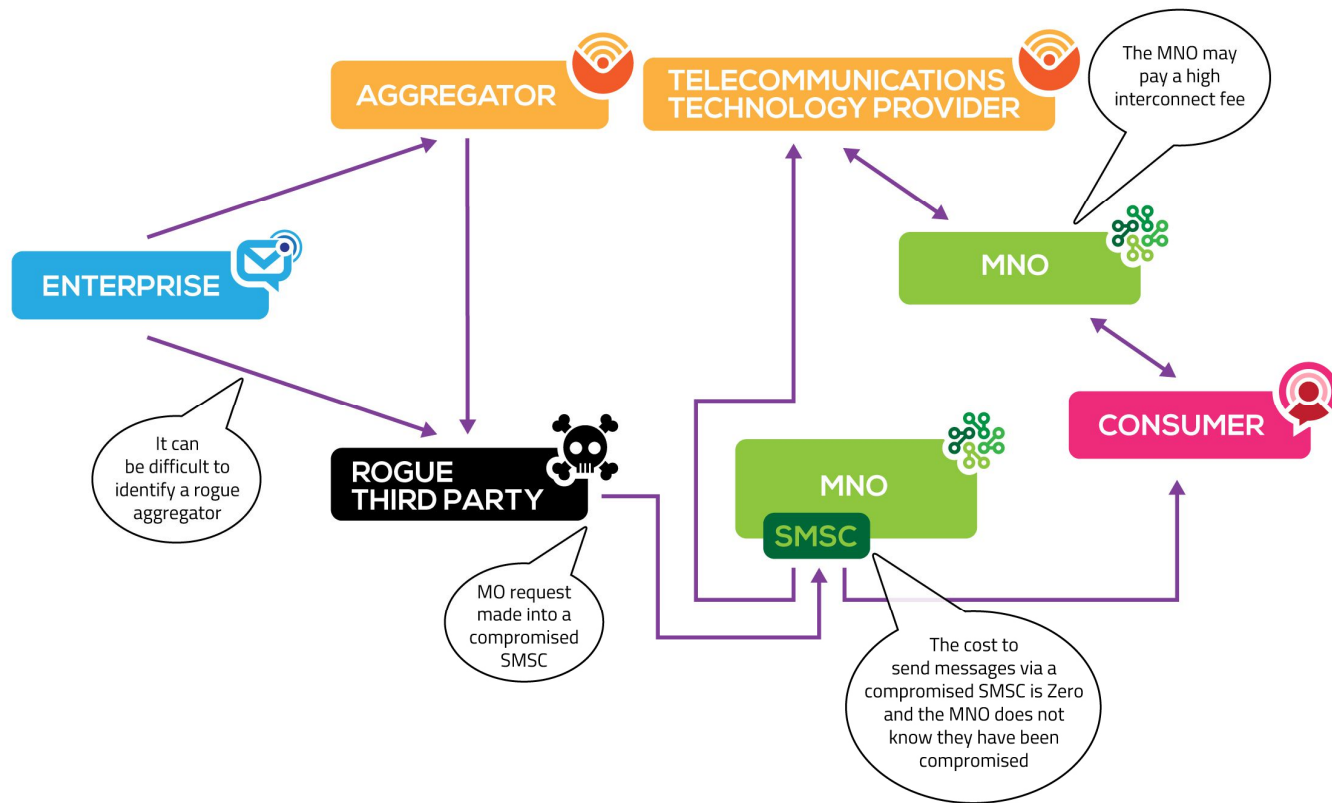
DEFINITION

SMSC Compromise Fraud is the act of reaching an MNO SMSC at MTP level (signalling point code) within the International SS7 Network and using the SMSC to relay and send messaging globally without paying for them. The owner of the SMSC will be liable for payment of the termination charges.

CAUSE

- Exploitation of weaknesses in the security precautions taken by an MNO to prevent their SMSC from being used as a relay
- A messaging provider can avoid all interworking costs
- A business can buy SMS at a cheaper rate than the official MNO rate

#14 SMSC COMPROMISE FRAUD



COMBATTING FRAUD



COMBATTING FRAUD



This Fraud Framework is part of MEF's self-regulatory service [Trust in Enterprise Messaging](#) ('TEM') whose goal to accelerate market clean-up and help educate business messaging solution buyers about the threats of fraudulent practices and poor procurement processes.

Its Business SMS Code of Conduct sets out best practice for all actors operating within the business SMS sector and is based on 10 principles offering detailed guidance on commercial, procedural and technical requirements as well as an emphasis on consumer protection.

First launched in 2018, it is overseen by an independent Compliance Committee which includes expert fraud & security representatives from other trade associations and independent advisors.

V2 of the Code of Conduct was published in December 2020. TEM is open to all companies (whether a MEF member or not) who advocate industry best practice to tackle fraud in Business SMS. Please copy and paste the URL below into your web browser to see the latest list of code signatories.

<https://mobileecosystemforum.com/programmes/future-of-messaging/fraud-management/trust-in-enterprise-messaging#signatories>



BUSINESS SMS CODE OF CONDUCT

NUMBER AND STATUS:	V2.0 RELEASED
DATE:	14TH DECEMBER 2020
CODE CLASSIFICATION:	SELF-REGULATED CODE
PREPARED BY:	MOBILE ECOSYSTEM FORUM (MEF) AND MEF'S FUTURE OF MESSAGING PROGRAMME PARTICIPANTS
NOTES:	THIS CODE ADDRESSES BUSINESS SMS INCLUDING A2P (APPLICATION TO PERSON) AND P2A (PERSON TO APPLICATION)



GLOSSARY





GLOSSARY

A2P SMS (Application to Person)

Messages originated by computer or application and intended for delivery to the subscribers of MNOs. A2P SMS is typically used by enterprises to communicate and share information with their customers, for example, bank balance alerts, retail order or delivery confirmation, appointment reminders and offers. A2P SMS is generally used to send messages one way but two-way communication is possible in certain markets.

Access Hacking, Hacking

The act of gaining access to an app, device, platform or any other IT infrastructure by someone without the permission of the owner.

Aggregator

A company that provides connectivity between Message Generators and MNOs.

Artificial Inflation of Traffic (AIT)

The act of artificially generating messages which are sent by a rogue party to itself in order to generate profit.

Business SMS

See A2P and P2A

CPaaS (Communications Platform as a Service Providers)

Companies providing their customers (e.g., developers) a cloud-based platform where they can add real-time communications features (voice, video, and messaging) in their own applications without needing to build backend infrastructure and interfaces.

Firewall

A filtering system which enables MNOs to monitor, detect, block and report suspicious or unauthorised messages destined for delivery through their network and to their subscribers

FSM (Forward Short Message)

The second of two SS7 requests sent by an SMSC when a message is being sent, the first being an SRI. Both an SRI and FSM request are required to send a message.

Global Title (GT)

An address used in the SCCP protocol for routing messages through an MNO's network. A Global Title is a unique address which refers to a single destination, though in practice, destinations can change over time.

Grey Route

A connection used for the delivery of enterprise messages, but which is not explicitly authorised for that use, for example, where the absence of a commercial agreement for a connection is exploited as a lower cost option at the expense of the terminating MNO.

HLR (Home Location Register)

The database within a GSM Network which stores all mobile subscriber data, including the subscriber's location (eg, home or roaming), phone status, (eg, on, off, inbox full etc) and their mobile network.

IMSI (International Mobile Subscriber Identity)

A unique number, usually fifteen digits, which identifies a GSM mobile network subscriber.

MAP Global Title Faking

Manipulation of specific technical parameters by disguising a Message Processor's true identity in order to gain access to an MNO's network to deliver messages which would otherwise be flagged as unauthorised and rejected by an MNO or subject to interworking charges.

Message Generator

This is the company or brand from which the message is being sent. Even if the message is technically created by a 3rd party on behalf of the brand, the brand is still regarded as a message generator.

Message Processor

This is any company in the ecosystem that is involved in the processing, routing, or carrying the message en-route to its final destination.

Message Recipient

This is typically a person that is a customer or employee of the Message Generator.

Message Terminator

This is any company in the ecosystem that is responsible for delivering the message to the consumer handset. Usually a Mobile Network Operator.

Mobile Network Operator; Mobile Operator (MNO)

An MNO provides wireless or mobile communication services and owns or controls all of the elements of the network infrastructure necessary to deliver services to a mobile subscriber. All MNOs must also own or control access to a radio spectrum license which has been issued by a regulatory or government body. An MNO typically controls provisioning, billing and customer care, marketing and engineering organisations needed to sell, deliver and bill for services, though these systems and functions can be outsourced.

Mobile Originated (MO)

A Mobile Originated message is a message where the message is sent from a customer or employee to an enterprise.

MSISDN (Mobile Station International Subscriber Directory Number)

The unique mobile phone number attached to a SIM card used in a mobile device.



GLOSSARY

Mobile Terminated (MT)

A Mobile Terminated message is a message where the message is sent from an enterprise to a customer or employee of that enterprise.

Originating Mobile Operator; Originating MNO

The MNO at the start of the end-to-end message delivery chain which accepts messages from a messaging provider for onward delivery.

Originator/SenderID

The term used to describe the number or word which identifies who a message is from upon receipt. It is also known as a SenderID. An alphanumeric originator enables a brand name to be set as the identified 'sender' of a message.

Phishing, SMS Phishing, SMiShing

The act of misleading a mobile subscriber by presenting to be a known and trusted party to gain access to online systems, accounts or data such as credit card, banking information or passwords for malicious reasons.

P2A

Person-to-Application. Messages sent from a person to interact with an application interface.

Roaming Intercept Fraud/SMS Roaming Intercept Fraud

The act of deliberately intercepting a message while a consumer is roaming.

SCCP (Signalling Connection Control Part) Provider

A company which manages the SCCP layer protocol.

SCCP Global Title Faking

The act of sending a message in a way that deceives the terminating MNO about the true identity of the sender through the misuse of a Global Title.

Short Code, Short Number

A special numbers, significantly shorter than a full 11-digit phone number, which can be used as the SenderID of SMS and MMS messages.

Signalling Providers

Companies providing the connectivity that enables roaming and messaging between an MNO and its roaming partners. It ensures continuity of service for mobile users by enabling them to make or receive mobile calls, send or receive SMS and use mobile internet while travelling all around the globe. Synonymous with SCCP Provider.

SIM; SIM Card (Subscriber Identity Module)

A smart card inserted into a mobile device which carries a unique identification number, stores personal data and prevents operation of the device if removed.

SIM Farms

A method of using a bank of SIM cards for the delivery of messages for which the SIMs are not designated, for example retail SIMs intended for use by individual mobile subscribers which are instead used for the delivery of enterprise messages.

SIM Swap Fraud or Porting Fraud

The act of obtaining control of a mobile number by cancelling the SIM linked to a consumer's handset and activating a new SIM with that number linked to a different handset, and so causing all calls and texts to be routed to and from a different handset, outside of the control of the consumer.

SM (Short Message Services)

A text messaging service component of phone, web, or mobile communication systems which uses standardised communications protocols to allow fixed line or mobile phone devices to exchange short text messages.

SMSC (Short Message Service Centre)

An element within an MNO's network which receives messages from mobile network users (enterprise and individual mobile subscribers), stores, forwards and delivers messages to mobile network users, as well as maintaining unique timestamps in messages.

SRI (Send Routing Information)

This is the first of two SS7 requests sent by a SMSC when a message is being sent, the second of which is an FSM request. An SRI request is made by the originating MNO's SMSC to the HLR/VLR of the MNO owning the prefix of the MSISDN to which the message is being sent to request routing information and determine the IMSI of a mobile subscriber. Both an SRI and FSM request are required to send a message.

Spam

A broad term for an unsolicited message, namely, one which is not wanted by the recipient, whether the message has been sent with good intentions or maliciously.

SMS Originator Spoofing, Spoofing

The act of changing a message originator to hide the sender's true identity.

SS7 (Signalling System 7)

A set of telephony signalling protocols that enable the sending of SMS messages as well as performing number translation, local number portability, prepaid billing and other mass market services.

Terminating Mobile Network Operator; Terminating MNO

The MNO at the end of the end-to-end message delivery chain.

Traffic

A common term used to refer to the movement of messages, e.g., "the [SMS] traffic has been successfully delivered."

ABOUT





ABOUT THE PROGRAMME



Established in 2015, MEF's Future of Messaging Programme is a worldwide, cross-ecosystem approach to promote a competitive, fair and innovative market for mobile communication between businesses and consumers. Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of Business SMS solutions
- Promote Business SMS as a premium and trusted channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving messaging landscape
- Develop the value-chain to support new use cases and business

FOR FURTHER INFORMATION ON THE FUTURE OF MESSAGING PROGRAMME AND TO GET INVOLVED PLEASE VISIT:

WWW.MOBILEECOSYSTEMFORUM.COM

Established in 2000, the Mobile Ecosystem Forum is a global trade body that acts as an impartial and authoritative champion for addressing issues affecting the broadening mobile ecosystem. As the voice of the mobile ecosystem it provides its members with a global and cross-sector platform for networking, collaboration and advancing industry solutions. The goal is to accelerate the growth of a sustainable mobile ecosystem that delivers trusted services that enrich the lives of consumers worldwide.

Launched in 2015, **MEF's Future of Messaging Programme** is a dedicated industry programme that promotes a competitive, fair and innovative market for mobile communication between businesses and consumers. Programme participants represent different regions and stakeholder groups working collaboratively to:

- Produce and publish best practice frameworks, papers and tools to accelerate market clean-up and limit revenue leakage
- Educate buyers of messaging solutions
- Promote business messaging as a premium and trusted channel
- Drive knowledge across the ecosystem of new platforms, technologies and procedures to address the evolving messaging landscape
- Develop the value-chain to support new use cases

ACCELERATING YOUR MOBILE OPPORTUNITY

WWW.MOBILEECOSYSTEMFORUM.COM

