Reducing scam calls from abroad which spoof UK mobile numbers:

Options for addressing consumer harm Call for Input
Published 29 July 2024

NON-CONFIDENTIAL VERSION

This is PXCs response to Ofcom's "Reducing scam calls from abroad which spoof UK mobile numbers:

Options for addressing consumer harm" Call for input paper published 29 July 2024.

Introduction

PXC is firmly committed to tackling the issue of scams. We consider ourselves to be industry leaders in this area as indicated by our history of introducing blocking measures to prevent consumer harm from scam calls from abroad. These blocking measures have since been formalised through an industry standard (NICC ND1447) and mandated by Ofcom.

Summary

We include specific responses to Ofcom's consultation questions below. In summary, we principally agree that more needs to be done to tackle scam calls, to avoid further erosion and confidence in voice network services. Of the options present PXC's preference is: 2d CAMEL home routing (allowlist). We also agree that any approach needs to be multifaceted to tackle the multi-channel approach adopted by fraudsters and welcome Ofcom's "call for input: Reducing mobile messaging scams".

Analysis

Question 1:

a) Do you agree with our characterisation of the ways in which mobile calls enter the UK? Please give an explanation for your answer where appropriate.

We agree that there is no commonly agreed approach to distinguish between calls from legitimate roaming UK callers phoning back into their home country. From a terminating network provider perspective, we are unable to determine the validity and origin of mobile traffic, beyond assessing whether there is a complete, dialable CLI associated with the traffic.

b) What do you think is the relative importance and / or significance of each of the different routes used for calls to enter the UK? Please provide evidence for your answer.

PXC receives internationally originated traffic made by UK mobiles to terminate and transit on its network via bilateral interconnect agreements and international gateway providers. An open question remains across industry as to whether any traffic from roaming mobiles should be able to use international transit routes at all, rather than routing directly to the MNO in question.

Our experience of complaints (received from CPs) and observations of the same mobile phone number making exceptional call volumes has led us to conclude that there is significant variability between international gateway and interconnect CPs. Some operate highly effective measures on the traffic they permit. From a geolocation perspective European providers typically are of higher quality, whereas others have been observed as less diligent.

c) If you provide mobile services to UK consumers, what international gateway provider(s) does your organisation use (including in-house services)? In addition, please explain the nature of the international gateway services you rely on.

We do not provide mobile services to UK consumers.

***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?**

PXC recognises the need to address issues stemming from spoofed UK mobile numbers. We remain committed to exploring viable solutions to mitigate these harms, aligning with broader industry initiatives to combat fraud.

We note that UK Finance provides a breakdown of APP fraud enablers in their Annual Fraud Report 2024. We would urge additional engagement with UK finance in order to secure a further breakdown of data (now or in the future), to determine the specific details around the telecommunication channels that scams originated through. Not only would this information be invaluable to support any cost -benefit analysis but would also provide a tracking measure to determine the ongoing efficacy of any changes and to target further remediation activity. We note some scams have moved into the Social Media/ Instant messaging arena. This data would also allow the ongoing ability to monitor mobile spoofing related fraud in comparison to Online Communication Services or other communication channels.

Mobile fraud spoofing exploits international transit routes which cannot have blocking measures applied due to the presence of mobile roaming traffic. We think it would be appropriate to consider the proportionality of costs / impacts of change outside of MNOs.

Question 3:

a) What is the scope and scale of consumer harm caused by spoofed UK mobile numbers?

PXC are unable to provide data in this space as we do not service end users.

b) What are the consumer impacts of spoofed UK mobile numbers more broadly? Please provide evidence to support your responses.

PXC cannot offer specific end user harm details as we operate as a wholesaler, although we agree with, and acknowledge the financial and emotional impact of fraud as cited in the "Reducing scam calls **….**" call for input document.

It is our belief that telecommunications-initiated scams, will have an impact on end consumers' levels of trust and confidence in telecommunications services in general. We believe that consumers are less likely to answer calls as a consequence of fraud concerns, which ultimately harms the reputation of the telecoms industry.

Question 4:

a) How significant is the volume of spoofed mobile calls from abroad?

It is very difficult to quantify the difference between a mobile CLI which has been spoofed and a mobile CLI from a genuine roamer, as we are unable to validate the call.

We recently assessed 1 gateway provider's Mobile Originated data, where a CP to CP scam query was raised. **[redacted]** calls were identified in a 14-day sample period where individual mobile numbers were associated with hundreds/ thousands of calls, which we believed falls outside of standard usage patterns.

b) Is there any evidence that scammers are moving from spoofing fixed to mobile UK CLI? Please provide evidence to support your responses.

The introduction of NICC ND1447 has resulted in the increased blocking of UK geographic CLIs. Anecdotal reports indicate an increase in complaints (received from other CPs), as spam and scam calls have exploited routes through certain UK OLOs and VoIP CLI ranges. We have also seen patterns of high call volumes to individual mobile CLIs, but we are unable to determine calls which have been spoofed. Technically, we believe this now remains one of the few exploitable routes available, other than where upstream providers have not effectively applied NICC ND1447 rules.

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.

We expect that implementing VoLTE Home routing will significantly enhance the security of mobile roamers by eliminating the need for gateway/ transit providers to route traffic.

It is essential that mobile network operators provide clear timelines and solutions to industry regarding VoLTE home routing. Mobile networks have established roaming agreements amongst themselves but often rely on the incumbent fixed PSTN networks of the destination country to route traffic based on the called party number routing back to the UK.

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)?

Having reviewed the latest options presented within this consultation, Option 2d CAMEL home routing (allowlist) is the PXC preferred option with calls being blocked.

The CAMEL home routing approach, while requiring some development, leverages existing network architecture and interconnects. Mobile networks inherently possess the roaming status of devices and

information on network porting, which is typically unavailable to other networks acting as ingress or transit points.

This capability enables the mobile network to validate the Mobile CLI and route calls to their intended destinations accordingly. The temporary home routing number having been applied from a verified mobile source, ensures that international and transit networks, regardless of the number of hops back to the UK, will then route calls based on the temporary home routing number. Longer term there could be greater reliance upon VoLTE but option 2d would address fraud issues in the interim.

It is our view that it is a better solution to address mobile network security issues via this route than via the gateway/transit networks, which handle the ingress of mobile roaming traffic to various destinations.

In relation to Group 1: proactive checks by the international gateway. The proactive check will only determine whether a mobile is currently roaming. In the absence of other checks, we believe it would be relatively easy for fraudsters to adapt and circumvent these measures. As an example, pay as you go SIM cards could be purchased, registered and sent overseas to then have CLIs to legitimately present as roaming mobiles.

Furthermore, each of the options is ultimately reliant upon the availability of the service and an up to date, data feed. Delays in call set up whilst checks are made, albeit small may provide a worsened end user experience.

We agree with Ofcom's view that the 1a: Gateway roaming query (direct) solution would likely be problematic where numbers have ported several times and that the process of identifying the correct network and ascertaining whether the caller is legitimately roaming may quickly become complex and prone to delays and error.

Whilst the 1b & 1c design overcomes the porting challenges presented by option 1a, we would be concerned with broader cost /complexity implications and the ease that fraudsters could circumvent these measures.

Should a shared industry database holding roaming data be progressed, then a full security impact assessment is needed to ensure bad actors could not harvest roaming data.

Group 2 solutions 2b and 2c require gateway providers to treat numbers as 'withheld' which would only be updated via the home network. Consideration would be required on the interplay of these changes with Anonymous call rejection. Where ACR is activated by a customer (number withheld), the calling party may receive instruction to call again but to not withhold their number or that withheld numbers were not accepted. If for any reason contact was legitimate this could create caller confusion.

In the (withheld CLI+) option, the way additional information is added to the call metadata would need to be assessed. There is risk of gateway manipulation of metadata. If encryption were required to prevent, the solution would have similarities to the STIR/SHAKEN proposals, which have previously been discounted.

Option 2d with call blocking applied, would ensure that the calls never reach the end user thus preventing the risk of fraud. Where a CLI is deleted or withheld, this may provide greater anonymity to fraudsters, and only reduce rather than eliminate fraud risk.

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.

We expect Mobile Network Operators have visibility of which countries are and are not capable of VoLTE home routing. Where the country is neither VoLTE nor CAMEL capable, a potential option would be to implement direct connections from those remote MNOs to the domestic MNOs. This would then enable us to block all international traffic at the gateway with UK CLIs.

c) What would be the advantages and disadvantages of obtaining more information about, and oversight of, the international gateway providers which bring calls into UK networks, in the context of tackling use of telecommunications networks to facilitate fraud and scams? Please give an explanation for your response.

In respect of data, careful consideration would be required, regarding the level of information needed and intended purpose and usage. Any quantitative data may offer insights into traffic patterns. For example, mobile call volumes for the same CLI and frequency of instances of suspect traffic by international gateway provider. In order to take action in response to such data will likely necessitate in-depth data queries. Detailed data analytics are resource-intensive and require additional processing power and specialist software capable of handling significant data volumes.

The actionable insights from such data may also be limited. Whilst the data would offer insights, it would not provide direct causation information. To allow direct correlation, additional data sharing, such as that collated by UK finance could prove beneficial.

There is also the question of where the data analytic responsibility should lie. Data and analytics would ideally be requested from international gateway providers directly rather than any terminating networks. This may encourage proactive action by the international gateway provider in response to findings.

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.

The NICC are well placed to offer guidance on a technical solution. We believe regulatory intervention may be required to ensure change is implemented. Reliance upon commercial or contract arrangements to elicit change are likely to be limited in effectiveness, with breach of contract providing poor recourse for non-adherence and with no enforcement capability.

As revenues are decreasing on voice traffic, any industry solution needs to be cost conscious. Enforcing an expensive solution in the case of roaming traffic, would inevitably translate to increased consumer roaming costs. With VoLTE home routing on the horizon, costly investment (in particular on gateway/transit networks) would inevitably be resisted.

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.

We do not have any comments in relation to this question.

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? Please explain your response where appropriate.

We are in broad agreement with the evaluation framework proposed. In relation to other implications, consequences or adverse effects, we would hope to see specific assessment of the interplay of proposed changes with the Privacy and Electronic Communications Regulations and GDPR of any shared data. Furthermore, the operational practicalities and implications in order to remain compliant with privacy law associated with any intervention.

As the mobile CLI loophole for scammers is directly connected to the mobile roaming capability within the MNO product set, we believe that is it proportionate for onus to be on MNOs changes to resolve, rather than to create financial overhead for international gateway providers

In reference to the effectiveness of the intervention we would welcome consideration of the ease/ difficulty and probability that fraudsters could adapt their approach to circumvent any new intervention measures to support maximum benefits.