SOMOS®

Somos, Inc. reply to Ofcom's Call for Input
Reducing scam calls from abroad which spoof UK mobile numbers

Somos is an independent, not-for-profit company that administers and manages all country code +1 numbers in North America on behalf of the Unites States ('US') government. Somos supplies this reply to the Call for Input as a numbering administrator to shed light on areas where Somos has relevant experience that may be useful to Ofcom.

Somos Numbering Administration Services

Somos' number administration responsibilities fall into three neutral administrator service roles which Somos provides on behalf of the US Federal Communications Commission ('FCC').

The North American Numbering Plan Administrator ('NANPA') which provisions and assigns 10-digit numbers in 10,000 or 1,000 geographic blocks. The NANPA also monitors number resource utilization, manages the forecast reporting process and opens up new area codes, when necessary, based on forecasted utilization.

The Reassigned Numbers Database ('RND') is the most recent administrator service Somos provides with the objective of minimizing unwanted or nuisance calls to consumers. This database contains all disconnected telephone numbers in the US, and service providers are required to update the RND monthly. The RND enables authorised robocallers / marketers to check that a number is held by the correct subscriber who has previously approved contact by robocallers / marketers. If the number changes subscriber, the robocallers / marketers no longer have the right to call that number as they are not authorised by the new subscriber. To date, there are over 460 million numbers in the RND and over 216 million unwanted calls or texts have been prevented.

Somos is also the Toll-Free Numbering Administrator ('TFNA') and manages Toll-Free numbers ('TFN's), also known as 800 numbers (Freephone in the UK), and serves as a one-stop shop administrator service. TFNs are non-geographic numbers, assigned in real-time and at the individual number level. As the TFNA, Somos also manages TFN portability, routeing, and fraud mitigation services.

As a numbering administrator, Somos believes in good governance, this means protecting the integrity of the numbering system and the numbers themselves. Somos offers this reply to the Call for Input in the context of our experience as a numbering administrator.

Benefits of adopting a Proxy Server approach

Introduction

Ofcom is currently consulting with industry to identify a range of technical solutions that could be put in place to reduce or eliminate the currently high level of scam calls received in the UK from overseas, where the calling number ('CLI') is spoofed such that it appears to the called party as originating from a UK mobile telephone.

In this response, Somos is proposing that rather than developing a very specific technical solution tailored to combat the current spoofing practice of bad actors, that a proxy server is established and accessible by those CPs offering International Gateways into the UK and, where appropriate, domestic carriers. The proxy could offer a platform to support a single ubiquitous solution implemented across all the UK's international gateways and domestic networks. Not only could such a solution be cheaper than each CP implementing their own solutions, but it would also offer improvements in blocking efficiency to a greater degree and faster than other more conventional approaches.

If such an approach were to be agreed and adopted, the proxy server could then be further developed and enhanced to meet other industry and regulatory requirements, in a straightforward manner.

Below we consider the advantages of this approach to the current Call for Input (**Is Roaming**) and then move on to discuss some of the other opportunities that could be subsequently exploited.

Somos would also like to take this opportunity to provide Ofcom with some background to the evolution of fraud tools and platforms in the US.

Background to US Governance

The North American Numbering Plan ('NANP') was developed by AT&T in 1947 to facilitate direct dialling of long-distance calls. The NANP Administrator ('NANPA') is the neutral body who administers the NANP resources under a Federal Communications Commission ('FCC') contract. FCC regulations require the NANPA to be a non-governmental entity that is neutral, impartial, and not aligned with any particular telecommunications industry segment.

The Telecom Act 1996 provided regulation, put in place by the US Congress, which allowed for competition of communication services across all markets and required communication's carriers to provide number portability. The methodology adopted in the US was different from that implemented in the UK and required the establishment of a centralised Local Number Portability ('LNP') database and Number Portability Administration Centre ('NPAC'). The FCC contracts with commercial organisations to provide the NPAC with its associated databases and registries and in 2003 it allowed communication providers to raise a monthly charge to consumers for the provision on number portability. This was consistent with the approach used in the US for charging consumers (and businesses) monthly for the provision of additional services (e.g. 911 Emergency Services, Telecommunications Relay Services ('TRS'), and 988 Suicide and Crisis Lifeline). Examples of the types of charges made to the consumer are demonstrated on Annex 1.

The TRACED Act ('Telephone Robocall Abuse Criminal Enforcement and Deterrence Act'), which became law in 2019, required voice service providers to develop call authentication technologies and initiate rulemaking to protect a subscriber from receiving unwanted or malicious calls or texts. This resulted in the Robocall Mitigation Database ('RMD'), the implementation of STIR / SHAKEN, the use of a reasonable DNO list and other forms of mitigation.

This has resulted in a number of disparate, unrelated platforms, databases and processes which have been developed for each adaptation. This approach has created cost to the industry and the consumer while not allowing the flexibility to quickly and efficiently adapt to the next threat.

Whilst underlying processes in the UK may be different from those deployed in the US, the relevance of the datasets remain absolutely relevant to the issues faced in the UK; the detection and prevention of scam calls, reducing the volume of tromboning of ported traffic, automated end-to-end call tracing, calling / messaging authentication and the introduction of PAYG SIM card registration.

In this submission, Somos suggests that before considering the important and very focussed questions about the reduction of spoofed calls from abroad, Ofcom should consider the bigger picture. As the UK moves into an era devoid of the signalling limitations of C7-based Public Electronic Communications Networks ('PECNs'), Ofcom has a unique opportunity to set the industry on a new path. A path better suited to IP-based call routeing, cost efficiency, and that will enable the adaptability for other issues to be addressed – allowing more opportunities to be exploited, including those which may not be currently apparent.

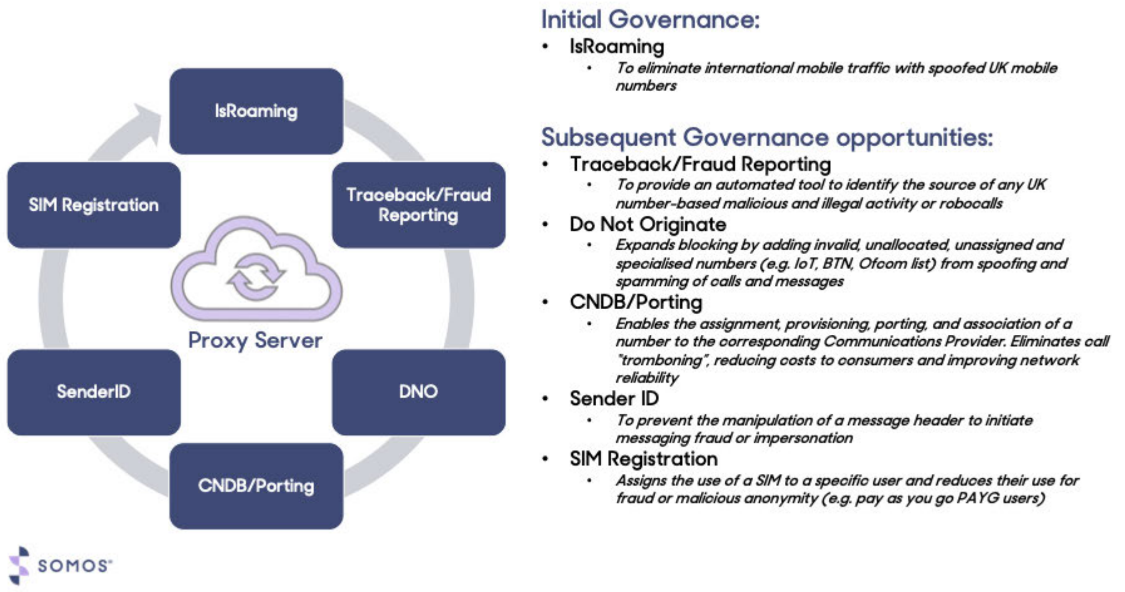
With this in mind Ofcom could move towards a single governance model verses the three independent structures which have been developed in the US; therefore, benefiting from a reuseable interface and reduced implementation costs for future solutions.

By starting with this goal in mind, Ofcom will enable the UK to derive the benefits of a much faster, cheaper and more complete reduction in the volume of scam calls from abroad than would otherwise be the case with a solution tailored solely to the very narrow problem statement currently being considered. The UK is in the position to learn from the North American experience and exploit the technological investments made there, available and in use in the UK today.

Somos' observations

In response to Ofcom's call for inputs on addressing international scam calls utilising spoofed +44 7 mobile numbers, Somos would propose that the UK considers utilisation of a central proxy server in order to establish an initial interface to sit between the UK's international gateways ('IGW's), MNOs and thick MVNOs to supplement an HNR ('Home Network Routeing') or CAMEL ('Customised Applications for Mobile network Enhanced Logic') based solutions. Given the current industry interest in developing new standardised approaches to Network Application Interfaces, it would be the intention to monitor such initiatives and implement them when appropriate.

This interface would then create the primary portal for which many other solutions could then be developed.



Initial Governance:

- IsRoaming
  - *To eliminate international mobile traffic with spoofed UK mobile numbers*

Subsequent Governance opportunities:

- Traceback/Fraud Reporting
  - *To provide an automated tool to identify the source of any UK number-based malicious and illegal activity or robocalls*
- Do Not Originate
  - *Expands blocking by adding invalid, unallocated, unassigned and specialised numbers (e.g. IoT, BTN, Ofcom list) from spoofing and spamming of calls and messages*
- CNDB/Porting
  - *Enables the assignment, provisioning, porting, and association of a number to the corresponding Communications Provider. Eliminates call "tromboning", reducing costs to consumers and improving network reliability*
- Sender ID
  - *To prevent the manipulation of a message header to initiate messaging fraud or impersonation*
- SIM Registration
  - *Assigns the use of a SIM to a specific user and reduces their use for fraud or malicious anonymity (e.g. pay as you go PAYG users)*

Figure 1. Is Roaming via Proxy Server providing an interface for other needed solutions.

A proxy server acting as the interface should not be the monopoly provider for future solutions but would provide the initial point for the connection to other solutions. This would then enable the UK to progress other fraud mitigation tools, be adaptive and flexible towards the ever-challenging whack-a-mole which is currently being played.

This initial point of connection would allow the UK to grow a comprehensive set of tools similar to the Toll-Free Number ('TFN') platform provided in the US. This includes the one-stop shop provided by the Toll-Free Number Registry ('TFNR') for searching, reserving, routeing, and porting. Responsible Organisations ('Resp Orgs'), are vetted entities that manage TFNs on behalf of subscribers and use the TFNR to interface with the Toll-Free Number Administrator ('TFNA').

The TFNR is a search and reserve system where Resp Orgs can search and reserve either individual TFNs or tens of thousands of TFNs. The Resp Orgs provide routeing and number portability at an individual or number block level, this allows for the rapid identification of the carrier associated with a spoofed or impersonated number.

As mentioned above, the US has a number of different platforms each developed for a unique purpose which has resulted in disparate databases with different funding and governance models supporting each solution.

The proxy, as the initial point of connection, would allow the UK to grow a comprehensive set of tools on a base similar to the Toll-Free platform provided in the US saving time when implementing any further enhancements and reusing existing connections to any future solutions.

Is Roaming

Without the use of a proxy server, each terminating entity (MNO or MVNO) will need an **Is Roaming** route with each IGW (i.e. many-to-many). The use of a proxy would enable each IGW and each terminating entity to connect for the purposes of **Is Roaming** to the proxy alone.

Today, there are a number of different signalling standards and methodologies, all of which are supported by proxy solution. The proxy not only reduces the number of 'connections' each party needs to establish but also prevents the need for any party to develop alternative signalling capabilities where a mismatch would occur in the alternative many-to-many approach.

Another benefit of the proxy approach is that should any party wish to make an engineering change to its network or move to one of the other signalling protocols / methodologies, they can do so seamlessly without impacting or requiring change of any other party.

The core of the proxy solution is to enable one party to run zero touch queries on any given mobile telephone number against the systems of the terminating MNO / MVNO without exposing the entire dataset or replicating the dataset in a central record. Given the increasing convergence of fixed and mobile telephone network infrastructures and systems, this approach can easily and cheaply be widened beyond mobile telephone numbers to both geographic and even non-geographic numbers.

Possible operating models

For **Is Roaming** solutions to be effective, they need to be functional, be uniformly adopted across the UK interconnection landscape and be trusted by market participants, policy makers, consumers and other stakeholders. Whilst the adoption of a centralised proxy server simplifies implementation and minimises the complexity faced by "one to one" interface solutions; care needs to be taken in designing the operating model in order to achieve these goals.

Clearly, the proxy server could be operated by a commercial entity contracting with each of the relevant parties on an individual basis, likely on a transparent basis with regard to "terms and conditions" to promote confidence that it is abiding by "FRAND" principles. However, this might not be sufficient to ensure the necessary level of trust across all stakeholders, so the adoption of some form of oversight could be considered. There are a number of approaches that could be adopted, including forming a new cross industry governance framework or joining forces with an existing one such as TOTSCO.

Whatever the approach used, it is, however, vital that consumers and others have visibility into how the process works and how decisions are taken. Equally, Ofcom, as the regulator for the sector, will have an important role to play to encourage adoption and, if necessary, intervene if some market participants do not engage or fail to abide by the underlying agreed operating "rules".

Other potential applications

Having built out the signalling connectivity, the value of the proxy solution can then be easily leveraged by the inclusion of other numbering and validation datasets held centrally alongside the proxy server, preventing the need for "dipping" into CP records to answer individual queries. An easy and perhaps less controversial approach (confined to the **Is Roaming** solution) would be for the proxy server to provide a short-term cache of query results with an appropriate latency on storage duration[1].

Traceback

Currently, where a CP has cause to trace a domestic UK number to its point of origin, the process used is manual, requires a skilled individual with the correct systems access in each CP involved in the end-to-end transmission which would require the following entities to be involved, at a minimum:

- Terminating CP
- Transit CP
- Range-holder CP
- Recipient CP (who has imported the number from the range holder).

In the first instance, an API type approach could be built allowing the switch manager systems of all UK CPs to be interrogated, where appropriate, from a single search request. The terminating CP would submit to the proxy server a request detailing the timestamps of the relevant call, the originating CLI, the dialled number, the CP from whom the call was received and any other relevant signal flags. The proxy server would then interrogate the previous CP in the chain, as identified in the query, and gain the relevant call data to the transmission path across that CP and so on, until the complete path has been identified to the point of origin. This would require a development for each UK CP to interface their switch manager solution to the proxy server. Safeguards, controls and security measures would need to be put in place to appropriately restrict the use of this process and maintain appropriate levels of confidentiality around the data.

If the proxy server already has access to a dataset setting out the network details of every telephone number in service in the UK (effectively a Central Numbering Database, 'CNDB'), then no switch manager development would be needed. The proxy server would be able to return the source of the call solely by access the "CNDB" data file. If any CP acts nefariously or fails to maintain its data in the CNDB in a timely manner, then a very small number of queries would solicit an incorrect answer. Any such errors would quickly highlight the CP behaving in that manner.

Do Not Originate (DNO)

DNO, a list of UK telephone numbers which should not be used to originate telephone calls, could be stored on the proxy server thereby allowing international gateways

[1] For example, having confirmed with a query to a particular MNO that a call from a given +44 7 number in a particular country is legitimate, any subsequent calls from that number in that location to other UK numbers within a, say, 1 hour period could be validated without querying the customer's MNO a second / third / fourth time.

(and CPs) to identify and block scam traffic purporting to be from such a number through spoofing. Listed below are the datasets that could be included in such a scheme, in ascending order of complexity (and cost of implementation):

1. Number Blocks as listed by Ofcom as being unallocated, in quarantine or protected
2. Telephone numbers associated with financial institutions and other business but declared by them as never used for outgoing calls[2]

The existing scheme has worked satisfactorily but is cumbersome and essentially manual and restricted in scope. It does not for instance include those numbers allocated by Ofcom to CPs (or sub-allocated by those CPs) but not in use with a consumer or business)[3].

The first of these options could be made available at very low cost as an add-on to the **Is Roaming** solution, providing a mitigation where a range-holder MNO lookup fails or is delayed.

The second option would require ongoing administration but again, from a technical implementation perspective, it could be used to extend the usefulness of the **Is Roaming** solution and even provide an additional data source to MNOs for SMS validation (see Sender ID below). Further extension to include unused numbers from allocated ranges would also be feasible.

Centralised Numbering Database (CNDB)/ Porting

The potential benefit of a CNDB in enabling direct routing of ported traffic has long been recognised within the UK. Previously, in the context of TDM networks, the implementation costs have been estimated to be extremely high making it difficult to justify implementation. TDM network switches route on number blocks and direct routeing required these to route, instead, on the full dialled digit string. IP Voice networks do not have the same constraint and are built around eNum capabilities (i.e. the ability to discriminate on the full digit string and not just the number block). Therefore, as the UK moves into an All-IP environment the opportunity to put in place an exploit a CNDB becomes a realistic possibility.

If a proxy server is in place supporting an **Is Roaming** solution, with signalling connectivity into all the MNOs, then it is essentially a simple matter for that solution to be expanded to enable direct routeing of ported traffic between the mobile operators. The opportunity to eliminate Average Porting Conveyance Charges and transit fees would soon drive fixed CPs to join in. The platform is very scalable and well suited to this purpose.

Sender ID

Fraudsters have long used SMS to engage with their victims, frequently posing as banks or other financial institutions in the identity presented in the message header and displayed on the display of the recipient's mobile phone. These IDs are normally the CLI of the originating mobile handset, but for A2P applications and those based on RCS (Rich

[2] Bad actors sometimes generate traffic using a CLI used by a bank, for example, as their main contact number in order to lull the called person into believing the call is actually from their bank.

[3] The proxy server needs to be supporting a UK CNDB for this scenario.

Communication Services) alpha characters can be used. In a bid to constrain the opportunities for fraud, a list of proscribed terms (such as 'Bank' and 'Payment') is now enforced by the UK MNOs.

In tackling innovative use of SMS for fraudulent purposes, the ability for Receiving Party's Provider ('RCP') to quickly identify with zero touch the source of a message with a particular Sender ID would prove invaluable in identifying any such security breaches in the UK SMS infrastructure. At the moment, an RCP may aggregate suspicious messages with a particular Sender ID and then prioritise those for analysis based on volume, using a proxy solution to identify the source of each message would be useful in those scenarios where the bad actor is subtly changing the Sender ID on each successive message it sends. Aggregation could then be based on the entry point into the UK SMS infrastructure rather than the particular Sender ID.

SIM Registration

The original objective of Pay As you Go (PAYG) SIMs was to enable those consumers who were unable to afford monthly contracts for mobile services to gain access to the mobile phone networks and more recently to access the internet in a manner that suited their personal financial circumstances from day to day. Increasingly over the years, the use of PAYG SIMS has become synonymous with the concept of burner phones used for criminal activity.

In many countries around the world, the requirement for SIM Registration has been put in place to make it more difficult for criminals to hide their identity when using the mobile phone network and accessing the internet. Out of the box, the purchaser of a PAYG SIM has to register their SIM card providing personal details and address information, the SIM card providing connectivity limited to this registration process alone. In some countries, biometric data is also captured and stored. It is also possible to deploy advanced screening processes, such as using ePassport metrics to help assure the identity of the individual registering the SIM card. Only once this registration process fully complete is the SIM card fully enabled for normal use.

This database could be further expanded for the benefit of law enforcement agencies by linking the mobile device IMEI number with the SIM card and the associated mobile telephone number. This could prove particularly useful where the subject of an investigation is using multiple SIM cards with one mobile handset.

Conclusion

Somos intends this reply to the Call for Input as a helpful guide to how numbering administrations have evolved in the US and hopes this submission provides an indication of lessons learnt over this period. Somos is happy to provide any further information if required.

Annex 1

The items highlighted below illustrate examples of surcharges and fees which are additional elements seen on a consumer bill in the US, these are in addition to federal, state, county and city taxes:

Surcharges	
Federal Universal Service Charge	$0.xx
Regulatory Charges	$0.xx
Admin & Telcom Recovery Charges	$x.xx
State 911 Surcharge	$0.0x
State 988 Surcharge (Suicide and Crisis Lifeline)	$0.xx
LNP Surcharge (Local Number Portability)	Variable by provider
State Telecommunications Relay Services (Text Relay)	$0.0x
Various other state and county charges.	$0.xx

For some of the surcharges and fees there may be a fixed duration (i.e. 5 years) associated to them for a specific cost recovery period.