XConnect's response to Ofcom's Call for Input (29th July 2024): Reducing scam calls from abroad which spoof UK mobile numbers - Options for addressing consumer harm

XConnect welcomes the opportunity to respond to Ofcom's Call for Input. We support Ofcom's open approach to understanding the various solutions which can be taken towards validation of mobile calls originating abroad and genuinely roaming. We fully support Ofcom's objective of creating trust in numbers to protect end users from receiving harmful and malicious calls.

Introduction to XConnect

XConnect[1] provides a trusted global registry of network and subscriber information, based on privacy compliant phone number data, including global number portability, global number ranges and prefixes and mobile phone subscriber status.

Established in the UK in 2005, XConnect delivers mission critical carrier-grade numbering information services to over 200 operators globally, including MNOs, business messaging (A2P) hubs, aggregators, carriers, interconnect providers and enterprises. XConnect annually processes over 50bn queries per year and is an ISO 27001 certified company. Our number information services are used for voice and message routeing, fraud protection, phone number validation as well as fraud mitigation and risk scoring. XConnect also supports the deployment and evolution of next-generation communications, such as VoLTE[2] and RCS[3]. Our Number Information Services[4] are accessed through our global distributed hybrid cloud platform using simple, secure, scalable real-time protocols and APIs.

In 2020, XConnect was acquired by Somos, Inc., a USA-based company providing number information and services to over 1,400 organisations and is the trusted USA telecom sector administrator for over 3 billion numbers throughout the USA and North America. Somos helps to enable seamless communications between enterprises and consumers through the management of the USA regulatory agency's ("FCC") mandated databases including North American Numbering Plan ("NANP"), Toll-Free Number Administrator ("TFNA") and the Reassigned Numbers Database ("RND"). In addition, Somos administers the USA's largest Do Not Originate ("DNO") list.

First Steps

XConnect agrees that technology changes are a significant enabler for bad actors to continually find new ways to cause harm and that trust must be restored in the number being displayed to the end-user, enabling them to answer calls without being fearful of the outcomes. That trusted communication can only be achieved where there is a verified CLI the end user can have faith in being genuine and representing a legitimate call.

[1] About XConnect: https://www.xconnect.net/about-xconnect/

[2] VoLTE - Voice over Long-Term Evolution (VoLTE) is a LTE high-speed wireless communication standard for mobile phones and data terminals

[3] RCS - Rich Communication Services protocol is designed as a modern take on texting that rolls features from Facebook Messenger, iMessage, and WhatsApp into one platform

[4] About XConnect Number Information Services: https://www.xconnect.net/services

The CLI sanity checks which Ofcom has recently implemented[5] to validate the CLI against the authoritative sources (National Number Plan, the Do Not Originate ("DNO") list, Know Your Customer Check ("KYC"), blocking fixed +44 calls originating from aboard) are all important tools which support the journey to restoring trust in the CLI. We would suggest that these steps are the first of many interlocking initiatives necessary between industry and Ofcom, but which must also be underpinned by a robust regulated ecosystem in order to achieve the ultimate goal of "trusted communications".

If Ofcom is to restore trust in communications for the consumer, there must be a comprehensive approach to dealing with calls and messages to ensure that, however the consumer is contacted, they can have confidence in engaging with the originator of the call or text. We would suggest a zero-risk approach to call and text validation must be taken.

Responses to Ofcom Questions

Ofcom Question 2

What variables and factors should we take into account when considering whether – and, if so, how - to address the harms caused by spoofed UK mobile numbers?

Of the four points raised in section 3.8 of the CFI, the last is the most pertinent:

- the timescales over which legacy 2G and 3G technology will remain in other countries – we are interested in this because later technologies are inherently able to prevent mobile roaming spoofing.

XConnect would highlight the recent assessment[6] (dated 19 March 2024) carried out by the GSMA. This article reinforces the XConnect view that the continuing burden to support 2G and 3G roaming will last, globally, beyond the next 10 years. The GSMA also suggests there could be an expansion of legacy networks in the medium term.

The key takeaways from the GSMA article are as follows:

- *Sunsetting is not yet a priority for most African operators. The shift from 2G/3G to more advanced technologies will be slower in Africa due to economic, social, and infrastructural factors as well as the strong dependence on existing legacy ecosystems. A gradual approach is recommended to maintain digital inclusiveness in Africa.*
- *South Africa is the only country in SSA with an established plan to sunset 2G and 3G networks. Cell Analytics® data shows a large concentration of 2G and 3G users in suburban and rural areas as well as along transportation routes. South Africa plans to decommission these networks by 2027, but most countries, including Nigeria, have*

[5] Statement: Improving the accuracy of Calling Line Identification (CLI) data. https://www.ofcom.org.uk/consultations-and-statements/category-2/improving-cli-data-accuracy, https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/updating-cli-guidance-to-tackle-scam-calls

[6] https://www.gsma.com/get-involved/gsma-membership/gsma_resources/sunsetting-networks-in-africa-will-be-gradual-and-more-selective-than-in-other-regions/

not yet set a date. We expect network sunsetting to be in full swing from 2030 onwards.

- *Operators should strike a balance between driving progress and maintaining the inclusivity of their services. African operators should continue to support and potentially expand their legacy networks to ensure continued access to critical communication services for most of the population while investing in the roll-out of 4G and 5G networks*.

While the GSMA notes Nigeria's slow progress, India also appears to have no plans to close 2G.

Given that a large proportion of fraud calls originate in India, which is also now the most populous country, it should be noted that there are approximately 250-300 million Indian 2G subscribers[7], with industry data indicating some 50 million 2G handsets are sold annually. The 500,000 2G base stations deployed throughout the country are primarily owned by Bharti Airtel, Vodafone Idea and state-run BSNL/MTNL, with both Bharti Airtel[8] and Vodafone Idea[9] both publicly stating that currently there are no plans for closure of the 2G networks. It is believed that while 2G sunset is to be expected there will be no announcement in the next 3-4 years. This is in addition to the Department of Telecommunications (DoT) currently declining to interfere in any decision regarding the closure of 2G.

XConnect has highlighted Nigeria and India as two countries which, to date, have made no indication of the timelines to withdraw 2G. Research shows that there are many more countries which have no immediate plans for withdrawal due to high levels of deprivation, the low availability and high cost of smartphones in addition to the major cost of deploying new networks across large rural areas. We also suggest, that, when looking at closure announcements, there is generally a lag of 3 years until the network is closed. We should be mindful that even in the UK we expect the last 2G network will not be turned off until at least 2033[10].

We have provided further country information in Annexes 1 and 2.

There are c.900 networks around the world and according to the GSMA only 142 networks have announced plans to shut down 2G networks and 163 have announced plans to shut down their 3G networks. More critically, only 71 have announced plans to shut down both their 2G and 3G networks, the latest of which is planned for 2035. It is crucial to understand

[7] https://www.business-standard.com/industry/news/dot-will-not-intervene-in-2g-network-shutdown-parks-decision-with-telcos-124022300252_1.html

[8] https://economictimes.indiatimes.com/industry/telecom/telecom-news/bharti-airtel-focusing-capital-investments-on-5g-no-plans-to-shut-down-2g-network/articleshow/98986814.cms

[9] https://www.thehindubusinessline.com/info-tech/vodafone-idea-opposes-jios-proposal-for-sunset-date-for-2g-networks/article67822101.ece

[10] https://www.ofcom.org.uk/phones-and-broadband/coverage-and-speeds/2g-and-3g-switch-off-our-expectations-of-mobile-providers/

that UK MNOs wish to provide their subscribers the maximum possible roaming coverage, however obscure the visited destination may be. That means, where they face the choice of providing coverage on a legacy technology or no coverage, consumer demands dictate that coverage on 2G and 3G will be required. In other words, we can assume that international 2G and 3G roaming will remain in place until the vast majority of the long tail of roaming partners have evolved to 4G and 5G or beyond.

Additionally, we also note the research (slides below) conducted by Kaleido[11] Intelligence carried out in 2023 on "VoLTE Roaming: Deployment & Prioritisation Outlook Q2 2023 MNO Survey". Key points to take away from this research are:

[redacted]

[redacted]

[redacted]

XConnect believes there is a clear conclusion to be drawn from this research, that VoLTE roaming is not a relevant technology in terms of providing a ubiquitous technology to address scam calling.

VoLTE Roaming: Deployment & Prioritisation Outlook Q2 2023 MNO Survey

Ofcom Question 5

How will developments in deployment of mobile technologies in the UK and abroad affect the problem of spoofed UK mobile calls from abroad? Please provide evidence to support your response.

XConnect would emphasise that globally there is a long tail of operators slowly moving to 4G, 5G and VoLTE, as highlighted in the section above. Any solution to stop spoofed UK calls from abroad will need to recognise that 2G and 3G roaming partner networks will remain for the longer term, potentially to 2034 and beyond (note, the GSMA dataset[12] specifically lists one network as planning their 3G shutdown for 2035). Until the last 2G & 3G networks globally has been switched off, bad actors will move from country to country as necessary in order to exploit this weakness. Ofcom must therefore ensure that 100% of roaming calls are validated.

[11] https://kaleidointelligence.com/accelerating-volte-roaming-2024/

[12] https://membergateway.sharepoint.com/sites/wg-WAS/_layouts/15/Doc.aspx

Since scams continually evolve, consideration must also be given to a longer term approach to fraud which will allow for any solution to keep in step with changes in scam behaviours. XConnect would urge Ofcom to mandate outcomes which provide flexibility for the ever changing and evolving nature of fraud, which will capture 100% of roaming calls and be quick to implement. XConnect would submit that a mixed approach of a proxy and Home Network Routeing ("HNR"), a hybrid approach of this sort would enable all of these outcomes.

Ofcom Question 6

a. What is your preferred option for addressing scam calls made from abroad using spoofed UK mobile numbers, and why (including the pros and cons of the different solutions)?

XConnect would propose that Ofcom considers carefully the benefits of a hybrid solution, as outlined below.

If the CAMEL HNR approach alone were to be adopted, it is XConnect's view that this would take a number of years to be effective due to the large number of CAMEL agreements yet to be established or requiring amendment (see the Kaleido Intelligence slides in our response to Question 2). Unless all MNOs and MVNOs have CAMEL agreements with all of their roaming partners and provisioned for all of their subscribers (pre- and post-paid), CAMEL is unlikely to act as a complete solution. We would suggest that the implementation would require coordination between the MNOs and Ofcom with respect to which countries are addressed and in which order with respect to agreeing CAMEL agreements, targeting those countries known to have a high level of criminal activity first. If Ofcom does not coordinate and monitor the MNOs' progress with respect to the implementation of CAMEL agreements, any benefits of this solution will be delayed and diluted. Moreover, further implementation of CAMEL to support the HNR solution may require network capacity expansion and additional licensing (resulting in additional licensing costs). Finally, not all roaming partner networks are able to support CAMEL or support the implementation of a CAMEL agreement.

Given that a "CAMEL only" solution will take a substantial time to fully implement without such targeted prioritisation, a large proportion of scam calls would continue to be presented to the consumer without validation for a considerable period. We would add that, even once the CAMEL solution has been fully deployed, a proportion of calls will remain unvalidated and would still reach the consumer. [redacted] These two elements alone raise doubt as to the immediate and long-term effectiveness of this solution and how long it would be before consumers would feel the benefits.

Not only should any solution authenticate 100% of roaming calls but it must also be able to identify and validate all +44 7 allocated and unallocated numbers. Not all +44 7 numbers are used purely for mobile calls (in motion) and there are a considerable number of +44 7 use cases (for example, remote PBX, remote call centre, CPAAS platforms, etc.) which may be legitimate and would not be validated by the "HNR only" solution. If the "Is Roaming" check does not examine all +44 7 numbers this will immediately provide a loophole for bad actors to exploit.

CAMEL home routeing with real-time "Is Roaming" lookup – a hybrid solution

The hybrid solution is where a CAMEL Home Routeing Solution (CAMEL HNR) and an "Is Roaming" proxy server, (as described below) are both deployed in the national network.

The "Is Roaming" proxy function connects to the International Gateways ("IGWs") on one side and MNOs (including "thick" MVNOs) on the other, enabling:

- hubbing, so that each MNO and IGW only need to connect to the proxy and not the MxN connections required to mesh.
- mediation, enabling each MNO and IGW to select the connection protocol best suited to their network implementation.
- a centralised tool kit which supports services such as: MNP checking, number validation (against Ofcom number range data and DNO) and white or black lists (e.g. to specifically allow or bar "A" numbers).

The proxy is designed to provide carrier class performance and availability with no single point of failure and includes geographic resilience.

The proxy can be deployed in the national network and connected to:

- MNOs via an appropriate 'query' interface:
  - This may use C7 MAP in which case the proxy will be connected to the national SS7 network using authorised Global Titles to access the MNO.
  - HTTP API. Some MNOs have already deployed an HTTP API which provides roaming status.
  - Other methods. Some MNOs may have roaming data which can be 'onboarded' to the proxy or accessed via a query to an MNO held database.
- IGW via an appropriate 'query' interface:
  - Services have been implemented with many operators, today, to provide query based services such as "A" and "B" number validation, DNO checking, MNP checking, etc.
  - There are a range of query interfaces for this purpose including ENUM, HTTP and SIP (including a number of bespoke SIP based implementations)
  - IGW operators can readily adapt their IGWs (and supporting systems) to integrate with the proxy, as has been seen in implementations to date.

The proxy can operate as an alternative to CAMEL HNR, however, in this scenario the proxy operates in tandem with CAMEL HNR to maximise accuracy of the roaming check.

XConnect has provide services to IGWs utilising the interface listed above and there have been no significant development requirements thus minimising IGW costs, with no implementation impact.

This solution can be configured to work in two operating modes depending on the MNO requirements and capabilities:

1. MNO supports either CAMEL HNR or "Is Roaming" API, but not both.
   a. Each MNO chooses whether to use the CAMEL HNR or "Is Roaming" API methods, according to their preference and capabilities.
   b. When receiving a call with a UK mobile "A" number (+44 7), the IGW queries the proxy (using whichever protocol the IGW has selected). The IGW does not need to know whether the MNO supports CAMEL HNR or real-time query
   c. On receiving the query from the IGW, the proxy determines whether the owning MNO operates in CAMEL HNR or "Is Roaming" check mode (using MNP lookup to resolve the MNO ownership). Note:
      i. The proxy can also check that the "A" number is valid, not on the DNO, not blacklisted, etc., if required.
      ii. If the +44 7 number does not belong to an MNO (e.g. the number is being used to provide remote PBX/CPAAS service), then the proxy can also check against a white and black lists to determine whether the call should be allowed.
   d. The proxy determines the roaming status of the calling subscriber according to the MNO preference (i.e. performs an "Is Roaming" check via real-time query, or CAMEL HNR range check).
   e. The proxy returns the "Is Roaming" status back to the IGW.
   f. Depending on the determined roaming status the IGW will either onward route the call (the subscriber is roaming) or block the call/modify the "A" number (the subscriber is not roaming).
      i. The decision to block or modify (and the format of such modification) is dependent on national regulation and agreed operating procedures.
2. MNO with both CAMEL HNR and "Is Roaming" API capabilities.
   a. MNOs may support both the CAMEL HNR and "Is Roaming" API methods for determining the roaming status. The aim of this implementation is to enable a better result for the MNOs roaming customers where CAMEL interaction fails for whatever reason (e.g. not supported by the visited network). A CAMEL failure would normally result in the roaming call being blocked (or the "A" number being modified), but in this case the proxy will then perform an "Is Roaming" check to the MNO API to determine the status and more genuine roaming calls will proceed correctly.
   b. When receiving a call with a UK mobile "A" number (+44 7), the IGW has a choice, it can send a query to the proxy for all calls (using whichever protocol it prefers) or only those which do not have an IMRN "B" number.

c. On receiving the query from the IGW, the proxy determines whether the owning MNO operates in CAMEL HNR or "Is Roaming" check or both (using MNP lookup to resolve the MNO ownership). Note:

   i. The proxy can also check that the "A" number is valid and not on the DNO, not blacklisted, etc., if required.

   ii. If the +44 7 number does not belong to an MNO (e.g. the number is being used to provide remote PBX/CPAAS service), then the proxy can also check against a white or black list to determine whether the call should be allowed.

d. The proxy determines the roaming status – if the "B" number is an IMRN then the proxy returns "Is Roaming" to the IGW, if the "B" number is not an IMRN then the proxy launches a query to the MNO "API" (the API used depends on the MNO preference) to determine the roaming status.

e. The proxy returns the "Is Roaming" status back to the IGW.

f. Depending on the determined roaming status the IGW will either onward route the call (the subscriber is roaming) or block the call or modify the "A" number (the subscriber is not roaming).

   i. The decision to block or modify (and the format of such modification) is dependent on national regulation and agreed operating procedures.

[redacted]

The high-level design is outlined below.

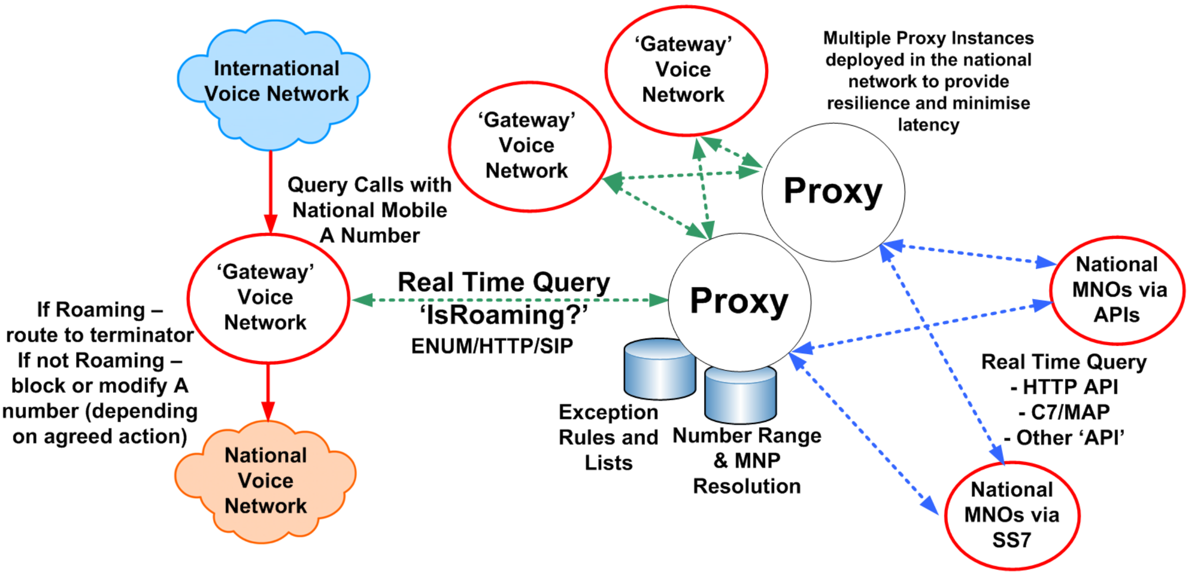
International Voice Network
Query Calls with National Mobile A Number
'Gateway' Voice Network
'Gateway' Voice Network
'Gateway' Voice Network
Multiple Proxy Instances deployed in the national network to provide resilience and minimise latency
Proxy
Proxy
Real Time Query 'IsRoaming?'
ENUM/HTTP/SIP
National MNOs via APIs
If Roaming – route to terminator
If not Roaming – block or modify A number (depending on agreed action)
National Voice Network
Exception Rules and Lists
Number Range & MNP Resolution
Real Time Query
- HTTP API
- C7/MAP
- Other 'API'
National MNOs via SS7

Figure 1 Proxy Solution High Level Design

Pros and Cons associated to a real-time "Is Roaming" lookup via proxy

	Pros	**Cons**
1	There are multiple vendor solutions available, therefore, allowing choice.	All MNOs and IGW providers will require a development in one form or another to support any of the solutions proposed in Ofcom's Call for Input.
2	Proxy solutions are recommended by CEPT and being implemented in other countries	
3	[redacted]	
4	Some mobile networks have APIs already implemented, however, trusted C7 can be used where no API exists.	
5	IGWs can select which 'query' protocol to use based on their network. Typically, a SIP validation is the standard implementation for IGWs and requires no specific development.	
6	The proxy allows for a one-to-many model of connectivity reducing operational overheads across the whole ecosystem. Each gateway and MNO requires a single logical connection to the proxy.	In the unlikely event that all proxy instances are unavailable, IGWs will be programmed to support a failover scenario and pass all calls for the duration of the problem. However, the proxy solution will be designed for high availability (including geographic resilience).
7	Operators have the ability to shop around – and can reuse the capability for other validation solutions.	A proxy solution will require internal resource to select a supplier and complete the necessary security checks. However, any solution will require resource.
8	Unlike the situation with TOTSCO where progress has been slow agreeing processes etc, the proxy solution is available day 1 from several suppliers under commercial terms. Only light touch industry/Ofcom governance would be required.	
9	Whilst there will be an ongoing cost from sustaining a proxy solution, one has to offset this against the reduced costs faced by IGWs and MNOs for a many-to-many solution. Overall, the proxy solution can only be cheaper	
10	This solution would be implemented with a high level of resilience by design and a high availability carrier grade proxy server. Additionally, should the proxy be expanded to include DNO or other validation scenarios, it can reduce the validation load on individual MNOs and mitigate against	

	Pros	**Cons**
	any MNO validation process failure or delay.	
11	The one-to-many nature of this solution will require less cost to achieve necessary levels of resilience than a many-to-many solution.	Any additional latency or post dial delay would be no more than that incurred via other solutions (which would introduce further transit and validation steps).
12	The proxy eliminates costly operational impacts to connected partners associated with moves and changes within a IGW or MNO network configuration or connection to the proxy.	
13	Provides Mobile Number Portability resolution to minimise "Is Roaming" validation query load as this is provided by the same HLR query method used today[13].	
14	Supports caching to minimise query load on the IGW and MNOs.	Where no MNO API exists, the proxy relies on C7 MAP to interrogate the MNO network for roaming status. C7 access is being restricted by the MNOs for security reasons. However, the proxy will be a trusted C7 endpoint in the UK national network with trusted Point Codes and Global Titles so should be unaffected by any tightening of security (in the same way as C7 interconnects between CPs will continue to be supported).
15	XConnect already work with a number of IGW operators across the world providing similar query services (e.g. for "A" number validation including DNO).	While the solution requires the IGW to 'query' to an external platform as part of the call set-up, the proxy offers a number of known and proven interfaces to ensure development is minimised and is more configuration than development.
16	The proxy will **not** require any of the additions listed below to implement, therefore, saving time, development and internal resource costs: • Additional capacity to facilitate additional call traffic load • Network changes to reverse call blocking rules • Reduces the need to rewrite CAMEL HNR to interact with CAMEL • Does not require home mobile networks to able to re-insert the CLI	

[13] With respect to clause 4.8 in the Call for Input document, Ofcom notes the UK Mobile Number Portability ("MNP") process and the potential for multiple ports of a number which could create multiple query hops, therefore, a query could become complex, prone to error and delay. [redacted].

	Pros	Cons
17	Provides security[14] and compliance to all existing legislation and ISO 27001. Checks to ensure that only legitimate actors are connected to the proxy can be developed with Ofcom and industry. Stringent internal processes will be undertaken as part of sign-up due diligence. These will be in line with TSA Vendor Assessment requirements.	
18	Mass call generation by fraudsters will be managed by reporting, alerts with respect to high volume failure percentages and appropriate enforcement action would be taken immediately an event is identified or via contractual enforcement.	Vulnerable to fraudsters scanning by generating mass calls with mobile CLIs until a roaming subscriber CLI is found that can be exploited (could potentially be mitigated by call treatment on +44 7 CLIs found not to be roaming) Ofcom should note that this type of behaviour is normally a breach of contract in respect of interconnect agreements and should in any case be policed by IGWs and CPs.
19	Fraudsters attempting an "Is Roaming" check for the potential of physical security threats is much less than the current problem or the future problem given that CAMEL HNR is not ubiquitous.	Vulnerable to fraudsters checking that an individual subscriber is roaming then using this information for physical security threats (e.g. burglary at vacant home). If it is believed that this is significant threat then additional checking can be performed by the proxy to the MNO to see whether the roaming subscriber is actively making a call. Most MNOs now support an API for performing this check which could be seen as an additional security check beyond simple "Is Roaming".
20	DOS attacks – automatic processes will enable immediate blocking mid-event.	All networks need to have in place processes and procedures to manage the risk of attack.
21	Failsafe – if a visited network doesn't support the CAMEL interaction (at all, or response is delayed), use of the proxy will mean that call will succeed. This may apply to high percentage of roaming calls will not be supported where CAMEL is not implemented.	

[14] We note in BT's response, point 3.7, to Ofcom's 2023 Consultation: "Calling Line Identification (CLI) authentication – a potential approach to detecting and blocking spoofed numbers", that BT supports an independent function for Traceback. We would suggest that the security issues would be the same as those for a proxy server. In fact, a proxy server could form a pillar of any Traceback solution.

	Pros	Cons
22	The proxy is based on existing standards and will supply expected responses (including error codes) and will not require any development on the part of the IGWs or MNOs.	

In response to Ofcom's footnote 39 "*For any solution that allows for a third party to either query directly or indirectly if a mobile number is currently roaming, the security requirements should be carefully considered including the end-to-end framework that would govern who has access to this data*", we would point out that a similar risk already exists in the commercial solutions deployed in the market today allowing businesses to access the MNO HLRs. The security measures deployed by the MNOs in that instance could, of course, be replicated here.

As we have mentioned, a proxy server solution is available today which would cache queries, this removes the need to continually query the mobile networks once a CLI has been queried initially. The proxy server, therefore, negates the need for the mobile networks to provide "live" mobile roaming information. Therefore, the proxy would provide a more secure solution than a 'live' database and reduce the number of queries required by CAMEL only.

Ofcom Question 6

b) Do you think it is possible to identify a solution that could be implemented relatively quickly now, and which would enable implementation of a more robust and effective solution in the future? If yes, what solution fits these criteria? Please give an explanation for your response.

XConnect would propose that the hybrid proxy solution, as outlined in the section above, is the quickest and cheapest solution to implement. [redacted].

As detailed above in the pros and cons, the proxy would be compliant with all necessary security, GDPR and other legislation requirements and would provide carrier grade resilience. As there are a variety of ways for both the IGWs, MNOs and thick MNOs to interface with the proxy it would be the quickest solution to implement. Whilst there may be the need for some internal development by the IGWs, MNOs and thick MNOs we believe this would be minimal compared to the work required by an MNO for the home network routeing scenario.

XConnect would suggest that a proxy service could incorporate other numbering datasets and validation services either immediately or in a phased approach. It could therefore provide the initial building block which could organically grow into supporting a comprehensive Centralised Numbering Database ("CNDB"). This in turn would then enable the implementation of multiple and dynamic fraud mitigation tools.

If the implementation of a proxy were considered as part of a long-term strategy (to support all potential fraud mitigation requirements such as Traceback) it would provide the flexibility to accommodate currently unforeseen new requirements to keep pace with the ever-changing tactics of the bad actors.

Ofcom Question 6

d) What would be the advantages and disadvantages of industry-led solutions, and where might regulatory intervention be required? Please give an explanation for your response.

XConnect suggests that any industry-led solution(s) is always a balance of competing interests and One-Touch-Switching highlighted the difficulty, in the UK, of balancing those interests and implementing a solution at speed.

The situation with fraudulent calls and the subsequent consumer harm cannot allow for these types of delay and any solution must be agreed and established in the shortest timeframe feasible. Industry must be mandated to implement a solution or there will be delays, fragmentation, further loss of trust in mobile numbers and further significant consumer harm. Therefore, this must be a regulator led solution which addresses the key technical requirements and outcomes without being distracted by individual preferences and politics. Without a regulator led solution, it is hard to imagine that parties terminating calls into the UK will be able to validate the roaming status of UK roaming subscribers. In other markets around the world, regulatory intervention has been required to address this point alone.

XConnect suggests that the requirement to check if a call is roaming or not is self-evident and, as discussed above in the proxy description, there are commercially available solutions operating in the market today, with multiple ways of working incorporating existing industry standard protocols and APIs.

Ofcom Question 7

Are there any international experiences of tackling this issue that you think are particularly relevant for the UK? Please provide evidence and an explanation for your answer.

XConnect considers both CEPT's recommendations and the work undertaken by ComReg in Ireland and Finland's Traficom, as international examples which Ofcom should give thought to.

CEPT

As Ofcom have noted in point 4.41, CEPT's ECC Recommendation (23)03 *Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers,* covers a number of scenarios and recommendations relating to identification of roaming calls[15]. In A1.1 scenario 1, the recommendation states:

> *This check could also be done through a centralised neutral entity (roaming check proxy), or through a distributed solution, to ensure that the querying operator does not get more information than needed and has no direct access to the other operator's Home Location Register (HLR).*

If Ofcom were to implement a proxy, it would be consistent with Belgium, Finland, Saudi, Oman and the Swedish recommendation. This would support an emerging common set of principles and a harmonised approach to technology, creating a better net globally to stop fraudsters and reduce the burden on international carriers.

ComReg

XConnect fully supports the path taken by ComReg with respect to their holistic approach incorporating a number of fraud mitigation tools with a phased implementation and we would urge Ofcom to look at use cases and solutions in the round. XConnect believe that this is the most effective way to close all the loopholes used by fraudsters across the telecommunications ecosystem.

In this way, an "Is Roaming" proxy could be the first step / building block to support other tools to fight fraud, such as Traceback. If the proxy is extended to include other pieces of numbering information it could become the basis for a centralised numbering lookup.

Traficom

Finland has adopted a proxy solution based on the existing number portability proxy.

Ofcom Question 8

Are the factors outlined in the section 'framework for evaluating options' the right things to think about when making a decision on options to address spoofed UK mobile numbers, and are there any additional factors which we should consider?

XConnect believes that any solution must validate 100% of calls in order to prevent consumers from harm which a proxy solution could achieve. Any loophole will be exploited by fraudsters.

[redacted]. The evidence on consumer harm is well documented and even volumes as low as hundreds of thousands could be incredibly damaging. However, the volume of calls could be far, far higher than that.

[15] CEPT, 2023. *Measures to handle incoming international voice calls with suspected spoofed national E. 164 numbers.*

If Ofcom were to mandate a proxy solution, XConnect believes the implementation costs for IGWs and MNOs would be minimal as set out below, and there would be no costs for legitimate businesses or other third parties:

- Selection costs: there will be a cost of vender selection for all parties that wish to participate in the process but this would be no more than for any other third party selection process carried out today. Therefore, this should be considered normal operational cost.

[redacted] Implementation and set-up costs: these are expected to be minimal due the availability of a variety of ways to interface with the proxy, therefore, keeping any IGW and MNO development costs low. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

A further proposal would be for the Home Office to directly contract with a supplier alleviating many of the problems and concerns which have been expressed to date.

[redacted] Ongoing costs: there are a variety of ways these could be considered. XConnect already provide third party lookup services which are utilised by a number of existing customers and many in the A2P ecosystem [redacted]

Alternatively, XConnect has provided a number of other suggestions:

- Option 1: a price structure based on banding could be used similar to the banding currently used by Ofcom for the Administration Fee, smaller operators paying a smaller annual flat fee. MNOs, thick MNOs and IGWs paying a higher flat annual or monthly fee.

- Option 2: tiering could be developed with respect to number allocations.

- Option 3: an annual / monthly rate for the bigger players, an annual/monthly rate for the MNOs and a reduced annual/monthly rate for smaller players who would require access.

Of the points raised in section 4.47 of the CFI, the following is of particular importance:

- relevant practical and operational implications of any proposed solution, including any complexities that may arise with respect to, for example, governance, privacy, security and resilience considerations.

Governance: as mentioned previously, there are commercial proxy solutions available which provide similar carrier-grade real-time number information lookup services which are being used in the UK market today, for example, for CLI validation and routeing services.

Ofcom must state the clear criteria, expectations and timescales for their proposed outcomes to be achieved by industry.

We would suggest that the process undertaken to select the provider of British Sign Language ("BSL") for emergency calls should be replicated so as to deliver a rapid implementation of these consumer protection measures. This would be in contrast to the implementation timeline of the One Touch Switching initiative.

By applying the same process as that used for BSL the need for industry governance would be removed or considerably reduced, given that Ofcom can impose the same "fair and reasonable" trading terms on its chosen proxy supplier.

- Privacy: XConnect does not believe there are any privacy issues with the proxy as operators will not have access to the database and unlike a live database the proxy would not hold live roaming information.
- Security: any solution provider must comply with all TSA requirements to enable Tier 1 operators to utilise the service. This would also be in line with commercial practices today.
- Resilience: as described, this solution should be implemented to the highest levels of resilience including diversely distributed servers (whether physically distributed or the selection of dispersed cloud locations).

In considering the requirements emerging from the telecom and finance sectors Ofcom should be mindful of the rare opportunity to build a reusable capability. Historically the UK has sought silo solutions to each emerging fraud scenario. Even within the narrow confines of the current objectives, once current scam methodology has been addressed by which ever proposal Ofcom directs, history tells us that bad actors will once again morph their activities and we will continue to play whack-a-mole. Having the flexibility to address these subsequent manifestations of fraud without reinventing the wheel will reduce the costs and speed the implementation of further measures. There are commercial services already available in the market which would provide such a foundation out of the box.

We would remind Ofcom that such services have been developed in response to a variety of similar requirements around the world, for example:

- The COIN[16] solution in the Netherlands was originally put in place to address the introduction of the Number Portability Directive 2000. This had the flexibility to be expanded upon to support other requirements and now supports a suite of different services.

[16] https://coin.nl/en/services/nummerportabiliteit

- In Finland, the existing number portability function, which is provided by Numpac[17], developed a proxy server for mobile CLI screening and blocking.

A proxy solution for "Is Roaming" could become a fundamental cornerstone and critical enabler for further enhancements to the UKs network infrastructure, which could also include numbering information held by the proxy providing accurate routeing information in the event of an operator failure.

[17] https://numpac.fi/en/

Annex 1

Wireless Logic Global 2G & 3G Network Closures[18]

Wireless Logic provides an overview of the 2G and 3G closure plans across many countries. The list is not exhaustive; however, it serves to highlight how complex the situation is with respect to closure announcements.

Based on XConnect's analysis the time from a closure announcement to actual closure is a period of three to five years.

It is interesting to note that it is not only the less economically countries who have a slower path to removing 2G & 3G.

Of particular note are the following:

Country	Operator	2G/3G	Comment
Belgium	Orange	2G Dec-30	
Denmark	TDC	2G Dec-29	Estimated Timeframe for full 2G network closure
France	Bouygues Télécom	2G Dec-26	Estimated Timeframe for full 2G network closure
New Caledonia	Office des Postes et Telecommunications	3G Jan-30	Estimated Timeframe for full 3G network closure
Poland	T-Mobile Polska	2G Dec-30	Estimated Timeframe for full 2G network closure
Poland	Orange	2G Dec-30	
UK	Vodafone	2G	Before 2033
UK	EE	2G	Network closure estimated 2026-2029
UK	Virgin Media	2G	No plans announced for 2G network closure

[18] https://wirelesslogic.com/global-network-closures/

Annex 2

Kore Wireless[19] also tracks network closure announcements for 2G & 3G. The list is not exhaustive, however is serves to highlight how complex the situation is with respect to closure announcements.

Of particular note are the following:

Country	Operator	2G/3G	Comment
India[20]	Vodafone Idea	2G	no specific planning
Indonesia	XL Axiata	2G	no specific planning
Liechtenstein	Salt (Liechtenstein) AG	3G	no specific planning
Liechtenstein	Telecom Liechtenstein AG	3G	network closure postponed
Philippines	Smart Communications, Inc.	3G	no specific planning
Serbia	VIP mobile d.o.o.	2G	no sunset planned as necessary for M2M

[19] https://eu.korewireless.com/2g-3g-network-sunset-dates

[20] It is estimated that the number of 2G users falls between 250-300 million in the country.