Reducing scam calls from abroad which spoof UK mobile numbers

Options for addressing consumer harm

Call for Input

Published 29 July 2024
Closing date for responses: 23 September 2024

Contents

Section

Annex

1. Overview

1.1 Protecting consumers from harm caused by scams facilitated by phone calls is a priority for Ofcom. A common tactic used by scammers is to 'spoof' telephone numbers to disguise the origination of the call, or to make their call appear to be from a trusted person or organisation. Where scam calls appear trustworthy, victims are more likely to share personal information or to make a payment, which can lead to significant financial and emotional harm.

1.2 We have already implemented a number of measures to make it difficult for scammers to use UK telecoms networks to harm consumers. These include:

- requiring operators to block numbers that are never intended to make outbound calls and are recorded in the Do Not Originate (DNO) list;
- requiring operators to identify calls from abroad which spoof a UK fixed Network Number and block them; and
- tightening the requirements on operators to carry out appropriate due diligence when sub-allocating numbers to other UK operators.

1.3 We are concerned that some of the scam calls which are received by UK consumers may come from scammers who are spoofing +447 (UK mobile) numbers.[1] This call for input (CFI) builds on our programme of work to reduce the harms caused to consumers by scam calls. In our *Calling Line Identification (CLI) authentication assessment and future roadmap*, published in February 2024, we noted that we would explore options for blocking calls or preventing calls from abroad presenting a spoofed UK mobile number.[2] [3] We are now investigating whether we should change our rules, or consider other measures, to fix this issue, and this document sets out our initial thinking.

1.4 Ofcom sets out the requirements for the display of CLI Data in the General Conditions of Entitlement (GCs), under GC C6. The CLI Guidance sets out what is expected of providers to comply with GC C6. This includes guidance on blocking calls from outside of the UK which use a UK CLI. Our current rules do not, however, address inbound international calls spoofing UK mobile numbers. This is because our current blocking guidance specifically sets out an exemption for calls from abroad which are made with a UK mobile CLI from a +44 range. One of the reasons for this exemption is to allow UK roamers who are calling back home to have their number recognised when they are calling friends and family. The scope of this CFI is limited to considering this exemption in our CLI Guidance.

---

[1] In this CFI, references to +447 numbers refer to UK mobile numbers only. This document does not address 070 personal numbers and 076 paging numbers.

[2] Ofcom, 2024. *Calling Line Identification (CLI) authentication assessment and future roadmap*.

[3] A telephone number is also referred to as 'CLI data'. 'CLI data' refers to the contents of the signalling messages, which are used between providers and/or between a provider and an end user, to signal the point of origin of the call and/or the identity of the calling party. This includes any associated privacy markings, which indicate whether the number can be shared with the recipient of the call or whether it is withheld. There are two numbers associated with CLI data: the Presentation Number and the Network Number. Call recipients see the Presentation Number when they answer a call. The Network Number is shared with providers to identify the origin of the call. It is common for these two numbers to be the same for mobile calls.

1.5 The NICC has also been working to find technical solutions to address this issue by identifying legitimate UK roamers and blocking or reducing calls which spoof UK mobile numbers, but has not yet reached a conclusion on a preferred approach.[4] We will continue to work alongside the NICC on this matter.

1.6 There are two broad technical solutions being actively explored both in the UK and abroad. One group of options under consideration involves the provider that is bringing the call into the UK (referred to in this document as the 'international gateway provider') proactively undertaking checks to ascertain whether a specific number calling from abroad is indeed roaming. The second group under consideration involves the international gateway provider identifying mobile calls coming from abroad, modifying the data associated with such calls, and then usually forwarding them to the caller's home mobile network, where further validation checks may take place.

1.7 However, there is no clear consensus across industry on the preferred solution. Our evidence on the scope and scale of the problem of calls spoofing UK mobile numbers is also limited. Anecdotally, industry has told us that, as we have closed other spoofing routes, scammers are moving to spoof UK mobile numbers. This means that, while current volumes of such calls may be low, there is a risk that scammers will exploit this opportunity further in the future.

1.8 We are therefore publishing this CFI to seek initial views and evidence on the effectiveness, costs, risks and timescales of different options to address spoofed UK mobile numbers. We are also seeking further information on the scope and scale of the problem to help inform any proportionality assessment.

1.9 This CFI closes for responses on 23 September 2024. We will use responses, together with a programme of stakeholder engagement and information gathering, to ascertain whether or not to consult on a preferred option. If we decide that we need to introduce new regulation on this issue, we anticipate consulting in Spring 2025.

[4] The NICC is the UK telecommunications network and service interoperability standards body.

2. Introduction and background

Purpose of this document

Exploring options for identifying and blocking spoofed UK mobile numbers

2.1 The rules for the display of CLI are set out in General Condition (GC) C6. The CLI Guidance sets out what is expected of providers to comply with GC C6. This includes guidance on blocking calls from outside of the UK which use a UK CLI. There is currently an exception for calls which are made from abroad using +447 (UK mobile) numbers.[5] This is because there is currently no commonly-agreed approach to distinguishing between calls that are from legitimate roaming UK callers phoning back into their home country, and calls that are spoofing UK mobile numbers.[6]

2.2 We are concerned that some scam calls which are received by UK consumers may come from scammers who are exploiting this gap in our rules by spoofing UK mobile numbers. In our *Calling Line Identification (CLI) authentication assessment and future roadmap*, published in February 2024, we noted that we would explore options for blocking calls or preventing calls from abroad presenting a spoofed UK mobile number.[7] We are now exploring whether we should change our rules, or consider other measures, to fix this issue.

2.3 We have undertaken preliminary work to better understand the options currently under consideration and to explore further solutions, including methods for identifying genuine mobile roamers, and measures introduced by other jurisdictions. We have also closely followed investigations by the NICC to agree on a preferred technical solution for identifying legitimate UK roamers and blocking or preventing calls coming into the UK from abroad which spoof UK mobile numbers.[8] We note that there is, at the time of publication, no clear consensus on the most effective, efficient and proportionate option for addressing these calls.

2.4 This CFI seeks initial views on proposed options to address spoofing of UK mobile numbers. We acknowledge the significant work already undertaken by industry and other stakeholders to prevent scam calls from reaching customers. We expect that, as some channels for scammers to use are closed, they may switch to other methods. Although we have received anecdotal evidence that use of spoofed UK mobile numbers has at least partly replaced the use of spoofed fixed numbers as opportunities to use these have been reduced, there is little quantitative data on the scope and scale of the potential issue. We are also aware that there are different views across industry and other stakeholders about the relative effectiveness of each of the proposed solutions. We want to ensure that we are able

[5] In this CFI, references to +447 numbers apply to UK mobile numbers only. This document does not address 070 personal numbers and 076 paging numbers.

[6] We note that the Bailiwicks of Jersey and Guernsey and the Isle of Man (which are constitutional dependencies of the British Crown, known as the 'Crown Dependencies') use +44 numbers but are not subject to our regulation. The Crown Dependencies have their own Telecommunications legislation and communications regulators.

[7] Ofcom, 2024. *Calling Line Identification (CLI) authentication assessment and future roadmap*.

[8] These circumstances are referred to throughout the document as 'spoofed UK mobile numbers' for brevity.

to undertake a full assessment of potential remedies to help inform any interventions in this area.

2.5 We are therefore seeking specific views on the proposed options which have been identified. We are also seeking data on the scale of the problem and the timescales associated with potential solutions. We will use the responses to this CFI to help inform our assessment of the proposed solutions, including consideration of a detailed counterfactual, to determine whether it is appropriate to proceed with a consultation on a preferred option to address spoofed UK mobile numbers.

2.6 At this stage, the scope of this work does not include investigating calls from UK mobile users who are legitimately roaming, even if these are being used for scam calls.

Scams context

Background

2.7 Protecting consumers from harm caused by scams facilitated by phone calls continues to be a priority for Ofcom. Scam calls can result in significant financial and emotional harm to victims. They can also lead to a reduction in trust in telephone calls.

2.8 As we set out in our February 2022 statement, our ongoing strategy to counter scam calls seeks to make it harder for scammers to operate at every stage of the value chain.[9] We aim to achieve this by focusing on three key areas of intervention:

- **Disruption**: We aim to disrupt scams by making it harder for scammers to use communications services to reach consumers, using regulatory measures and encouraging technical innovation. We have strengthened our rules and guidance, while at the same time supporting providers in developing their own technical solutions to detect and prevent scam traffic.
- **Collaboration**: Scams are becoming increasingly complex, and a coordinated approach is vital to ensure that as many scam attempts are blocked or disrupted as possible. We share information and collaborate with relevant stakeholders, including Government, regulators, law enforcement and consumer groups.
- **Informing consumers**: We are working to help consumers to avoid scams by raising awareness and understanding, so that people can more easily spot and report them.

2.9 Scammers continually adapt their tactics, so we have already worked with industry and government stakeholders to develop and implement several measures to make it harder for scammers to succeed across the scams value chain, and to reduce scam calls and texts.[10]

2.10 This CFI explores ways in which we can further disrupt the use of voice calls by scammers. Voice calls are one of a range of channels which are used by scammers to manipulate people into divulging personal details or transferring money to scammers (known as authorised push payment fraud or "APP"). While most APP scams start online, phone calls can play a significant role even where first contact is made through other means. For example, a malicious SMS or email might lead the recipient to a fraudulent website (used to obtain

[9] Ofcom, 2022. *Tackling scam calls and texts: Ofcom's role and approach*.
[10] For further details of our work to-date on addressing scam calls, please see pages 6-14 of our February 2024 document, *Calling Line Identification (CLI) authentication assessment and future roadmap*.

information about the victim) and the scammer may then contact the victim by phone (e.g. impersonating their bank) to request a payment.[11]

2.11 A common tactic used by scammers is to 'spoof' telephone numbers to make them appear to be from a trusted source. When a scammer makes a call from abroad, they may try to spoof their number to make it look like the call is coming from the UK. We are concerned that, because we have reduced opportunities for scammers to spoof UK fixed numbers, they may be switching to attempting to spoof UK mobile numbers instead.

Legal and regulatory context

General Condition C6 and CLI Guidance

2.12 As part of our 2017 review of the General Conditions (GCs), we introduced GC C6, which applies to all providers of Number-based Interpersonal Communications Services and Public Electronic Communications Networks over which Number-based Interpersonal Communications Services are provided.[12] We have also published Guidance to support GC C6.[13]

2.13 GC C6 includes requirements for providers to:

- provide CLI facilities by default unless they can demonstrate that it is not technically feasible or economically viable to do so;
- ensure, so far as technically feasible, that any CLI data provided with, or associated with a call, includes a valid, dialable telephone number which uniquely identifies the caller; and
- take all reasonable steps to identify and block calls in relation to which invalid or non-dialable CLI data is provided.[14]

2.14 In a statement in November 2022, we made changes to the Guidance on GC C6.6 which meant that calls from abroad could only use a UK CLI as a Network Number in a limited number of legitimate use cases.[15] We explained that we expected telecoms providers to block calls from abroad which use a UK CLI as a Network Number, except in a number of specified use cases, and referring to the examples set out in the standard ND1447[16]:

- UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range;
- calls to a mobile user who is roaming in the UK;
- where the traffic has originated on a UK network; or

[11] Frontier Economics 2022. *Frontier Economics, 2022. Tackling Fraud and Scams: An Ecosystem-Wide Approach*, pp.13-14.
[12] In our 2020 statement *Implementation of the new European Electronic Communications Code* we explained our decision to replace the term 'Publicly Available Telephone Service' with the new term 'Number-Based Interpersonal Communications Service' in GC C6 (see Section 3 of the statement). The term captures, for example, fixed and mobile telephone services, as well as VOIP outbound call services.
[13] Ofcom, 2023. *Statement: Guidelines for Calling Line Identification Facilities*.
[14] Ofcom, General Condition C6, *General Conditions of Entitlement*.
[15] Ofcom, 2022. *Guidance on the provision of Calling Line Identification facilities and other related services.*
[16] NICC Standards, 2021. *Guidance on blocking of inbound international calls with UK Network Number as CLI*.

- where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.

2.15 At the same time as this publication, we have also issued a Presentation Number statement, which includes an update to our Guidance to change the wording on the provision of CLI facilities.[17] This update confirms that providers are expected to identify and block calls from abroad that use a UK geographic or non-geographic telephone number as a Presentation Number, except in a limited number of legitimate use cases.

Crown Dependencies

2.16 In addition, although they are not part of the UK and are subject to their own regulation, there is an arrangement for the Crown Dependencies to use numbers from the +44 UK Country Code.

2.17 In our November 2022 Statement we explained that most calls from the Crown Dependencies enter the UK network via a national interconnect.[18] Therefore, they would not be affected by a change to reduce scam calls from abroad which spoof UK mobile numbers.

2.18 We have further clarified that calls from the Crown Dependencies continue to be exempt from this blocking in our Presentation Number statement which updates our CLI Guidance.[19]

General duties

2.19 This section provides a brief overview of the main UK legislative provisions relevant to this call for input. It is not a full statement of all the legal provisions which may be relevant to Ofcom's functions or to numbering. The applicable legal framework derives from our duties and powers in the Communications Act 2003 (the Act).

2.20 When formulating this CFI we have had regard to our general duties including our principal duty under section 3(1) of the Act to further the interests of citizens in relation to communication matters; and consumers in relevant markets, where appropriate by promoting competition.[20]

2.21 Section 3(4) of the Act provides that we must have regard, in performing our duties, to a number of matters, as they appear to us to be relevant in the circumstances, including the desirability of ensuring the security and availability of public electronic communications networks and services; the needs of disabled people, of the elderly and of those on low incomes; the desirability of preventing crime and disorder; and the opinions of consumers in relevant markets and of members of the public generally.[21] Additionally, Ofcom must have

[17] https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/updating-cli-guidance-to-tackle-scam-calls/

[18] Ofcom, 2022. *Improving the accuracy of Calling Line Identification (CLI) data*, para 4.147

[19] https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/updating-cli-guidance-to-tackle-scam-calls/

[20] 'Consumer' is defined in section 405(5) of the Act and includes people acting in their personal capacity or for the purposes of, or in connection with, a business.

[21] We also have public sector equality duties, in particular we must have due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it. This involves considering the need to: remove or minimise disadvantages suffered by people due to their protected characteristics; and take steps to meet the needs of people with protected characteristics.

regard to the interests of those consumers in respect of, among other things, quality of service.[22]

2.22 In performing our duties, we are required to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice (section 3(3) of the Act).

Our functions and powers relating to telephone numbers

2.23 Ofcom also has a general duty under section 63 of the Act in carrying out its telephone numbering functions to, among other things:

a) secure that what appears to it to be the best use is made of the numbers that are appropriate for use as telephone numbers; and
b) encourage efficiency and innovation for that purpose.

2.24 Section 4 of the Act requires us, when carrying out our functions, such as our numbering functions, to act in accordance with six requirements for regulation which include to promote the interests of all members of the public in the United Kingdom.

[22] Section 3(5) of the Act.

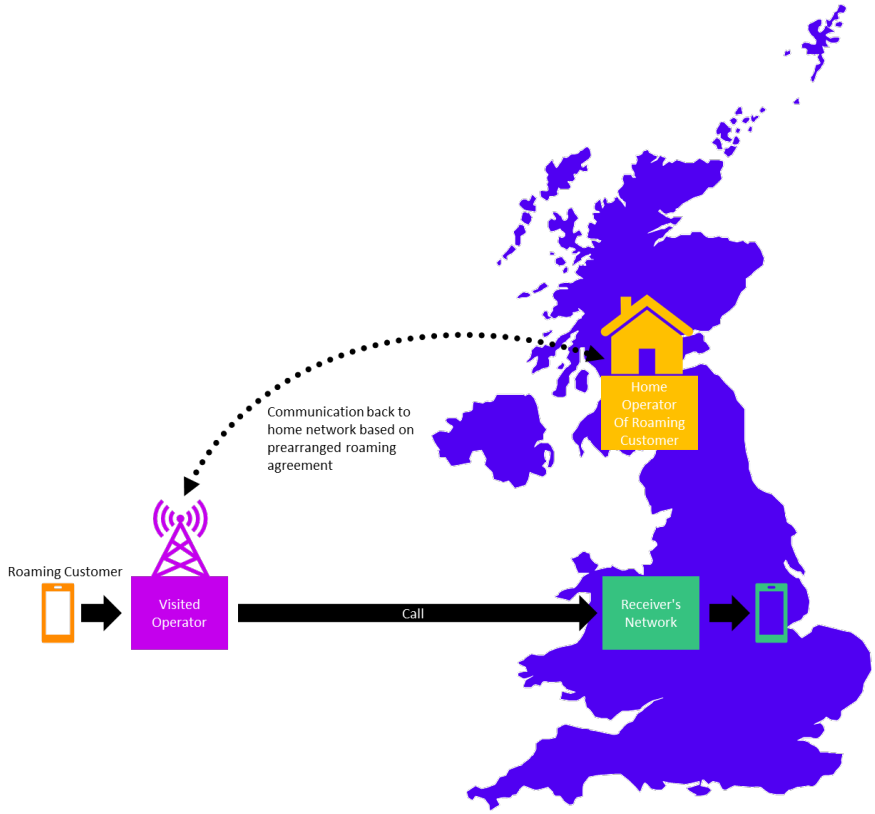
3. What is the problem with spoofed UK mobile numbers?

What is mobile roaming?

3.1 'Roaming' refers to the ability of a mobile provider's customer to connect to and make use of a network other than their own. For international roaming, this is achieved through the home mobile provider having one or more roaming agreements in place with the visited country's mobile provider(s).[23] When the customer's mobile device connects to a supported local network in the visited country, the visited network will communicate back to the customer's home network in the UK to establish what services are supported for the customer. Assuming that these steps are successful, and the customer's device has the relevant permissions, services such as voice calls (the focus of this CFI) and data may then be used over the visited network.

3.2 Figure 1 shows a schematic diagram of how roaming works when a mobile user roams outside of the UK.

Figure 1: mobile roaming away from the UK



[23] Mobile Network Operators (MNOs), as well as some Mobile Virtual Network Operators (MVNOs) and Mobile Virtual Network Enablers (MVNEs), will often have hundreds of roaming agreements in place with multiple providers in other countries.

3.3 When a UK mobile customer is roaming abroad and makes a call destined for a UK number, the call will typically display the UK CLI of the mobile making the call.[24] This means that, in normal circumstances, when the customer looks to see who is calling, it will appear that a UK mobile number is making the call, even if the person who is making the call is doing so from another country.

Routes into the UK network can provide opportunities for scammers to exploit

3.4 Calls from UK users roaming abroad will enter the UK with a +447 number. There is currently an exception in the CLI Guidance for all +447 numbers so that calls from UK (and Crown Dependency) users roaming abroad are not blocked. When a call is delivered into the UK from a UK roaming mobile customer, there are several possible ways for the call to enter the UK telephone network.

3.5 One route is via an entity providing international gateway functionality (an 'international gateway provider').[25] International gateway providers tend to operate on a global scale and facilitate data and voice connections between discrete networks around the world. In line with our Guidance, we expect that international gateway providers currently have a general exception for numbers that start +447.[26]

3.6 International gateway providers connecting into the UK may not have a direct relationship with the calling party's home mobile provider, and therefore they may not have a method to validate the legitimacy of the specific number being presented. This provides an opportunity for a scammer to generate calls which spoof a UK mobile CLI in order to make scam calls from abroad to UK consumers appear as if they are originating from a UK mobile number.

3.7 In other cases, networks may have bilateral interconnect agreements with each other, over which data and voice calls can pass. However, even in these cases, it may not be possible for the operator(s) to validate incoming calls. Without other measures, these operators would therefore not be able to mitigate scam calls which use spoofed UK mobile numbers.

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.

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.

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.

---

[24] The CLI presented might be withheld but the underlying network number would still represent a UK mobile number.

[25] In this call for input, we use 'international gateway provider' to refer to any telecommunications provider which brings a call into the UK telephone network for the first time in the call's routing journey. The ITU defines an international gateway as "any facility through which electronic communications (voice, data and video) can be sent between the domestic networks of one country and another" (ITU, *Liberalising International Gateways,* accessed 15 July 2024).

[26] Some of the other exceptions for the legitimate use of UK CLI from abroad, noted at para 2.14, may require the UK network provider receiving the call in the UK to understand whether the caller has the right to use those numbers. In those cases, the call may need to be long-lined into a UK network provider directly, rather than through an international gateway provider.

Data on the scope and scale of the problem is limited

3.8 UK communications providers have told us that scammers are seeking to spoof UK mobile numbers in increasing volumes as opportunities to spoof UK fixed numbers diminish. However, there is limited information on the following variables. We think that a better understanding of these would help us, in turn, to better understand this problem:

- the impact on consumers and the scale of consumer harm associated with scams where overseas callers spoof mobile CLI;
- the scope and scale of this problem in terms of volumes and proportions of calls processed;
- whether or not developments in voice roaming technology will decrease opportunities for scammers to spoof UK mobile numbers; and
- 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.

3.9 We discuss each of these variables below. We are keen to hear from stakeholders about these and other matters and variables that may need to be considered.

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?

Consumer impact of spoofed UK mobile CLI and the scale of consumer harm

3.10 Call recipients are more likely to answer a call which appears to come from a UK mobile number than an international or withheld number.[27] Where scam calls appear trustworthy, victims are then more likely to share personal information or make a payment, which can lead to significant financial and emotional harm.[28] While 16% of APP fraud cases in 2023 originated from telecommunications (including SMS messages), these cases tended to be higher value, such as impersonation scams, and they accounted for 43% of total losses.[29]

3.11 More generally, the prevalence of scam calls and other unwanted calls leads to many calls going unanswered. Our 2024 research into suspicious calls and texts found that a majority of consumers do not always answer the phone, even when they could easily do so.[30] When

[27] Ofcom / Yonder, 2024. *Ofcom Scams Survey: Online fieldwork 31 January to 1 February 2024 data tables*, Qs.14 and 15 (pp.42-73). Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slides 17 and 18 - Question: How likely is it that you would pick up a call from the following types of numbers? This could be on your landline, or on your mobile.

[28] For examples of the ways in which consumers can be taken advantage of by scammers, and the impact this can have on individuals and business, see *Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?* (Communications Consumer Panel, 2020), and, *Scams and subjective wellbeing* (Which? and Simetrica Jacobs, 2022).

[29] UK Finance, *Annual Fraud Report 2024*, p.43.

[30] Ofcom / Yonder, 2024. *Ofcom Scams Survey: Online fieldwork 31 January to 1 February 2024 data tables*, Q.5 (pp.13-14) and Q.9 (pp.21-22). Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slides 8 and 12. Question: If your landline / mobile phone rings and you could easily answer it and are not otherwise busy, what do you generally do?

asked for the reason for not answering, the top option selected by both landline and mobile respondents was "I don't want to deal with marketing calls/ spam/suspicious callers".[31] Where this leads to calls being declined even when they are legitimate, it may undermine the effectiveness and efficiency of the telephony system.

3.12 While we collect and hold general data on the consumer impact of scam calls and texts, we do not currently hold evidence about consumer harm which specifically identifies the impact of scam calls which spoof UK mobile numbers.

Question 3:

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

b) What are the consumer impacts of spoofed UK mobile numbers more broadly?

Please provide evidence to support your responses.

Volumes of calls which spoof UK mobile CLI

3.13 While we collect data from network providers on volumes of blocked and failed calls more generally, together with the total number of inbound calls, we do not have quantitative evidence that could inform any assessment of the volume of scam calls to UK citizens that have spoofed a UK mobile number. Our understanding is that it is unlikely that providers could give comprehensive data on this because, unless there is a complaint or a report, they will struggle to identify which calls are spoofed and which are not. There may, however, be ways in which providers could obtain an indication of the extent of this activity. We are keen to explore whether this is possible.

3.14 Our expectation is that, with many of the alternative opportunities to make a scam call to the UK being addressed, it is reasonable to assume that spoofing UK mobile numbers may become more attractive to scammers in the absence of other measures. This is supported by the responses from stakeholders to our CLI authentication consultation which indicated - anecdotally - that the introduction of ND1447, and stronger rules on blocking calls which spoof UK CLIs, has resulted in scammers shifting from spoofing fixed numbers to mobile numbers. For example, in its response to our CLI authentication consultation published in 2023, BT Group noted that 'while difficult to verify, we strongly suspect that the gradual reduction in the numbers of overseas invalid and spoofed CLI calls being blocked by BT after July 2022 was due, in part, to scammers switching to mobile UK CLIs'.[32]

Question 4:

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

b) Is there any evidence that scammers are moving from spoofing fixed to mobile UK CLI?

[31] Ofcom / Yonder, 2024. *Ofcom Scams Survey: Online fieldwork 31 January to 1 February 2024 data tables*, Q.6 (pp.15-16) and Q.10 (pp.23-24). Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slides 9 and 13. Question: Given that you aren't busy and could easily answer it, what are the main reasons why you don't answer [some/any] landline / mobile calls?

[32] BT Group response to the 2023 CLI authentication consultation, paragraphs 4.10.

Please provide evidence to support your responses.

Developments in voice roaming technology and timescales

3.15 Mobile network technology continues its rapid pace of development, and each new generation of mobile technology has introduced new options for how international roaming can be implemented by operators.

3.16 These technologies maintain backward compatibility to facilitate interworking. The backward compatibility accommodates the fact that mobile providers are rolling out new technology across the globe at different rates. There are also differences between the technology generations in terms of how they support calls made from mobile devices which are roaming outside of their home network.

3.17 The underlying technologies which deliver 4G and 5G services make it generally much harder for scammers to spoof a roaming calling number than when a call originates on a 2G or 3G network, and it is the home network which determines how the call can be routed when it reaches UK networks. The pace of 4G and 5G rollout internationally may therefore affect the ability of scammers to spoof UK mobile numbers in volume, with a consequent impact on the harm caused to UK consumers and the proportionality of any measures we may consider introducing. However, the timescales for widespread international introduction of 4G and 5G services are uncertain, and there are likely to be pockets of ongoing 2G and 3G provision in the medium to longer term which scammers could continue to exploit.

2G / 3G international voice roaming

3.18 2G/3G international voice roaming standards allow for two approaches to facilitating international calls from roaming mobile devices:

a) the call is first sent back to the caller's own UK mobile provider before being onward routed to its destination; or
b) more typically, the call is not routed via the caller's own UK mobile provider, but is instead sent directly to its destination.

3.19 The option which is used can depend on several technical as well as commercial considerations. These can vary both between mobile providers and within a single mobile provider's own network, for different countries, networks, and subscriber types.[33]

4G international voice roaming

3.20 The rate of rollout for 4G roaming was initially restricted by the complexity of the interworking of technical options between mobile providers. A simpler alternative architecture was subsequently developed, which has now been adopted as the de facto implementation. This is known as S8HR ('Home Routing').[34]

[33] For example, a mobile provider may use one solution for pre-pay (pay-as-you-go) customers, and another solution for pay monthly (contract) customers.
[34] See GSMA | Your guide to accelerating VoLTE Roaming, and its importance to your business - Industry Services for an overview.

3.21 Where S8HR is deployed between a UK mobile provider and the visited country's mobile provider, the call is always first sent back to the caller's UK mobile provider before being onward routed to its destination. This allows for inherent checks to be carried out by the home network, prior to the call being delivered, which make it more difficult to spoof the calling number.

5G international voice roaming

3.22 5G roaming for voice services is dependent on a number of prerequisites, with the focus for most mobile providers currently being on data roaming. The current expectation is that 5G roaming for voice will not be common for at least one to two years.[35]

3.23 The technology supporting 5G voice over New Radio (NR) roaming follows the same principles as S8HR above but instead uses the 5G Core N9 interface. It is therefore referred to as N9 Home Routed (N9HR) roaming.[36]

Uncertainty about timescales for the global adoption of 4G and 5G technology

3.24 UK mobile providers are rolling out 4G and 5G roaming services at pace, and with the widespread adoption of 4G and 5G mobile handsets by consumers across the globe, it is likely that there will be a dramatic decrease in calls which originate on 2G or 3G roaming networks. The ways in which 4G and 5G roaming solutions are implemented make it inherently difficult for a scammer to spoof a number and so we are not concerned about mobile calls that are originated on those networks.

3.25 In its response to our CLI authentication consultation, Vodafone, for example, noted the view that "VoLTE[37] roaming, which will increasingly become the norm over the next few years, inherently passes all calls via the home network, so will remove the necessity for the loophole – we are not seeking to dismiss consideration with an excuse of 'wait for VoLTE roaming', but we must be wary of designing a solution which is both expensive and only delivers at the point it becomes redundant in any case".[38]

3.26 We accept that home routing will eventually be adopted as the default route for roaming voice calls. However, the proportion of traffic using each of these solutions varies between each of the UK mobile providers, and voice calls and data may also be treated differently. For example, a mobile provider may prioritise the introduction of 4G roaming data services, while still maintaining 3G services for voice calls. Internationally, the rate of implementation of 4G and 5G services also varies significantly. Therefore, since we anticipate that 2G and 3G networks will continue to exist in many countries globally where UK people may travel for some time, we believe that we should continue to explore how to address the problem of spoofed UK mobile numbers calling back to the UK.

Impact of AI-based blocking technologies

3.27 We also consider that AI-based technologies, including 'voice firewalls', could reduce opportunities for scammers to spoof UK mobile CLIs when calling the UK from abroad. However, the extent to which these will be implemented across different networks, and the timescales for their introduction, mean that there is uncertainty about the impact of these

---

[35] Kaleido Intelligence / BICS, 2022. *Strategic Guide to 5G Roaming: MNO Outline 2022*.
[36] GSMA May 2020, *GSMA 5GS Roaming Guidelines Version 2.0.*
[37] Voice over Long-Term Evolution is a technology that enables voice calls over a 4G network, rather than via 2G or 3G connections.
[38] Vodafone response to CLI authentication consultation, p.4.

alternative measures. We may consider whether or not a layered approach to addressing the issue of spoofed UK mobile numbers, in line with broader security best practice principles, would best meet our objectives.

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.

4. Potential solutions

Introduction

4.1 This section outlines the broad range of approaches that we have identified from our research looking at solutions that are either being implemented, or are under consideration, to address the issue of calls made from abroad which spoof home mobile numbers. They include those covered by the work of the NICC to examine the technical feasibility of solutions that could be implemented in a UK context. In addition to an overview of the potential solutions, it also considers the possible consumer outcomes that may result (for example, in how calls may be presented to a user). The section concludes by discussing the range of factors that we would need to take into account when considering the relative merits of these, and any other, solutions.

Options

4.2 In this section we discuss what we consider to be credible approaches to addressing scam calls from abroad which spoof UK mobile numbers. There are two broad technical solutions being actively explored both in the UK and abroad; however, each broad solution features various options and variants, and hybrid (or combined) approaches may also be feasible. There are also non-technical approaches that could be possible, implemented either on their own or in conjunction with the technical approaches described. We have divided these options into two groups of roughly similar technical approaches.

4.3 The first group involves the provider that is bringing the call into the UK (referred to in this document as the 'international gateway provider') proactively undertaking checks to ascertain whether a specific number calling from abroad is indeed held by a UK consumer roaming ('roaming check').[39] In this approach, calls identified as spoofed can be blocked by the international gateway provider and will therefore not reach the end user.

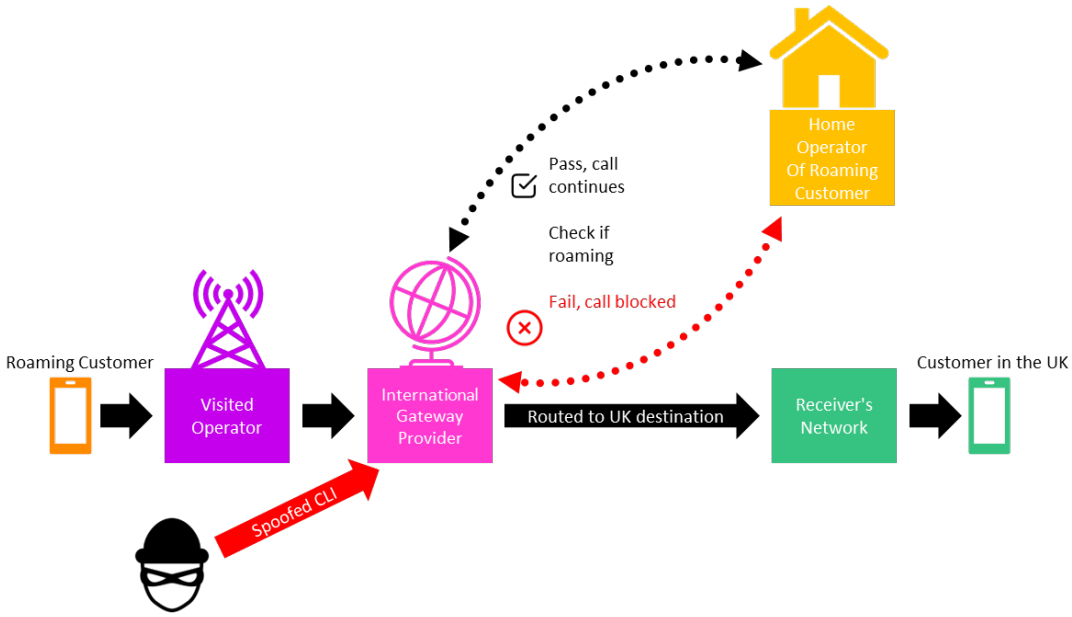
4.4 The second group involves UK mobile network operators pre-agreeing, with the overseas mobile operators with whom they contract to support international roaming, how 2G/3G calls back to the UK are to be routed. The approach uses an existing and widely-adopted protocol and can ensure that calls from callers roaming abroad are always routed back to the home network before being onward routed. As a result, when international gateway providers identify a mobile call from abroad with a '+44...' number, they would be expected to modify the data associated with such calls (details and options set out below), and then to onward route them. Calls from legitimate international roaming callers would be routed to the home network that can revert the modification to the call data (for example, by re-inserting the CLI) before the call is delivered to the end user. Calls that are not from legitimate roamers will not be routed back to the home network, and the modifications to the call data would remain when the call is delivered to the end-user (for example, the CLI could remain withheld). This means that, while potentially illegitimate calls would reach the

[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.

end user - in that they would not be blocked along the way - they would be more easily recognised as illegitimate by the end user (because, for example, there would be no calling number displayed). This could limit the effectiveness of number spoofing.

Group 1: proactive checks by the international gateway provider

Figure 2: Schematic of 'roaming check' approach



4.5 Solutions using this approach require the international gateway provider to perform certain checks on the specific number being presented by the caller. If the caller is legitimately roaming, then this fact would be known by the caller's home mobile network (as the phone would need to register itself as such to make and receive calls). Therefore, the international gateway provider could ascertain whether the mobile number matches that of a phone which is registered as roaming abroad and act accordingly. Figure 2 provides a broad schematic diagram of the 'roaming check' approach.

4.6 There may be some variants and options associated with this general approach, mainly in relation to how such checks are conducted and the actions which are taken if a call is considered to be illegitimate. These are discussed below.

1a: Gateway roaming query (direct)

4.7 In this solution, when a call is made into the UK showing a UK mobile number, the international gateway provider checks directly with the caller's home mobile network to see if the phone has registered on a network abroad, indicating that the caller is legitimately roaming.

4.8 In the UK, because of the way that number portability has been implemented, calls to customers who have ported their number from Network A to Network B first get routed to A before being onward routed to B. This means it may not be possible for the international gateway provider to immediately identify the caller's home network because the number

may have been ported from network to network as a result of customer switching.[40] In such cases, the network to which the number was initially allocated may either respond to the query with the details of the subsequent operator to which the number was ported (so that the international gateway provider can repeat the query to the operator to whom a customer has ported), or it may query the next network itself. In either case, for numbers that have been ported several times, 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. The full details of this solution and all associated scenarios and processes have yet to be established.

1b: Gateway roaming query (proxy)

4.9 In this scenario, instead of each international gateway provider needing to be able to query all mobile network operators (and relevant mobile virtual network operators), a third-party intermediary (or 'proxy') is introduced through which queries and their responses are given. This simplifies the processes implemented by international gateway providers and mobile operators (they only need to support interfaces with one intermediate organisation), but may not avoid the need for the proxy to query multiple networks in the event that a number has been ported without an additional method to check this. A further refinement would be to have a database that contains call porting records that the proxy could query, and which may mitigate the need for multiple checks, but this could, conversely, add to the complexity and costs of this solution.

4.10 This approach requires that a proxy function is created and operated and so introduces additional cost. We would need to consider how this function could be implemented, including whether this would be something that industry could do collectively, or whether regulatory intervention would be needed. There may of course also be issues of data privacy which would need to be managed appropriately.

1c: Gateway roaming query (database)

4.11 This approach is similar to the proxy solution described above, but instead of a third-party organisation making and returning queries between gateways and mobile operators, a dedicated live database is created that contains details of mobile numbers which are roaming abroad. This database would be dynamically populated by the mobile network operators, updating (and removing) numbers as phones register abroad (and back home). This would avoid the need to make multiple queries in the event of network number porting as the details of the number would be held in a single, central database.

4.12 UK mobile network operators would be required to update the database in near real-time to ensure that the data was current and accurate, and the database would need to have the necessary interfaces to allow international gateway providers to query it as required. A central database would simplify and speed up the process of identifying whether a SIM had registered abroad (i.e. a user is legitimately roaming abroad) and therefore whether a call from that number was likely to be legitimate.

4.13 We note that such a database does not exist in the UK, and its creation would potentially add complexity and cost to successful implementation of this option.

[40] The number associated with a SIM does not, in itself, identify the mobile network to which it is registered.

4.14 When we published our CLI authentication consultation, we invited views on the feasibility of such a database.[41] In response, COLT noted its view that 'a live database with roaming and porting information would be incredibly valuable, however, it is critical to underline the risks involved with its implementation'.[42] In the context of the possible introduction of CLI authentication, TalkTalk suggested that 'the introduction of a roaming mobile look-up solution' could provide a better solution to scam calls than CLI authentication.[43] Three also suggested that blocking of UK mobile numbers at international gateways could be achieved based on 'roaming status lookup on MNO databases'.[44]

4.15 If this option were to be taken forward, further work would be needed to consider the technical and operational implications of this approach, not least of which is the potential security risk of a central repository which lists all UK customers currently roaming abroad.

Outcomes

4.16 Regardless of whether an international gateway provider were to directly query all mobile networks, use a proxy to do so on its behalf, or access a central database, the common theme of these solutions is that it is the international gateway provider that is responsible for checking and validating incoming calls with UK mobile numbers. International gateway providers would then need to take action depending on the result of the response to the query. This would affect the experience of the individual receiving the call.

4.17 If the checks were returned with a positive response, i.e. that the number was associated with a person who is roaming, then the international gateway provider would allow the call to be onward routed displaying a UK CLI, potentially through more intermediate networks, to the destination.[45] No further checks would be made and routing decisions (i.e. which operator(s) the call traverses) would be unchanged.

4.18 If the checks were returned with a definitive but negative response, then either the caller would be registered in, and calling from the UK, but the call had been somehow routed to the gateway provider as if it had come from abroad – or, more likely, the number had been spoofed.[46] It would therefore be likely that the call was a scam call.

4.19 However, there could be a risk that some checks would be unsuccessful, in that no definitive response is obtained, positive or negative. This may be because:

a) it is not possible to identify the network to which the mobile is currently registered;
b) the querying process times out before a response is found;
c) queries to a mobile network are unavailable at the time of query; or
d) a malfunction occurs.

---

[41] Ofcom, 2023. *Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers*, pp.46-47.
[42] COLT response to the CLI authentication consultation, p.5.
[43] TalkTalk response to the CLI authentication consultation, p.2.
[44] Three response to the CLI authentication consultation, p.2.
[45] Whether the check is accurate would depend on the quality of the information that the international gateway provider relies upon when it makes its query.
[46] In a small number of use cases, although a call may originate from and be destined for the UK, it may be routed outside of, and then back into, the UK network. This can be for a number of reasons and steps should be taken to allow for this where appropriate. An example could be a fallback route for calls which should be pre-arranged between the respective operators.

4.20 In either of the latter two scenarios (the query is returned negative or failed), then the international gateway provider could take different approaches:

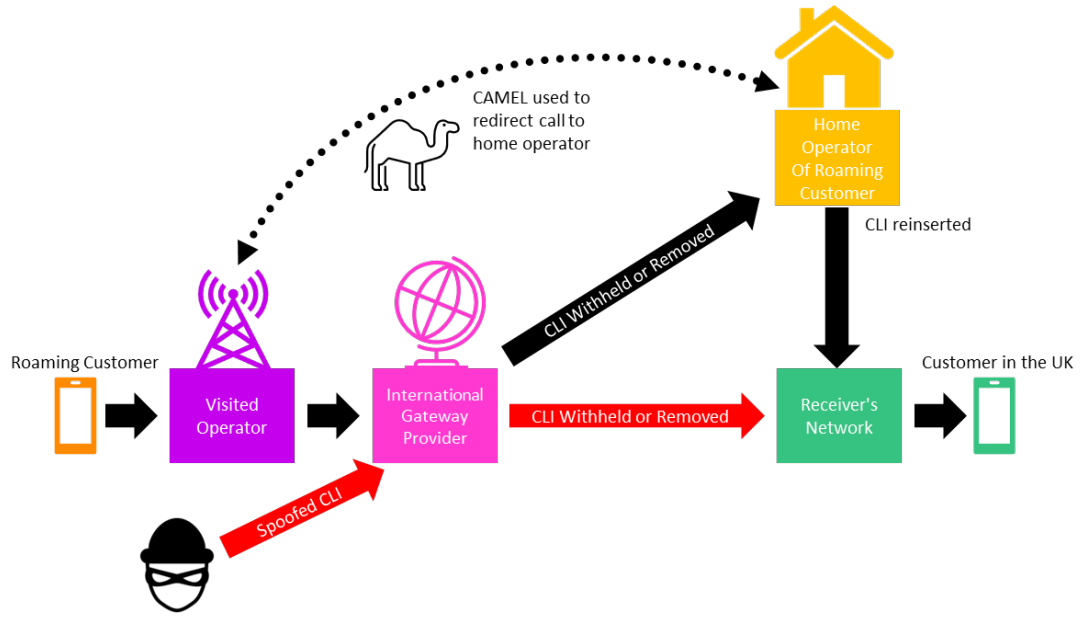
a) it can block the call. The called party will not know that they have been called. The calling party may not receive a notification as to why the call was not successful;
b) it can route the call, but introduce a marker or other signal to indicate that it has not passed relevant checks and therefore it may be a scam call; or
c) it can route the call unaltered.

4.21 Accordingly, any implementation of these Group 1 solutions would require a specific and standard specification across all international gateway providers to ensure consistent outcomes for consumers.

Group 2: Broad categorisation of incoming calls from abroad by the gateway provider without specific number checks

4.22 In this set of options, the international gateway provider performs a basic check on the inbound call to establish whether it appears to be from a UK mobile number. The international gateway provider is therefore only required to follow basic algorithms (for example, to confirm that the number is of the type '+447…' and is coming from an operator abroad). The international gateway provider does not need to validate the specific number, nor query any other party to determine how to route the call. This simplifies and speeds up call handling and routing for the gateway provider. Figure 3 shows a schematic diagram of the 'home routing' approach.

Figure 3: Schematic of 'home routing' approach



4.23 However, for these options, calls from abroad bearing +447 numbers are not routed normally to the destination number. Instead, the call is routed to the mobile network operator to which the phone is registered (the 'home' network). The technology that enables this group of solutions is based on a set of standards which are designed to work on 2G and 3G networks, known as 'Customised Applications for Mobile Enhanced Logic'

(CAMEL). These standards support a number of services, including the ability to redirect calls to the caller's home network.

4.24 In this solution, when a phone registers with a mobile network abroad, the CAMEL protocol is invoked so that, when a call is made, regardless of destination, the call is routed back to its home network. When the call reaches the home network, the call is then onward-routed to its destination, which may be a UK fixed or mobile network, or a network abroad.

4.25 There are several phases and options for how these CAMEL standards are implemented. This may mean that not all UK mobile providers and all their roaming partners support the necessary capability today.

4.26 Even though, in this solution, the international gateway provider is not required to conduct complex queries or processing, there are a variety of options as to how the call is routed from the international gateway provider to the home network. The consequences of each option will depend on whether the call is successfully routed to the home network.

2a: CAMEL home routing (removed CLI)

4.27 In this approach the international gateway would remove the CLI to be displayed. As a result of the implementation of CAMEL, legitimate calls (where the caller is roaming abroad) would be routed to their home network, which would then restore the CLI. The home network then onward-routes the call, and the called party would then see the correct number displayed on the handset.

4.28 If, on the other hand, the call were a scam call spoofing a mobile number, then the call would reach the terminating network without first being redirected to the home network. In this case, the terminating network would be unable to restore the CLI as it would not have the necessary information to do so, meaning that the end user would receive a call with no number displayed.

4.29 It is possible that this option would require modification to our existing General Conditions regarding the provision and preservation of CLI information.[47] As this approach requires that the CAMEL protocol is implemented between UK mobile operators and all international mobile operators with whom they have roaming agreements, it could be that some legitimate calls from some countries/networks may not be home routed. In such an event they would be treated as if they were illegitimate and the CLI would be irrevocably removed. As all calls are delivered to customers in this scenario, it could be that end users might take calls even if the CLI were missing, and therefore scammers could still reach victims and adapt their approach accordingly. As part of our broader assessment, we would need to explore whether the numbering regulations could or should be amended to accommodate this solution.

2b: CAMEL home routing (withheld CLI)

4.30 In this approach, the international gateway provider marks the calling CLI as 'withheld' before onward-routing. Similar to option 2a, if the call is legitimate, the home network can remove this marker, and the end-user would receive a call with the correct number displayed. If the call is not routed via the home network, then the call would be presented to the end user as 'number withheld'.

[47] GC 6 requires providers to provide CLI facilities, and C6.4 requires that the CLI data provided with a call includes a valid and dialable telephone number, so removing this data could conflict with these requirements.

4.31 While in the majority of cases the call would still reach the end user, our research indicates that customers are less likely to answer their phone if the calling number is withheld.[48] This could reduce the likelihood that consumers will answer the phone to a scammer.

2c: CAMEL home routing (withheld CLI+)

4.32 This option is identical to option 2b (CAMEL home routing – withheld CLI), except that the international gateway provider must also add additional information to the call metadata which identifies the gateway which brought it into the UK. This additional data would provide more information on the calls which are coming into the UK and how they are entering UK networks.

4.33 There is currently limited information on the international gateway providers which bring calls into the UK. The inclusion of details of the international gateway provider, together with increased oversight, could provide useful intelligence on how and from where scam calls are entering the UK.

4.34 This option, while using the same underling basis as the other options, would impose greater requirements on gateway providers not only to remove (or alter) the CLI information, but also to generate and convey additional information associated with the call.

2d: CAMEL home routing (allowlist)

4.35 In this approach the international gateway provider would be required to block the call or remove the CLI for calls from UK mobile numbers where the destination number does not match a predefined 'allowlist' of numbers that represent the UK home networks.[49]

4.36 This option differs from previous options as it would require the international gateway provider to maintain what could be a large list of numbers belonging to each of the UK mobile network operators used to deliver the home routed calls. It is currently unclear how large this list would be or how frequently it would need updating.

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)?

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.

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.

---

[48] Ofcom / Yonder, 2024. *Ofcom Scams Survey: Online fieldwork 31 January to 1 February 2024 data tables*, Qs.14 and 15 (pp.42-73). Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, Slides 18 and 19. Question: How likely is it that you would pick up a call from each of the following numbers?

[49] To redirect the call via the caller's home network the dialled number is changed (using CAMEL) to a temporary number allocated from a pool of numbers belonging to the operator (for example, an IP Multimedia Routing Number (IMRN)). This will only be used to redirect the call to the home network, where it will then be changed back to the originally dialled destination CLI. The allowlist would include only these 'temporary home routing' numbers.

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.

International developments

4.37 Other countries have so far adopted a range of approaches to tackling the issue of spoofed mobile numbers coming into their networks. There does not appear to be an emerging international consensus on the most efficient and effective method for tackling this problem.

4.38 Some jurisdictions require status checks on incoming calls against the mobile roaming status of a user, with a real time query sent to check the roaming status of the customer directly to the operator which owns the number (similar to option 1a outlined above).[50] These include Oman, Poland and Saudi Arabia.

4.39 Ireland has proposed a two-stage solution, including a proxy. A broad overview of the approach in Ireland is outlined below. Finland is also implementing a proxy-based solution.

4.40 We also note that some jurisdictions have more complete information on the participants in their communications networks (for example they may have a licensing regime for international gateway providers, and / or a smaller number of operators in the market) which can reduce the challenge and complexity of implementing some of the solutions which we have outlined.

CEPT

4.41 In November 2023, CEPT's[51] Electronic Communications Committee (ECC) published ECC Recommendation[52] 23(03) on *Measures to handle incoming international voice calls with suspected spoofed national E.164 numbers*, covering a number of scenarios and recommendations relating to identification of roaming calls.[53] The first scenario, 'Call from a national outbound roamer', is relevant to this call for input and provides a high-level overview of the challenges, including some potential broadly-sketched approaches. Our discussion of the solutions outlined in this call for input covers the approaches considered in this paper.

ComReg

4.42 The Irish regulator ComReg has published an assessment of the responses to its consultation on the issue in its document *Combatting scam calls and texts: Response to Consultation on*

[50] GSMA, 2023. *Improving CLI Validity – Solutions and Regulatory Assessment*, p.8.
[51] CEPT (the European Conference of Postal and Telecommunications Administrations) consists of 46 European countries cooperating to regulate post, radio spectrum and communications networks. One of CEPT's groups is the Electronic Communications Committee (ECC). ECC considers and develops policies on electronic communications activities, taking account of European and international legislations and regulations.
[52] ECC Recommendations are measures that national administrations are encouraged to apply. They are principally intended as harmonisation measures or as guidance to national administrations.
[53] CEPT, 2023. *Measures to handle incoming international voice calls with suspected spoofed national E. 164 numbers*.

network-based interventions to reduce the harm from Nuisance Communications.[54] ComReg has proposed a two-phase option.[55]

4.43 In phase 1, international gateway providers are required to check roaming status directly with the home network; however, this proposal also allows for an international gateway provider to use a wholesale service (such as another operator) to carry out this check on their behalf.

- We note that this solution is similar to the options we have identified in Group 1. Following consultation, ComReg noted concerns in relation to the costs and complexities of this solution, which could potentially disadvantage smaller players and new entrants, and consequently updated its position to only include operators with revenue greater than €50m.

4.44 In phase 2, the international gateway provider would check the status of a call via a common proxy.

- The details of this solution are yet to be established. We note that Eir and Vodafone challenged this proposal on the grounds that it would be made redundant by the advent of widespread VoLTE rollout, although ComReg asserts that the pace of VoLTE rollout is uncertain;
- Three highlighted that, as it 'home routes' calls regardless, this provides the same assurance as VoLTE processes: 'Three is of the view that this is a simpler approach and should be examined alongside other alternatives by the Nuisance Communications Industry Taskforce (NCIT)[56] before Q1 2024'.[57] In response, ComReg noted its concerns that this would take too long to deploy.[58]

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.

Framework for evaluating options

4.45 In this section we identify, in general terms, the factors that we would be minded to consider as part of our assessment of any proposed options to reduce calls from abroad that spoof UK mobile numbers.

Assessing relevant impacts

[54] ComReg, 2024. *Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications*.
[55] ComReg, 2023. *Combatting scam calls and texts: Consultation on network based interventions to reduce the harm from Nuisance Communications*, p.75.
[56] ComReg established the NCIT in early 2022, comprising fixed and mobile network operators whose networks collectively carry more than 90% of fixed voice traffic and 100% of mobile voice traffic in Ireland.
[57] ComReg, 2024. *Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications*, p.64.
[58] ComReg, 2024. *Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications*, p.69.

4.46 Any proposed intervention would be informed by an impact assessment. Our general approach to impact assessments is set out separately in our impact assessment guidance.[59]

4.47 As part of our impact assessment, we expect to consider at least the following:

- the effectiveness of any proposed intervention in terms of reducing harms to consumers caused by scam calls from abroad which spoof UK mobile CLIs, and the resulting benefit to consumers;
- the effectiveness of any proposed intervention in allowing legitimate calls to continue to take place;
- the potential costs incurred by legitimate businesses, including direct costs of implementing any changes, as well as any indirect costs that might arise for communications providers or other third parties;
- 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;
- timescales for implementation of solutions, particularly in relation to the counterfactual and potential technology developments that may affect the impact of any intervention over time; and
- any other potential unintended consequences or adverse effects identified through our work, including – for example – any impacts on competition.

Counterfactual

4.48 We intend to assess the impacts of any proposed intervention by comparing the potential outcomes against the outcomes in an alternative scenario where the intervention does not take place (referred to as the counterfactual).

4.49 The counterfactual is inherently uncertain and would not constitute a detailed description of future outcomes. Instead, we would expect to consider the counterfactual in a broad sense, focusing on significant changes or trends where there are reasons to believe that these could affect our impact assessment, for example by altering the nature or scale of the relevant harms.

4.50 Our counterfactual would consider the scope and scale of the harm caused by scam calls originating abroad but spoofing UK mobile numbers, and how this might evolve in the future in the absence of an intervention. As part of this, we would expect to consider relevant technological developments (such as those referred to in section 3 above), as well as evidence about any other regulatory interventions or relevant industry initiatives. Such evidence includes, but is not limited to, any evidence received in response to this Call for Input.

[59] Ofcom, 2023. Impact assessment guidance.

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.

5. Next steps

5.1 This call for input will close on 23 September 2024. We will use responses, together with a programme of broad stakeholder engagement and potentially formal information requests, to ascertain whether or not to consult on a preferred option.

5.2 If we decide we need to introduce new regulation on this issue, we anticipate consulting in Spring 2025.

A1. Summary of questions

A1.1 This section provides a summary of the questions asked in this CFI.

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.

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.

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.

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?

Question 3:

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

b) What are the consumer impacts of spoofed UK mobile numbers more broadly?

Please provide evidence to support your responses.

Question 4:

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

b) Is there any evidence that scammers are moving from spoofing fixed to mobile UK CLI?

Please provide evidence to support your responses.

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.

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)?

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.

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.

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.

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.

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.

A2. Responding to this call for input

How to respond

A2.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 23 September 2024.

A2.2 You can download a response form from https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-options-to-address-mobile-spoofing. You can return this by email or post to the address provided in the response form.

A2.3 If your response is a large file, or has supporting charts, tables or other data, please email it to Mobilespoofingresponses@ofcom.org.uk as an attachment in Microsoft Word format, together with the cover sheet.

A2.4 Responses may alternatively be posted to the address below, marked with the title of the consultation:

Cat Kelly
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A2.5 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

- send us a recording of you signing your response. This should be no longer than 5 minutes. Suitable file formats are DVDs, wmv or QuickTime files; or
- upload a video of you signing your response directly to YouTube (or another hosting site) and send us the link.

A2.6 We will publish a transcript of any audio or video responses we receive (unless your response is confidential).

A2.7 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A2.8 You do not have to answer all the questions in the call for input if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A2.9 It would be helpful if your response could include direct answers to the questions asked in the call for input. The questions are listed at Annex 1. It would also help if you could explain why you hold your views.

A2.10 If you want to discuss the issues and questions raised in this call for input, please contact Cat Kelly by email to Cat.Kelly@ofcom.org.uk.

Confidentiality

A2.11 Calls for input are more effective if we publish the responses before the response period closes. This can help people and organisations with limited resources or familiarity with the

issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A2.12 If you think your response should be kept confidential, please specify which part(s) this applies to and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A2.13 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A2.14 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A2.15 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A2.16 Following this call for input, we will consider the options available. If we choose to consult, this is likely to take place in Spring 2025.

A2.17 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

A3. Call for input coversheet

Basic details

Call for input title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

Please tick below what part of your response you consider is confidential, giving your reasons why

- Nothing ☐
- Name/contact details/job title ☐
- Whole response ☐
- Organisation ☐
- Part of the response ☐

If you selected 'Part of the response', please specify which parts:

If you want part of your response, your name or your organisation not to be published, can Ofcom still publish a reference to the contents of your response (including, for any confidential parts, a general summary that does not disclose the specific information or enable you to be identified)?

Yes ☐ No ☐

Declaration

I confirm that the correspondence supplied with this cover sheet is a response that Ofcom can publish. However, in supplying this response, I understand that Ofcom may need to publish all responses, including those which are marked as confidential, in order to meet legal obligations. If I have sent my response by email, Ofcom can disregard any standard e-mail text about not disclosing email contents and attachments.

If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)