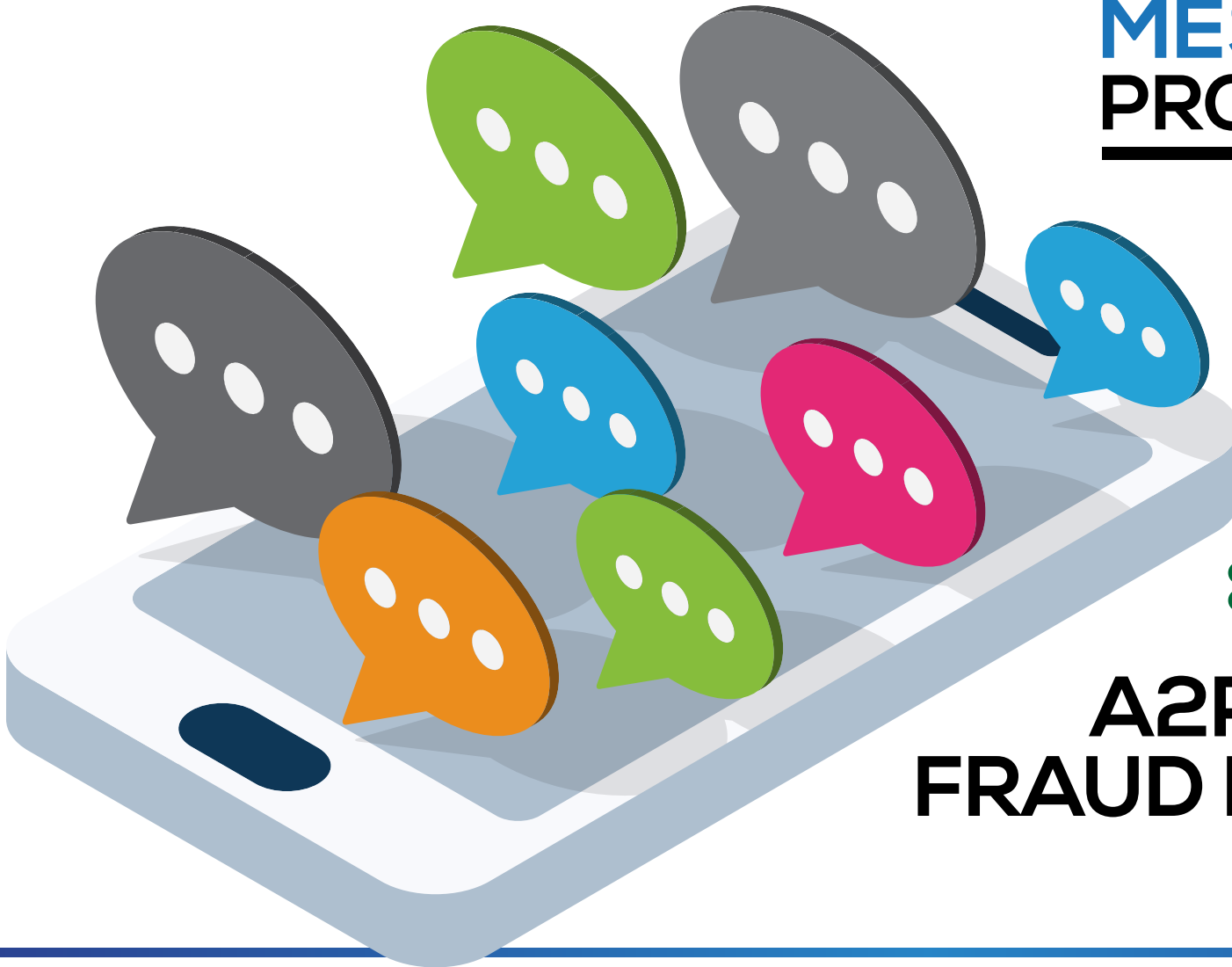




MEF

**MOBILE
MESSAGING
PROGRAMME**



**A2P MESSAGING
FRAUD FRAMEWORK
VERSION 1.0**



TABLE OF CONTENTS

OVERVIEW

- Introduction
- Framework Development

FRAUD TYPES IN THE MOBILE MESSAGING ECOSYSTEM

1. SPAM
2. SMS Originator Spoofing
3. SMS Phishing
4. SMS Malware (SMS Hacking)
5. Access Hacking
6. Grey Routes due to absence of AA19 / AA60 Agreement
7. MAP Global Title Faking (created through MAP or other manipulation)
8. SCCP Global Title Faking
9. SMSC Compromise Fraud
10. SIM Farms
11. Artificial Inflation of Traffic (AIT)

ANNEX

- Mapping Fraud in the A2P Messaging Ecosystem
- Glossary
- About MEF's Future of Messaging Programme
- Programme Founders
- About MEF



INTRODUCTION

MEF's Mobile Messaging Programme: The Future of Messaging, provides a unique opportunity to unite all parties within the mobile messaging ecosystem. Its common goal is to promote and accelerate best practices in order to limit fraudulent behaviours and identify new opportunities for mobile messaging.

The Programme, established in Q4 2015, has two work streams: Market Development and Fraud Management. The Programme is open to all stakeholders in the messaging ecosystem and full details of the Founders of the Programme can be found in the Annex.

Mobile messaging has long been a dynamic and effective method of direct communication, from the early days of peer to peer messaging, to the global market that exists today. New entrants are changing market dynamics for next generation mass communication and new use cases are presenting themselves from across ever expanding enterprises and sectors.

However, the prevalence of fraud within the global mobile messaging ecosystem impacts on consumer trust, undermines market value and raises questions about the channel as a viable method for enterprise and brands to engage with consumers in the long term.

It is estimated by the Programme Founders that fraud in the Application to Person (A2P) messaging sector is costing the ecosystem at least \$2Bn annually. Many types of fraud are complex and not well understood by those affected. Fraud creates volatility in the market and a poor quality experience for all those impacted, leading to uncertainty, slower adoption rates for new services and sectors and lower market growth.

Fraud within the mobile ecosystem is complex and varied, impacting all stakeholders in some way, be it financially, technically, legally or in the ability to build and sustain trust. However, awareness and understanding is not consistent across the value chain.

Some types of fraud continue to exist due to lack of investigation or consequence. Historically, there has been a lack of accountability and arguably a lack of

commitment from some parties to address ongoing messaging fraud. However as messaging channels and the market opportunity grows, so does the significance and impact of fraud on its monetisation.

Market innovation and best practice can shape the sustainability and future of messaging. However, no one stakeholder can successfully address fraud on its own, making a cross-ecosystem approach essential to accelerate the clean-up of the market and create a more transparent ecosystem which is free of fraud. MEF's Mobile Messaging Programme provides a forum by which the industry as a whole can promote and share mechanisms to limit fraudulent practices across the messaging ecosystem.

This A2P Messaging Fraud Framework has been created by an International Working Group to identify the different types of fraud which currently take place within the mobile messaging ecosystem. It assesses the cause and impact of the different types of fraud, as well as looking at methods for both detection and prevention. This Framework is the first output of the Fraud Work Stream and the initial step by the industry in making a real and positive change towards limiting fraud in the market.

This Framework is intended for those from within the mobile messaging ecosystem with a working knowledge of the A2P value chain, for potential entrants to the messaging market, and any interested party with comprehensive telecommunications expertise, as well as the buyers of bulk messaging.





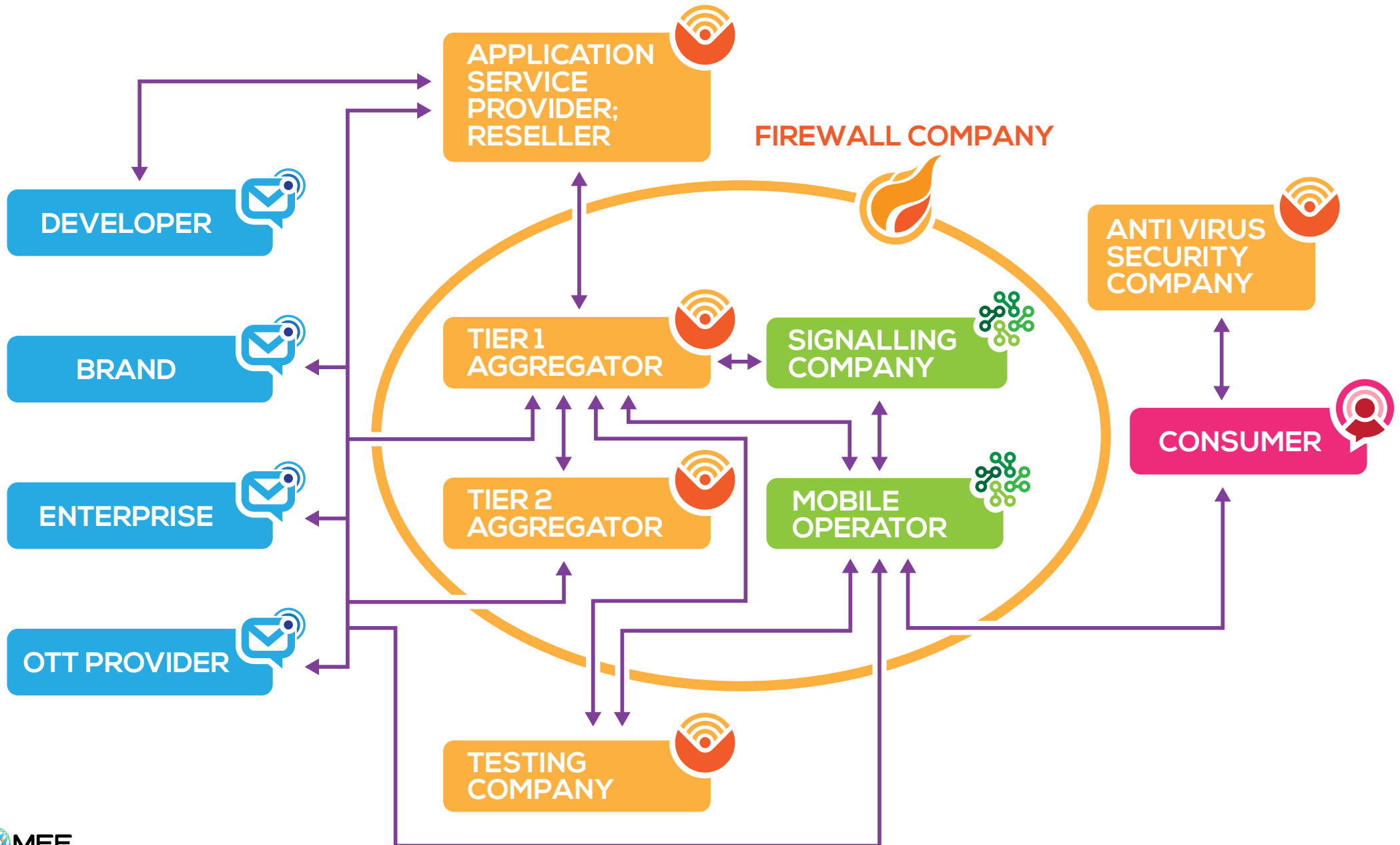
FRAMEWORK DEVELOPMENT

An International Working Group was formed by the Programme Founders, represented by senior executives across Commercial, Operator Relations, Product and Technical teams. The Framework will be the basis for the future work of the Programme in order to develop best practice guidelines for industry and buyers as well as provide the framework for an industry wide certification programme.

For the purpose of developing the Framework, the mobile messaging ecosystem is defined by the Working Group below, identifying key stakeholder groups and mapping the complexity of the relationships that exist which is a fundamental principle of why fraud continues to exist.







MAP OF THE A2P MESSAGING ECOSYSTEM



ECOSYSTEM MAPPING





The Working Group established that some types of fraud can only be prevented at certain points within the value chain and four subgroups were set-up to enable a detailed analysis of those types of fraud that are most within their control. The four subgroups encompass all of the players within the mobile ecosystem, as identified below:



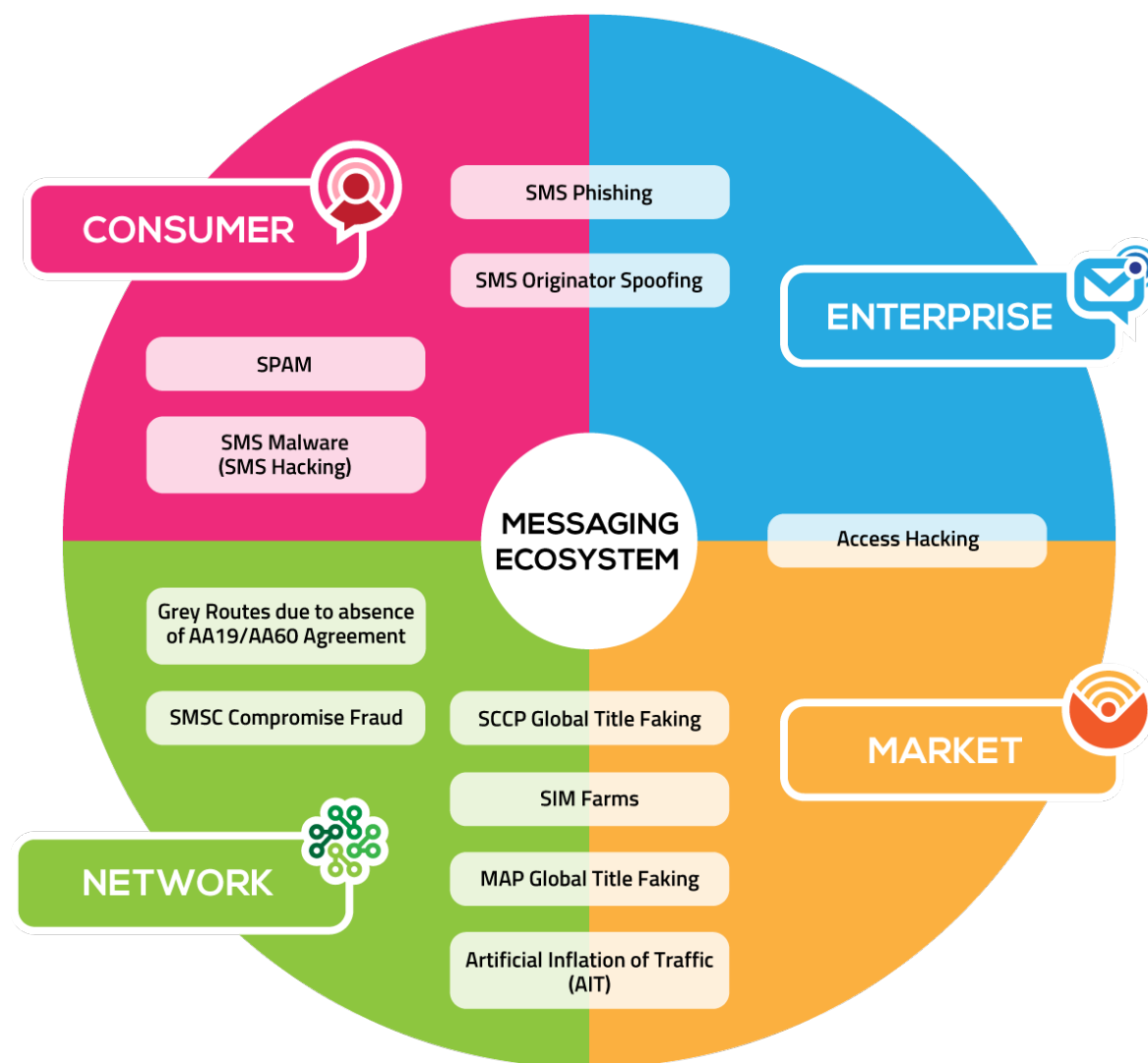
 NETWORK	 MARKET	 ENTERPRISE	 CONSUMER
MOBILE OPERATOR	AGGREGATOR: A TIER 1 AGGREGATOR HAS DIRECT CONNECTIONS INTO A MOBILE OPERATOR'S NETWORK; A TIER 2 AGGREGATOR MUST CONNECT WITH A TIER 1 AGGREGATOR TO REACH A MOBILE OPERATOR'S NETWORK	ENTERPRISE BRAND	CONSUMER: WHERE THE RELATIONSHIP IS WITH AN ENTERPRISE
SIGNALLING COMPANY	APPLICATION SERVICE PROVIDER	OTT PROVIDER	MOBILE SUBSCRIBER: WHERE THE RELATIONSHIP IS WITH A MOBILE OPERATOR
	RESELLER	DEVELOPER	
	TESTING COMPANY		
	ANTI-VIRUS COMPANY		
	FIREWALL COMPANY		

FRAUD MAPPING

Eleven different types of fraud were identified as impacting on the four stakeholder subgroups, some of which are highly complex and cut across a large amount of the value chain. The direct impact of these different types of fraud are addressed within each section.

AFFECTED STAKEHOLDER GROUP	TYPES OF FRAUD
 NETWORK	GREY ROUTES, SIM FARMS, SMSC COMPROMISE FRAUD, MAP GLOBAL TITLE FAKING (CREATED THROUGH MAP OR OTHER MANIPULATION)
 MARKET	ACCESS HACKING SPAM, SMS PHISHING, SMS MALWARE (SMS HACKING)
 ENTERPRISE	SCCP GLOBAL TITLE FAKING, SMS ORIGINATOR SPOOFING, ARTIFICIAL INFLATION OF TRAFFIC (AIT)
 CONSUMER	SPAM, SMS PHISHING

THESE 11 FRAUD TYPES ARE MAPPED AS FOLLOWS:



FRAUD MAPPING

The following criteria were analysed by each of the subgroups with the purpose of creating recommendations for the detection and prevention of each of the 11 fraud types identified.

FRAUD ANALYSIS CRITERIA

SCOPE & DEFINITIONS

CAUSE

IMPACT

DETECTION

PREVENTION

EXAMPLES

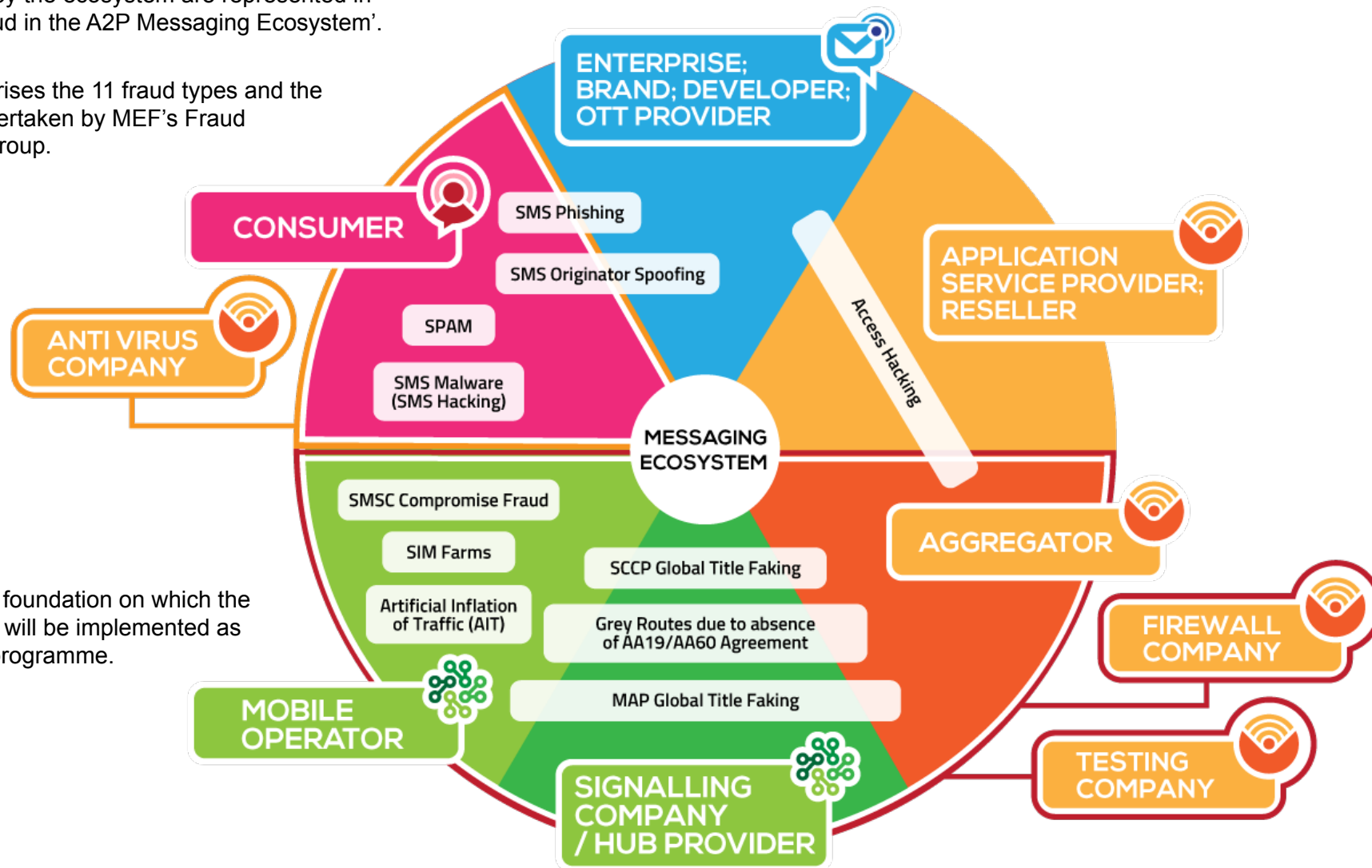
SUMMARY

The complexities faced by the ecosystem are represented in this chart: 'Mapping Fraud in the A2P Messaging Ecosystem'.

This Framework summarises the 11 fraud types and the analysis of the work undertaken by MEF's Fraud Management Working Group.

The solutions which have been identified include technical, procedural and educational requirements and will require cross-ecosystem collaboration to fully address and successfully implement.

Together, they provide a foundation on which the recommendations made will be implemented as part of MEF's two-year programme.



FRAUD TYPES IN THE MOBILE MESSAGING ECOSYSTEM



1: SPAM



AFFECTED PARTY

 NETWORK

 MARKET

 CONSUMER

DEFINITION

SPAM is an unsolicited message sent to a mobile subscriber who has not agreed to receive it from the sender. SPAM is commonly commercial in nature and can be sent legitimately if a mobile subscriber has opted-in to receive specific messages from a sender. Typical ways to opt-in to receiving commercial messages are to agree as part of a sign-up process online, on a physical form or via a Mobile-Originated (MO) message. In some cases, mobile subscribers may think they have received SPAM simply because they do not remember opting-in to receive messages as a result of an engaging with a service. Some examples of SPAM are messages from Payment Protection Insurance (PPI) companies in the UK or debt clearance firms.

In some countries where recycling of telephone numbers is common practice by mobile operators, it is possible that an individual may be assigned a recycled number that has been legitimately opted-in by the previous owner of the number. In these countries, mobile operators are obliged to tell the ecosystem about these recycled numbers and the ecosystem is obliged to remove these numbers from any opt-in marketing databases.

Not all SPAM is commercial in nature, such as those messages which may be sent with politically sensitive content, but they may still be messages which are unexpected or unwanted by the recipient.

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

CAUSE

The primary cause of SPAM is overzealous marketers who knowingly send promotional messages to bought or farmed lists of telephone numbers in an attempt to increase sales. In some cases, numbers will be automatically generated through brute force sequencing and then checked against a Home Location Register (HLR) to determine which numbers have been activated and are actually live.

Similar to email SPAM, this is a volume game: the more people who are made aware of a product, the more sales can be achieved. Targeted messaging campaigns have a very high conversion rate due to the high delivery and open rates of Short Message Services (SMS) compared to most other forms of marketing making it particularly attractive. In countries where the market price is very low, either by design or due to pervasive fraudulent routes, and regulation is light, SPAM can become a major issue as was seen in India, for example, before the TRAI regulations were introduced in 2011.

It is also the case that brands and enterprises may sometimes fail to properly manage consumer data correctly. They may ask for a mobile number during the course of an interaction with a consumer, but then either fail to verify that the mobile number supplied is indeed correct and belongs to the individual who provided it, or they fail to obtain explicit consent confirming how and when the mobile number may be used for marketing purposes in future, for example, if it were to be made available to third parties for marketing purposes.



SPAM



IMPACT

For the most part, SPAM is harmless and typically ignored by most mobile subscribers. It can, however, spiral out of control in some countries, leading to high churn of subscribers from one mobile operator to another, especially those on prepay, rendering the SMS channel ineffective for legitimate communication. In countries where the prevalence of SPAM is low, it does erode consumer trust in the SMS channel, possibly causing some to believe that legitimate messages are somehow fraudulent.

In countries where regulation on SPAM is severe (e.g. Japan, Australia, USA) and where non-compliance could attract heavy fines or litigious conditions in the form of class actions, this exposes innocent companies to perceived high risk and may negatively impact the growth of the market and overall adoption of the SMS channel by brands and enterprises.

In most cases, the recipient does not normally pay to receive a message and so SPAM does not generally result in any direct financial impact to the receiving party. However, this is not the case in the USA and Canada which are 'receiver pays' markets, thus making SPAM a much more serious matter.

DETECTION

Detecting SPAM can be difficult due to the fact that the opt-in information lies with the sender of the message. It is not easily accessible without asking the sender to provide the relevant opt-in information after a complaint has been made.

Many mobile operators have installed firewalls and filters to try and prevent SPAM, but these are typically configured to detect static keywords and can in some cases even stop legitimate messages from being correctly delivered.

The easiest way to detect SPAM is to crowd-source information from actual users where possible. Many mobile operators allow consumers to report instances of SPAM by forwarding the suspected message to a short code (e.g. 7726 in both Brazil and the UK).

Cross ecosystem co-operation based on this kind of crowd-sourced information would be the best way to detect SPAM.



SPAM



PREVENTION

Recommendations for the prevention of SPAM are as follows:

- Block fraudulent, grey and retail Subscriber Identity Module (SIM) card routes that may be keeping the price of a message artificially low
- Increase the price of a message so that the price of an A2P SMS is sufficiently high to avoid mass, non-targeted SPAM campaigns
- Introduce a global standard cross-mobile operator method of reporting SPAM and create a way to share this information across the ecosystem in an automated way so that all parties can be proactive in detecting and blocking SPAM
- Mobile operators should introduce a Home Router which prevents number cleaning via HLR without a specific agreement with a legitimate provider
- Create and share a global blacklist of companies who are found to frequently send SPAM
- Secure enterprise networks, Short Message Service Centres (SMSC) and SMS Portals to ensure that marketers cannot exploit hacks to send SPAM
- Promote good housekeeping when communicating through SMS, such as agreeing to abide by minimum standards on using STOP commands to opt-out etc
- Mobile numbers should be verified by a brand or enterprise, either via the delivery of a PIN to the number which can be used to verify it online, or by asking the individual to reply to confirm that they are opting in to the receipt of specific future marketing messages
- Outlaw the sale of 'number lists' and ensure that providers of HLRs do not allow their systems to be used to clean number lists which have been created by brute force sequencing
- Sending SPAM is against the law in most countries, but instances of SPAM are very rarely investigated: To truly prevent SPAM, more cases need to be detected, properly investigated and reasonable fines levied where appropriate, with possible prison sentences for repeat offenders

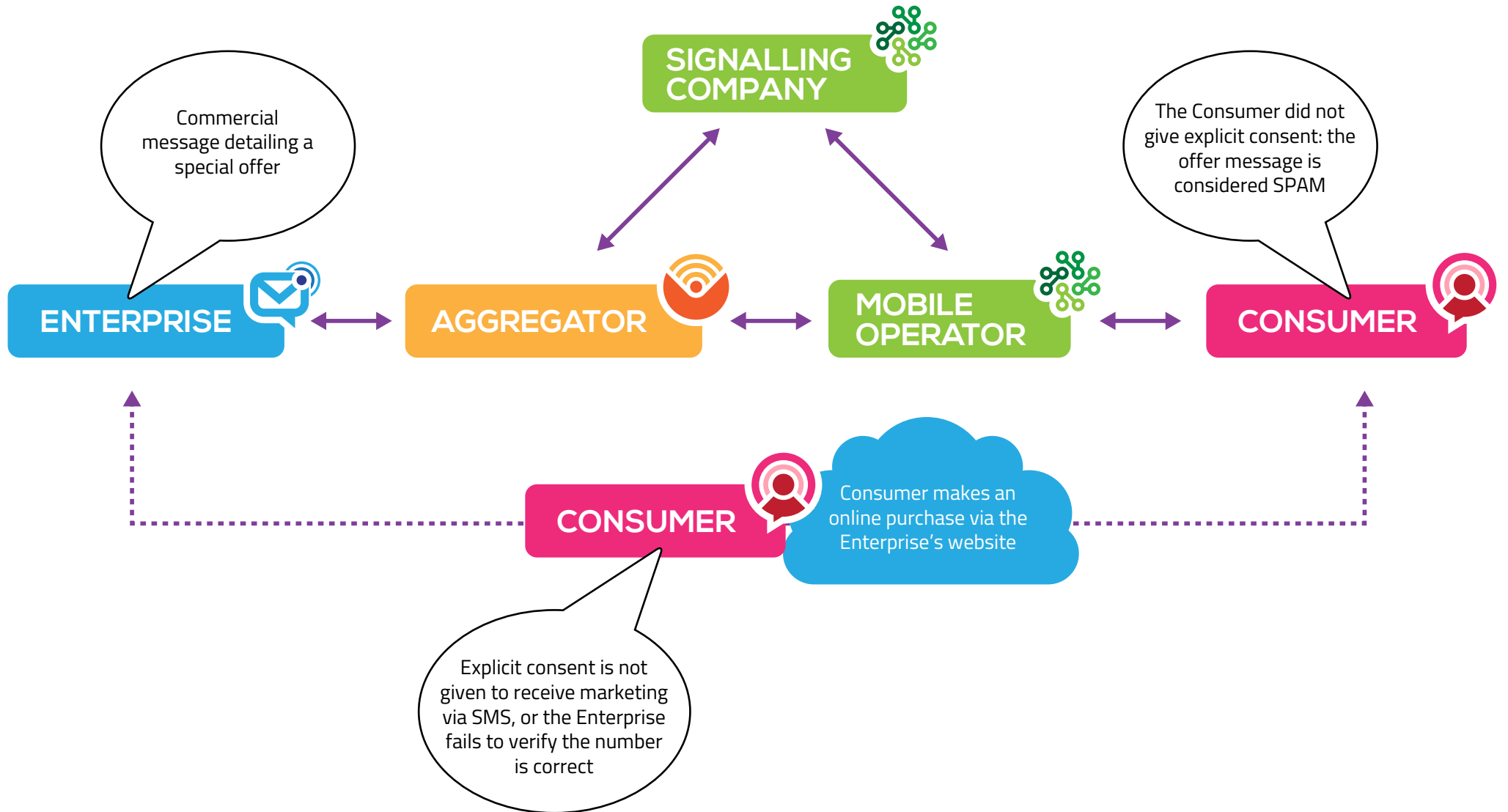
EXAMPLES

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



2: SMS ORIGINATOR SPOOFING



AFFECTED PARTY	
	NETWORK
	MARKET
	ENTERPRISE
	CONSUMER

DEFINITION

SMS Originator Spoofing (Spoofing) is the act of hiding the sending party's true identity by changing the originator to someone or something that is designed to trick a consumer into thinking the message is from someone familiar to them. For example, using the originator 'Apple' to pretend to be "Apple", or "HMRC" (UK Tax Office) or "your parent's number".

Using a random originator would be more akin to SIM Farm fraud than Spoofing and as such, the use of random originators is specifically excluded from this definition.

CAUSE

There are a range of reasons why a sender would want to alter an originator without legitimate cause:

- Lead generation, by pretending to be a known company, e.g. a sender pretends to be Vodafone to try and determine if a Vodafone consumer contract is up for renewal
- Abuse: sending abusive messages to an individual but pretending to be someone else
- SMiShing (SMS Phishing): extracting sensitive personal and confidential financial information for the purposes of trying to steal from a mobile subscriber

The vast majority of Spoofing cases occur where there is no concrete contractual back-to-back arrangement with the sending party and the value chain. As such, the weakness comes from the following areas:

- Free sending sites, where originators can be manipulated without registration or validation of identity
- Online portals where free credits are given in order to test a service and through which originators can be manipulated using these free credits
- Sites intended to assist with this fraudulent practice e.g. <https://www.youtube.com/watch?v=M8JwR5AINgQ>
- There is no automatic end-to-end way to validate whether an originator belongs to a brand or not



SMS ORIGINATOR SPOOFING



IMPACT

As a consequence, regulators have attempted to control Spoofing by limiting the power of SMS. For example, some countries have implemented the following restrictions:

- a. Pre-registration so that an originator cannot be used until it is registered and approved
- b. No-alpha originators allowed (e.g. only short codes)

The issue with these restrictions is that they can be easily circumvented and as such, legitimate parties find it harder to use SMS, whilst others find back doors.

This creates a confusing market whereby originators can influence message pricing and required features are only available on Grey Routes.

DETECTION

Some methods of detecting Spoofing include:

- a. A database of SMS Originator Spoofs and SPAM that aggregators can access both nationally and internationally
- b. Content filtering to look for specific originators
- c. Collaboration with mobile operators to limit the ability of messages containing unauthorised or unregistered originators being delivered



SMS ORIGINATOR SPOOFING



PREVENTION

Recommendations for preventing SMS Originator Spoofing are as follows:

- a. Global solution: Tier 1 aggregators should use a brand's Canonical Name (CNAME) record in their Domain Name System (DNS) record to determine whether they are the true sender of the message and anything suspicious can then be blocked
- b. Suspicious Messaging processes should form part of every mobile operator and aggregator's overall processes
- c. Verify a Dunn & Bradstreet (D&B) number registration for portals before message sending is allowed
- d. Require credit card registration before message sending is allowed
- e. Permit only long numbers until a customer proves that they are who they say they are
- f. Secure back-to-back contractual provisioning from a mobile operator down to a brand or enterprise, requiring that originators must be a recognised company name or the trading name of the sending party
- g. Law enforcement must be involved for serious issues
- h. Educate consumers: advice from the UK Communications Regulator, Ofcom, is to, *"Never give out your personal information in response to an incoming call, or rely upon the Caller ID as the sole means of identification, particularly if the caller asks you to carry out an action which might have financial consequences."*

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. It can be used to identify an enterprise or to leave a contact number that could be used to reply to a message.

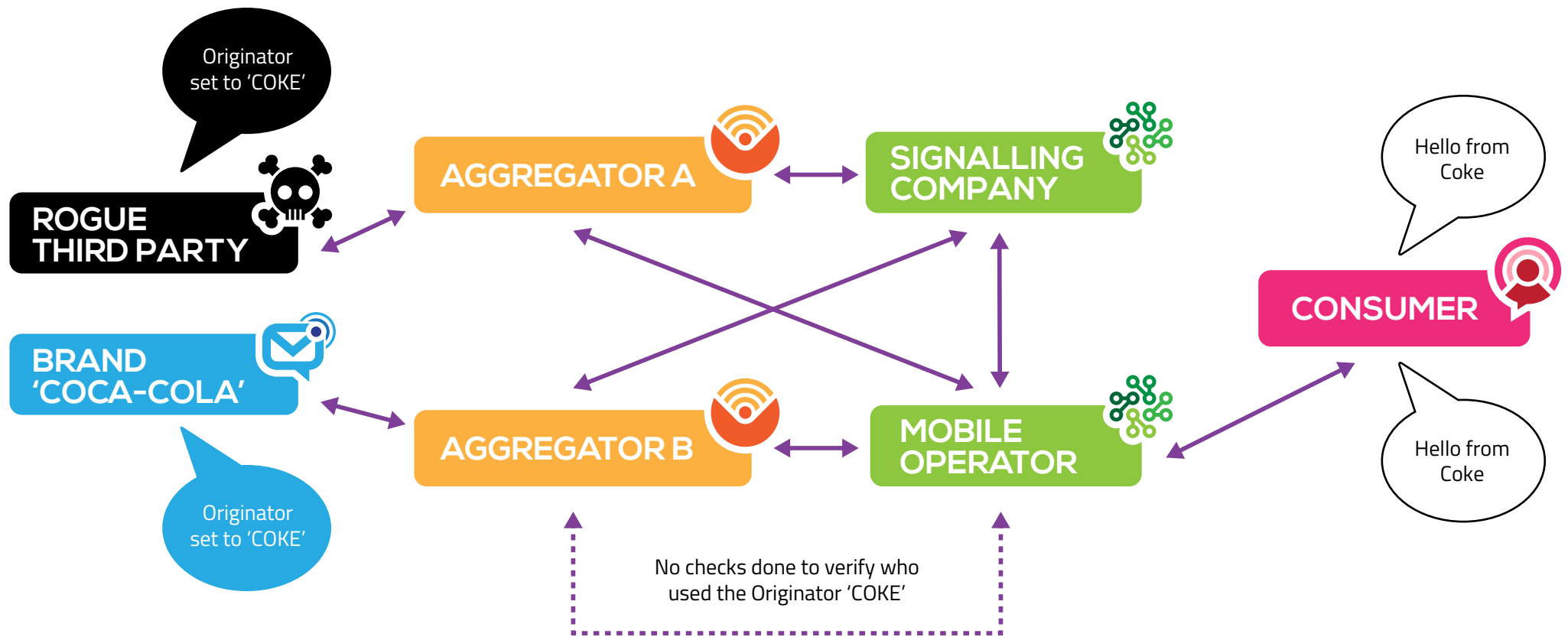
However, an alpha originator needs to somehow be tied to the sending company name in an automated way to ensure that this aspect of messaging is not eroded or damaged, whilst doing everything possible to protect the consumer.

EXAMPLES

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



3: SMS PHISHING (SMiShing)



AFFECTED PARTY

-  NETWORK
-  MARKET
-  ENTERPRISE
-  CONSUMER

DEFINITION

SMS Phishing (SMiShing) is a form of criminal activity combining SPAM, SMS Originator Spoofing and social engineering techniques to gain access to online systems, accounts or data such as credit card, banking information or passwords for malicious reasons by masquerading as a trustworthy entity.

Mechanism:

1. A rogue third party sends a call-to-action message to potential victims
2. The message has an originator that masquerades as a legitimate enterprise (e.g. a Bank)
3. The message contains a URL that looks valid, or is potentially misspelled (e.g. "Abode Flash Player"), or will not be easily noticed on a smartphone screen due to its length, but which actually points to a website hosted by the rogue third party
4. The unsuspecting recipient supplies personal information that can be used to gain access to sensitive information and services, most likely for the theft of money directly, or to extort money indirectly, such as through the theft of a domain or handle

CAUSE

The primary cause of SMS Phishing is the promise of financial gain, either directly or indirectly (through data loss) and the ease at which consumers can be fooled through the use of basic social engineering and masquerading techniques.

- a. The cost of the message has less bearing due to the large gains that an SMS Phishing campaign can generate but may still be a factor
- b. Consumers respond automatically to familiar situations and messages and may not be on the lookout for, or aware of, potential risks due to the trusted and intimate nature of the situation which is created by the rogue third party
- c. An indirect cause may be an enterprise not effectively managing a relationship with a consumer, such as inadequate data management and education on what channels they are likely to use to communicate with their customers and what information they are likely to request from them

Those parties which carry out SMS Phishing employ a percentage-based approach. They do not need to know that the victim has a relationship with the enterprise they are pretending to be, although having this information will improve the likelihood of success.

Other contributing causes include:

1. An increased reliance on mobile applications
2. The use of Two Factor Authentication (2FA) codes creates a perceived layer of trust
3. A lack of awareness, among both consumers and enterprises, of potential risks
4. Network support for "dynamic" alpha-tag originators
5. A lack of effective regulation of A2P vendors
6. Number harvesting

SMS PHISHING (SMiShing)



IMPACT

Illegal activity through SMS Phishing can result in significant inconvenience or financial detriment to a consumer or enterprise through:

- a. Possible disclosure of personal and confidential information
- b. Unknowingly authorising fraudulent transactions
- c. Bank accounts could be taken over using diverted one-time PINs
- d. Credit scores and personal financial status is at risk of damage

Consumers who are tricked will lose trust in the SMS channel and in the masqueraded enterprise.

There are various estimates of the scale of the problem, but all point to an increasing incidence in line with the growth of smartphone adoption.

DETECTION

Detection requires a combination of identifying legitimate originators and active monitoring of messaging traffic:

- a. Register enterprise and brand names and associated short codes and originators
- b. Pattern detection
- c. URL detection

Monitoring both patterns and message volumes is key as SMS Phishing tends to be targeted towards a large number of mobile subscribers.



SMS PHISHING (SMiShing)



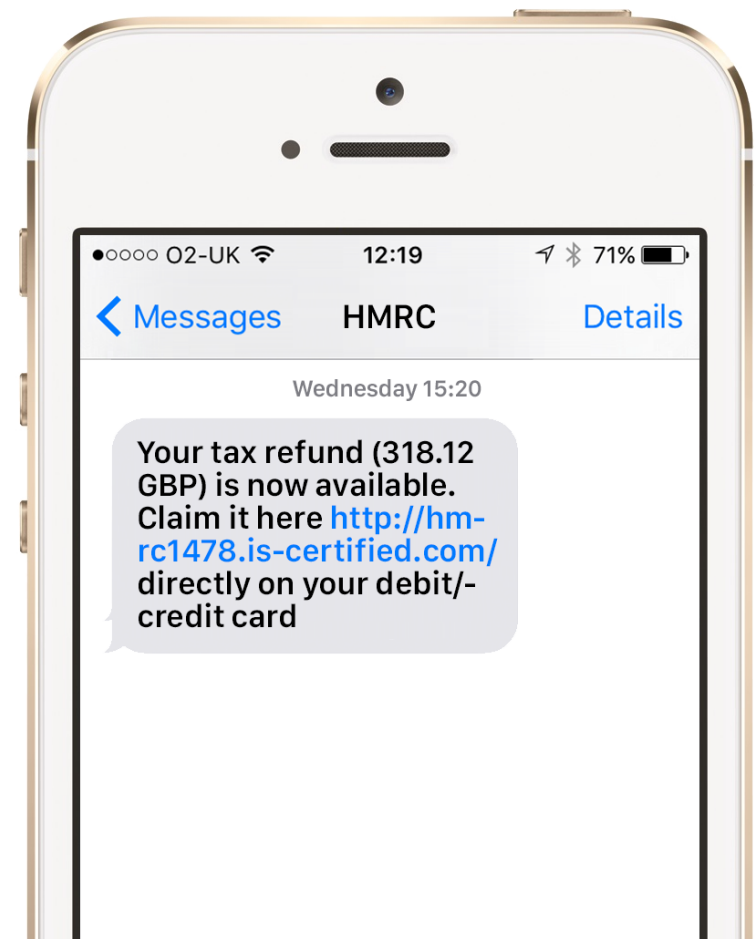
PREVENTION

Recommendations for the prevention of SMS Phishing are as follows:

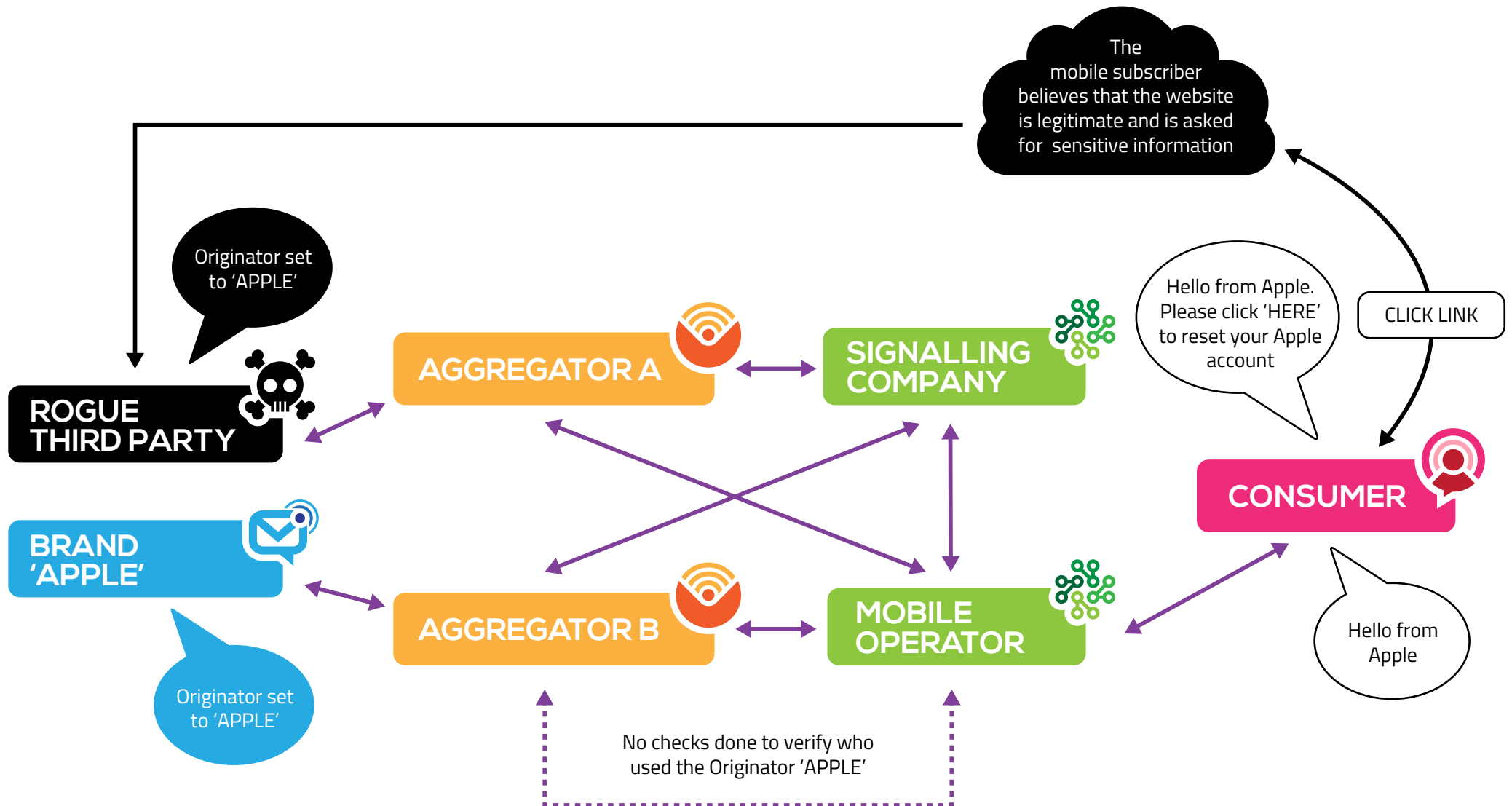
- a. Tier 1 aggregators and mobile operators should block messages which use unregistered or unauthorised originators
- b. Create a central registration of enterprise and brand names and all associated short codes and originators
- c. Enterprises should advertise their short codes on their web sites, together with information detailing what a consumer should or should not expect to be asked by a bank or retailer, for example, within a legitimate communication
- d. Effective data management is essential
- e. Raise enterprise awareness of the risks of fraud and their levels of understanding of how they can help to protect their customers
- f. Enterprises should communicate 'personal' information in messages such as a forename, secret word or phrase which the consumer has shared with them in advance
- g. Enterprises should initiate communication with any affected consumer which explains the next steps, follow up and actions
- h. Educate consumers to help them better protect themselves and be able to locate useful information if affected by fraud
- i. Share knowledge of fraud cases within the global ecosystem
- j. Implement a Code of Conduct for A2P platform providers and aggregators
- k. Facilitate joint enterprise, mobile operator and government initiatives to raise awareness

EXAMPLES

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



SMS PHISHING



4: SMS MALWARE (SMS HACKING)



AFFECTED PARTY	
	NETWORK
	MARKET
	ENTERPRISE
	CONSUMER

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 mobile subscriber’s operating system and access information about accounts or data such as credit card, banking information or passwords for malicious reasons.

Software is installed on a device without the mobile subscriber’s knowledge or is disguised as an innocent app that acts silently in the background, compromising sensitive data or exploiting the connectivity of the device.

Similar to SMS Phishing, SMS Malware messages are used to direct a victim’s smartphone browser to a malicious URL that installs malware which can:

- a. Re-configure phone settings, applications or data
- b. Send messages or make calls to premium rate services
- c. Access the SMS inbox to obtain messages containing bank balance alerts or PIN codes etc
- d. Access the contact list and other personal information
- e. Use the contact list to spread the malware via a communication from a “trusted source”, namely, the victim

CAUSE

Similar to SMS Phishing, the primary cause of SMS Malware is the promise of financial gain either directly or indirectly, through the ability to sell connectivity to third parties and the relative ease at which mobile subscribers can be exploited through the use of basic social engineering and masquerading techniques.

In addition to the causes of SMS Phishing which apply here, 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 by rogue third parties.



SMS MALWARE (SMS HACKING)



IMPACT

Illegal activity through malware or hacking can result in significant inconvenience or financial detriment to a mobile subscriber or enterprise through:

- a. Possible disclosure of personal and confidential information
- b. Unknowingly authorising fraudulent transactions
- c. Bank accounts could be taken over using diverted one-time PINs
- d. Credit scores and personal financial status is at risk of damage
- e. Bill shock if, for example, the phone is used to send premium rate messaging or used as a relay for SMS or voice calls

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 their web browser to an SMS Phishing or Malicious URL.

Malware can affect any smartphone connected to the internet – Android, Apple, Windows etc. Such malware can often go undetected until there is a direct financial or personal impact.

Consumers who are tricked will lose trust in the SMS channel and in the masqueraded enterprise.

DETECTION

Detection requires a combination of identifying legitimate originators and active monitoring of messaging traffic:

- a. Register enterprise and brand names and associated short codes and originators
- b. Pattern detection
- c. URL detection

Monitoring both patterns and message volumes is key as SMS Malware tends to be targeted towards a large number of mobile subscribers.



SMS MALWARE (SMS HACKING)



PREVENTION

Recommendations for the prevention of SMS Malware are as follows:

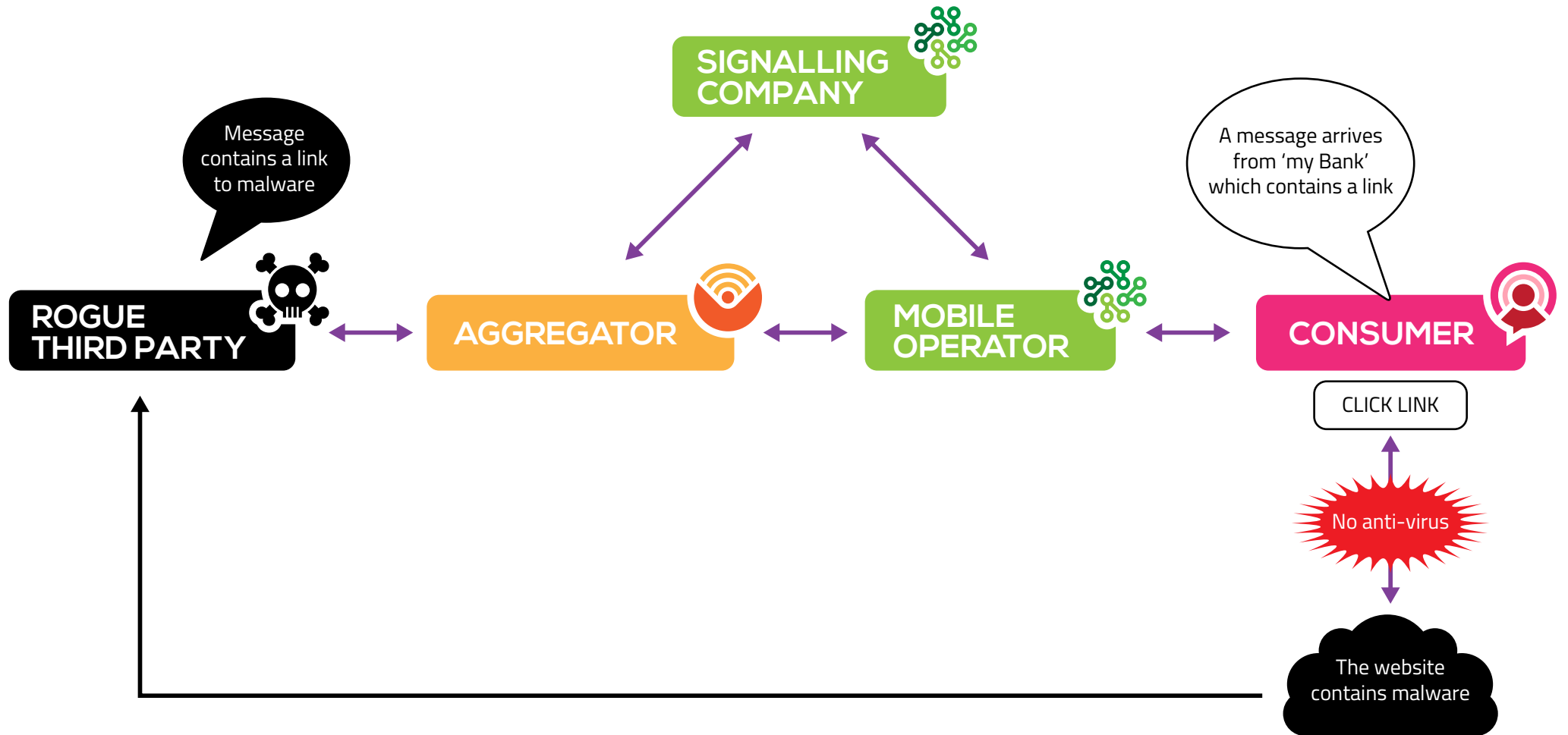
- Enterprises should publish clear guidance for consumers of how to use their services, what signs of potential fraud to look for and how to report suspicious activity
- Implement cross-border registration schemes for alpha-tag originators
- Provide industry-wide resources for monitoring, recording and mitigating fraud
- Operating system software vendors have a duty to ensure that handsets are secure and should work with distribution channels, including mobile operators, to ensure that devices are kept up to date and patched to detect and remedy vulnerabilities before they can be exploited
- Educate consumers around the risks of their preferred operating system and of downloading apps from non-trusted sources, thus allowing them to make a more informed purchasing decision and / or supplement the security of their device with third party security and anti-virus software

EXAMPLES

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)



5: ACCESS HACKING



AFFECTED PARTY	
	NETWORK
	MARKET
	ENTERPRISE
	CONSUMER

DEFINITION

Access Hacking occurs when a party tries to hijack the credentials of a legitimate third party or send a message using one or all of the following techniques:

- Hacking techniques (e.g. accessing a website that has the capability to send SMS messages)
- Provide inaccurate or fake company information
- Use a stolen credit card or other payment method
- Buy messages without having any intention of paying for them

CAUSE

The primary motivation for this type of fraud is to send SPAM or SMS Phishing messages and not be held liable for any consequences by remaining anonymous.

A secondary motivation may be for smaller aggregators to make money by getting credit from large mobile operators or aggregators and then selling these messages but without any intention of paying for them, thus defrauding the mobile operators and aggregators.

The availability of free credit on SMS portals also gives opportunity to those parties who may want to commit fraud.

IMPACT

- Liability falls to the aggregator or mobile operator for SPAM or SMS Phishing messages
- Financial loss is suffered by the aggregators and mobile operators
- Reputational damage is caused where rogue third parties steal the credentials of legitimate enterprises and send messages in their name

DETECTION

Generally, consumer reports of SPAM or SMS Phishing will lead to the discovery of this type of fraud, but the following can also help:

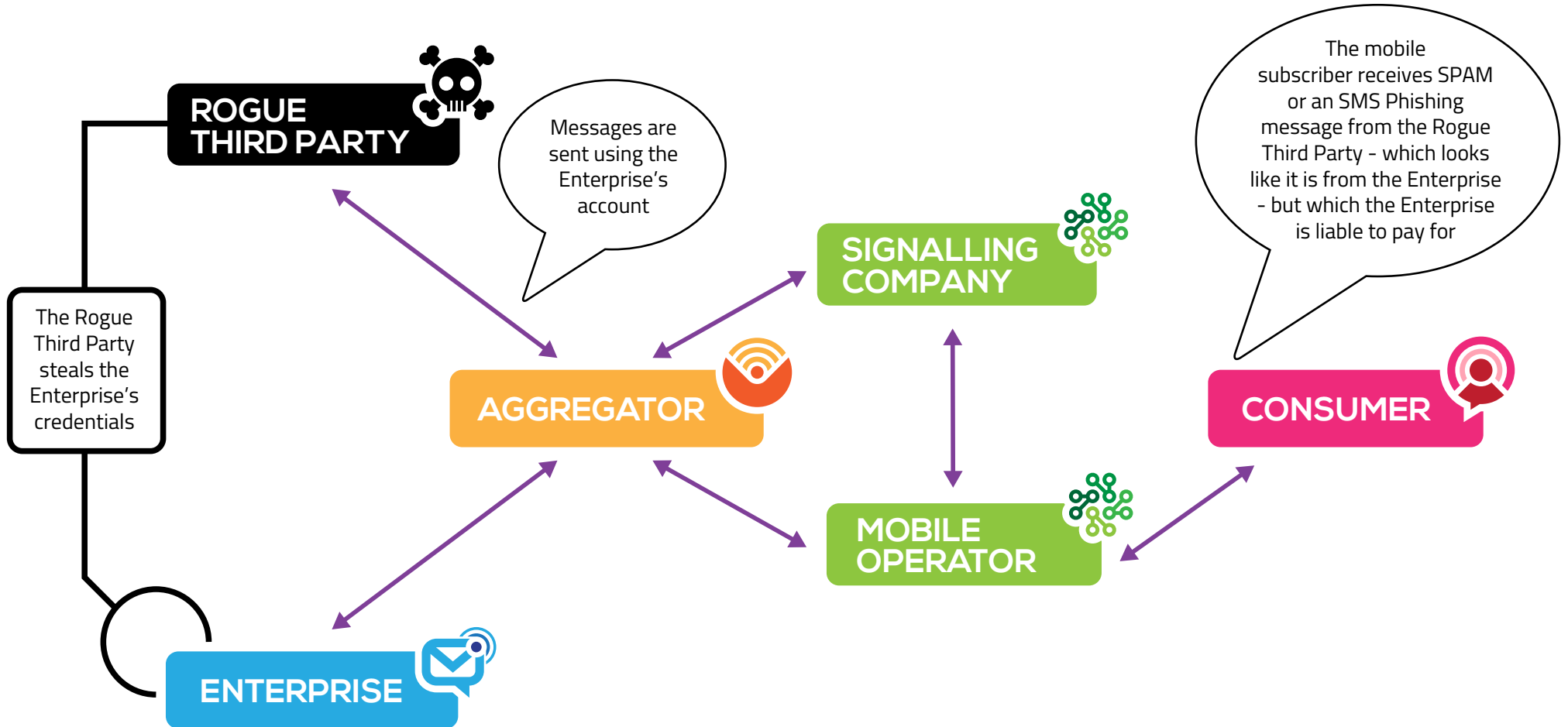
- Monitoring within aggregator and mobile operator systems
- Monitoring of credit utilisation for new customers

PREVENTION

Recommendations for the prevention of Access Hacking are as follows:

- Ensure extensive scrutiny is given to the allocation of credit to new customers
- Ensure proper protection is in place on websites and SMS portals etc.
- Ensure that where free credit is given, bots cannot automate the creation of accounts

ACCESS HACKING



6: GREY ROUTES DUE TO ABSENCE OF AA19 / AA60 AGREEMENT



AFFECTED PARTY

-  NETWORK
-  MARKET
-  ENTERPRISE

DEFINITION

The sending of A2P messages between mobile operators in the absence of an AA19 / AA60 agreement is fairly common practice, but where the absence of a commercial agreement is exploited as a way to avoid paying for message termination, it is regarded as a Grey Route.

Where the technical capability exists to use a route which is open and where there is no AA19 or AA60 agreement in place, this is **not** considered to be fraudulent under this definition, but instead, opportunistic and is the result of a 'sender keeps all' legacy policy dating back to the early days of SMS and the Global System for Mobile Communications (GSM) when the A2P market was small. In this scenario for A2P traffic, it does prevent the consumer's mobile operator from monetising messages which are sent.

The 'sender keeps all' policy was common practice at a time when only Person to Person (P2P) messages were exchanged, with a balance in place in terms of the volume of traffic being both sent and received. As a consequence, only small net amounts needed to be settled between the sending and receiving parties.

Where no other way exists to send a message, i.e. the sending mobile operator is unwilling to sign commercial agreements either directly via an A2P agreement or through AA19 on Signalling System 7 (SS7) or via a Hubbing connection for the termination of messages, then sending a message without a commercial agreement in place, will be deemed legitimate and falls outside of this definition.

If a message is manipulated in any way, either by changing the Global Title in the Mobile Application Part (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

The cause is generally due to parties trying to gain competitive advantage:

- a. Aggregators seeking to reduce the cost of sending a message in order to **1)** make more money on existing traffic, or **2)** attract more traffic by having a competitive advantage
- b. Aggregators trying to compete with each other, i.e. if one aggregator is using a Grey Route then the rest must also do so in order to remain competitive
- c. The perceived commoditisation of SMS ("It's just an SMS") allows aggregators and application service providers (ASP) to blend direct connections with Grey Routes
- d. There is a one-size-fits-all view of SMS messaging and its business applications
- e. Price-led procurement activities carried out by aggregators and some Over The Top (OTT) players via SMS auctions
- f. The absence of a joined-up digital communications strategy within enterprises
- g. The ease with which parties can obtain Global Titles and point codes from certain regulators
- h. Where there is a disconnect within mobile operators between P2P, A2P wholesale and enterprise functions, as well as between business stakeholders and procurement



GREY ROUTES DUE TO ABSENCE OF AA19 / AA60 AGREEMENT



IMPACT

This type of fraud results in financial, service quality and ultimately reputational damage:

- a. The availability of cheaper but unauthorised routes causes confusing and volatile market prices
- b. An estimated 20% of A2P global revenue is not being monetised by the consumers' mobile operators
- c. Resource is spent on identifying unofficial routes in order to establish a commercial agreement or to close them
- d. Reliability of message delivery is low, especially in the support available for ported numbers
- e. Routes can be good quality as long as there is no filtering which results in very unpredictable quality of service
- f. Routes can be terminated or changed with little or no notice as mobile operators apply filters
- g. The closure of routes can result in the sudden failure of all messages
- h. The ability to meet an enterprise's SLAs can be affected
- i. Reputational damage can result from the unpredictable results of using Grey Routes
- j. Poor levels of service quality and delivery can reduce an enterprise's trust and satisfaction
- k. Consumers may discover that a service is not working reliably, and in turn, negatively affect their response to an enterprise or messaging as a whole

DETECTION

Detection of the use of Grey Routes which are not subject to commercial agreements requires the following:

- a. Firewalls and routers within mobile operator networks to detect messages coming in from unauthorised channels
- b. Promote a consistent mobile operator approach to monitoring and filtering
- c. Raise enterprise awareness of the causes and risks of Grey Routes
- d. Create cross-industry resources for awareness of authorised pricing



GREY ROUTES DUE TO ABSENCE OF AA19 / AA60 AGREEMENT



PREVENTION

Recommendations for the prevention of the use of non-commercial Grey Routes are as follows:

- a. Install firewalls and routers within mobile operator networks and have these constantly monitored. To note: Ongoing monitoring is essential as firewalls can block A2P traffic but some aggregators using Grey Routes will always try to bypass filters, such as by using a mobile number as an originator, changing the message content or by using several Grey Routes to reach one destination
- b. Close and migrate bilateral 'sender keeps all' routes to SMS Hubs in order to monetise traffic without impacting P2P message streams
- c. Keep important bilateral routes open, imposing commercial AA19/AA60 agreements where required
- d. Create educational resources for enterprises across the following departments:
 - Business stakeholders
 - Procurement and finance
 - Technology and security
 - Legal and compliance
 - Executive level

EXAMPLES

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.

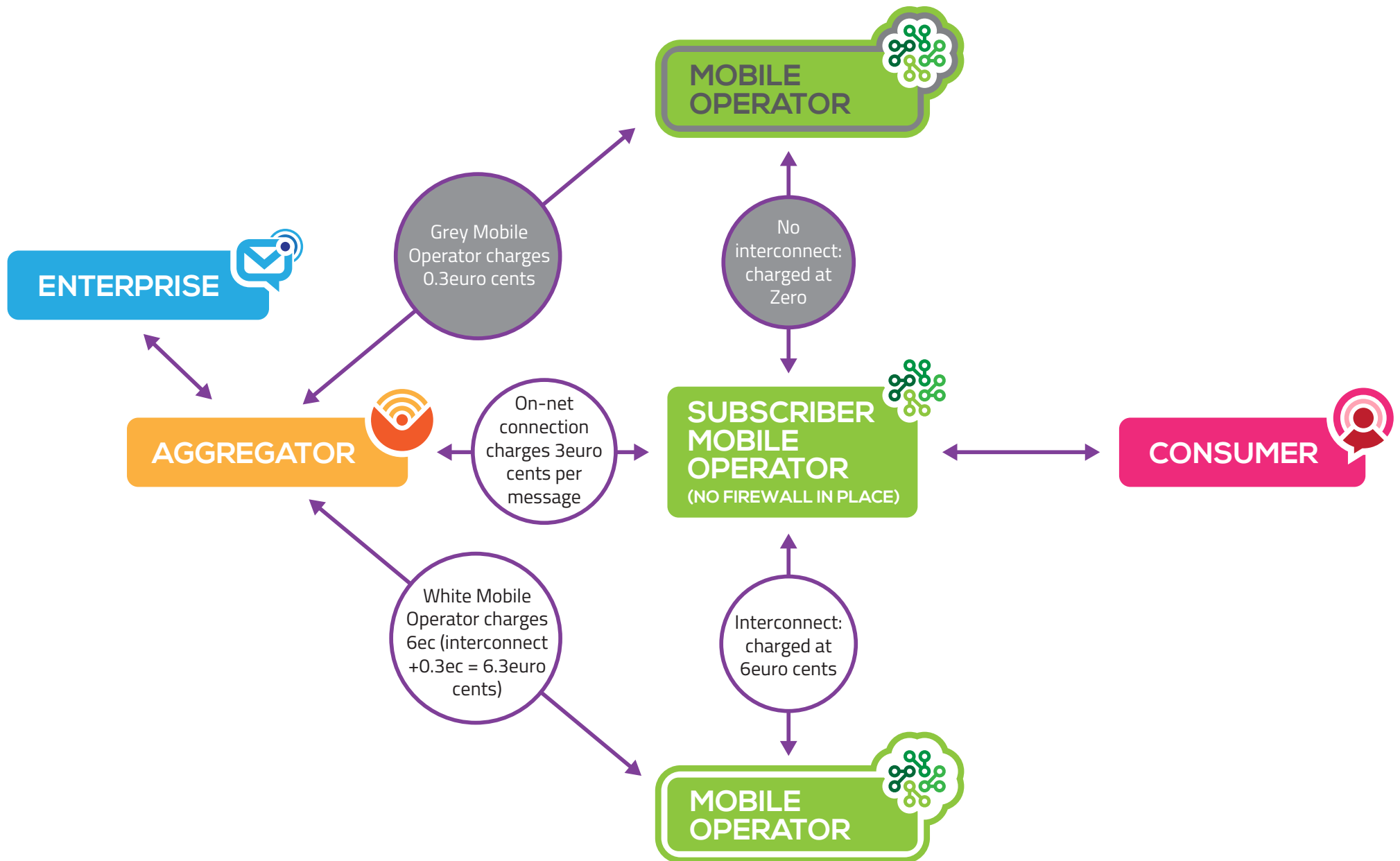
```

Signature
+447... UK Sender ID
Source TON/NPI
1/1
Timestamp
Unix Time: 1440750831
28/08/2015 10:33:51 +0200
SMSC Timestamp
15/08/28 09:08:00 +0100
SMSC
+1... SMSC +1 region
Data Coding Scheme
0
Encoding
0 (Default GSM)
Has UDHI
No
Concatenation
Group: 0 Count: 0 No.: 0
Flash/Alert
No
Message Text
Ihr Verifizierungscode lautet 837485.

```

A2P Enterprise One time password SMS

GREY ROUTES DUE TO ABSENCE OF AA19/AA60 AGREEMENT



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



AFFECTED PARTY



NETWORK



MARKET



ENTERPRISE



CONSUMER

DEFINITION

MAP Global Title Faking is the effect of a person or company manipulating a message by changing a MAP parameter, by changing the originator in order to prevent detection by a firewall or by pretending to be a mobile operator 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 a mobile operator's firewall, they can reach a mobile operator's SMSC at the Message Transfer Part (MTP) level, the signalling point code.

CAUSE

The cause is similar to that for Grey Routes, but here, an aggregator is trying to gain an unfair competitive advantage by manipulating the message to try and trick a mobile operator and their firewall implementation into letting through a message that would otherwise be blocked.

IMPACT

The impact is similar to that of a Grey Route, but in this scenario, in addition to messages not being monetised, a mobile operator will be required also to spend money trying to understand how messages are flowing into their network without being paid for.

Aggregators who do not manipulate messages in this way will be disadvantaged and less competitive, leading to less ethical aggregators growing in size and winning business unfairly.

DETECTION

Central processes can be put into place to identify where deliberate manipulation of a message has taken place:

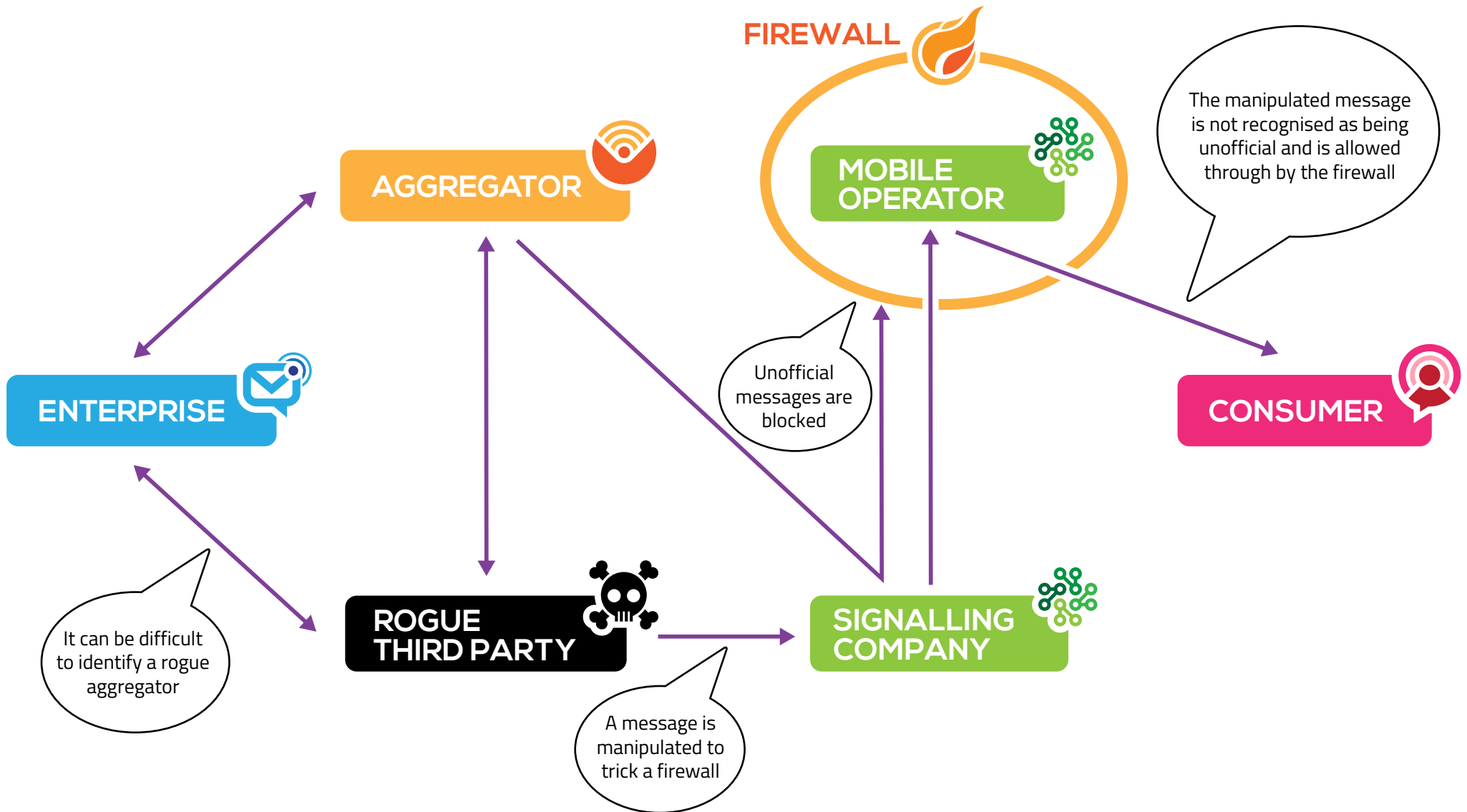
- Set firewalls to look for specific types of MAP manipulation
- Set SMS Hubs to look for specific types of message manipulation
- Ensure firewalls are correctly configured (see below) where reports or alarms can be created to detect whether a Service Centre address has been manipulated
- Set SCCP (Signalling Connection Control Part) 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
- Identify aggregators selling messages at below market price

PREVENTION

Recommendations for the prevention of MAP Global Title Faking are as follows:

- Ensure proper configuration of a firewall, i.e. compare the received Service Centre address and calling party Global Title in the Forward Short Message (FSM) instruction to ensure that these match or at least partially match (in terms of leading digits) and that the Service Centre address has not been manipulated
- SCCP providers should ensure that SCCP Global Titles and MAP Global Titles correspond
- Create clear guidance of what is and is not permitted in terms of message manipulation to remove any risk of ambiguity
- Create a 'best practice' policy to which aggregators agree and adhere to
- Name and shame those aggregators who refuse to comply with 'best practice' or who continually seek to exploit networks

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





8: SCCP GLOBAL TITLE FAKING



AFFECTED PARTY



NETWORK



MARKET



ENTERPRISE



CONSUMER

DEFINITION

SCCP Global Title Faking (Faking) is the act of sending a message to a handset originating from a Global Title that either **1)** does not belong to the sender or, **2)** has been leased from a third party and where the SCCP or MAP addresses are manipulated.

The entity generating the fraud has International SS7 capabilities at SMSC level and their manipulation of a Global Title allows it to initiate SMS Mobile Terminated (MT) call flows with the destination mobile operator which is unaware that the Global Title being used by the sender is not legitimate.

Faking occurs when a legitimate Global Title belonging to a rogue third party, obtained either directly from a regulator or leased, is used to send only the Send Routing Information (SRI) request in order to obtain necessary information such as the International Mobile Subscriber Identity (IMSI) and Visitor Location Register (VLR). Another Global Title, belonging to a third party mobile operator who has not given permission for this second Global Title to be used by the rogue third party, is then used to send the FSM.

Sending the FSM is purely unidirectional as an FSM response confirmation is not needed in 99% of cases, provided that the FSM request was made very shortly after the SRI. The reason for the use of different Global Titles is that in order to send a message, an SRI response is needed and this can only be achieved using a legitimate Global Title that will allow for the response to be returned correctly.

Please note that only SCCP Global Title Faking is addressed here. While IMSI Faking does occur, it is incredibly rare and difficult to achieve.

CAUSE

Faking enables a party to gain a competitive advantage and make money from messages by selling them at slightly below market rate. The termination cost will be close to zero for the sending party, as they only pay for signalling, so this can be very lucrative. This can happen for the following reasons:

- Mobile operators selling SRIs and giving out the full International IMSI which is required to achieve this fraud
- SCCP providers typically only check once if they own the address space and therefore it can be easily manipulated
- SCCP providers are not incentivised to do anything about this as they make money on Message Signal Units (MSU)
- Mobile operators not adequately protecting their own network, namely receiving traffic into their network versus someone using their Global Title to get into another network
- The absence of any end-to-end process to unambiguously identify the fraudulent parties who therefore remain in plain sight without facing any consequences



SCCP GLOBAL TITLE FAKING



IMPACT

The main impact of this type of fraud is financial, but can also be reputational as service delivery can be affected through the manipulation of the routing environment:

- a. Mobile operators get charged interworking charges for traffic that they never sent
- b. Mobile operators lose profits directly as the A2P traffic terminating into their network via faked routes is not paid for, or alternatively, they suffer higher OPEX related to the work needed to identify interworking fee discrepancies and negotiate incorrect fees with the mobile operator's interworking partner(s)
- c. Legitimate aggregators lose business to rogue third parties
- d. Enterprises are being lured by cheap rates to send traffic over routes that are inherently unstable (due to the preventive measures deployed throughout the ecosystem) which can result in loss of messages or complete service disruption
- e. Consumers risk not receiving requested A2P messages

DETECTION

The vast majority of Faking comes from the ecosystem because in order to exploit this fraud, the fraudulent party must be able to sell messages within it. As such, the fraudulent party must be a known entity within the ecosystem and mobile operators should therefore monitor for this type of fraud on their networks.

Possibility for Aggregators

- a. Fake delivery notifications can be an indication of this type of fraud. To note: fake delivery notifications are not believed to be a fraud in themselves but are a symptom of fraud.
- b. Lower market pricing to a particular destination coming from known Global Titles that cannot be explained. This is especially relevant if there is an interworking agreement between the sending (according to the Global Title being used) and receiving mobile operators, market pricing is below this interconnect level and traffic need not be balanced across all networks in the destination country - if there is a requirement to balance traffic the seller of the message might be selling some networks at a loss but intends to make money on the total traffic.
- c. Report any suspicions to the targeted mobile operators as quickly as possible as the aggregators are the eyes and ears of the ecosystem

Possibility for Mobile Operators

- a. Monitoring to determine whether the SRI request is being sent from a different Global Title as the FSM request
- b. Monitoring of whether a response to an FSM request is being received but where an FSM request was never sent
- c. Carry out thorough reconciliation of the interworking feed. A discrepancy might indicate that the mobile operator's Global Title is being used for Faking. Where it will be difficult to identify the rogue third party in a historical scenario (as interworking reconciliation typically happens a few months after traffic was sent) the fraud might still be on-going and can then be stopped and investigated.



SCCP GLOBAL TITLE FAKING



PREVENTION

Recommendations for the prevention of SCCP Global Title Faking fall within the realm of the mobile operators and are as follows:

- a. Implement systems that ensure the SRI request and the subsequent FSM request are sent from the same Global Title. If there is a mismatch then the FSM is blocked. This prevents Faked messages being terminated on the mobile operator's network.
- b. Implement systems that trigger an alarm if a response to a FSM request is being received but where a FSM request was never sent. This does not prevent the Faking but it enables the sending mobile operator to contact the receiving mobile operator which uses the first mobile operator's faked Global Title.
- c. Do not provide the full Global Title when selling SRI's. A country code fulfils the vast majority of legitimate use cases and if more of the Global Title is to be provided, the mobile operator should only do this for identified use cases.
- d. Block lone FSMs destined for its subscribers where an SRI does not precede it. A mobile operator would not be able to do this for roaming subscribers as it would never see the SRI for a message terminated to a roaming subscriber because 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.
- e. Return scrambled IMSIs.
- f. Include a contractual requirement that an SCCP provider checks that the address space being used by a sender is correct in real time.
- g. Treat suspected incidents extremely seriously, investigating the incident end to end with the full co-operation of the SCCP providers and mobile operators to determine the true sender before logs disappear. This will ensure fraudulent parties know that there is a high risk of being discovered.
- h. Establish a globally agreed process involving forensic investigators, where the co-operation of all parties is required. An independent company would be required to lead any investigation to ensure impartiality.

NOT RECOMMENDED

Mobile operators could try and block all SRI's related to A2P SRI traffic. However, this damages the ecosystem as it makes legitimate A2P SMS delivery less reliable which would have a detrimental impact for consumers, enterprise, aggregators and mobile operators alike by:

- a. Damaging the ability to support and troubleshoot within the ecosystem
- b. Making legitimate routing impossible in countries where mobile number porting does not exist

9: SMSC COMPROMISE FRAUD



AFFECTED PARTY	
	NETWORK
	MARKET
	ENTERPRISE
	CONSUMER

DEFINITION

The entity generating the fraud has access to the International SS7 Network, manages to reach a mobile operator SMSC at MTP level, the signalling point code, and is able to use this SMSC to relay and send messages around the world without paying for them. This leaves the owner of the SMSC to pay the message termination charges.

CAUSE

An aggregator, or other party, can gain competitive advantage by avoiding interworking costs while an enterprise can buy messages at a cheaper rate than the official mobile operator A2P rate.

The root cause is that the mobile operator has not taken sufficient security precautions to prevent the SMSC from being used as a relay.

Mechanism:

1. The aggregator sends an MO request to the compromised mobile operator SMSC
2. The compromised SMSC will send the message to the destination mobile operator
3. The aggregator will not receive a true Delivery Receipt (DLR)
4. The compromised SMSC mobile operator receives the bill for any interconnection fees incurred

IMPACT

On Aggregators:

- a. The aggregator delivers the message to the destination mobile operator free of any interworking cost, with just one Messaging Signalling Unit (MSU) cost, or free of any charge where an SMSC is compromised over IP.

On Enterprises:

- a. The enterprise may be able to buy messages to a specific destination at a lower rate than the official mobile operator A2P message rate.
- b. Delivery quality is poor. No real Delivery Receipt (DLR) is received and often the originator is replaced, with the intention of it being accepted by the compromised SMSC at the time of sending by matching the compromised mobile operator's Mobile Station International Subscriber Directory Number (MSISDN) range. There is no alphanumeric support.

On Mobile Operators:

- a. The mobile operator will charge the compromised SMSC mobile operator for the messages received. However, there will be a dispute due to the fact that the sending party has not intentionally sent the traffic. In most cases, the mobile operator will not be able to collect the funds owed.

On P2P Hubs:

- a. If the compromised SMSC uses a P2P SMS Hub to deliver traffic, the compromised SMSC will be invoiced by the SMS Hub and but the charges will be disputed as the traffic was not sent intentionally.

On Third Parties:

- a. The compromised SMSC owner will be charged by the receiving mobile operator for traffic not intentionally originated by it, nor charged to its customer. In cases of low cost assurance and reporting capabilities, especially in emerging markets, the compromised party may not recognise the fraud and will pay the mobile operator charge.

On Consumers:

- a. In some instances, an aggregator will send an SMS MO to the compromised SMSC where the originator will be a random number belonging to an actual mobile subscriber. This mobile subscriber will then be invoiced for messages they never sent. This is one of the only scenarios where there is a direct financial impact on a consumer. In many cases, the mobile operator owning the compromised SMSC will have to reimburse the mobile subscriber while also having to pay termination charges.



SMSC COMPROMISE FRAUD



DETECTION

Detection of this type of fraud can be achieved through a combination of protective processes and the education of buyers of messages:

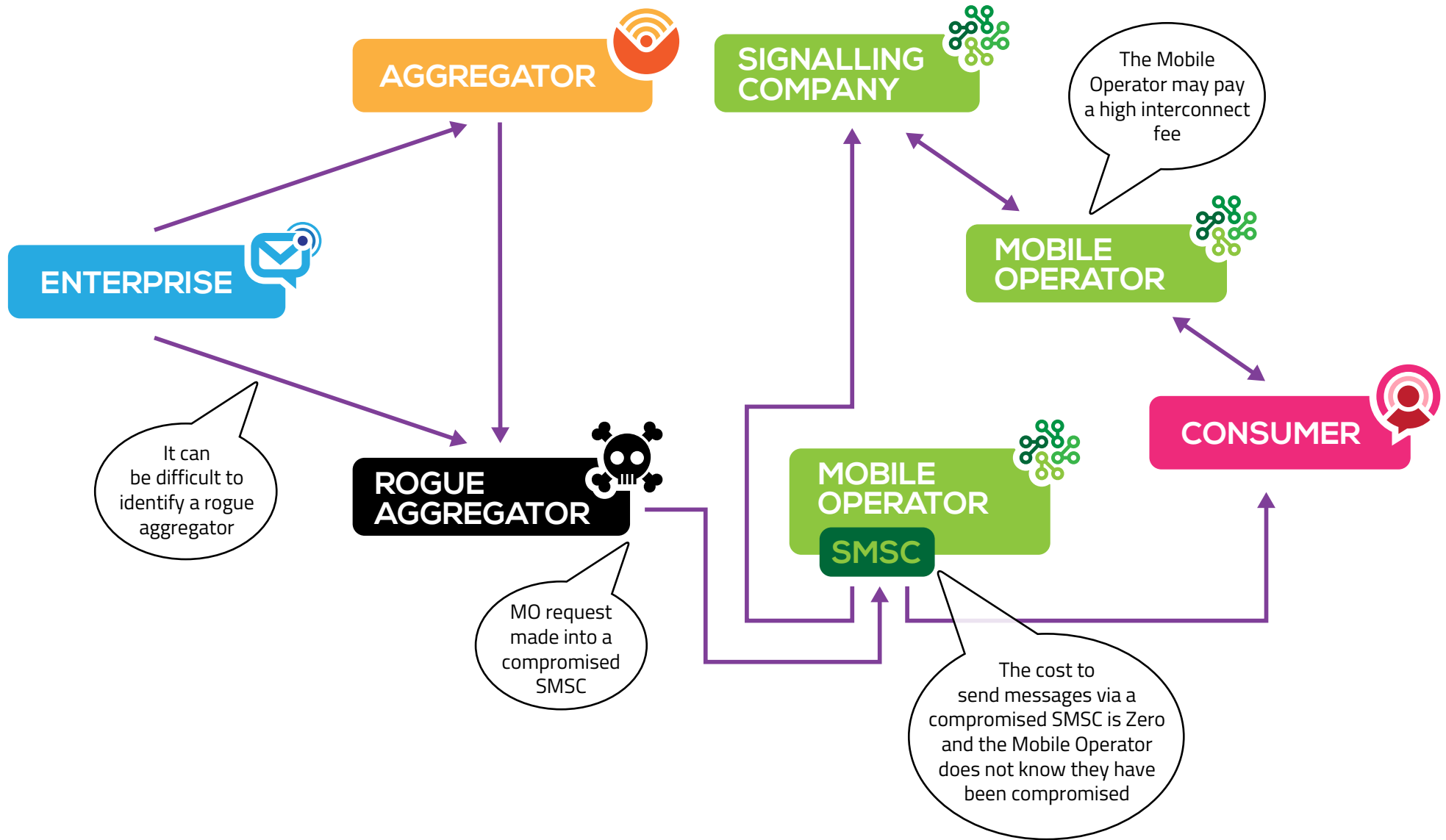
- a. Mobile operators should implement processes and tools to detect MT messages being terminated to suspicious destinations in large quantities and for reconciliation of traffic before moneys billed are paid in error.
- b. SMS P2P Hubs have advanced reporting tools and can support mobile operators by detecting and alerting them to abnormally high traffic peaks.
- c. Educate enterprises to stress the relationship between cheaper messaging and poor delivery quality, lack of delivery receipts and no alphanumeric support which can result in potential loss of business, reputation and trust in their brand.

PREVENTION

Recommendations for the prevention of SMSC Compromise Fraud are as follows:

- a. All mobile operators and SMSC owners should take security precautions and secure their SMSCs.

SMSC COMPROMISE FRAUD



10: SIM FARMS



AFFECTED PARTY	
	NETWORK
	MARKET
	ENTERPRISE
	CONSUMER

DEFINITION

A SIM Farm is a method of using a bank of SIM cards for the delivery of A2P commercial messages. SIM cards used in SIM Farms are generally one of the following type:

- a. Consumer SIM cards with a specific retail offer, including a bundle of SMS on-net or off-net domestic messages, that allow messages to be sent inexpensively
- b. Legitimate Machine to Machine (M2M) or Enterprise SIMs that are sold without sufficient contractual protection to avoid them being used for A2P messaging

It is important to note that not all SIM Farms are used to commit fraud and it is incorrect to assume that all SIM cards are assigned for allocation to consumers.

CAUSE

An aggregator can gain a competitive advantage through bypassing an official Bulk SMS connectivity or interworking agreement and using a mobile operator's retail consumer SIM card offer or M2M SIMs, while an enterprise can buy messages at a cheaper rate than the official mobile operator A2P rate.

Mechanic:

1. The aggregator performs the SMS MT command using a SIM card instead of its own SMSC
2. The mobile operator will deliver the message as the SMS MT request was originated by a retail subscriber
3. The aggregator will likely send a fake DLR to the enterprise

A variant of SIM Farming is the technique whereby mobile subscribers are used as a "mini-SIM Farm", as follows:

1. A mobile subscriber downloads and installs an app provided by a rogue third party
2. The mobile subscriber must have data connectivity (Wifi or 4G)
3. The mobile subscriber agrees to become a "mini SIM Farm"
4. The rogue third party will send the SMS MT to the mobile subscriber who will terminate it to the destination number
5. The mobile subscriber must have a pricing plan with a low charge to send messages for this fraud to be effective



SIM FARMS



IMPACT

On Aggregators:

- a. The aggregator manages to leverage a mobile operator's retail consumer SIM card offer at a more competitive rate than by going via an official Bulk SMS connectivity or interworking agreement

On Enterprises:

- a. The enterprise may be able to buy messages to a specific destination at a lower rate than the official mobile operator A2P SMS rate
- b. Delivery latency is very low. However, the originator is replaced with the MSISDN of the SIM card being used to send the message. Alpha originators are not supported and DLR information is likely to be absent.

On Mobile Operators:

- a. Loss of revenue from the Bulk Messaging side of their business
- b. Loss of revenue due to sending off-net messages at interconnect but without being able to recoup those monies from the SIM card user.

On Mobile Subscribers:

- a. SIM Farms appear to be the SMS delivery channel of choice for rogue third parties who are sending unsolicited messages to mobile subscribers which claim that the recipient has come up in a draw and that they can claim a prize such as an iPhone or voucher in exchange for calling a number, normally at a premium rate, or by filling in a form-link provided within the message.

On Third Parties:

- a. No third party is involved

DETECTION

Education across the ecosystem is key to detecting this type of fraud:

- a. Educate enterprises to highlight the true nature of the low cost of messaging in terms of the originator being replaced with the MSISDN of the SIM card being used to send the message, that alpha originators are not supported and delivery receipt information is likely to be absent
- b. Increase communication between mobile operator Retail and Bulk teams in order to flag misuse of retail SIM cards
- c. Increase controls and checks on who is bulk buying SIM cards via retail channels
- d. Aggregators need to provide insights to the mobile operators as to which aggregators are selling or reselling such connections in the various markets in real time
- e. Messages are terminated with higher delay and modified A-numbers. As such, a modified A-number does not always mean that a SIM Farm is being used



SIM FARMS



PREVENTION

Recommendations for the prevention of fraud through the use of SIM Farms is as follows:

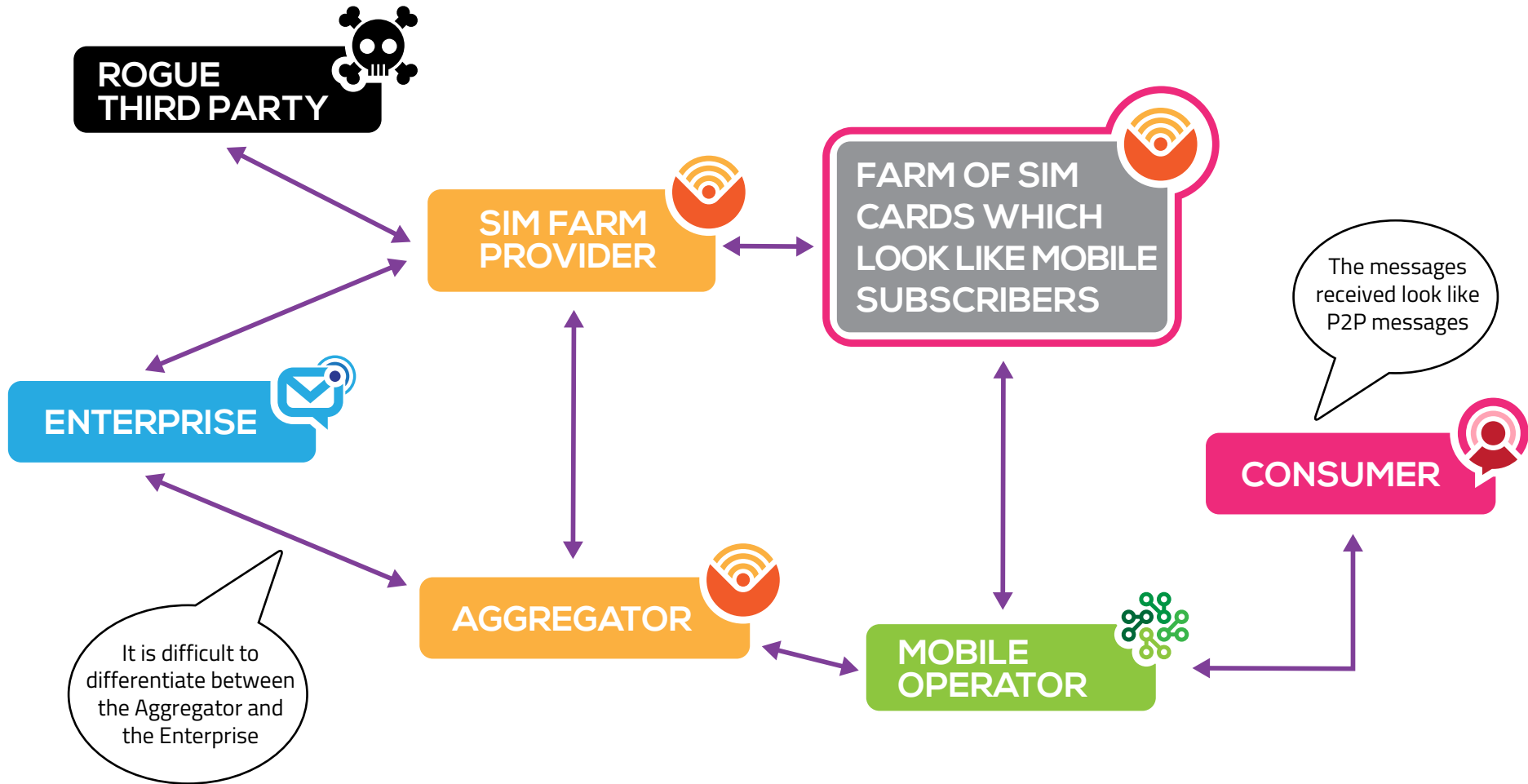
- a. Ensure that consumer SIM cards have sufficient contractual protections in place to prevent them from being used to send A2P messages
- b. Ensure that sufficient monitoring and revenue protection controls are in place to detect SIM cards which are being used to send A2P messages and ensure they are terminated quickly
- c. Ensure that all M2M and legitimate corporate SIM cards have contractual protections in place to prevent them from being used to send A2P messages
- d. Support local regulators and enforcement agencies to take action against SIM Farm Hardware and Software Providers and those who actively use SIM Farms for fraudulent means

EXAMPLES

An example of a message sent using a SIM Farm.



SIM FARMS



11: ARTIFICIAL INFLATION OF TRAFFIC (AIT) / / / /

AFFECTED PARTY

 NETWORK

 MARKET

 ENTERPRISE

 CONSUMER

DEFINITION

Artificial Inflation of Traffic (AIT) is caused when a party uses MO interconnect revenue share as a way of generating profit by sending messages to itself. This fraud is highly associated with SIM Farms as the cost of sending a message needs to be lower than the revenue share return of an interconnect agreement.

CAUSE

The promise of monetary gain by using very simple commercial and technical capabilities.

IMPACT

The primary impact of this type of fraud is financial:

- a. Revenue and profit loss by the mobile operator and the owner of the SIM cards used to send messages
- b. Revenue and profit loss from aggregators or anyone in the value chain that may pay out revenue share only to have it withdrawn by the mobile operator as soon as the fraud is detected

DETECTION

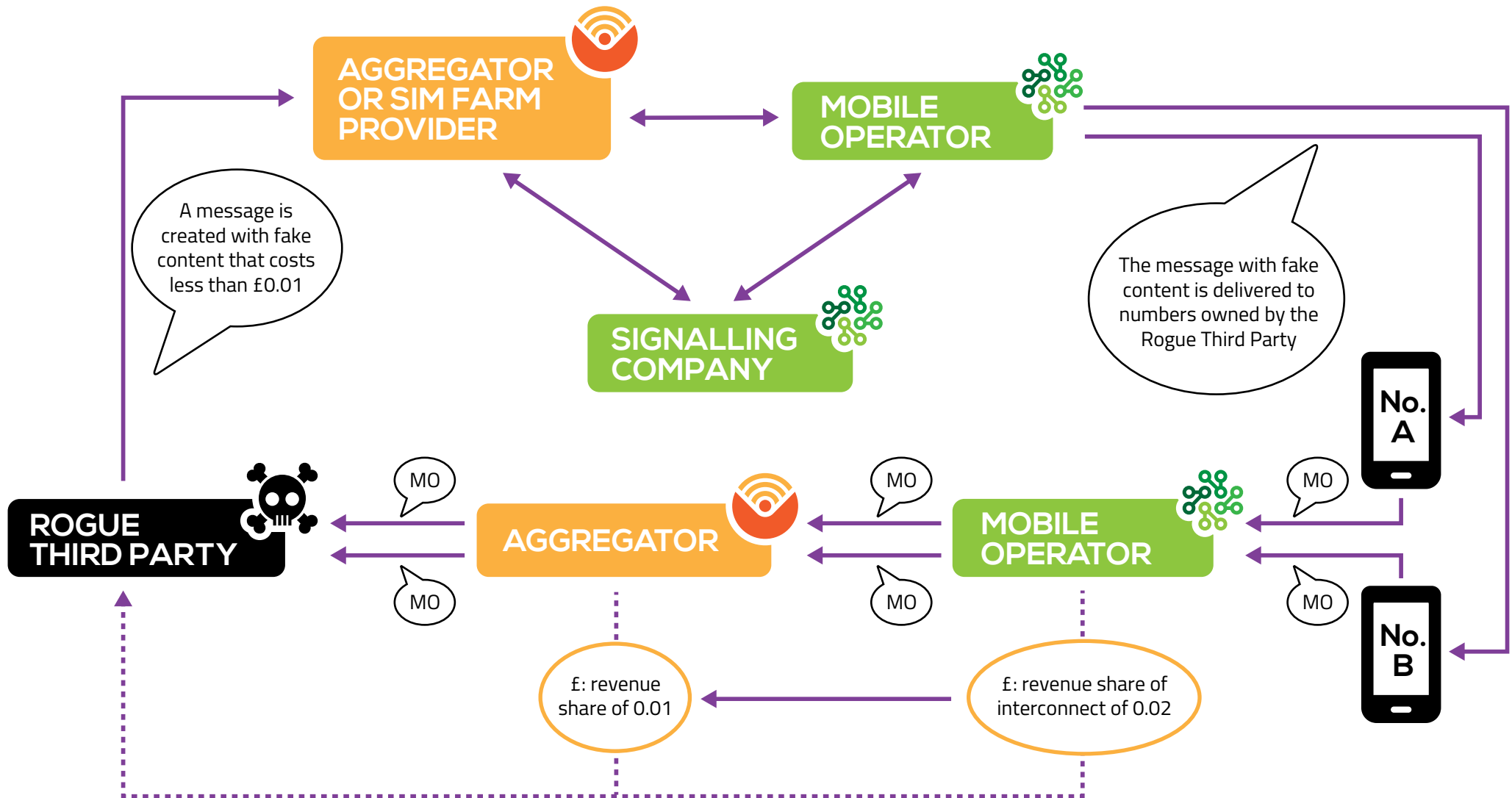
Monitoring for very large volumes of unexplained MOs is the most effective way of detecting this type of fraud. The message content within MO messages can also help to determine whether the messages are credible and have been generated for a legitimate purpose or not.

PREVENTION

Recommendations for the prevention of Artificial Inflation of Traffic are as follows:

- a. Mobile operators should 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
- b. Ensure that the cost of an MT is higher than the receiving revenue share from an MO

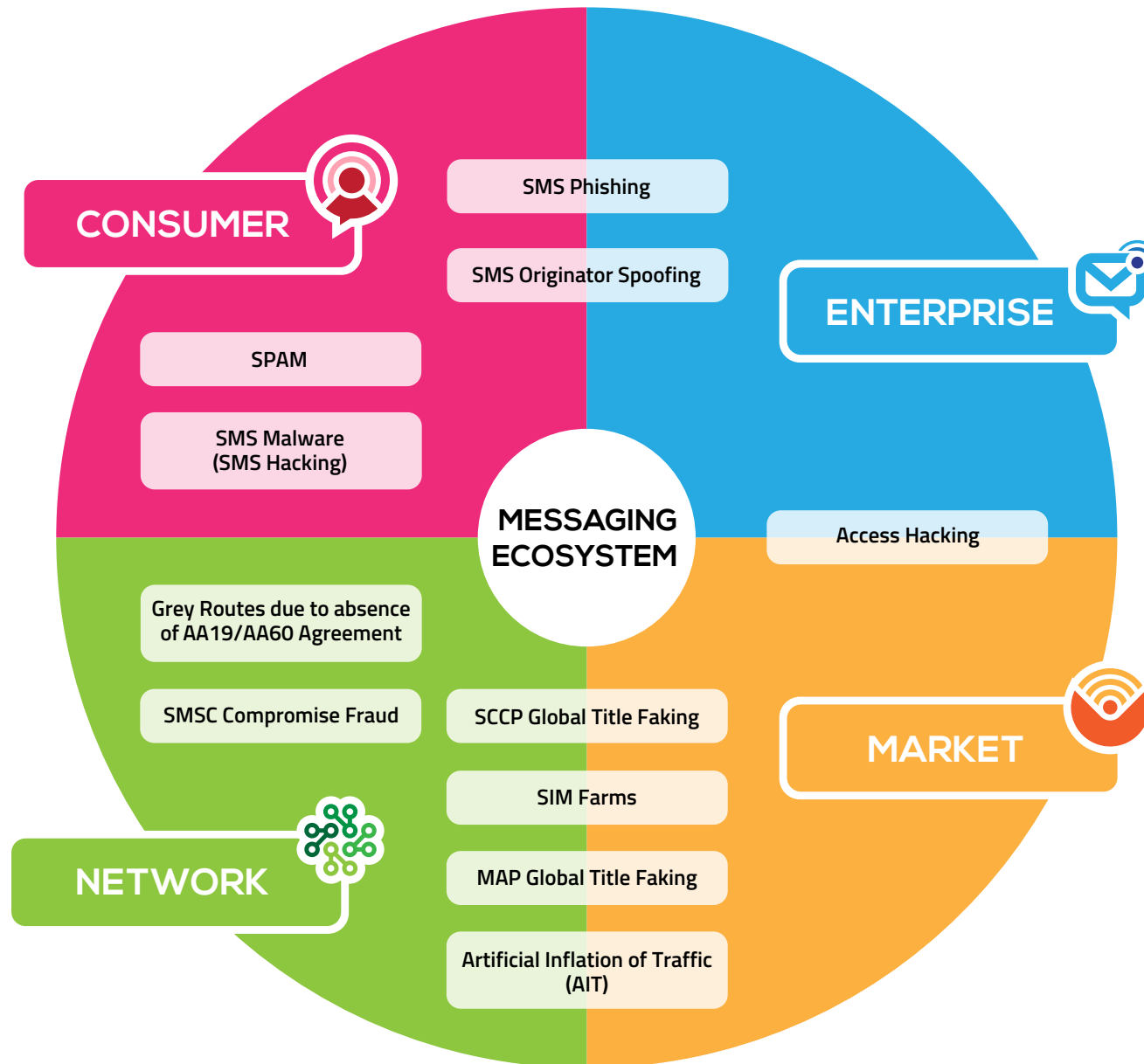
ARTIFICIAL INFLATION OF TRAFFIC (AIT)



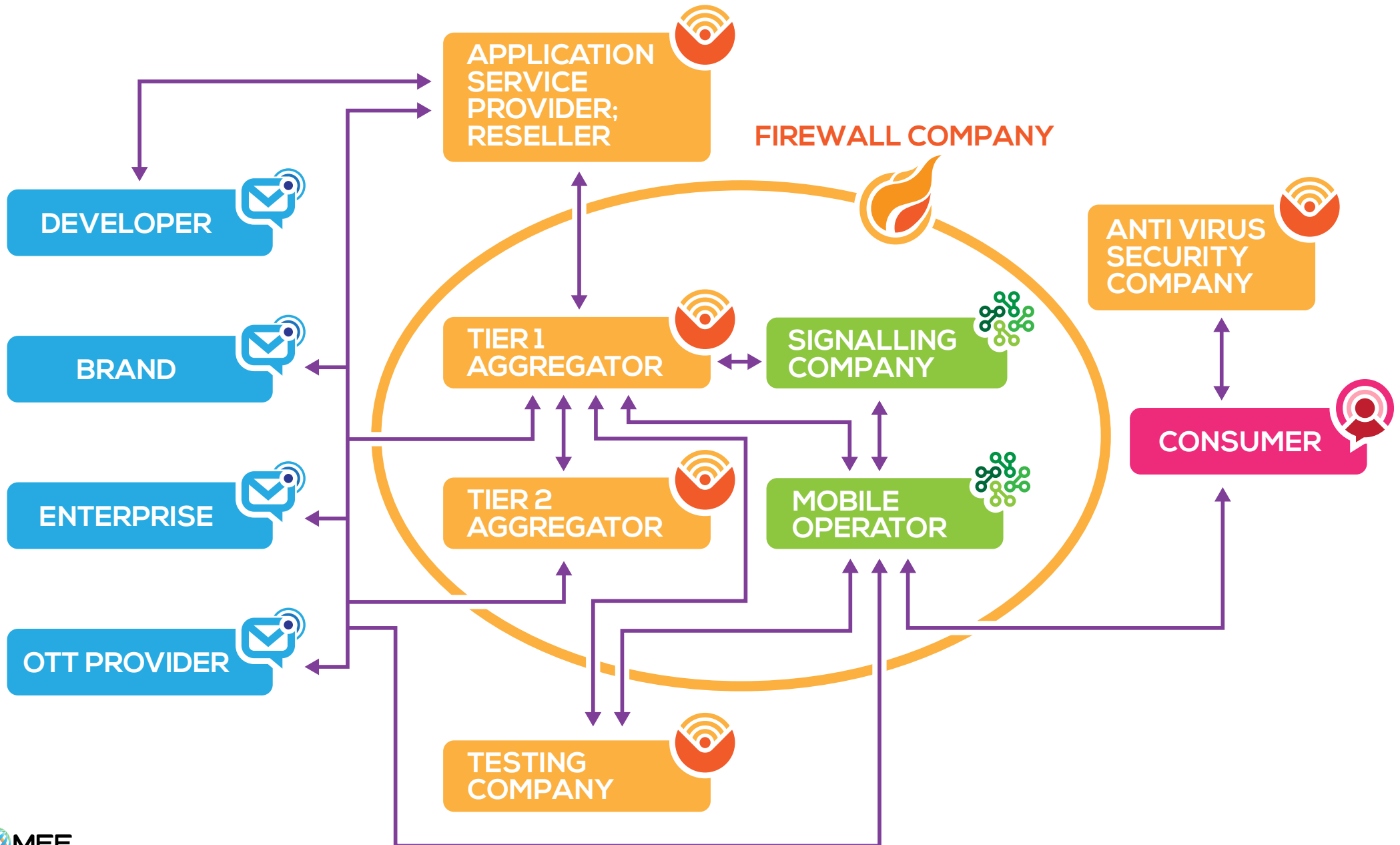
ANNEX



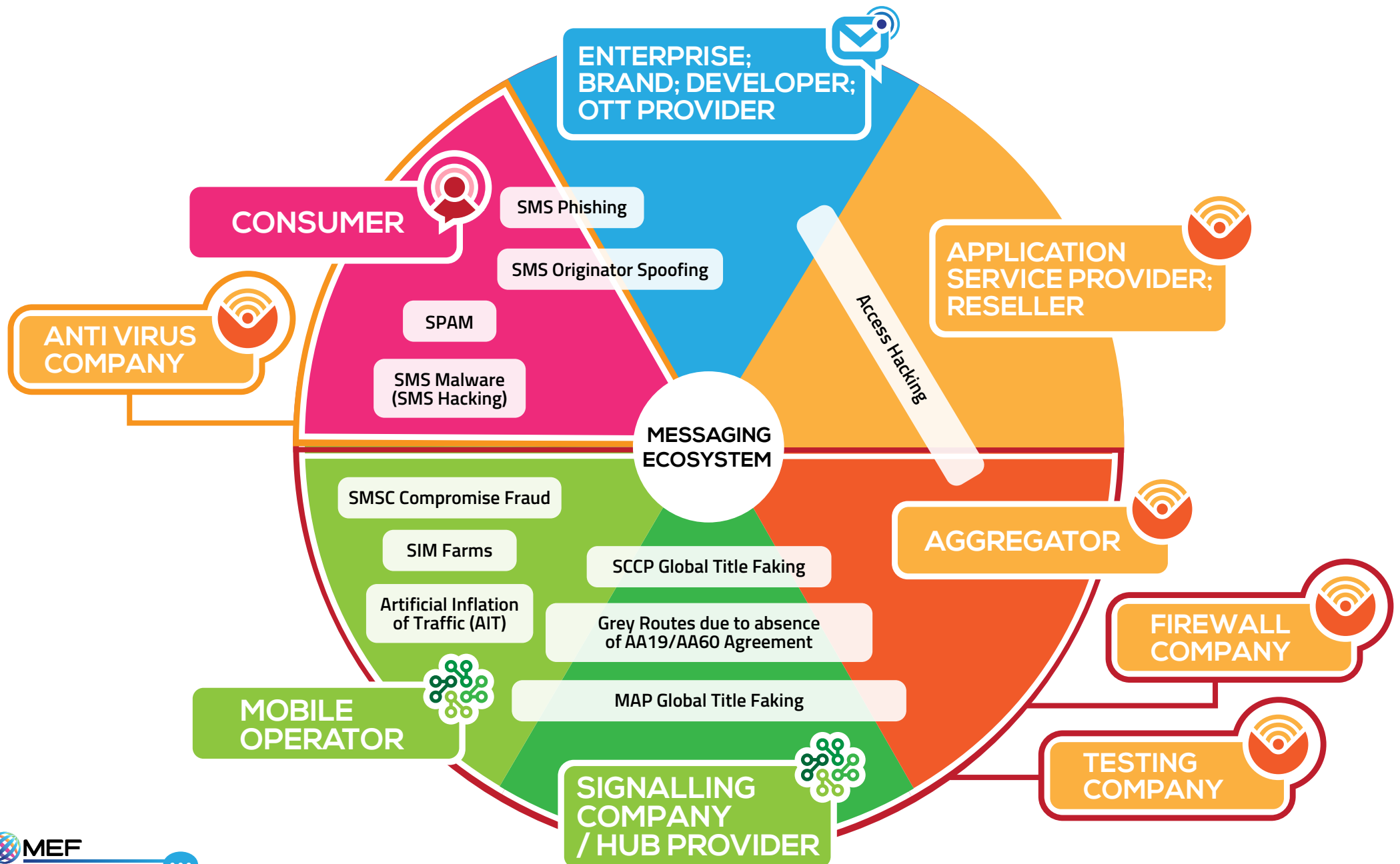
A2P MESSAGING ECOSYSTEM THREAT MAP



MAP OF THE A2P MESSAGING ECOSYSTEM



MAPPING FRAUD IN THE A2P MESSAGING ECOSYSTEM





GLOSSARY

2FA (Two Factor Authentication): This allows an entity to confirm a mobile subscriber's claimed identity by utilising a combination of two different components, namely, something that the subscriber knows, something that the subscriber possesses or something that is inseparable from the subscriber, for example, a mobile subscriber being in possession of a mobile device, plus a PIN.

A2P (Application to Person): This is generally one-way messaging such as marketing messages, appointment reminders and bank alerts.

AA19/AA60 Agreement: An agreement between mobile operators which defines the charges for terminating messages between their networks.

Aggregator: An entity that provides connectivity between mobile networks and mobile service providers.

Alphanumeric Originator; Alpha Originator, Alpha Tag: See **Originator**.

ASP (Application Service Provider): An entity that manages and distributes software-based services and solutions.

Bulk SMS: A messaging service that allows companies to send high volumes of non-premium rate SMS quickly and efficiently, usually at no charge to the receiving party.

Bulk Traffic: A term for mass marketing, where one message is sent to multiple recipients.

CNAME (Canonical Name): A type of resource record in the DNS which is used to specify that a domain name is an alias for another domain, the "canonical" name. All information, including subdomains and IP addresses etc, are defined by the canonical domain.

D&B Number; DUNS; D-U-N-S (Dunn & Bradstreet Number): A unique numerical identifier assigned to a single business entity and is recognised worldwide.

DLR (Delivery Receipt): A receipt sent to a customer after a message has been successfully delivered to a mobile subscriber's device.

DNS (Domain Name System): The Internet's system for converting alphabetic names into numeric IP addresses.

FSM (Forward Short Message): This is the second of two SS7 requests sent by an SMSC when sending an SMS message, the first being an SRI.

Global Title (GT): An address used in the SCCP protocol for routing signalling messages on telecommunications networks. In theory, a Global Title is a unique address which refers to only one destination, though in practice, destinations can change over time.

GSM (Global System for Mobile Communication): An open, digital mobile technology used for transmitting mobile voice and data services.

Hacking: The act of gaining access to a mobile operating system, app or device.

HLR (Home Location Register): The database within a GSM Network which stores all mobile subscriber data, such as location, phone status and mobile network.

Hubbing: A new structure for the international flow and mobile interoperability of SMS between mobile operators by implementing hubs to intermediate SMS traffic and to offer larger SMS coverage.

IMSI (International Mobile Subscriber Identity): A unique number, usually fifteen digits, which identifies a GSM subscriber.

M2M (Machine to Machine): Direct communication between devices using any communications channel, including wired and wireless.

MAP (Mobile Application Part): An SS7 protocol that provides an application layer which is 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.

MMS (Multimedia Messaging Service): A descendant of SMS, it extends text messaging to include longer text, graphics, photos, audio clips, video clips, or any combination of the above, within certain size limits. MMS is frequently used to send photos and videos from camera phones to other MMS phones or email accounts.



GLOSSARY

MO (Mobile Originated): This is the source from which a message is sent from, e.g. a consumer-originated MO is a message created and sent by a mobile subscriber.

MNO (Mobile Network Operator; Mobile Operator): A provider of wireless or mobile communication services that owns or controls all the elements necessary to sell and deliver services to a mobile subscriber. A key defining characteristic is that an MNO must own or control access to a radio spectrum license from a regulatory or government entity. A second key defining characteristic is that an MNO must own or control the elements of the network infrastructure necessary to provide services to subscribers over the licensed spectrum. An MNO typically also has the necessary provisioning, billing and customer care computer systems and the marketing, customer care and engineering organisations needed to sell, deliver and bill for services, though these systems and functions can be outsourced.

MNP (Mobile Number Portability): This allows a mobile subscriber to switch from one mobile operator to another while maintaining their MSISDN. 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 telephone number attached to a SIM card used in a mobile device.

MSC (Mobile Switching Centre): An MSC routes SMS messages, performs service billing as well as interfacing with other networks, such as the public switched telephone network (PSTN), in addition to performing communications switching functions. 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.

MT (Mobile Terminated): This is the destination that a message is delivered to, e.g. an MT is a message that terminates or is received onto a location such as a mobile subscriber's device.

MTP (Message Transfer Part): Part of the SS7 Network, the MTP is responsible for reliable, unduplicated and in-sequence transport of SS7 messages between communication partners.

Originator: This is what appears in the 'from' field when a message is received by a mobile subscriber. It is also known as a SenderID. An alphanumeric originator enables a business brand name to be set as the identified 'sender' of a message delivered to a mobile subscriber.

OTT (Over The Top): Instant messaging services which can be accessed over the internet.

P2P (Person to Person): Two way messaging.

PRS (Premium Rate Service): These are a form of micro-payment for paid-for content, data services and VAS that are subsequently charged to a mobile telephone bill or prepay account and tend to cost more than a normal phone call or text message

Reseller: A reseller will purchase a product or service and then repackage and then sell it as its own.

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

SCCP Provider: An entity which manages the SCCP layer protocol.

Short Code: Also known as a short number, these are special numbers, significantly shorter than full telephone numbers, which can be used to send SMS and MMS messages.

SIM; SIM Card (Subscriber Identity Module): A smart card inside a mobile phone, which carries a unique identification number, stores personal data, and prevents operation of the device if removed.

SMS (Short Message Service): This is a text messaging service component of phone, Web, or mobile communication systems. It uses standardised communications protocols to allow fixed line or mobile phone devices to exchange short text messages.



GLOSSARY

SMSC (Short Message Service Centre): The tasks of an SMSC are **1)** receipt of messages from wireless network users, **2)** storage of messages, **3)** forwarding of messages, **4)** delivery of messages to wireless network users, **5)** maintenance of unique timestamps in messages

SRI (Send Routing Information): This is the first of two SS7 requests sent by a SMSC when sending an SMS message, the second of which is an FSM request. An SRI request is made by the SMSC to the HLR / VLR in order to request routing information and determine the IMSI of a subscriber which is required to send a message, together with the subsequent FSM request.

SS7 (Signalling System 7): A set of telephony signalling protocols, which also perform number translation, local number portability, prepaid billing, SMS and other mass market services. SS7 is not permitted in some regions.

Throughput: This is the volume of messages which can be sent per second and can vary depending on cost and destination.

USSD (Unstructured Supplementary Service Data): A protocol used by GSM mobile phones to communicate with a mobile service provider's computers.

VAS (Value Added Service): This is a term which covers 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. The primary role of the VLR is to minimise the number of queries that MSCs have to make to the HLR.





ABOUT MEF'S FUTURE OF MESSAGING PROGRAMME



MEF's Future of Messaging Programme is a two-year industry programme that takes a cross-ecosystem approach to advance the sustainability of mobile messaging. It was founded in October 2015 and 25 companies representing different regions and stakeholder groups have participated in scoping the priorities of the Programme across market innovation and fraud management.

All participants of the self-funded programme have signed up to its common goals, namely:

- To create awareness and develop industry best practices of sending A2P SMS messages
- To exchange know-how and develop best practices for identifying and blocking fraud in messaging
- To create a framework to advance innovation in messaging

This A2P Messaging Fraud Framework is the first output of the Fraud Management Work Stream.

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

WWW.FUTUREOFMESSAGING.COM

WWW.MOBILEECOSYSTEMFORUM.COM





PROGRAMME FOUNDERS





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.

