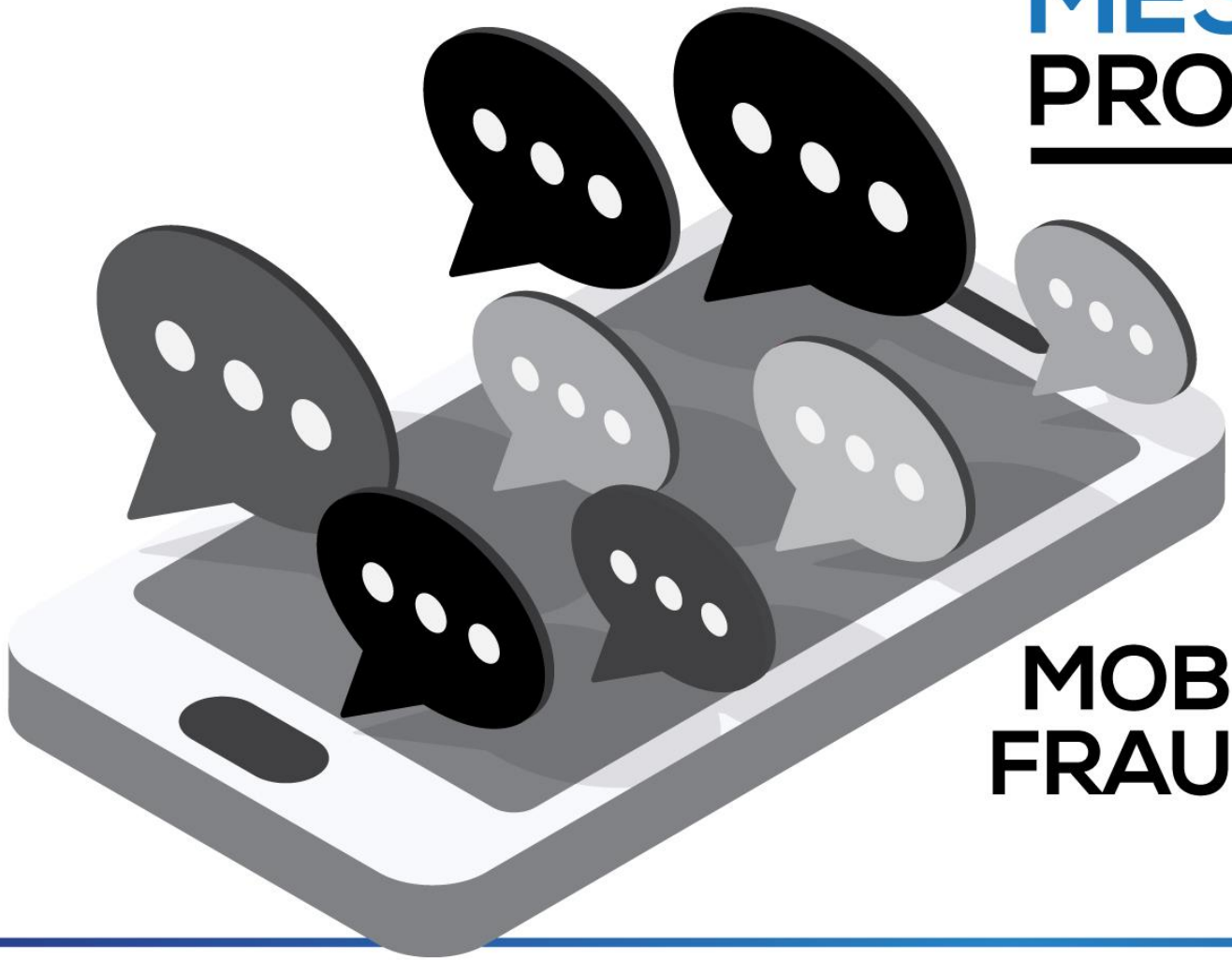
MEF

FUTURE OF MESSAGING PROGRAMME



ENTERPRISE MOBILE MESSAGING FRAUD FRAMEWORK

VERSION 2.0

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Enterprise mobile messaging is a well-established, safe, efficient and cost-effective way for enterprise to build relationships and communicate with their customers. This is reflected in our research which shows that when communicating with companies, consumers trust SMS (short message services) above any other channel. However, if left unchecked, there is a risk that levels of trust amongst consumers and enterprise will fall, impacting the adoption of messaging amongst new enterprise sectors, stifling innovation and ultimately slowing the long-term growth of the industry.

In May 2016, MEF published its A2P Messaging Fraud Framework Version 1.0. The framework was developed by a collaborative cross-ecosystem working group of participants of MEF's Future of Messaging Programme, represented by senior executives from across Commercial, Operator Relations, Product and Technical teams. The group identified 11 different types of fraud which take place within the enterprise mobile messaging ecosystem, often called the "A2P market" or "Application-to-Person market", together with their cause, the impact on different key stakeholder groups and the different means to detect and prevent fraud. Version 1.0 of the framework set the foundations for the future work of the Programme to develop best practice guidelines for industry and buyers of messaging solutions, as well as providing the structure for an industry-wide certification programme.

If we are to be effective in tackling and eliminating fraud within the ecosystem, we must continue to be proactive. This second version of the fraud framework is the result of a comprehensive review of the evolving market by our cross-ecosystem group of Programme participants, through which two new additional fraud types have been identified: SIM Swap Fraud and SMS Roaming Intercept Fraud. We identify, define and map a total of 13 different fraud types, providing recognisable, real life examples of how fraud can occur, sharing how the different communities within the ecosystem can detect and protect themselves and their customers against fraud.

The framework will help you to:

- Understand why fraud exists
- Recognise the 13 different types of fraud which affect the ecosystem today
- Identify the different communities and parties within the ecosystem
- Consider the impact of fraud on the whole ecosystem
- Learn what steps can be taken to protect against fraud

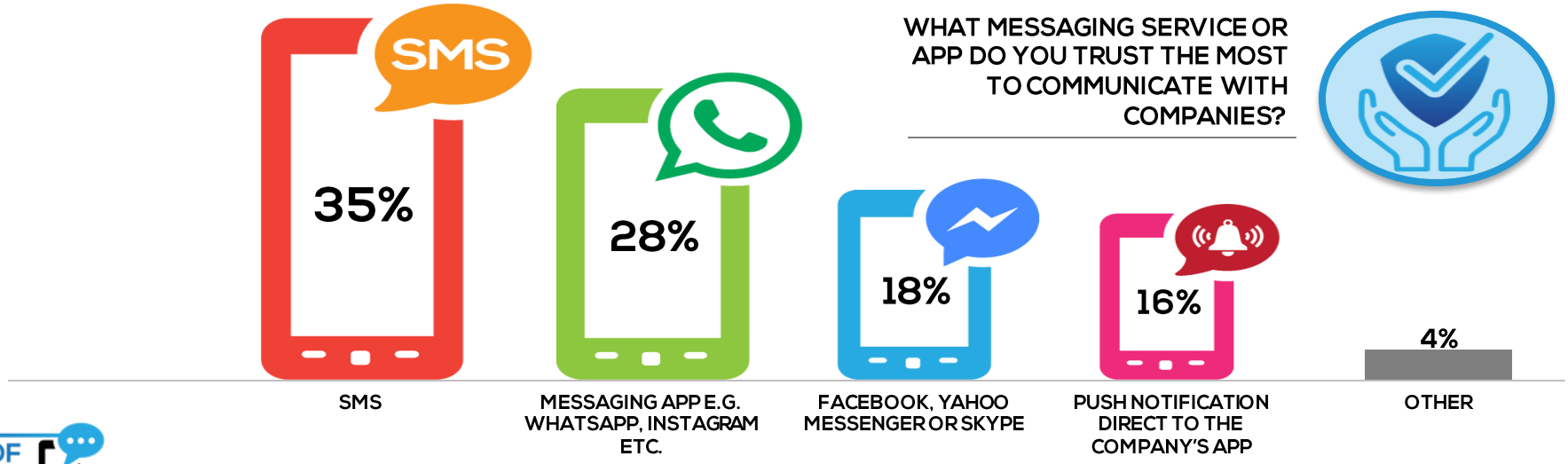


Chart: MEF Mobile Messaging Fraud Report 2016

INTRODUCTION

MEF's Future of Messaging Programme was established in October 2015 – its core objective is to unite all parties within the mobile messaging ecosystem to promote and accelerate best practices to limit fraudulent behaviours and identify new opportunities for enterprise mobile messaging.

Great opportunities exist to grow this exceptional and unrivalled communication channel, but continued trust in enterprise mobile messaging and adoption rates amongst enterprise is under threat from fraud. The Founding Members of the Programme acknowledged that unless proactive and positive steps were taken to reduce fraud, the development of innovative and dynamic solutions and use cases to meet the needs of the next generation of mass communication would be hindered. New entrants from across ever expanding enterprises and sectors would be discouraged from adopting messaging as a core solution for their business.

The enterprise mobile messaging ecosystem and the partnerships within it can seem complex and difficult to navigate, but each member within the message delivery chain has their role to play in providing the range of messaging solutions to the enterprise that continue to make enterprise mobile messaging unique in its ubiquity. However, no one stakeholder can successfully address fraud on its own, as some types impact only at certain points within the delivery chain, adding to the challenge of tacking fraud effectively.

Therefore, it is essential to adopt a cross-ecosystem approach to create a more transparent ecosystem and both identify and then accelerate the clean-up of the market. MEF's Future of Messaging Programme provides this collaborative cross-ecosystem forum, through which the industry as a whole can come together to achieve a shared objective to promote and share mechanisms to limit fraudulent practices.

The first output of the Programme was MEF's A2P Messaging Fraud Framework v1.0, published in May 2016. Version 1.0 of the fraud framework established a common set of definitions for the 11 different types of fraud identified by an International Working Group of Programme participants, together with the cause, their impact and the various means to both detect and prevent the different fraud types.

Since the publication of Version 1.0 of the fraud framework, significant work has been undertaken to educate and inform the whole ecosystem to support the core objective of the Programme. We have delivered consumer and industry research with our Mobile Messaging Report 2016 and Messaging Fraud Report 2016, we have explored use cases, platforms and technologies which are changing the landscape of messaging globally with our Future of Messaging Guide, and published MEF's Enterprise Mobile Messaging Guide, which is aimed at all buyers of enterprise mobile messaging solutions to support their understanding of the industry through the use of a common industry language. This includes the adoption of the term 'Enterprise Mobile Messaging' when speaking about A2P SMS to facilitate effective communication between the different communities within the ecosystem.

Within our Enterprise Mobile Messaging Guide, we have also identified the key features enterprise need to look for when procuring an enterprise mobile messaging solution, and importantly in terms of tackling fraud, we define the six authorised routes that are industry-qualified options to deliver enterprise mobile messages.

As the Programme has evolved over the last year and to ensure that our activities remain alighted with our objectives, we have undertaken a comprehensive review of the framework to ensure that it remains current. Utilising the same assessment criteria to review different types of fraud, definitions, cause, impact and the means to detect and prevent fraud, we have taken this opportunity to align the language and terms within version 2.0 of the fraud framework with MEF's Enterprise Mobile Messaging Guide to allow us to reach a broader audience. The review by the Programme Participants has also identified two new additional fraud types, taking the total number to 13 different types.

Version 2.0 of the Fraud Framework offers some further insight into the impact of fraud on all parties within the ecosystem, as well as categorisation of the means available to parties to detect and protect against fraud through the implementation of commercial solutions, technical solutions and through processes, compliance and legality.

Awareness and understanding of fraud remains inconsistent across the message delivery chain, but the important work of addressing fraud is only made possible through the continued collaborative cross-ecosystem activities within MEF's Messaging Programme.

INTRODUCTION

INTENDED AUDIENCE

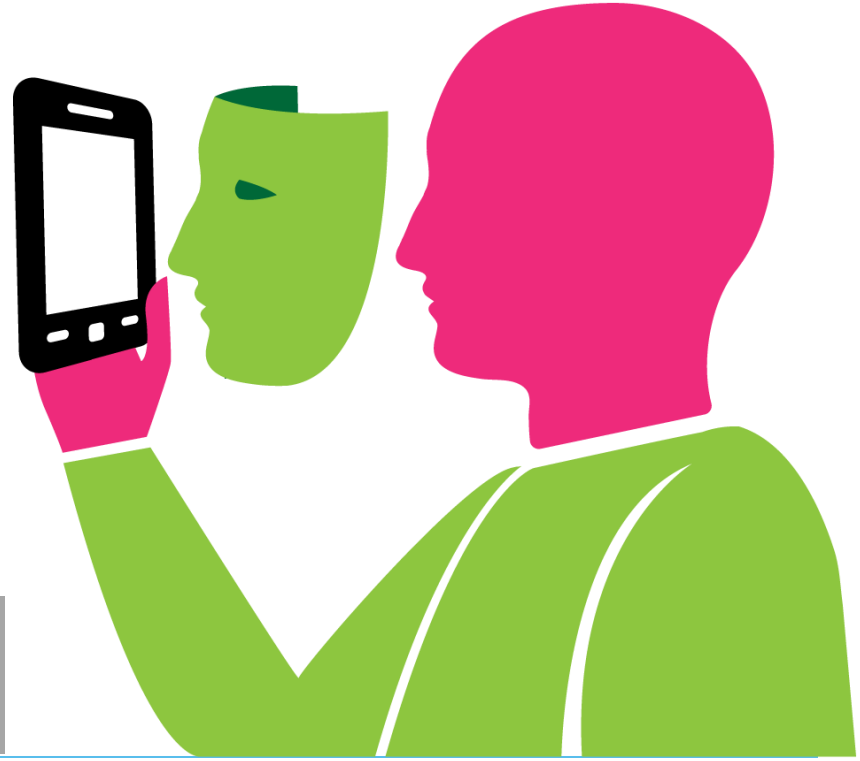
This fraud framework identifies and defines 13 different types of fraud which are present within today's global enterprise mobile messaging ecosystem. We look at their impact, cause and how the following communities can detect and protect against them :

1) MNO
2) Messaging Provider
3) Enterprise
4) Consumer

This framework is especially recommended for those in the following areas of a business:

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

HAVE YOU EVER RECEIVED A TEXT MESSAGE (SMS) FROM SOMEONE PRETENDING TO BE SOMEONE THEY ARE NOT, E.G., YOUR BANK OR A COMPANY THAT YOU HAVE AN ONLINE ACCOUNT WITH, ASKING FOR PERSONAL ACCOUNT INFORMATION OR FOR MONEY?



NO 45%

YES 33%

DON'T KNOW 21%

Chart: MEF Mobile Messaging Fraud Report 2016

HOW FRAUD IMPACTS ON REAL LIFE

Fraud is indiscriminate. It impacts on all parties within the enterprise mobile messaging 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
- **NETWORK / SYSTEM MANIPULATION:** to gain competitive advantage or perform illegal activities via the deliberate manipulation of a message or the exploitation of vulnerabilities within the message flow systems to bypass protection measures intended to safeguard MNOs and consumers
- **COMMERCIAL EXPLOITATION:** to gain competitive advantage by exploiting gaps within the commercial structures of the messaging ecosystem

In reality, the 13 fraud types identified within this framework are often carried out in combination. For example, deliberately manipulating a message to bypass an MNO's security systems to avoid termination fees and to enable the delivery of a phishing message which would otherwise be blocked from reaching a consumer. Below are some examples of fraudulent activities which 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, eg, *"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 account banking login details, phish credentials, intercept the 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 & Phishing

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, eg, *"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 site 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 publically 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 and 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.

As these examples show, fraud within the enterprise mobile messaging 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.

THE BASICS

THE BASICS

FRAMEWORK DEVELOPMENT

MEF's Future of Messaging Programme Founders established that the starting point to tackle fraud is from a collaborative and cross-ecosystem position. No one party has a true 360 degree view of the entire message delivery chain and the fraud that can infiltrate at various points. Therefore, the industry needed to come together and form an international Working Group, represented by senior executives across Commercial, Operator Relations, Product and Technical teams. The group worked together to identify how fraud was impacting the ecosystem, to map the complexity of the relationships that exist which are a fundamental principle of why fraud continues to exist, alongside their cause and how to detect and prevent fraud. This work culminated in the publication of MEF's A2P Messaging Fraud Framework in May 2016.

One year on, MEF's Future of Messaging Programme Participants have again worked together to review and update the fraud framework, in conjunction with an educational stream to support the buyers of enterprise mobile messaging solutions with MEF's Enterprise Mobile Messaging Guide.

The Group has identified two new additional fraud types, bringing the total to 13 different types. Furthermore, a full review of language and common industry terms has been carried out which to ensure that easy comprehension by all communities within the ecosystem. For example, for the purposes of Version 2.0 of the fraud framework and the ongoing work of the Programme, A2P SMS will be referred to as Enterprise Mobile Messaging.

HOW DOES THE INDUSTRY WORK?

Enterprise mobile messaging has developed and grown from the early days of person to person (P2P) messaging, offering a cost-effective and well-established means of connecting an enterprise directly to their customers globally, irrespective of their location or technology. A technical and commercial infrastructure has developed around this opportunity to enable and facilitate this relationship.

The nature of the enterprise mobile messaging 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 broad global enterprise customer base, or to offer a variety of effective and economical authorised solutions to the enterprise 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 ecosystem also contains parties which are not directly engaged within the end to end message delivery chain, but which provide support services to those within it, such as testing, reporting and data security companies.

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

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

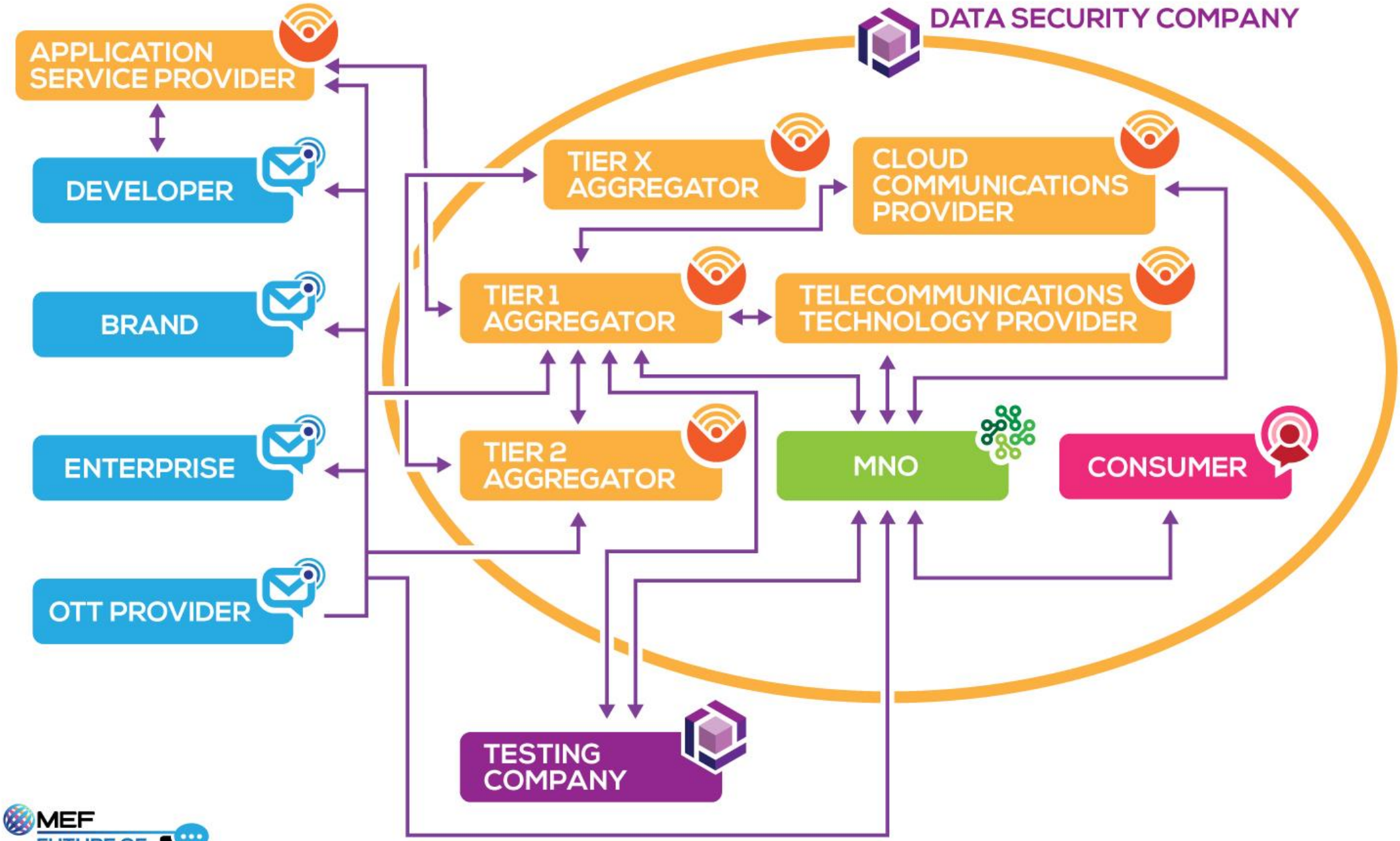
However, as more parties join the message delivery chain, an enterprise mobile messaging solution becomes more exposed to the risks of using unauthorised or fraudulent routes. Transparency is therefore key to knowing what will happen and what has happened after a message has left an enterprise on its way to the consumer.

ECOSYSTEM MAPPING

The following five groups represent the different communities within the enterprise mobile messaging ecosystem:

MNO	MESSAGING PROVIDER	ENTERPRISE	CONSUMER	SUPPORT SERVICE
MOBILE NETWORK OPERATOR (MNO)	TIER 1 AGGREGATOR TIER 2 AGGREGATOR TIER X AGGREGATOR TELECOMMUNICATIONS TECHNOLOGY PROVIDER CLOUD COMMUNICATIONS PROVIDER APPLICATION SERVICE PROVIDER	ENTERPRISE BRAND 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

MAP OF THE ENTERPRISE MOBILE MESSAGING ECOSYSTEM



MEF
FUTURE OF MESSAGING PROGRAMME

THE BASICS

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 mobile messaging ecosystem is not a uniform, one size-fits all environment. It 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 where they exist. 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.

Historically, there has been a lack of accountability and arguably a lack of commitment from some parties to address fraud for various reasons:

- Many types of fraud are complex and varied
- Fraud impacts different parties in different ways and to different degrees of severity
- Some types of fraud can only be prevented at certain points within the message delivery chain
- Levels of awareness and understanding of fraud are not consistent across the messaging delivery chain
- Affected parties may not be aware that they have been targeted
- A lack of investigation into or consequence for those engaged in fraudulent activities

The impact and consequences of fraud are felt globally. However, 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.

THE IMPACT OF FRAUD

In 2016, the global enterprise mobile messaging sector was forecast to be worth $17.2 billion, rising to $58.7 billion in 2020 [1].

However, 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.

The direct monetary losses being incurred by the industry through fraud are significant. In May 2016, MEF's Messaging Programme Founders estimated that fraud was costing the ecosystem at least $2Bn annually.

This number is relatively conservative when compared to figures from mobilesquared which calculated that between 2015 and 2020, revenue leakage within the global market which is attributed to traffic which cannot be monetised by an MNO due to the absence of an AA.19 Agreement is worth $82.1 billion.

Mobilesquared further calculated that if this area of revenue leakage was stopped and the traffic monetised, the global enterprise mobile messaging market would be worth $31.8 billion in 2016, rising to $70.1 billion in 2020.

However, the real impact of fraud on the global ecosystem extends beyond the direct financial losses incurred by MNOs failing to monetise enterprise mobile messaging traffic, as set out below:

[1] Source: mobilesquared - *Global A2P messaging forecasts overview 2015-2020*

THE BASICS

THE IMPACT OF FRAUD Cont./

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 one-time PINs
  - 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 the receiver pays for the receipt of messages, eg, 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 MNOs retail consumer offer can be leveraged at a more competitive rate than the official enterprise mobile messaging rate or interworking agreement rate
  - enterprise mobile messages can be bought for a specific destination at a rate lower than an MNOs 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

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 advertising

Loss of Trust in Enterprise Mobile Messaging

- Legitimate messages may be ignored if consumers believe them to be annoying, irrelevant or even intrusive
- Increased uncertainty amongst enterprise, consumers and regulatory agencies about enterprise mobile messaging 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 an enterprise
- 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 or even a known brand
  - innocuous messages masking something more sinister

THE BASICS

THE IMPACT OF FRAUD Cont./

Reputational Damage

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

Unfair Market Environment

- Messaging providers who do not participant 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 enterprise mobile messaging is 'high risk' and may discourage its adoption and negatively impact the growth of the market

COMBATTING FRAUD

As long as the short term but damaging opportunities to make money through fraud win out over the long-term health of the industry, the longer-term consequences for the whole industry will worsen. The bar will simply continue to drop if the incentives to act with integrity continue to be eroded by fraud. The 'bad' will simply move onto the next short-term opportunity, while the 'good' are forced to make certain decisions if they wish to remain on a level playing field. Ultimately, everyone will lose.

There is a chance to break the cycle of a race to the bottom in chasing low-cost traffic and instead to work together, cross-ecosystem, to protect this sector and engender trust in messaging as an established, viable, reliable and ubiquitous method of communication. There are opportunities to open messaging up to new verticals, and building on the solid foundations of the sector, to develop exciting new solutions including those described in MEF's Future of Messaging Guide.

The alternative to positively tackling fraud is the continued erosion of the sector through loss of trust in enterprise mobile messaging, closing the door to new opportunities, and eventually constricting the way in which businesses and their customers communicate with each other, in a world where access to telecoms for a significant proportion of the world's population currently remains via GSM network.

Cross-ecosystem collaboration is essential to tackle fraud effectively within the enterprise mobile messaging ecosystem. No one member of the community can make the necessary changes on their own without the support of the rest of the ecosystem. Raising levels of awareness about fraud is one of the most effective ways to proactively tackle it. This framework enables all of those within the ecosystem to understand how to better protect themselves and their customers and support the long-term and viable growth of the global enterprise mobile messaging ecosystem.

The support of the MNOs globally will be key to ensuring success – they control access at either end of the message delivery value chain, enabling a message to enter the chain and to exit on delivery to their own customer. There are currently no effective mechanisms at the forefront of the industry to address fraud on a comprehensive and global level. However, within MEF's Messaging Programme, with the active support of MNOs and in collaboration with the whole ecosystem, MEF's planned Certification Scheme will make significant inroads into addressing and reducing fraud globally.

FRAUD TYPES

IDENTITY THEFT: SMS ORIGINATOR SPOOFING

DEFINITION

SMS Originator Spoofing [Spoofing] is the act 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 random originators, which falls under SIM Farm Fraud.

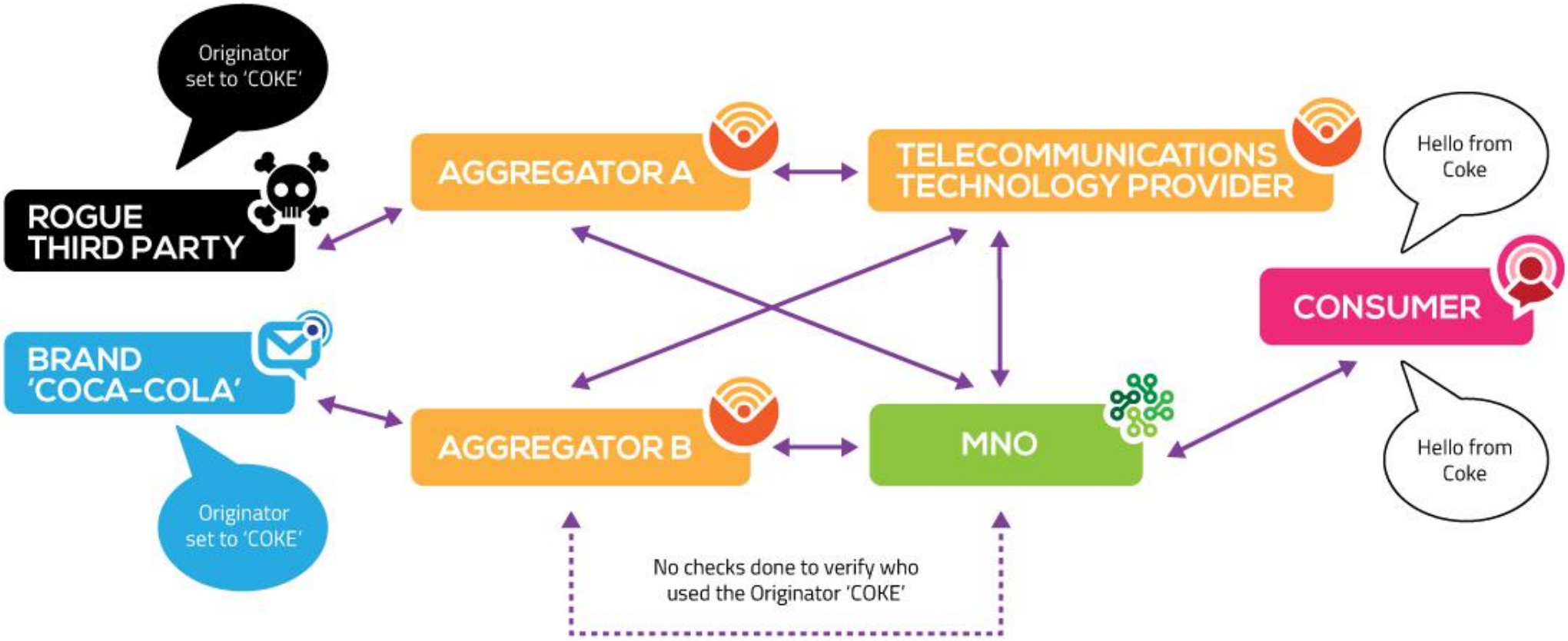
CAUSE

- Lead generation by pretending to be a known company to verify whether a MSISDN is live and active, or to generate new business, eg, 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
- SMiShing (SMS Phishing) to extract sensitive personal and confidential financial information to try and steal from a mobile subscriber

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.

SMS ORIGINATOR SPOOFING



IDENTITY THEFT: SMS PHISHING

DEFINITION

SMS Phishing (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.

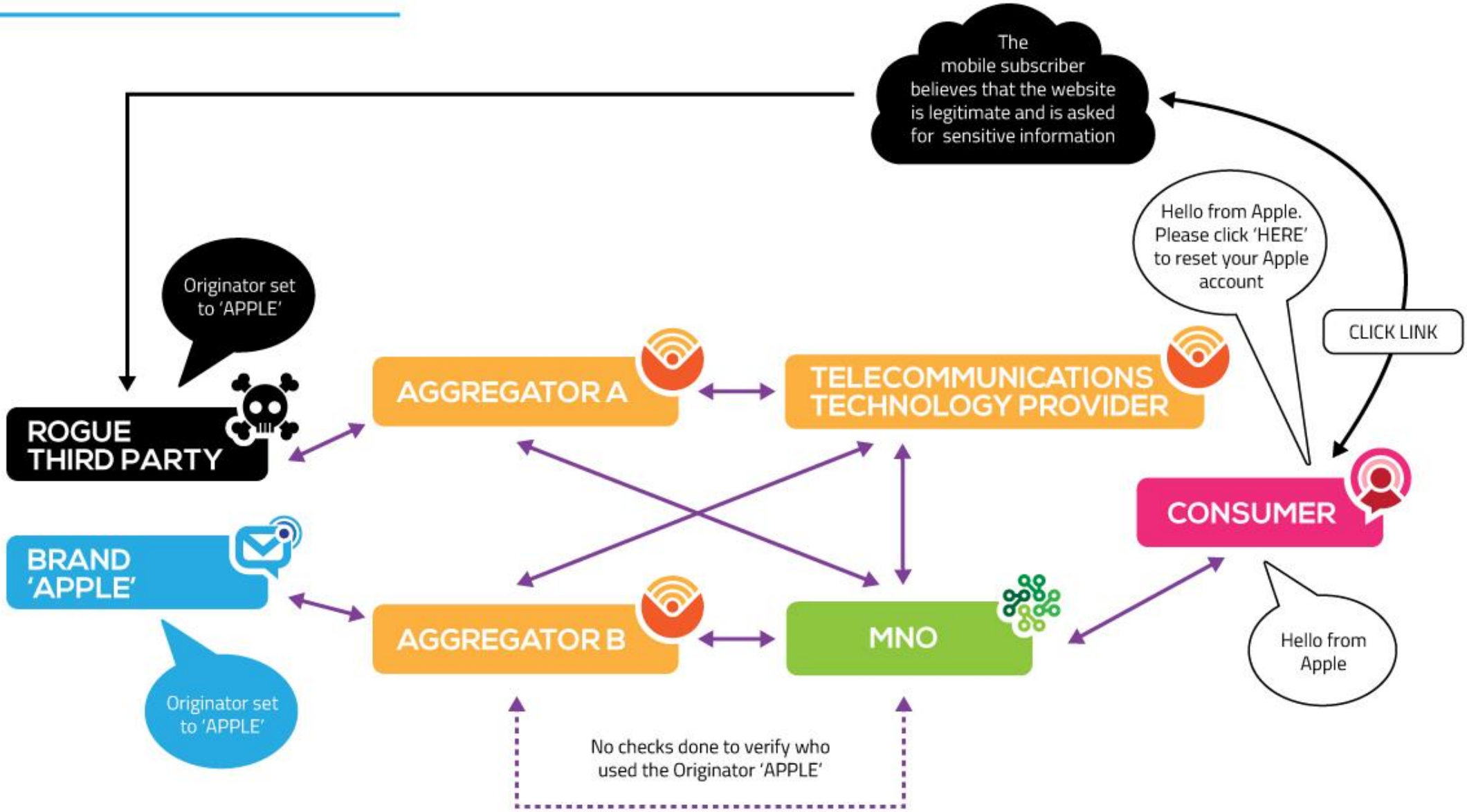
EXAMPLE

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 data loss
- Increasing incidence in line with the growth of smartphone adoption and reliance of mobile applications
- The ease with which consumers can be fooled through the use of basic social engineering and masquerading technique 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 and proactively reiterating what channels they use to communicate with their customers and what information and will not ask for under any circumstances
- Poor regulation of the providers of enterprise mobile 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

SMS PHISHING



IDENTITY THEFT: ACCESS HACKING

DEFINITION

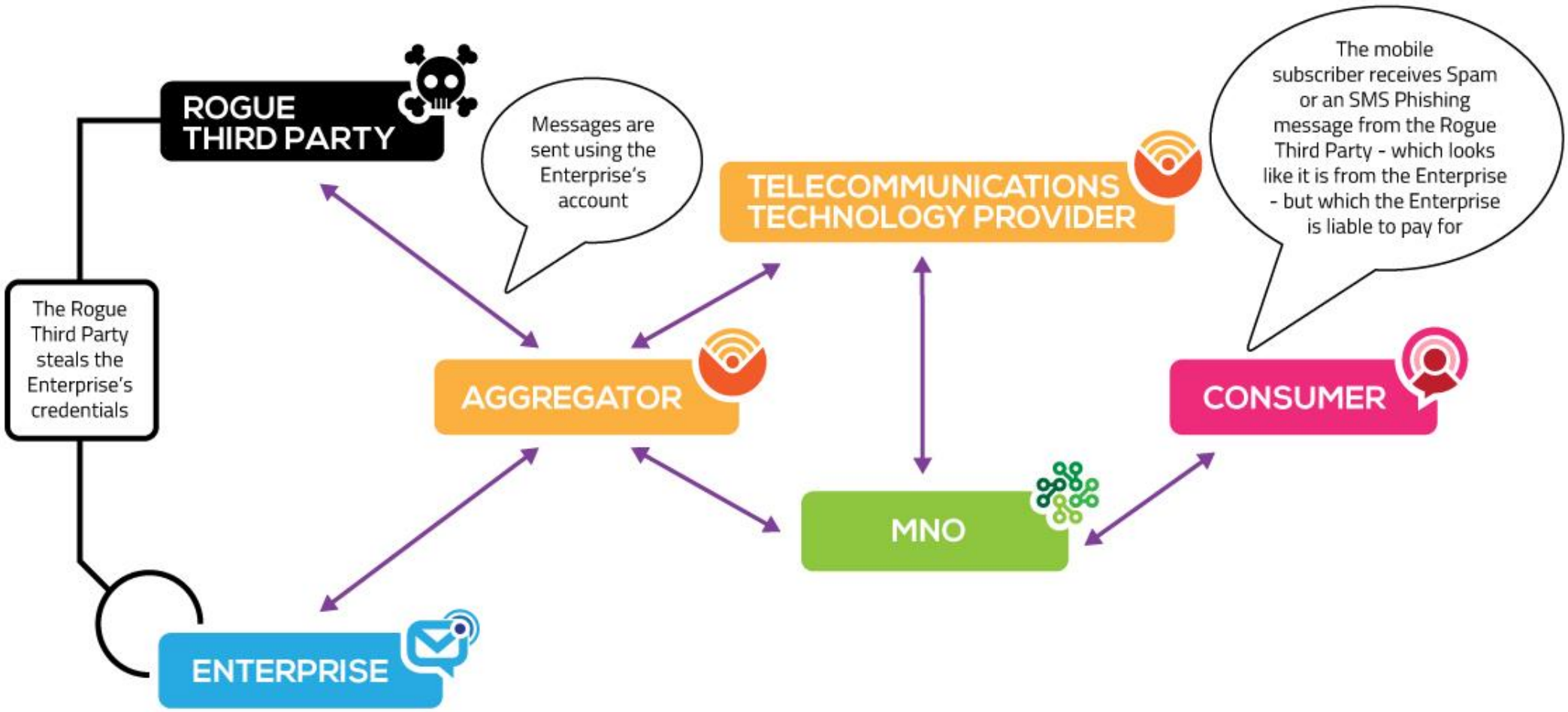
Access Hacking is the act of hijacking the credentials of a legitimate third party, using at least one of the following techniques and using those credentials to send messages:

- 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 with no intention of paying for them

CAUSE

- The promise of financial gain, either directly or indirectly through data loss
- 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, but without paying for those messages
- The availability of free credit on SMS portals

ACCESS HACKING



DATA THEFT: SIM SWAP FRAUD

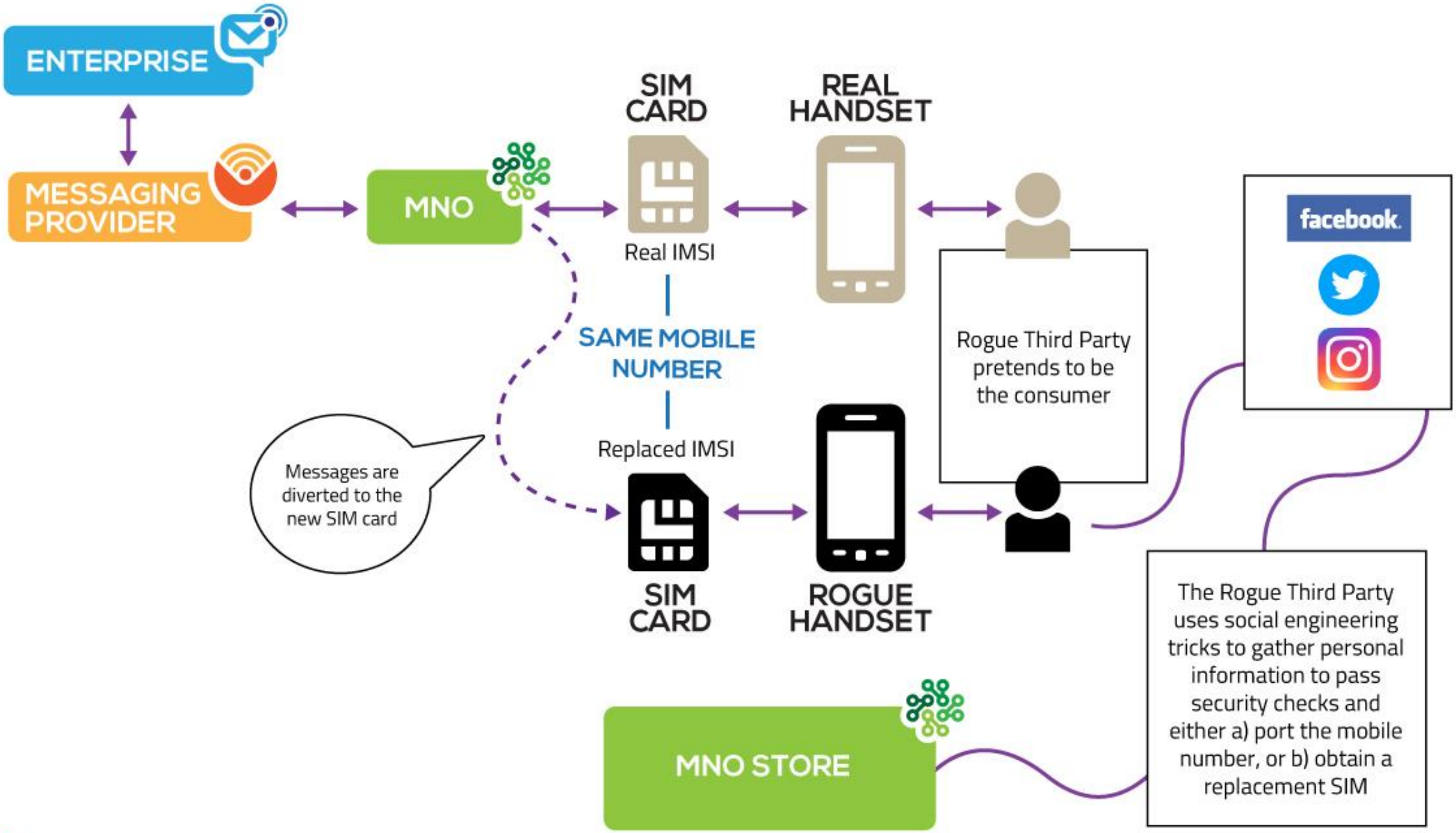
DEFINITION

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 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 gaining access to and control over a consumer's bank account 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 and address – with key personal information, a criminal can contact the consumer's MNO, purporting to be the account holder, to request a replacement SIM, perhaps due to loss or damage.
- A secondary cause enables the re-routing of SMS messages and calls to the new handset, including the diversion of activation codes or authorisations needed for online bank transfers, such as a one-time pin or password to the criminal's own handset – enabling the criminal to potentially access the customer's bank account and transfer funds.

SIM SWAP FRAUD



DATA THEFT: SMS ROAMING INTERCEPT FRAUD

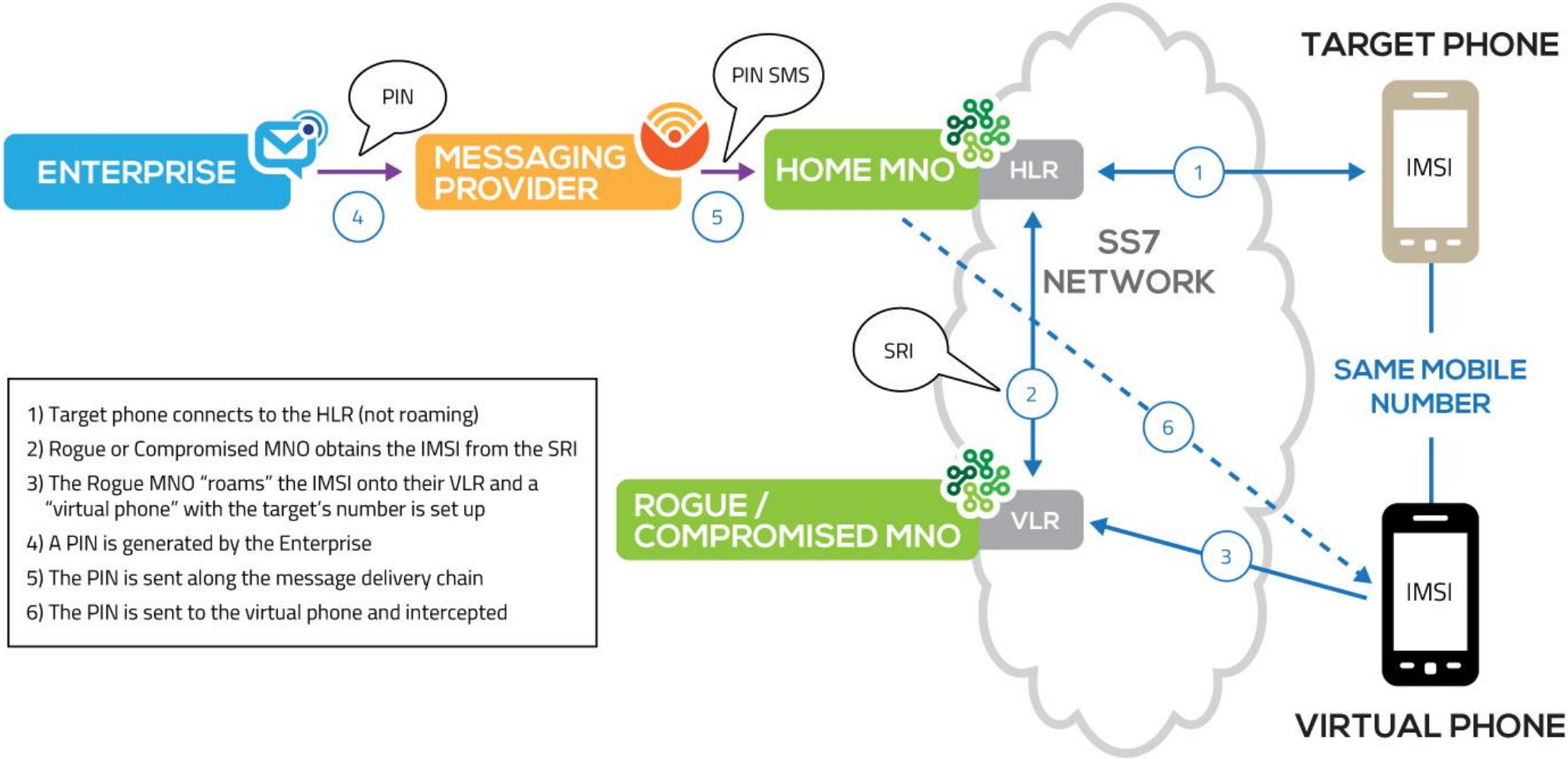
DEFINITION

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 a one-time password, 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

SMS ROAMING INTERCEPT FRAUD



1) Target phone connects to the HLR (not roaming)
2) Rogue or Compromised MNO obtains the IMSI from the SRI
3) The Rogue MNO "roams" the IMSI onto their VLR and a "virtual phone" with the target's number is set up
4) A PIN is generated by the Enterprise
5) The PIN is sent along the message delivery chain
6) The PIN is sent to the virtual phone and intercepted

DATA THEFT: 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.

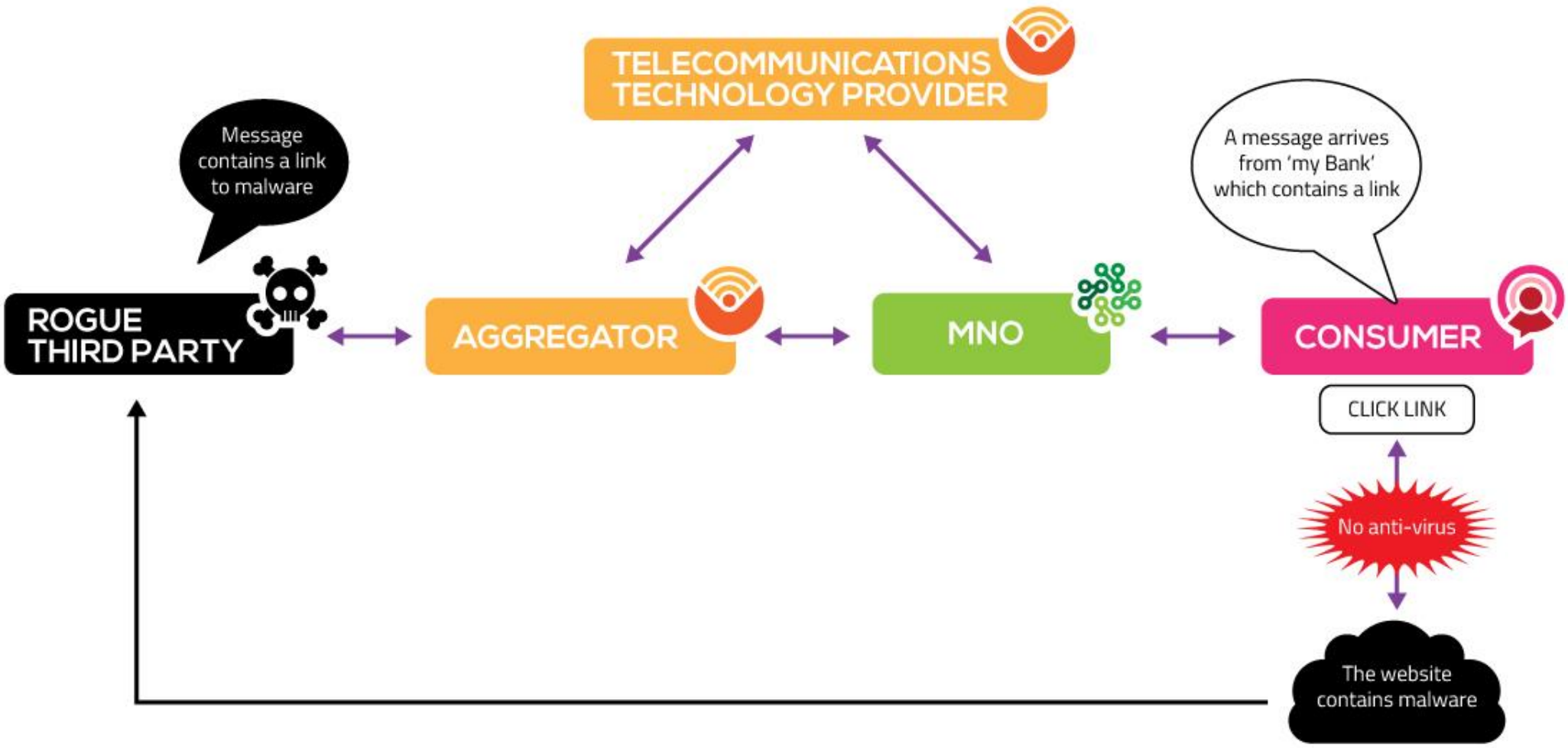
CAUSE

- The promise of financial gain, either directly or indirectly through data loss and through the ability to sell connectivity to third parties
- Increasing incidence in line with the growth of smartphone adoption - malware can affect any smartphone connected to the internet, on Android, Apple, Windows etc
- Malware can often go 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.

SPAM MALWARE (SMS HACKING)



NETWORK / SYSTEM MANIPULATION: MAP GLOBAL TITLE FAKING

DEFINITION

MAP Global Title Faking is the act of an individual or company manipulating the enterprise mobile messaging environment by:

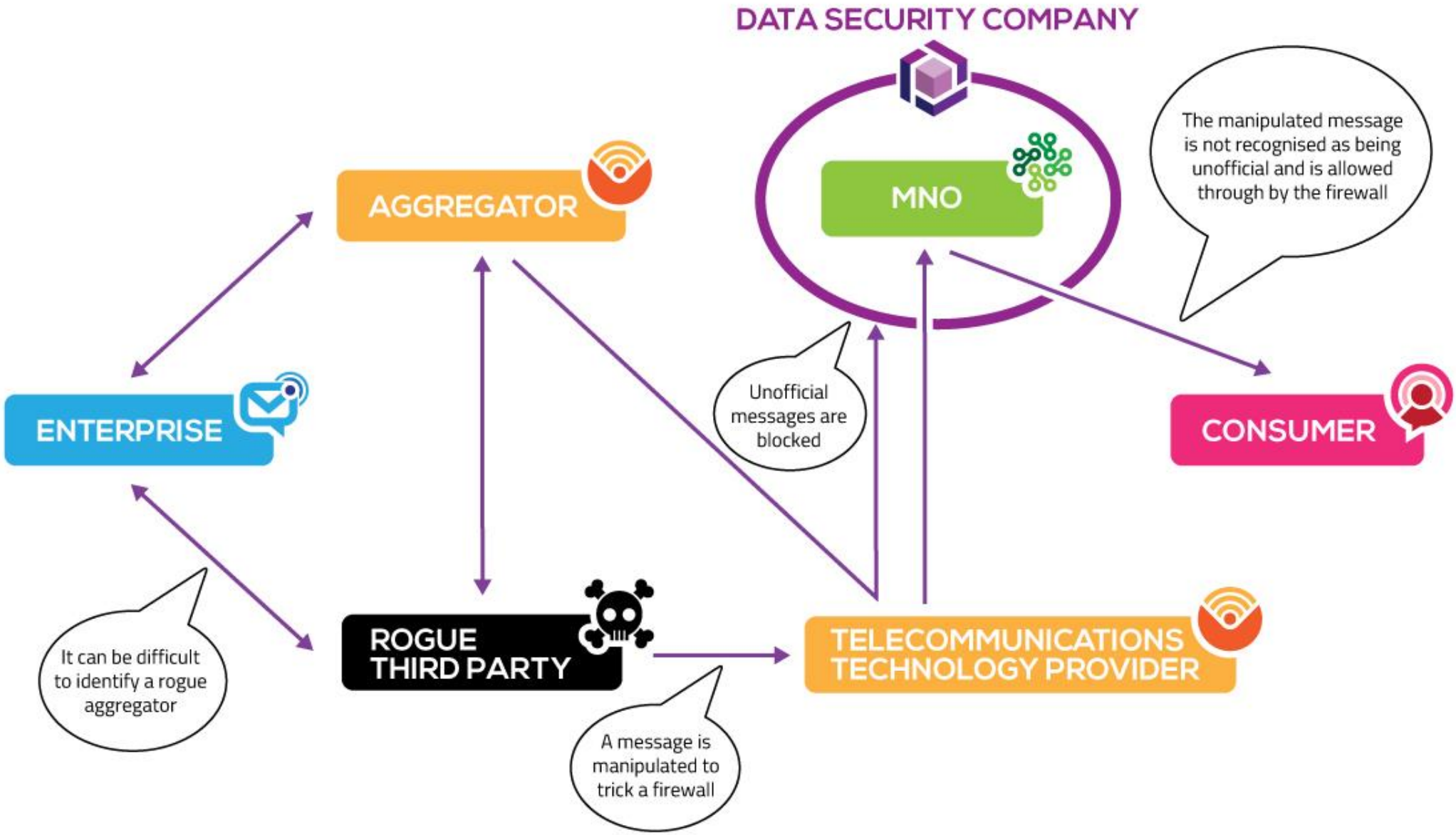
- manipulating a message by changing a MAP parameter
- changing the originator in order to prevent detection by a firewall, or
- pretending to be an MNO which does not have a commercial agreement in place with the sender

The entity generating the fraud has access to the International SS7 Network and by subverting 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 MNOs 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 enterprise mobile messaging 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 enterprise mobile messaging and its business applications
- Price-led procurement activities carried out by messaging providers and some OTT players via enterprise mobile 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 enterprise mobile messaging teams, as well as between business stakeholders and procurement teams

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



NETWORK / SYSTEM MANIPULATION: 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 either:

a) does not belong to the sender or,

b) has been leased from a third party but where the SCCP or MAP addresses are manipulated

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:

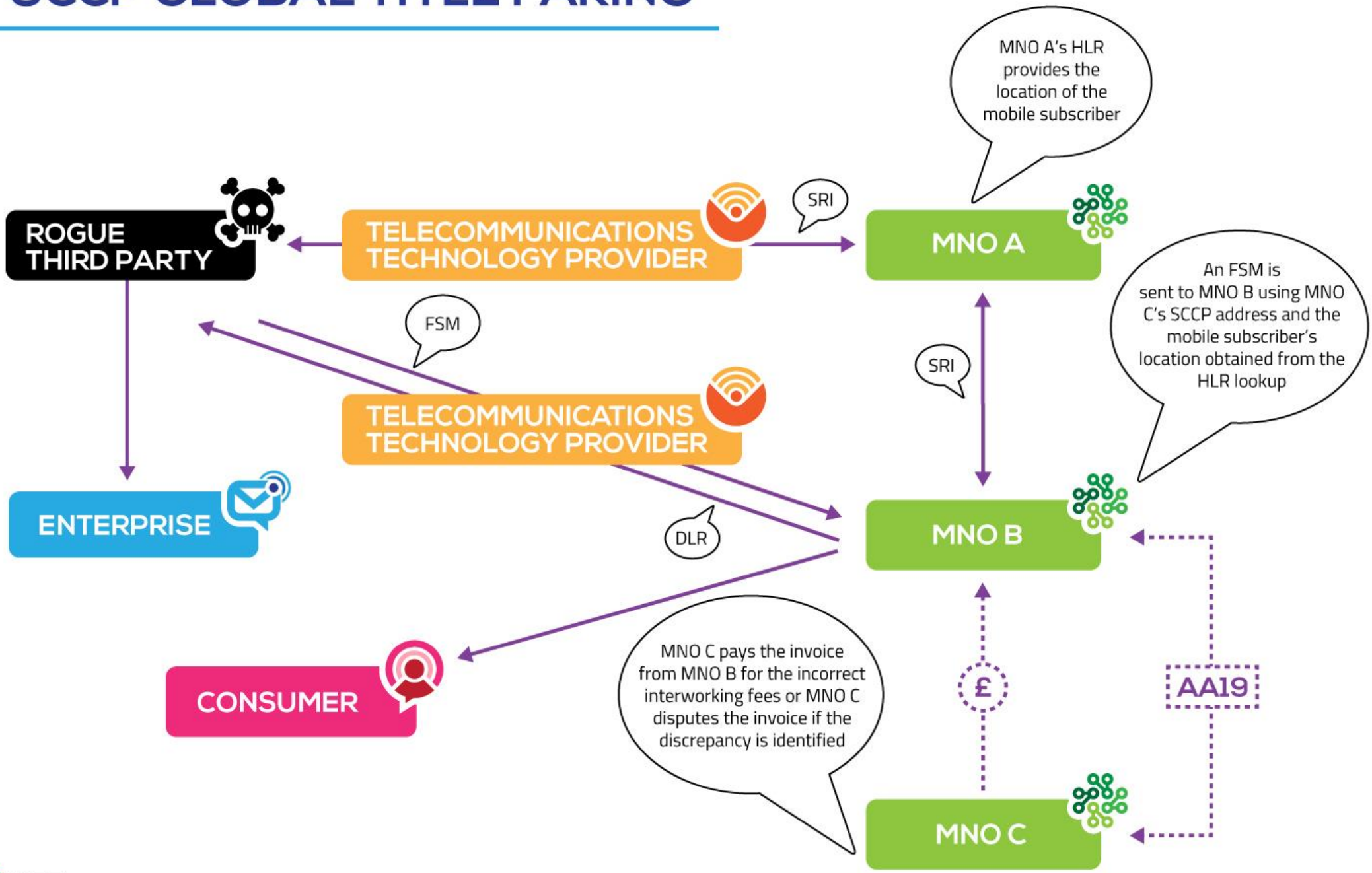
1. A leased Global Title is used to send both the SRI (send routing information) and FSM (forward short message) requests. Similar to a Grey Route, the messaging provider using the leased Global Title must have an agreement from the sponsor MNO [the Global Title owner] in order to use it and will normally pay a transit fee to the sponsor MNO. The Global Title is implemented on the messaging provider's side, so the messaging provider will send a message using this Global Title. It will appear to the destination MNO as if the sponsor MNO was sending the message. In addition, if the leased Global Title is implemented at the messaging provider side, the sponsor MNO must redirect all SS7 traffic to this leased Global Title under their agreement.
2. A leased Global Title is used to send only the SRI in order to obtain necessary information such as IMSI (international mobile subscriber identity) and VLR (visitor location register). Another Global Title is then used to send the FSM. Sending the FSM is purely unidirectional as a FSM confirmation is not needed. In order to send the SRI, a response is needed, so the MNO leasing out the Global Title needs to reroute the SRI back to the messaging provider. In this scenario, a different Global Title is used to send the SRI and the FSM.

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 they own the address space and it can therefore be easily manipulated
  - Telecommunications technology providers are not incentivised to proactively monitor their address spaces as they make money on Message Signal Units (MSUs)
  - MNOs are not adequately protecting their own network by assessing traffic which is legitimately destined for and arriving into their network versus a third party using their Global Title to send traffic to another MNO
  - An interworking agreement may exist between the sending (according to the Global Title being used) and receiving MNOs, but there is no requirement that traffic be balanced across all MNOs in a destination country, meaning that messages can be sent below the interconnect agreement level and not detected - if there is a requirement to balance traffic, the messaging provider might be selling some MNOs at a loss but will intend to make money on the total traffic delivered
  - There are no coherent end-to-end processes in place to identify unambiguously the fraudulent parties who therefore remain in plain sight without facing any consequences
  - 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

SCCP GLOBAL TITLE FAKING



NETWORK / SYSTEM MANIPULATION: SMSC COMPROMISE FRAUD

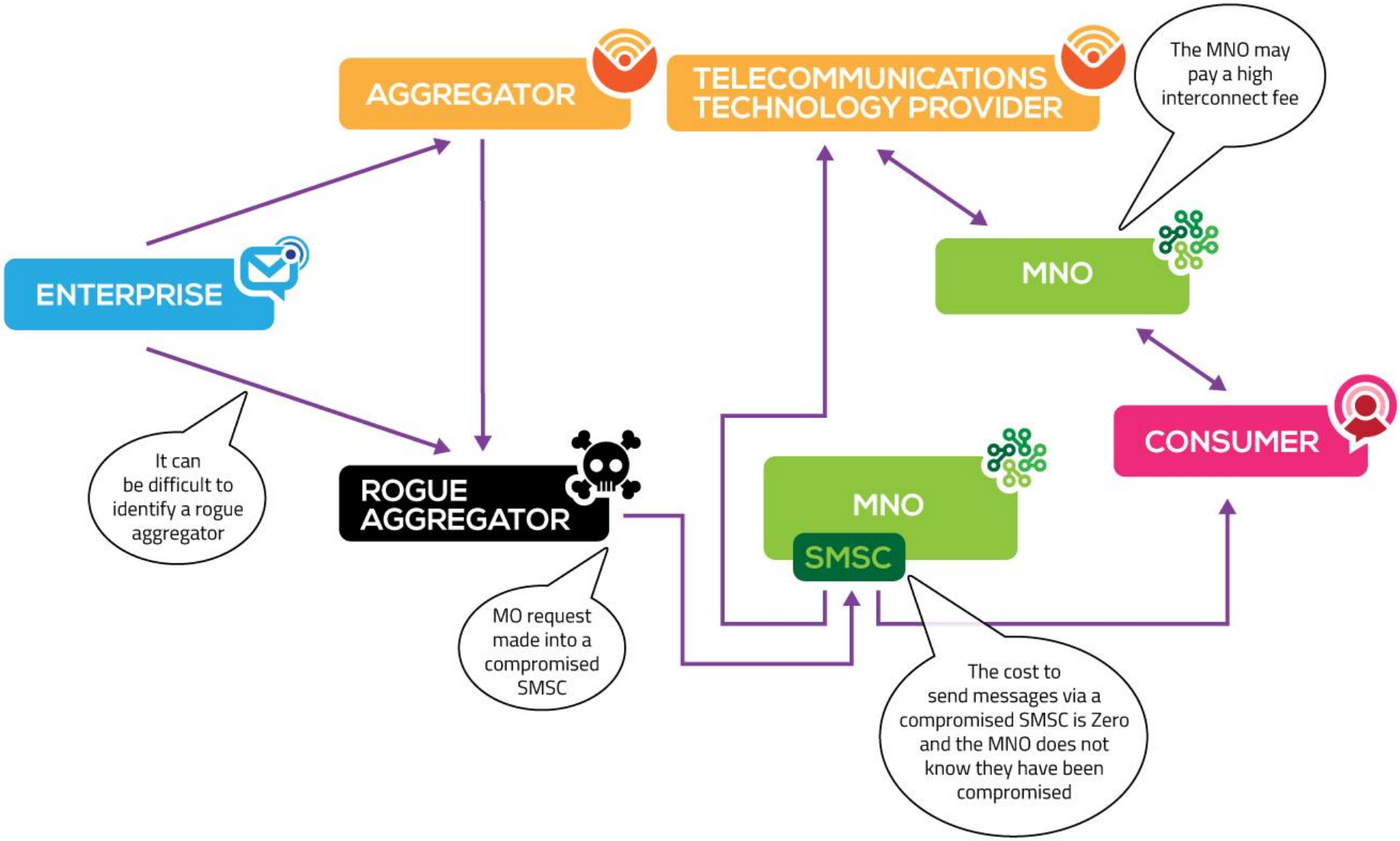
DEFINITION

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
- An enterprise can buy an enterprise mobile messaging solution at a cheaper rate than the official MNO rate

SMSC COMPROMISE FRAUD



COMMERCIAL EXPLOITATION:
GREY ROUTES, BYPASS, NON-INTERWORKED OFF-NET ROUTES

DEFINITION

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, sending enterprise mobile messages via an MNO's P2P Hub or via a roaming signalling link, which are not authorised by an MNO to carry such traffic, including the termination of international traffic via national routes designated only for delivery of domestic traffic which has a lower SMS interworking fee than on designated international routes.

It is currently common practice for enterprise mobile 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 enterprise mobile messaging, when P2P traffic between MNOs was generally balanced and only small net amounts needed to be settled between the sending and receiving parties.

The use of open routes without a commercial agreement in place is not fraudulent, but rather, opportunistic. Where there is no alternative way to send an enterprise mobile message, for example, if the sending MNO will not sign a commercial agreement for the termination of messages, either directly via an enterprise mobile messaging agreement, through AA19 on SS7, or via a Hubbing connection, then sending an enterprise mobile message without a commercial agreement in place will be deemed legitimate and falls outside of this definition.

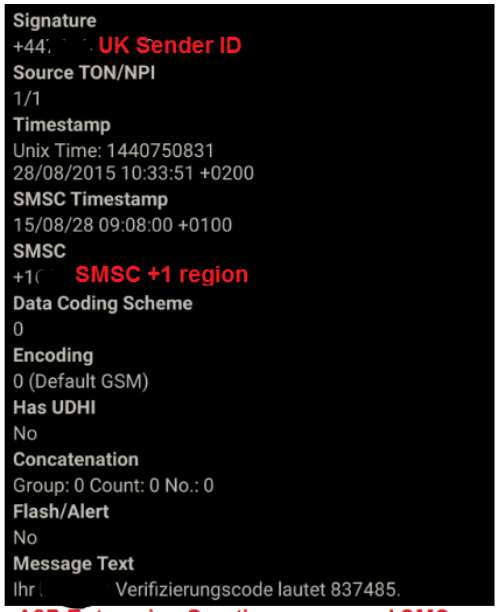
To note: If a message is manipulated in anyway, either by changing the Global Title in the MAP layer or, by changing the originator to subvert a firewall and avoid detection, then this is captured as a separate fraud type called **MAP Global Title Faking**.

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 enterprise mobile messaging 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 enterprise mobile messaging and its business applications
- Price-led procurement activities carried out by messaging providers and some OTT players via enterprise mobile 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 enterprise mobile messaging teams, as well as between business stakeholders and procurement teams
- Insufficient controls in place to track, monitor and block traffic which is arriving from unauthorised routes

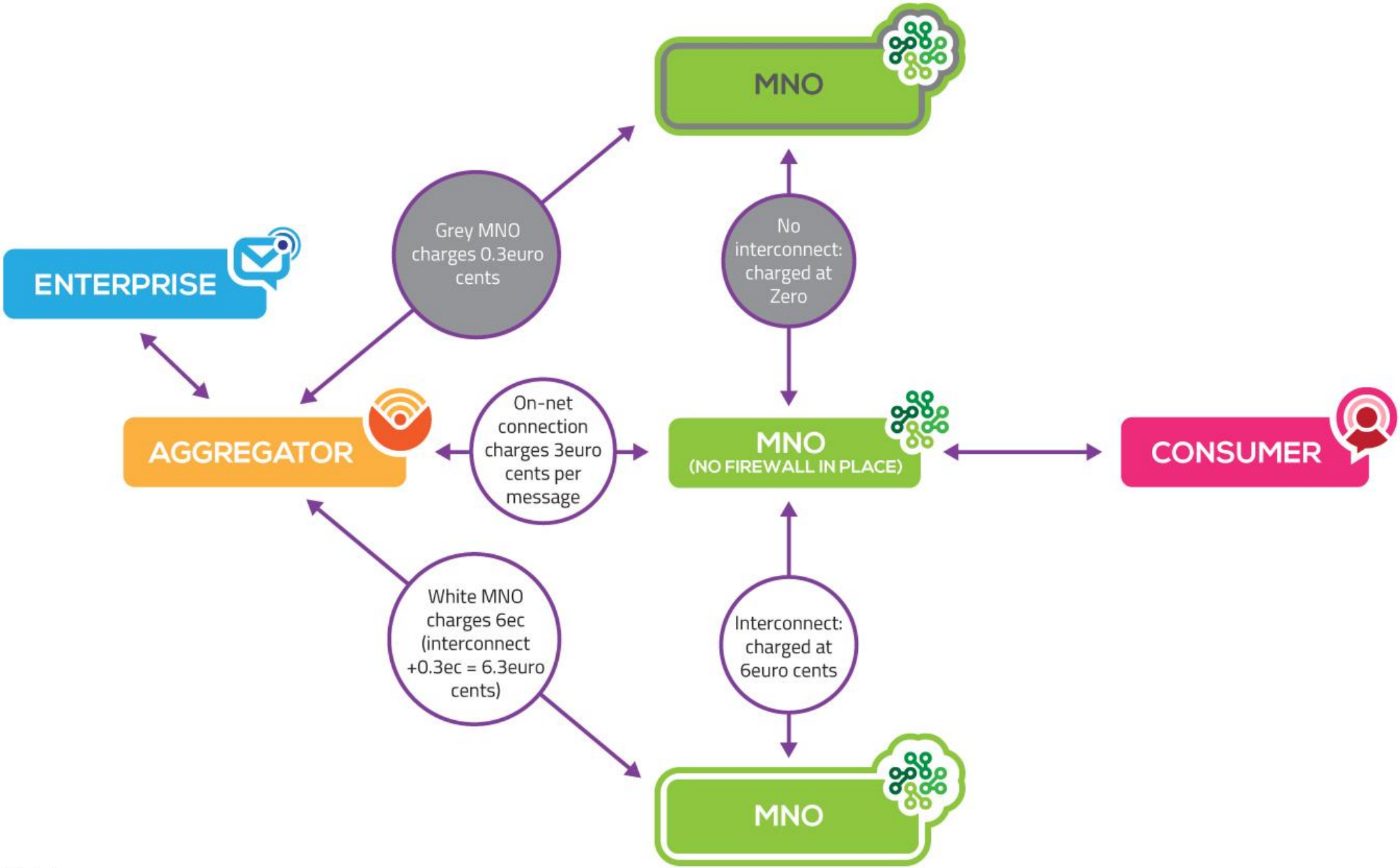
EXAMPLE

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



A2P Enterprise One time password SMS

GREY ROUTES DUE TO ABSENCE OF AA19/AA60 AGREEMENT



NETWORK / SYSTEM MANIPULATION: SIM FARMS

DEFINITION

A SIM Farm is a method of using a bank of SIM cards for the delivery of enterprise mobile messages 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
- Legitimate M2M or Enterprise SIMs which are sold without sufficient contractual protection to prevent them being used for enterprise mobile messaging

A variation of SIM Farming is the technique whereby a mobile subscriber acts as a "mini-SIM Farm" - a mobile subscriber downloads and installs an app provided by the perpetrator who then sends an SMS MT to the mobile subscriber who terminates it to the destination number.

This mini SIM Farm scenario requires:

- active participation by the mobile subscriber
- a consumer pricing plan with a low price for sending messages
- data connectivity (Wifi or 4G).

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.

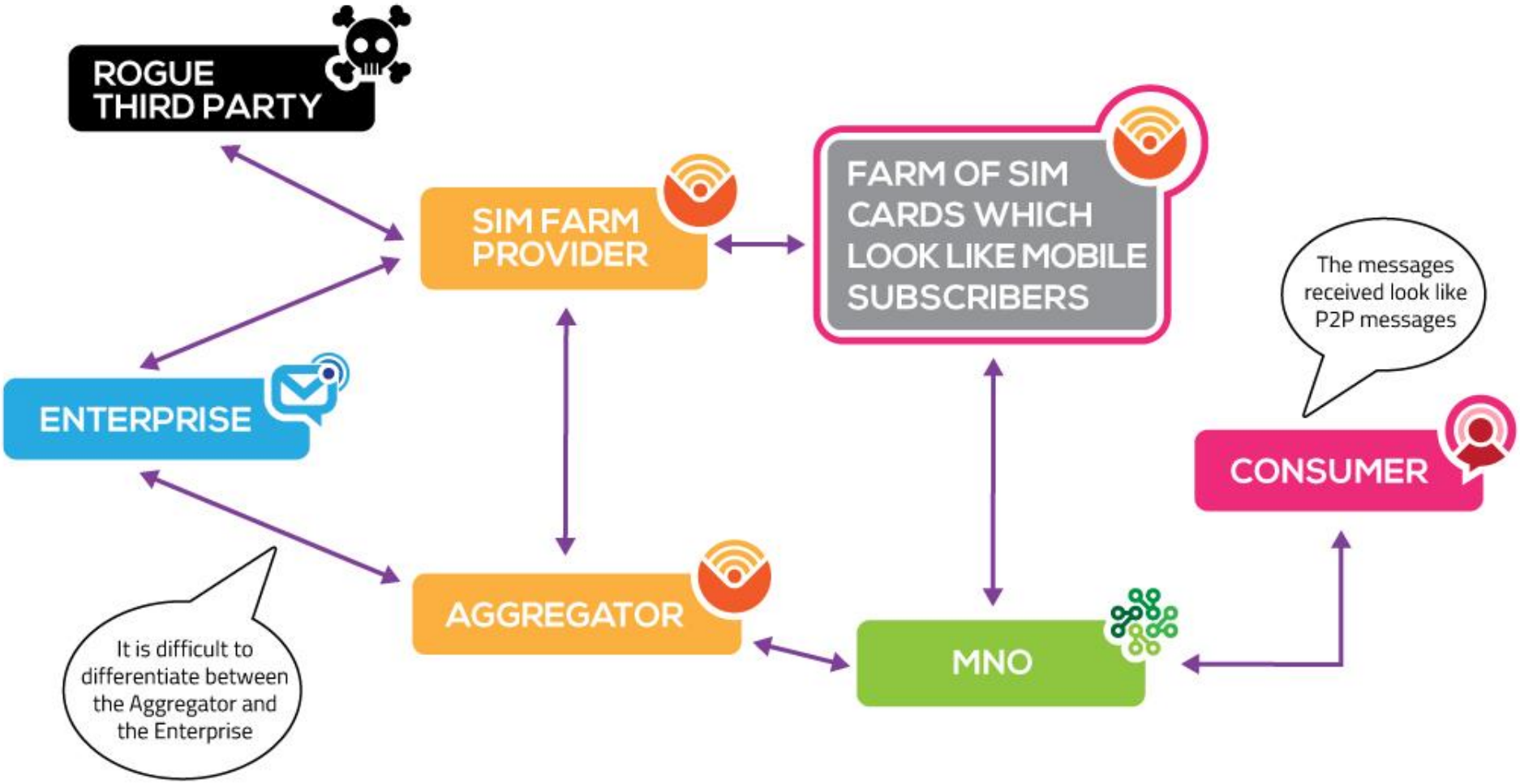
CAUSE

- Exploitation of an MNOs own retail, corporate or M2M SIM offeris, bypassing official Bulk SMS connectivity or interworking agreements and charges
- A messaging provider can avoid all interworking costs
- An enterprise can buy an enterprise mobile messaging solution at a cheaper rate than the official MNO rate

EXAMPLE

An example of a message sent using a SIM Farm.

SIM FARMS


ROGUE THIRD PARTY
SIM FARM PROVIDER
FARM OF SIM CARDS WHICH LOOK LIKE MOBILE SUBSCRIBERS
The messages received look like P2P messages
ENTERPRISE
CONSUMER
It is difficult to differentiate between the Aggregator and the Enterprise
AGGREGATOR
MNO

NETWORK / SYSTEM MANIPULATION: 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) companies in the UK
- 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 enterprise mobile messages and where those messages are all sent within the remit of a contractual agreement and national legislation, any such enterprise mobile message cannot be termed Spam for the purposes of this framework.

Typical ways to opt-in to and give permission for the receipt of enterprise mobile messages 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.

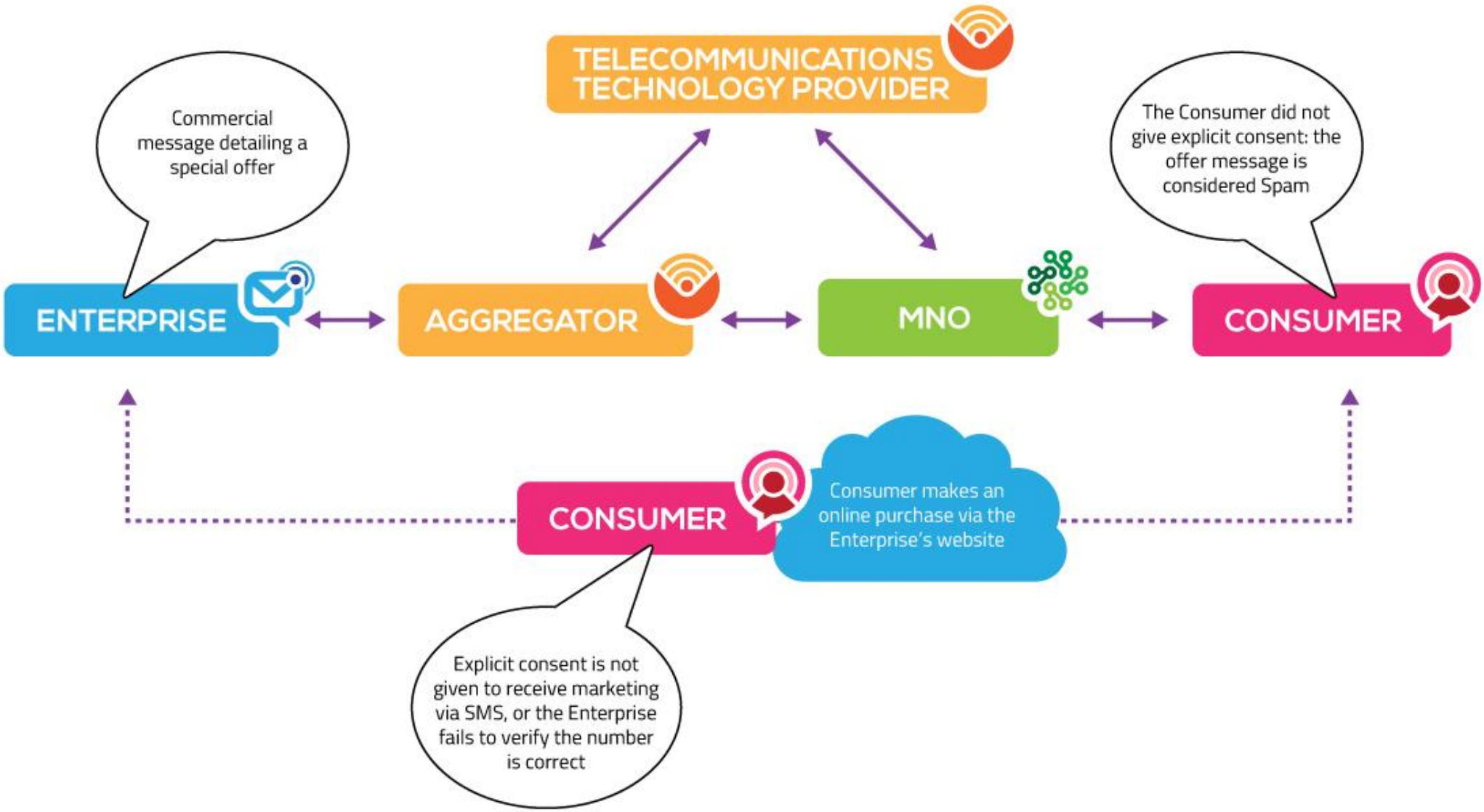
CAUSE

- 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
- Enterprise mobile messaging can be sent in large volumes - the more consumers who are made aware of a product, the more sales can be achieved
- Enterprise mobile messaging has significantly higher delivery and open rates compared to most other forms of marketing, 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.

SPAM


TELECOMMUNICATIONS TECHNOLOGY PROVIDER
Commercial message detailing a special offer
The Consumer did not give explicit consent: the offer message is considered Spam
ENTERPRISE
AGGREGATOR
MNO
CONSUMER
CONSUMER
Consumer makes an online purchase via the Enterprise's website
Explicit consent is not given to receive marketing via SMS, or the Enterprise fails to verify the number is correct

NETWORK / SYSTEM MANIPULATION: ARTIFICIAL INFLATION OF TRAFFIC (AIT)

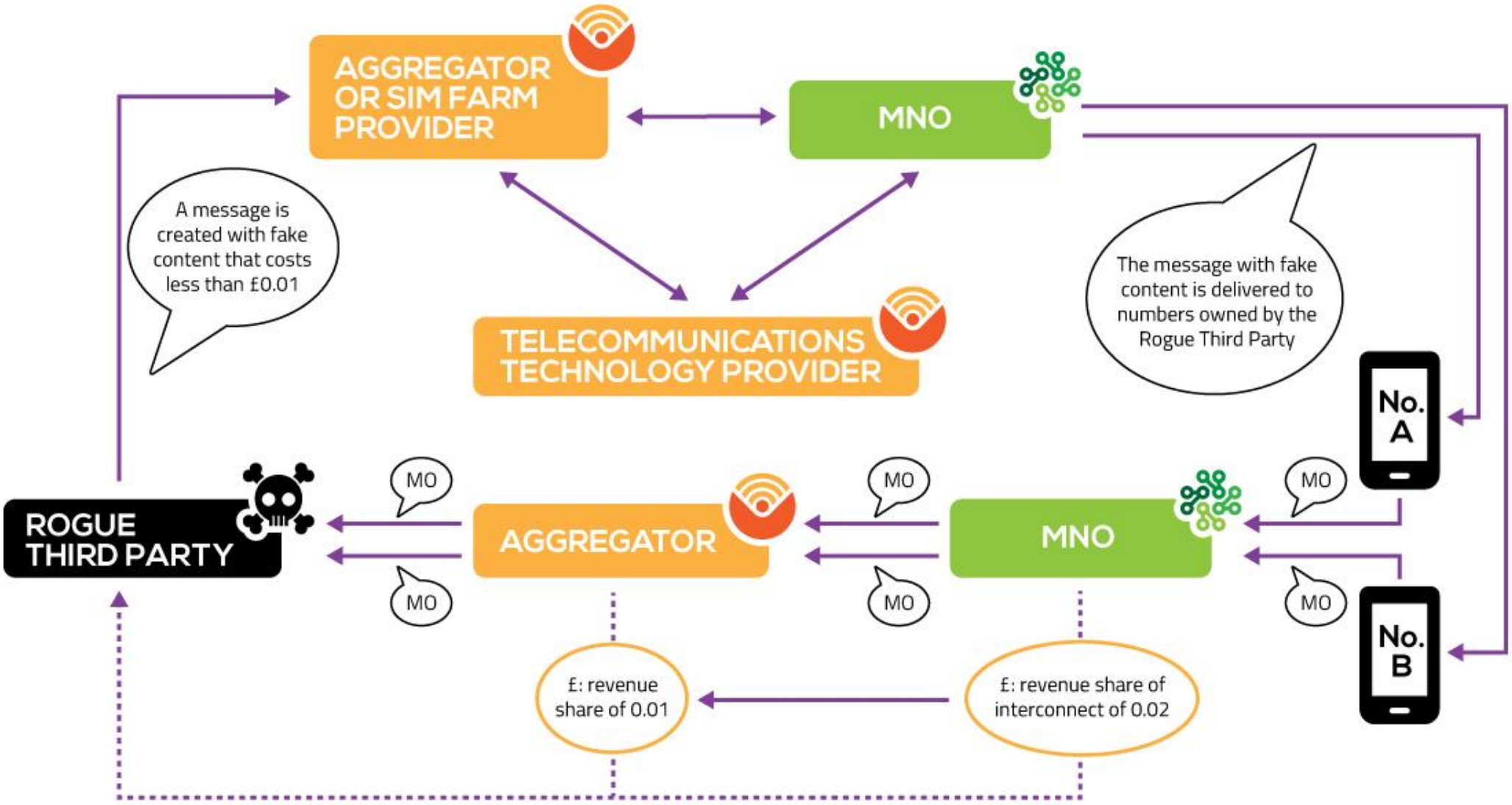
DEFINITION

Artificial Inflation of Traffic occurs when a party sends messages to itself 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

ARTIFICIAL INFLATION OF TRAFFIC (AIT)



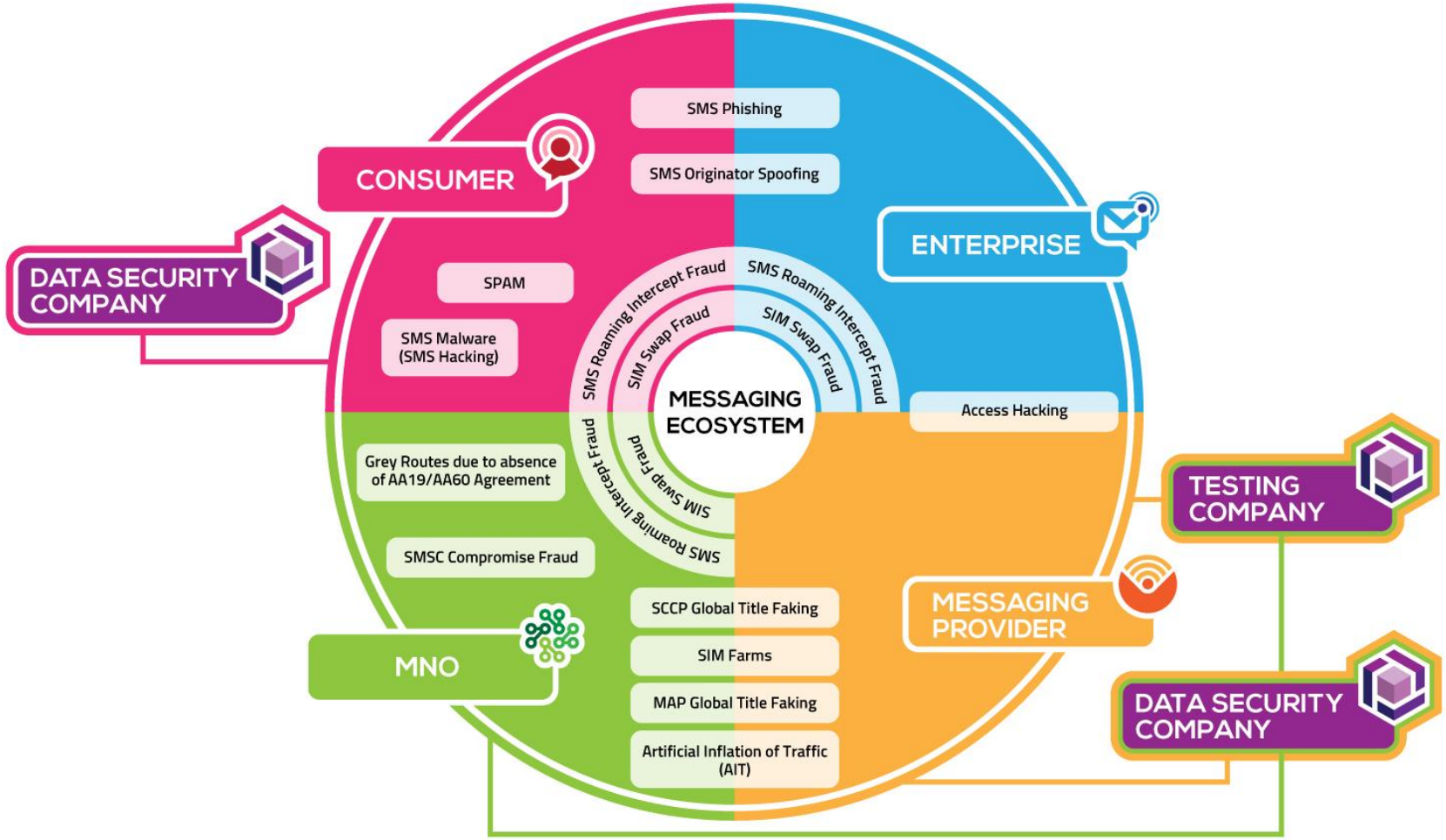
FRAUD MAPPING

This framework identifies 13 fraud types, each of which directly impacts on one or more of the four core communities within the enterprise mobile messaging ecosystem.

Some of the fraud types are highly complex and cut across a large proportion of the enterprise mobile message delivery chain.

The solutions identified to detect and protect against fraud include commercial, technical and process, compliance and legal requirements and will need cross-ecosystem collaboration to fully address and successfully implement.

THESE 13 FRAUD TYPES ARE MAPPED AS FOLLOWS:



PROTECTING AGAINST FRAUD

PROTECTING AGAINST FRAUD

Effective means to protect against fraud are already available, while others will require development and collaboration to make a long term impact on reducing fraud across the global ecosystem. Establishing and implementing consistent and coherent cross-ecosystem solutions will be key to targeting and driving out fraud from the enterprise mobile messaging sector.

COMMERCIAL SOLUTIONS

- Push and advertise the official market rates for enterprise mobile messaging
- Publish all MNO Exclusive Gateway Partners
- Publish all domestic Tier 1 Aggregators which are permitted to terminate international traffic into a specific country
- Publish all official routes:
  - Migrate bilateral 'sender keeps all' routes to SMS Hubs to monetise traffic without impacting P2P revenue streams
  - Keep open important bilateral routes under commercial AA.19/AA.60 agreements where required
  - Close any remaining unofficial routes
- Ensure that the price of an enterprise mobile message has a minimum threshold that can act as a barrier to mass, non-targeted campaigns, for example, set the cost of an MT message at a higher rate than the revenue share for an MO message
- Do not pay out revenue share on MO's for interconnect except in very special circumstances, for example, where a number of unique consumers are engaging in a service or there is an equal market share contribution across MO's
- Increase communication between MNO Retail and enterprise mobile messaging teams to flag the misuse of SIMs intended for the retail, M2M or corporate market
- Increase controls and checks on who is bulk buying SIMs via retail channels
- Place sufficient contractual protections on retail, M2M and legitimate corporate SIMs to prevent them from being used to send enterprise mobile messages
- Implement revenue protection controls so that SIM cards not authorised to send enterprise mobile messages can be quickly identified and terminated
- Carry out thorough reconciliation of interworking feeds as early in the reconciliation and payment flow process as possible to identify any discrepancies which might indicate that a Global Title is being used for Faking - where interworking reconciliation happens a few months after traffic was sent, and an ongoing discrepancy is identified, traffic can still be stopped and investigated by an MNO

PROTECTING AGAINST FRAUD

TECHNICAL SOLUTIONS

Available now

- Secure websites and SMS Portals to prevent them being compromised, for example, by preventing the automation of accounts and messages by bots where free credit is given
- Monitor the use of credit by new customers and flag any suspicious activity
- Install and configure firewalls and checks within MNO networks, SMS Hubs, enterprise networks, SMSCs and SMS Portals to:
  - filter and identify suspicious or unknown messages or messages arriving from an unauthorised source
  - allow the delivery of legitimate enterprise mobile messages where configurations are set to detect static originators
  - ensure active and continuous monitoring within a firewall to detect attempts to bypass filters, such as by:
    - the use of MSISDNs as an originators
    - changing message content
    - blending several Grey Routes to reach one destination
  - look for patterns within traffic, such as:
    - large volumes of unexplained MOs
    - MOs sent from a large range of sequential numbers
    - a majority of MOs sent across one MNO network
    - suspicious content, eg, messages containing random content that does not appear connected to the sender
    - Suspicious URLs
  - look for specific types of manipulation including:
    - any manipulation in a Service Centre address
    - comparing the received Service Centre address and calling party Global Title in the FSM to ensure that these match or at least partially match (in terms of leading digits)
    - whether the SRI request and the subsequent FSM request are sent from the same Global Title
    - whether a response to an FSM request has been received without any FSM request having been sent
    - lone FSMs destined for an MNOs subscribers where an SRI does not precede it
  - trigger an alarm if suspicious messages or manipulation is detected
  - block any message which is suspicious, unknown, is arriving from an unauthorised source, or appears to have been manipulated or subject to manipulation within the network - NB. An MNO cannot block a lone FSM for one of its subscribers where an SRI does not precede it if the subscriber is roaming as it would never see the SRI for a message terminated to a roaming subscriber - the SRI would be sent to the HLR of the roaming network. For example: FSM to a Proximus subscriber on Vodafone UK. Vodafone UK will only see the FSM. The SRI is sent to the HLR of Proximus.
- Monitor and manage the use of SCCP Global Titles and:
  - ensure that SCCP Global Titles and MAP Global Titles correspond
  - set SCCP alarms or reports, with random checks as a minimum, to verify that the calling party Global Title and Service Centre addresses match, or partially match
  - return only scrambled IMSIs

PROTECTING AGAINST FRAUD

TECHNICAL SOLUTIONS

Medium Term

- Allocate a dedicated national, cross-network short code to enable individuals to forward and report messages for investigation by MNOs. For example, 7726 (letters S.P.A.M. on a keypad) is assigned in Brazil (GSMA) the UK and the US.
- Install and configure fraud prevention software within enterprise networks to:
  - check and verify customer data and behaviours to assess risk, eg, date and time of the last SIM swap, date and time of change of handset, behaviour changes (sending/receiving messages or calls from locations the consumer has never been in), call forwarding, the number of calls made with the combination of handset and SIM card, associated connection with a tainted identity (identity confirmed to be fraudulent); SIM, device or TN used to commit fraud in the past, etc
  - analyse customers' historical mobile network data to help verify the authenticity of transactions and communications, eg, automatically flagging any data mismatches for certain actions, such as an account password request
  - Facilitate the communication of 'personal' information between an enterprise and their customer within an enterprise mobile message, such as a forename, secret word or phrase which their consumer has shared with them
- Secure HLR Lookup solutions to prevent them from being used to clean number lists created by brute force sequencing
- Permit the use of an HLR Lookup only with a specific agreement with a legitimate provider
- Monitor revenue flows to detect SIM cards which are not authorised to send enterprise mobile messages
- Share insights with MNOs about which companies are selling or reselling connections in different markets in real time
- Make information about recycled MSISDNs available so that number lists can be cleaned against it

Long Term

- Tier 1 aggregators should use a brand's CNAME in their domain (DNS record) to determine whether they are the true sender of the message - anything suspicious can then be blocked on a global basis
- Create a national and international register of enterprise, brands and all associated short codes and (alpha) originators
- Create a database of known suspicious and fraudulent messages which messaging providers can access both nationally and internationally
- Develop a global standard, automated cross-MNO method of reporting and sharing information about suspicious and identified fraudulent messages to support proactive detection and blocking of suspicious and unauthorised messages across the ecosystem

PROTECTING AGAINST FRAUD

PROCESS, COMPLIANCE & LEGALITY

Advice for Consumers

DO NOT:	DO:
ignore suspicious messages or activity, eg. if you stop receiving calls or texts, and you don't know why – report them to an MNO and enterprise	apply privacy settings to your social media accounts to limit access to you and your information only to those you proactively choose to share it with
disclose Internet banking password or personal identification number (PIN) to **anyone** - a bank will never ask for this under any circumstances	ask your bank to give you details of every financial transaction through two channels - for instance, SMS plus email alerts
share personal details on social media, eg, phone number, date of birth, maiden name etc	use separate email addresses for your Online Banking account / financial transactions and social media accounts
use the same password for all of your online activity - at the very least, have a completely separate password for your banking activity	be aware of fraudulent calls, e-mails or text messages which ask for personal details, or account details to be reset if not expected

PROTECTING AGAINST FRAUD

PROCESS, COMPLIANCE & LEGALITY

Advice for Enterprise

Communicating with your Customers

- Clearly display and promote in all customer-facing areas of your business:
  - your own short codes and keywords
  - customer care information
  - a summary of what a customer will and will not be asked for within a legitimate communication, eg, personal account information or PINs
- Initiate communication with any affected consumer which explains the next steps, follow up and actions

Data & Consent Management

- Implement effective data management processes, to include:
  - Update all consent and customer communication preferences immediately whenever a customer's status changes, eg, opting out of general or specific marketing communications, continued failed delivery of messages for a defined period of time etc
  - Reviewing and cleaning distribution lists against MNO recycled number lists
  - Monitoring complaints, particularly any spikes post campaign delivery or outside of formal campaign periods
  - Maintaining clear and accurate consent and opt-in details and customer communication preferences to ensure that all messages are properly targeted and their delivery is fully compliant

Data Security

- Invest in security technology to protect customer data and implement effective data security processes, including:
  - Solid authentication processes to protect customers, eg, with additional layers of security questions that cannot be answered by simply knowing a few personal details sourced from social media
  - Utilise number look-ups/checks as standard prior to sending confidential/personal messages, eg, checking for porting or SIM swapping etc
  - Utilise customer data (MNO/handset) and banking habits to assess risk, including SIM card information, device type, location data, and consumer behaviour
  - Ongoing training for contact centre and customer service teams to help agents better identify potentially fraudulent activity
  - Educate and inform customers to help them protect themselves
  - Company-wide escalation processes in the event of suspicious activity

Contractual Obligations

- Incorporate fundamental service requirements as contractual obligations for the provision of specific messaging solutions, eg, flexibility for originators, support for alpha originators were they are available, provision of DLRs for every message delivered etc
- Proceed with caution on the purchase of number lists
- Utilise tools such as number look-ups/checks as standard prior to sending confidential/personal messages, eg, checking for porting or SIM swapping etc

PROTECTING AGAINST FRAUD

PROCESS, COMPLIANCE & LEGALITY

Cross-Industry Recommendations

Collaborative Working

- Create a blacklist of companies which persistently send fraudulent messaging and share this within the global ecosystem
- Share knowledge of fraud cases
- Implement processes to:
  - Refer all suspected cases of fraudulent messaging to the relevant enforcement agency
  - Support the investigation of all cases by the relevant enforcement agency and imposition of appropriate sanctions for persistent repeat offenders
- Establish a globally agreed process involving forensic investigators, where the co-operation of all parties is required.
- Facilitate the end to end investigation of serious incidents by MNOs and SCCP providers to determine the true sender of a suspicious message before message logs disappear
- Greater oversight of free message sending sites, within which originators can be manipulated without registration or validation of identity of the message sender
- Support national and regional regulatory environments, including:
  - Outlawing the sale of 'number lists'
  - The use of originators defined for use in enterprise mobile messaging
  - The use of routes assigned for enterprise mobile messaging
  - The issue and use of Global Titles

Monitoring & Reporting

- Develop and implement a global Code of Conduct or Best Practice, to include what is and is not permitted within a messaging solution such as manipulation of messages, to remove any risk of ambiguity
- Develop a global standard, automated cross-operator method of reporting and sharing information about suspicious messages to all relevant national enforcement agencies to support the investigation of serious infringements
- Identify and report messaging providers selling enterprise messaging solutions at below market price
- Name and shame messaging providers who do not comply with agreed best practice or who continually seek to exploit MNOs
- Establish collaborative processes between MNOs and enterprise to share MNO customer data which can support combating SIM swap fraud, eg, making historical customer data available for lookup by a bank's fraud prevention solution that can then analyse the data to assess the risk of fraud
- Enable messaging providers to report any suspicious activity to a targeted MNO as quickly as possible, including:
  - Lower market pricing to a particular destination coming from known Global Titles that cannot be explained

PROTECTING AGAINST FRAUD

PROCESS, COMPLIANCE & LEGALITY

Cross-Industry Recommendations

Contractual Obligations

- Establish back to back contracts along the length of the whole enterprise mobile message deliverychain to ensure that the described route used to send an enterprise mobile message is authorised, legal and that all relevant parties are accountable
- Cloud Communications Providers must verify that the address space being used by a sender is correct in real time
- Establish Due Diligence and Suspicious Messaging processes for all new and existing buyers of messaging solutions, including but not limited to:
  - Verification of a D&B number registration for portals before allowing anymessages to be sent
  - Scrutinising the allocation of credit issued to new customers
  - Requiring credit card registration before allowing anymessages to be sent
  - Permitting only long numbers until a customer has demonstrated that they are who they say they are
  - Requiring under contract that message originators must be a recognised company name or the trading name of the sending partywhere alpha originators are permitted
  - Referral to the relevant regulatory or enforcement agencywhen serious infringements are detected
  - Withhold a full Global Title (MSC address) when selling SRI's - a country code fulfils the vast majority of legitimate use cases
  - Identify use cases where a full Global Title may need to be provided

Not recommended: Messages using alpha originators should **not** be prohibited. The ability to change an originator is an extremely important, flexible and popular feature of commercial messaging and can be used to identify an enterprise or to leave a contact number that could be used to reply to a message – alpha originators need to be tied to the sending company name in an automated way.

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 enterprise messaging solutions
- Promote enterprise mobile 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 and business

MEF FUTURE OF MESSAGING PROGRAMME

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

WWW.FUTUREOFMESSAGING.COM
WWW.MOBILEECOSYSTEMFORUM.COM

PROGRAMME PARTICIPANTS

BICS is recognized in the w holesale communications market as a top global voice carrier and the leading provider of mobile data services. It aims at bridging the telecom w orld w ith the new unconventional communication providers w orldwide.

BICS' innovative suite of solutions for Voice, Messaging, Data & Connectivity, Business Intelligence & Analytics, Fraud & Authentication, Roaming, MVNE and Asset Monetization bring value to its customers' businesses by enabling them to offer state-of-the-art communication services.

Its headquarters are located in Brussels and offers global connectivity with strong presence in Africa, Americas, Asia-Pacific, Europe and Middle East. Its regional offices are located in Bern, Madrid, Dubai, New York, San Francisco and Singapore, its satellite office is located in Beijing and its local representations are based in Accra, Cape Tow n, Miami, Montevideo, Nairobi and Toronto.

BICS is a pioneer into the future of next generation communications and have achieved a series of World's Firsts successes w ith the launch of the first LTE Roaming relation or the first VoLTE International call betw een Europe and Asia, to name a few . With a diverse and multicultural team of about 500 employees, BICS continuously strive to provide customers w ith the highest level of quality, reliability and interoperability, enabling them to maximize their end-user value.

CLX Communications connects enterprises to people and things. We combine programmable API's and cloud computing w ith our unparalleled Tier 1 Super Netw ork to make it easy for businesses to embed global communications, including voice, SMS and mobile data into their apps, business processes and IoT devices.

Our leading communications Platform-as-a-Service (CPaaS) delivers one of the highest service levels in the industry w hilst processing more than 1 billion API calls per month across 6 continents. We provide services to 4 of the top 5 CPaaS companies, and 3 of the top 5 global internet brands w ith Tier 1 connectivity on w hich many of their services rely.

CLX Communications (publ) is listed on the Nasdaq in Stockholm.

CM Telecom is a technology company that provides businesses w ith a single platform to enable (business critical) mobile messaging through push notifications, sms and voice messaging and mobile payments & security.

With offices around the w orld, CM Telecom serves more than 25.000 businesses including the largest internet companies. CM Telecom's platform is pow ered by its ow n self-designed infrastructure, supported by a 24/7 netw ork operations centre including in-house data centres and fibre netw orks across Europe.

Deutsche Telekom is one of the w orld's leading integrated telecommunications companies, w ith some 143 million mobile customers, 31 million fixed-netw ork lines, and more than 17 million broadband lines.

We provide fixed-netw ork/broadband, mobile communications, Internet, and IPTV products and services for consumers, and information and communication technology (ICT) solutions for business and corporate customers.

Deutsche Telekom is present in around 50 countries. With a staff of some 230,000 employees throughout the w orld, w e generated revenue of 60.1 billion Euros in the 2013 financial year, over half of it outside Germany.

PROGRAMME PARTICIPANTS

DIMOCO mobile messaging

DIMOCO Messaging provides carrier-grade, high quality messaging products enabling our clients to communicate to their customers on a truly global scale.

We leverage our relationships with Mobile Network Operators and in-country partners to offer clients Direct connectivity while combining local market expertise with fast message delivery.

DIMOCO Messaging holds an MNO license and operates a carrier-grade messaging platform with highest quality industry standards. We offer our clients the best way to optimize communication with their customers and employees by seamless integration to our platform, fully featured high quality products, multiple channels for instant support and advanced reporting and analytics tools.

Eclipsoft

Soluciones Tecnológicas del Nuevo Milenio

The Eclipsoft business group, operating as integrator of mobile services and working through a strategic alliance with mobile operators in Ecuador Claro, Movistar and CNT; We can bring our services to the large mass of users of cellular technology. We implemented interesting value-added messaging services.

– Technical and maintenance of the platform for sending and receiving messages Support.

– Mediation between the client and the cellular operator.

– Shipping Conciliation SMS messaging messages.

– Monitoring of traffic in the short codes from our customers.

– Mobile applications that can maintain real contact with their customers

We are leaders in this type of product at the level of banking

And we are innovative in content SMS portals.

iconectiv®

At iconectiv, we envision a world without boundaries, where the ability to access and exchange information is simple, secure and seamless. As the authoritative partner of the communications industry for more than 30 years, our market-leading solutions enable the interconnection of networks, devices, and applications for more than two billion people every day. Working closely with private, government and non-governmental organizations, iconectiv has intimate knowledge of the intricacies and complexities of creating, operating and securing the telecommunications infrastructure for service providers, governments and enterprises. iconectiv provides network and operations management, numbering, registry, messaging and fraud and identity solutions to more than 1,200 customers globally.

A US-based company, iconectiv, doing business as Telcordia Technologies, is a wholly owned subsidiary of Ericsson. For more information, visit www.iconectiv.com.

IMImobile

IMImobile is a leading provider of software and services that enables organisations with the ability to harness network, device and channel capabilities to improve service delivery and customer engagement.

We will help you to reduce the cost and complexity of digital service delivery across IT, marketing and customer support, leading to better customer journeys and customer experience.

With deployments in 60 countries, processing billions of digital touch points per month, we are a trusted vendor to blue-chip businesses around the world.

PROGRAMME PARTICIPANTS

Infinite Convergence provides innovative messaging and mobility solutions and next-generation wireless communication technologies to mobile operators and enterprises. Currently supporting more than 130 million subscribers and about 1 trillion messages per year globally,

Infinite Convergence offers, a complete range of scalable Enterprise Messaging Services, Rich Communication Suite, Converged Messaging, Public Safety Messaging, SMS, MMS, and Gateway solutions for businesses and Tier 1 wireless operators globally.

In addition to this, NetSfere is an award-winning, secure enterprise messaging service from Infinite Convergence, which provides enterprises with a private, reliable centrally managed and controlled, cloud-based messaging service.

Formed in 2010 from an alliance between Infinite Computer Solutions (BSE: 533154|NSE: INFINITE) and Motorola (now Nokia), Infinite Convergence has earned a reputation for delivering unparalleled performance and reliability in messaging and mobility. Although we are headquartered in Chicago, we are a truly global company, with a business presence in the USA, Germany, India and Singapore.

Since its start over a decade ago, Infobip has grown into an international business with 50+ offices and proprietary, in-house developed communications platform with the capacity to reach 6 billion mobile devices connected to over 800 telecoms networks.

Innovating at the intersection of internet and telecoms technologies, Infobip creates new opportunities for businesses and their end users to interact on mobile devices and over multiple channels – SMS, voice, push notifications, globally popular chat apps, or email.

Infobip's geo-distributed infrastructure is maintained by a 300-strong dev and engineering force, and quality tech support with industry's best response times.

With unsurpassed zero-hop connectivity to telecoms worldwide, and full control over the infrastructure that underpins its services, Infobip is the largest messaging network of its kind and the only full-stack cPaaS globally.

Infracast is a Managed Service Provider and Systems Integrator. We build and deliver strategic mobile customer engagement solutions for enterprise clients.

Our solutions are trusted and relied-upon by global enterprise customers as an integral component of their business processes. Our customers include global Banks & Financial institutions, Airlines, Retail, Telco, OTT and media organisations across the UK, EMEA, Latin America and world-wide. These organisations have one thing in common – the need to communicate reliably and effectively with their customers.

We understand your delivery promise to your customers. We understand that each message has a direct impact on customer satisfaction and your brand reputation.

We've been pioneers in value added services and specialised messaging products since 1995, providing universal solutions to scores of corporates, SMS aggregators, and resellers across the world.

At iTouch, we've developed an in-house, high performance and world-standard messaging platform **certified by leading international banks**. It delivers SMS MT, MO and Number Context services covering over 800 operators in 160 countries. And as leading specialists in Africa, we deliver OTP's, transactional, marketing and service messaging throughout the continent.

A company bent on Innovation since 1995, allow us to introduce our new generation of messaging platforms, MEMS: just as the feature phone led to the smart phone, our team developed SMS to MEMS - iTouch's very own *Multi-Channel Embedded Messaging Service* - a world-winner in interactive rich media messaging.

With infinite solutions to today's challenges, call iTouch to find out how we can help get your messages out faster, further and with complete freedom of mind.

PROGRAMME PARTICIPANTS

JT are a w orld class, Tier 1, global communications provider of a full suite of managed products and services.

Our range includes next-generation infrastructure with fixed line, mobile, broadband/ISP, netw ork connectivity and hosting as w ell as w orld-leading high-speed fibre broadband services.

With over 120 years' experience in telecommunications w e are dedicated to delivering w orld-class services. We are a full-service global consumer and business enterprise provider, w ith services covering domestic fixed land line through to leading-edge data hosting for the e-gaming industry.

For more than a decade, Mahindra Comviva has partnered w ith some of the w orld's largest and fastest growing mobile service providers, offering mobility solutions that have accelerated revenue growth, enhanced customer loyalty and delivered greater cost efficiencies. Today, w e have an established presence in more than 90 countries, providing over a billion mobile users access to our solutions globally. Our focus has alw ays been on creating value for our partners and customers. We have achieved this through our portfolio of productized solutions that not only enhance the end-user's mobile experience but also improve our partners' business performance.

We have enabled this by deploying solutions that exploit legacy investments and have incorporated advanced technology, service delivery and management techniques into its application, platform and service offerings.

As a global leader in mobility solutions, Mahindra Comviva has helped and continues to transform the lives of over a billion people across the globe.

There's a reason 75% of our customers come back for more. It's because **mobilesquared** analysts have been covering mobile since phones w ere brick-sized, and have tracked the evolution of mobile data every step of the w ay. We bring this vast know ledge to everything w e do. Based on our analysis, w e produce reports that create a buzz and forecasts that shape industries.

This is w hy we are a trusted research partner to some of the biggest names in mobile — from operators to regulators, service providers, vendors, aggregators, and advertisers alike. It's also because w e're passionate about w hat we do and that show s in our w ork. That's w hy our clients engage w ith us, and that's w hat makes mobilesquared tick.

With Headquarters in Zug, Sw itzerland and offices around the w orld, Mitto's agile approach, trusted mobile operator relationships and carrier-grade SMS Messaging platform improve conversions and increase the speed and reliability of global mobile communications for the w orld's largest OTTs, Enterprise and Mobile Operators.

Our mission is to provide customers w ith the most reliable, robust SMS Messaging service in the industry. That's w hy technology is at the heart of everything w e do. Our in-house team of developers make up more than a third of our staff and betw een them have designed a platform that guarantees our customers' SMS messages get to the right person, at the right time, in the right place – in the most cost effective w ay possible.

For more information about Mitto visit www.mitto.ch.

PROGRAMME PARTICIPANTS

MMDSmart Ltd, the smart messaging pioneer, provides smart communications solutions to organizations of all sizes. Started in 2007 as a voice transit company its product offering now includes retail and wholesale voice services, Fax over IP and chat solutions, as well as A2P messaging.

Its innovative smart messaging platform, the first results driven messaging solution, provides unique tools to improve message delivery, drive greater customer engagement and achieve higher conversion rates.

With headquarters in Tel Aviv, regional offices in Hong Kong and Kiev, and a development center in Nizhny Novgorod, Russia, it is focused on providing the highest quality communications solutions and services to its partners and clients around the globe, which include many tier 1 companies from more than 100 countries and more than 300 interconnections.

As it expands its global scope, its initial mission and commitment stays the same; MMDSmart. Connect. Engage. Smile

Movile is the industry leader for development of mobile content and commerce platforms in Latin America. With products for mobile phones, smartphones and tablets, our work makes people's lives better and a lot more fun.

Games, on-line education, entertainment apps for adults and kids and many options for buying with confidence and comfort. All of that gets to you through Movile.

For companies, Movile delivers complete products, integrating transactions in M-Commerce, M-Payments and content distribution, fast and with quality.

Millions of people use Movile apps every day. Always enjoying the most practical and reliable way of paying through their mobile devices.

Movile is the company behind the apps that make your life easier.

Vonage (NYSE: VG) is a leading provider of Cloud Communications for Business. Through innovative cloud technology, Vonage delivers more scalable, cost-effective and integrated communications to businesses.

The Company transforms the way people work and businesses operate through a portfolio of cloud-based communications solutions that enable internal collaboration among employees, while also keeping companies closely connected with their customers, across any mode of communication, on any device.

Nexmo, the Vonage API Platform provides tools for voice, messaging and phone verification services, allowing developers to embed contextual, programmable communications into mobile apps, websites and business systems to drive their businesses. Nexmo enables enterprises to reimagine their digital customer experiences by providing them with the tools they need to easily communicate relevant information to their customers in real time, anywhere in the world, through text messaging, chat, social media and voice.

OpenMarket helps the biggest brands in the world use mobile messaging to connect with their customers in the moments when it counts. When they need to be there and be responsive in real-time. When customer experience isn't just a buzzword: it's an obsession.

OpenMarket combines a powerful, scalable and reliable platform with a deep understanding of how text messaging can transform business processes. It works closely with clients to deliver timely, useful and context-sensitive mobile messages that surprise and delight their customers around the world at massive scale. OpenMarket calls this the Empathetic Interaction and its changing the way enterprises engage with their customers.

With trusted relationships with mobile operators across the globe, OpenMarket offers faster time to market, and ongoing support for its enterprise customers. OpenMarket is a division of Amdocs and is headquartered in Seattle, Washington, with regional offices in Detroit, London, Sydney, Guadalajara (Mexico) and Pune (India).

PROGRAMME PARTICIPANTS

R&D Communication represents a high standing reality in the Italian market and in 15 years it has accomplished to be a well renowned technological platform from which to send A2P messaging. The maximum level solutions offered by us permit you to plan and empower your business Marketing and Communication systems.

The strong passion and dedication that we have for the messaging world helped us extend and be efficient as well in the International market and we are now glad to be the Gateway that connects people around the world.

RealNetworks®, Inc. delivers digital entertainment services to consumers via PC, portable music player, home entertainment system or mobile phone.

Real created the streaming media category in 1995 and has continued to lead the market with pioneering products and services, including: RealPlayer®, the first mainstream media player to enable one-click downloading and recording of Internet video; the award-winning Rhapsody® digital music service, which delivers more than 1 billion songs per year; RealArcade®, one of the largest casual games destinations on the Web; and a variety of mobile entertainment services, such as ringback tones, offered to consumers through leading wireless carriers around the world.

Route Mobile Limited (RML), established 2004, is a leading global messaging and voice API company. Headquartered in Mumbai, India, the company has offices in the Middle East, Africa, Asia Pacific and Europe and services over 18.000 customers through a network of more than 300 employees.

Through its portfolio of comprehensive, flexible & innovative solutions including Enterprise as well as 2way Messaging, HLR Number Lookup, SMS Firewall, Interactive Voice Response (IVR), Click 2 Call, Chatbots, Outbound Dialer and SMS Hub, Route Mobile meets and exceeds its customer's requirements. With over twelve years experience RML provides tailored solutions to enterprises, aggregators, resellers and mobile network operators (MNOs).

Supporting over 850 global network connections, 150 of which direct, RML routes more than 2 billion messages per month. The company is uniquely placed encompassing approved open connectivity, SMS hub provision and SMSCs globally.

SAP Mobile Services, a division of SAP, provides cloud-based engagement services to enterprises that enable them to connect the "last mile" to their customers, cloud-based analytic services that aggregates and analyzes mobile operator data to provide deep consumer insight to brands and retailers, and interconnection services to mobile operators that allows any two people in the world text each other. We operate the world's largest, most reliable cloud messaging network, reaching 6.11 billion subscribers on 990 operators in 214 countries and processing over 1.8 billion messages per day.

As market leader in enterprise application software, SAP helps companies of all sizes and industries run better. From back office to boardroom, warehouse to storefront, desktop to mobile device – SAP empowers people and organizations to work together more efficiently and use business insight more effectively to stay ahead of the competition. SAP applications and services enable approximately 310,000 business and public sector customers to operate profitably, adapt continuously, and grow sustainably.

For more details about how SAP Mobile Services can transform your business and improve customer experiences in the digital economy visit us on the web at SAP Mobile Services. To learn more about intelligent and interconnected mobile engagements, join the SAP Mobile Services Community

PROGRAMME PARTICIPANTS

Telefónica is one of the largest telecommunications companies in the world in terms of market capitalisation and number of customers. With its best in class mobile, fixed and broadband networks, and innovative portfolio of digital solutions, Telefónica is transforming itself into a 'Digital Telco', a company that will be even better placed to meet the needs of its customers and capture new revenue growth.

The company has a significant presence in 24 countries and a customer base that amounts more than 315.7 million accesses around the world. Telefónica has a strong presence in Spain, Europe and Latin America, where the company focuses an important part of its growth strategy.

TIMWE Group is a global provider of mobile engagement solutions.

We ensure that mobile operators, governments and many other mobile-driven businesses increase revenue and reach, while reducing their operational costs, by delivering compelling end to end services and bespoke solutions on the cloud and on premise.

At the moment we are catering our clients through three business brands distributed globally: DIGIWE – Digital Mobile Solutions, TECHWE – Technology Solutions and GOVWE – Government Solutions.

With over 10 years of international experience and our proprietary, multipurpose mobile engagement platforms, we design, develop and deliver turnkey projects for our customers across all 5 continents.

TIMWE Group operates in 80 countries through 30 offices. Outside of our core Latin American and Middle Eastern markets, we are rapidly consolidating our position across Africa, Eastern Europe and the Asian regions.

Turk Telekom International (TTI) is 100% owned by Turk Telekom and acts as its international business unit handling all international data, wholesale voice business functions and roaming partnerships with all LTE/GSM/CDMA operators and MVNOs globally.

Turk Telekom International provides single account management and unified network operations over the entire Turk Telekom International network which includes 20 countries in Central and Eastern Europe, Turkey, Middle East and the Caucasus, covering a full range of Internet/data services, infrastructure and wholesale voice services to incumbents, alternative carriers, mobile operators, cable TV companies, Internet service providers and corporate customers.

Turk Telekom International offers premium quality telecommunication solutions in the form of: guaranteed SLA-s, local experts, dedicated staff, centralized end-to-end network management, trustworthy and reliable attitude, delivering on commitments, on-time delivery, tailor-made, scalable and cost-effective technical solutions and a proven management team with a full service portfolio. Covering over 40,000 km of fiber optic network and more than 150 interconnections worldwide Turk Telekom International is one of the most important players for the global telecommunications industry.

Twilio is reinventing telecom by merging the worlds of cloud computing, web services and telecommunications. Twilio hosts a telephony infrastructure web service in the cloud, allowing web programmers to integrate phone calls and SMS messages into their applications. Twilio's simple, powerful API minimizes the learning curve required to build advanced, reliable communications applications, and its Pay-As-You-Go pricing model means customers pay for capacity only when they need it, not before.

The company is funded by Bessemer Venture Partners, Union Square Ventures, Founders Fund, Mitch Kapor and other prominent investors, and is headquartered in San Francisco, CA.

PROGRAMME PARTICIPANTS

TWW is one of Brazil´s main SMS aggregators. We are directly connected to all the Brazilian carriers and MVNO´s. We are specialists in SMS and use only one route. Direct connect.

TWW's SMS service makes it possible for your company to connect w herever necessary in the Brazilian territory. With a secure and prepared technological infrastructure, we offer personalized service to guarantee the efficiency you want to reach with the results you need. Your company w ill find a technical team that is dedicated 24 hours a day, 365 days a year to identify adequate solutions, implement tools, integrate your systems and, above all, serve your needs w ith agility. After all, a quick and effective connection is the key to a successful relationship! We can make your life simple in Brazil.

Ubiquity Group is a global multi-channel messaging platform provider founded in 1999, focusing on ubiquitous communication for large enterprises and providing innovative solutions.

Over the years, Ubiquity has reached and consolidated a leadership position in the Italian market, w ith 95% of Italian financial institutions trusting Ubiquity as their messaging solutions provider.

In November 2015, Ubiquity became a certified ELITE company of the Italian Stock Exchange. In 2016, Ubiquity became a GSMA member, set up Ubiquity International SA in Sw itzerland and acquired Solutions Infini, a mobile communications platform market leader in India.
The company has its headquarters in Milan, Italy and an international presence beyond Europe in 10 locations. Ubiquity has 180 employees across Europe, India and the Middle East.

Founded in 2011, Veoo is a global mobile consultancy and leading provider of mobile messaging solutions; providing a cloud communications platform and one-stop-shop for any business looking to implement mobile. With a strong pedigree in mobile payments, mobile engagement and marketing and the online entertainment industry, Veoo is breaking new boundaries and challenging the status quo.

A global player, Veoo already has offices in 26 countries across Europe, Asia, Central America and South America and is set to expand into Northern America, the Philippines and Canada by the end of 2017. With a portfolio of over 150 large-scale customers, Veoo w orks across a variety of industries including retail, financial services, online entertainment and many more.

Vodafone is one of the w orld's largest telecommunications companies and provides a range of services including voice, messaging, data and fixed communications. Vodafone has mobile operations in 26 countries, partners with mobile netw orks in 49 more, and fixed broadband operations in 17 markets. As of 30 September 2016, Vodafone had 470 million mobile customers and 14 million fixed broadband customers. For more information, please visit: www.vodafone.com.

PROGRAMME PARTICIPANTS

WAU is Latin America's largest mobile transaction netw ork, providing a single point of contact for mobile messaging connectivity and billing services to global companies looking to expand their services to Latin America.

With headquarters in Miami, FL, offices in 15 countries and connectivity w ith over 45 w ireless operators, WAU simplifies doing mobile business in Latin America, helping its customers efficiently reach, engage and monetize the region's burgeoning mobile consumer base.

We are leaders in enterprise mobility in Brazil. Your company needs to be in all places at once. Must reach and impact all public and consumers.

We know the w ay, the technologies and also the behavior of mobile users and w e can assist you in this.

We are in the market for over 12 years and serve thousands of companies from different segments, sending and receiving millions of messages every day. Our history proves our credibility and leadership. Your result is our result.

MEF
MOBILE ECOSYSTEM FORUM

ABOUT MEF

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. We provide our 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 drives inclusion for all and delivers trusted services that enrich the lives of consumers worldwide. Established in 2000 and headquartered in the UK, MEF has Regional Chapters across Africa, Asia, Europe, Middle East, North and Latin America.

GLOSSARY

2FA (Two Factor Authentication)

A process which enables the confirmation of an individual's claimed identity by using a combination of two different components, namely:

1) something an individual possesses or is inseparable from them, and

2) something the individual knows

For example, a 2FA process for a mobile subscriber might require their being in possession of a mobile device, plus a PIN.

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 enterprise to communicate and share information with their customers, for example, bank balance alerts, retail order or delivery confirmation, appointment reminders and offers. A2P is generally used to send one-way messages but two-way A2P SMS communication is possible in some markets.

AA Agreements

A range of template agreements issued by the GSMA which establish contractual and commercial protocols between originating MNOs, terminating MNOs and messaging providers for the delivery of messages, including:

- AA.12 International Roaming
- AA.13 International Roaming
- AA.14 International Roaming
- AA.19: Commercial agreement for message termination
- AA.60: Commercial agreement for message termination

Access Hacking, Hacking

The act of gaining access to a mobile operating system, app or device by someone without the permission of the owner.

Aggregator

A company that provides connectivity between MNOs and messaging providers. See also Tier 1 Aggregator and Tier 2 Aggregator.

Alphanumeric Originator; Alpha Originator, Alpha Tag

See Originator.

Anti-Virus Software

Software designed to protect internet-connected devices, including mobile devices, from malicious software, also known as malware, or viruses. See also SMS Malware.

Artificial Inflation of Traffic (AIT)

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

Application Service Provider, Application2Person Service Provider (ASP)

A company that manages and distributes software-based services and solutions.

Availability

This describes the reliability or 'uptime' of a route in terms of the percentage of time that a connection is fully operational within a specified period of time. A route which has 99.999% availability within a single and continuous 24 hours period is more reliable than a route with 99.9% availability during the same period. See also Redundancy.

Blending

The use of two of more connections within an end to end message delivery chain for the delivery of messages to one destination.

Bulk SMS

A service which enables enterprise to send high volumes of non-premium rate messages quickly and efficiently. Bulk SMS is usually delivered with no charge to the receiving party, but local exceptions do exist.

Bulk Traffic

A term for mass marketing, whereby multiple recipients receive the same message.

Cloud Communications Provider

A company which delivers internet-voice and data communications applications and services.

CNAME (Canonical Name)

A type of resource record in the DNS which specifies that a domain name is an alias for another domain, namely the "canonical" name. All information, including subdomains and IP addresses etc, are defined by the canonical domain.

GLOSSARY

Connection, SMS Connection, A2P Connection

The technical and commercial infrastructure which enables the delivery of messages through an end to end message delivery chain between a sender and recipient.

D&B Number; DUNS; D-U-N-S (Dunn & Bradstreet Number):

A unique numerical identifier assigned to a single business entity which is recognised worldwide.

Delivery Receipt (DLR)

A receipt to confirm that a message has been successfully sent by a messaging provider or that a message has been successfully delivered to a subscriber's MNO or handset. See also Message Status.

DNS (Domain Name System):

The Internet's system for converting alphabetic names into numeric IP addresses.

Expired Message

A message which has not been sent by a messaging provider within a specified time.

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 generated by an SMSC when a message is being sent, the first being an SRI. Both an SRI and an FSM request are required to send a message.

Global Title (GT)

An address used in the SCCP protocol for routing messages through an MNOs 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 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.

GSM Network (Global System for Mobile Communication)

An open, digital mobile technology used for transmitting mobile voice and data services.

GSMA

A global membership organisation which represents the interests of MNOs and companies within the broader mobile ecosystem The GSMA issues technical standards and template agreements which establish contractual and commercial protocols between originating MNOs, terminating MNOs and messaging providers for the delivery of messages. See also AA Agreements.

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.

Hop

This refers to the point within an end to end message delivery chain where one partner connects to the next.

Hub

A structure for the international flow and mobile interoperability of SMS between MNOs to intermediate messages and to offer greater coverage, also known as Hubbing. A Hub can be established to connect an MNO's subsidiary companies to each other, or to other MNOs or MNO Group Hubs for the delivery of enterprise messaging. A P2P Hub is designated for the delivery of P2P messages only.

Group Hub

See 'Hub'.

IMSI (International Mobile Subscriber Identity)

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

Interconnection / Interconnect / Interworking Agreement

A technical, operational and / or commercial contract between two parties within an end to end message delivery chain which connects an enterprise to their customer for the delivery of messages.

GLOSSARY

International Message

A message which has originated at source from an IP address not registered within the country of delivery

Latency

This describes the time taken from the acceptance of a single message into the delivering MNO's SMSC to a mobile subscriber's device. It is also commonly used to describe the time taken for a message to travel from the sender to the recipient.

M2M (Machine to Machine)

Direct communication between devices using any communications channel, including wired and wireless.

MAP (Mobile Application Part)

An SS7 protocol used to access the Home Location Register, Visitor Location Register, Mobile Switching Centre, Equipment Identity Register, Authentication Centre, Short Message Service Centre and Serving GPRS Support Node.

MAP Global Title Faking

Manipulation of specific technical parameters or disguising a message sender'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 an MNO.

Message Status

Every message which enters a messaging provider's systems for delivery to a mobile subscriber is assigned a status, the most common of which are:

- Sent: message submitted towards the terminating MNOs SMSC
- Delivered: message delivered to the mobile subscriber's handset
- Rejected: message rejected by the terminating MNO's SMSC
- Invalid Number: mobile subscriber's number is invalid (eg, missing digits)
- Undelivered: message not delivered to the mobile subscriber's handset
- Expired: message not delivered within the pre-set time period
- No Credits: insufficient prepay credit available to send the message
- Absent Subscriber: handset is off or out of network coverage

See also Delivery Receipt (DLR)

Messaging Provider

An enterprise-facing company which sells end to end enterprise mobile messaging solutions. A messaging provider may have one or more technical or commercial roles and will commonly partner with others within the messaging ecosystem, by way of agreements to deliver end-to-end solutions.

MMS (Multimedia Messaging Service)

A descendant of SMS, which extends SMS messaging to include longer text, graphics, photos, audio clips, video clips, or any combination of the above, within certain size limits.

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)

This describes the source of a sent message, ie, the beginning of the end to end message delivery chain. See also Originating Mobile Operator.

MNO Exclusive Gateway Partner

A provider which offers the only authorised way to send messages to a specific MNO. Please refer to the MEF Enterprise Mobile Messaging Guide for more information.

MNP (Mobile Number Portability)

This lets a mobile subscriber move from one MNO to another while keeping their number, also known as porting. MNP has made it impossible to determine the mobile network of an MSISDN by its prefix.

MSISDN (Mobile Station International Subscriber Directory Number)

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

GLOSSARY

MSC (Mobile Switching Centre)

An MSC routes messages, performs service billing and interfaces with other telecoms networks, such as the public switched telephone network (PSTN). All forms of communication, whether between two mobile phones or between a mobile phone and a landline telephone, travel through the MSC.

MSU (Message Signal Unit)

An individual MSU is required for each SRI request, SRI response, FSM request and FSM response when delivering a message.

Mobile Subscriber, Subscriber, End User

An individual who is a customer of, and connected to, a domestic MNO's network for services, including voice calls, SMS, MMS or data.

Mobile Terminated (MT)

This describes the destination of a sent message, ie, the end of the end to end message delivery chain. See also Terminating Mobile Operator.

MTP (Message Transfer Part)

Part of the SS7 Network, the MTP is responsible for reliable, unduplicated and in-sequence delivery of messages between partners within the end to end message delivery chain.

MVNO (Mobile Virtual Network Operator)

A wireless or mobile communications services provider which does not own the network infrastructure over which it provides services to subscribers. An MVNO will contract with an MNO to obtain bulk access to network services at wholesale rates and then set the retail prices independently. An MVNO may use its own customer service, billing support systems, marketing and sales personnel, or it could engage a third party.

Off-net

Describes the environment outside of an MNO's own network. For example, messages which are delivered Off-Net are sent from one MNO to a second MNO, either nationally or internationally.

On-net

Describes the environment inside an MNO's own network. For example, messages which are delivered On-net never leave the MNOs national or international group network.

Originating Mobile Operator; Originating MNO

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

Originator

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.

OTT (Over The Top)

Instant messaging services which are accessed over the internet.

P2A SMS (Person to Application)

Messages originated by a mobile subscriber and intended for delivery to a business, for example, a customer responding to a message received from an enterprise.

P2P (Person to Person)

This describes a channel whereby one mobile subscriber creates and sends a message to another mobile subscriber.

P2P Hub

See 'Hub'.

PRS (Premium Rate Service)

Services which enable mobile subscribers to pay for content, data services and VAS via their mobile phone bill or prepay account.

Reseller

A company which buys a product or service, repackages and then sell it as its own.

Phishing, SMS Phishing, SMiShing

The act of misleading a mobile subscriber by pretending 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.

Roaming

This describes an environment in which a mobile subscriber has left their home MNO network but retains the ability to access services without a break their connection by being connected to a visited MNO's network.

GLOSSARY

Reach

This is the breadth of coverage available in terms of how many mobile subscribers can be reached, for example, nationally, across multiple mobile operator networks or internationally. Reach may be determined by the types of connections available to a messaging provider.

Redundancy

This is the term for a secondary backup or fail-over route which assures the continuity of services in the event that an available connection fails for any reason. See also Availability.

Route, Routing

This describes the path that a message takes along an end to end message delivery chain, through different partners and connections.

SCCP (Signalling Connection Control Part)

A network layer protocol that provides extended routing, flow control, segmentation, connection-orientation, and error correction facilities within the SS7 Network. The SCCP relies on the services of MTP for basic routing and error detection.

SCCP 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.

Service Provider

See Messaging Provider.

Short Code, Short Number

A special numbers, significantly shorter than a full 11-digit phone number, which can be used to send SMS and MMS messages.

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.

SMS (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.

SMS Roaming Intercept Fraud

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

SIM Farms

A bank of SIM cards used to deliver 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

The act of obtaining control of a mobile number by cancelling the SIM linked to a consumer's handset and activating a new SIM 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.

SMPP (Short Message Peer to Peer Protocol)

A proprietary protocol used to send messages within the messaging ecosystem which can support non-GSM SMS protocols and is commonly used for the exchange of messages outside of the SS7 network.

SMSC (Short Message Service Centre)

An element within an MNO's network which receives messages from mobile network users (enterprise and individual mobile subscribers) and also 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 generated 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 to request routing information and determine the IMSI of a mobile subscriber. Both an SRI and FSM request are required to send a message.

SMSC Compromise Fraud

The act of sending messages in a way that exploits an MNO's SMSC to relay messages without paying.

SMS Malware

Malicious software which is installed on a device without the mobile subscriber's knowledge or disguised as an innocent app that acts silently in the background to disrupt connectivity, gain access to and gather personal or sensitive information, display unwanted advertising, or access a contact list to further spread the software.

GLOSSARY

STP (Signal Transfer Point)

A router that relays SS7 Network messages between signalling end and signalling transfer points. STPs are typically provisioned in mated pairs to meet stringent reliability requirements.

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 someone or something known to the recipient to deliberately 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. SS7 is not permitted in some regions.

Telecommunications Technology Provider

A company which provides technological infrastructure to support the flow of voice calls, data or messages between different locations or companies.

Tier 1 Aggregator

A company which has a contract in place directly with a terminating MNO for the delivery of messages.

Tier 2 Aggregator

A company which has a contract in place with a Tier 1 Aggregator in order to connect to a terminating MNO for the delivery of messages.

Tier X Aggregator

A company which does not have a contract in place directly with a terminating MNO, but has contracts with a range of Tiers of Aggregator.

Terminating Mobile Operator; Terminating MNO

The MNO at the end a message delivery chain, to which your customers are subscribed.

Throttling

The control and temporary restriction by an MNO of the flow of messages through its network to enable it to manage capacity effectively within its systems.

Traffic

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

Throughput

The capability that a MNO or aggregator has to carry a certain volume of messages across their infrastructure within a certain unit of time, for example, 300 SMS per second.

UCP (Universal Computer Protocol)

A standard for transmitting SMS over mobile networks.

USSD (Unstructured Supplementary Service Data)

A protocol used by GSM mobile phones to communicate with a messaging provider's computers.

VAS (Value Added Service)

Any non-core mobile services, namely, those beyond standard voice calls and messaging.

VLR (Visitor Location Register)

A database which contains information about mobile subscribers roaming within an MSC's location area. Its primary role is to minimise the number of queries that MSCs have to make to the HLR.

ACCELERATING YOUR MOBILE OPPORTUNITY