# Tackling scam calls

Updating our CLI Guidance to expect providers to block more calls with spoofed numbers

**Statement**

# Contents

## Section

## Annex

# 1. Overview

1.1 Scam calls can result in significant financial and emotional harm to victims. They can also lead to a reduction in trust in telephone calls. A common tactic used by scammers is to 'spoof' their telephone number to disguise the origin of the call, or to make their call appear to be from a trusted person or organisation. Where a scammer makes a call from abroad, they may spoof their number to make it look like the call is from a UK-based organisation.

1.2 A telephone number is also known as Calling Line Identification (CLI) data. Ofcom sets out the requirements for the display of CLI data in the General Conditions of Entitlement (GCs), under GC C6. This is accompanied by the CLI Guidance, which sets out what is expected of providers to comply with GC C6.

1.3 There are two numbers associated with an incoming call: the Network Number, which identifies where the call is being made from, and the Presentation Number, which identifies who is making the call. In most cases the Network and Presentation Number are the same, but there are some scenarios in which a legitimate caller may wish to display a different number to the line that the call is being made from (for example, a call centre that makes calls on behalf of different businesses, or businesses which may wish to display a single number for outbound calls).

1.4 In November 2022, we published a statement that included a decision to update the CLI Guidance to confirm that communications providers are expected to identify and block calls from abroad which are spoofing a UK CLI as Network Number, except in a limited number of use cases.

1.5 Following this, stakeholders informed us that calls with UK numbers entering the UK from abroad remained a problem,[1] and in February 2024 we published a consultation proposing to update the CLI Guidance to extend blocking to international calls which display a UK number as a Presentation Number.

1.6 We received 16 responses to this consultation. All respondents agreed that blocking more calls from abroad with a UK number as a Presentation Number would help to protect UK consumers from scam calls. All respondents, except Three, supported our proposal to block calls from abroad with a UK number as a Presentation Number if they didn't fall into one of the exceptions set out in the CLI Guidance. We received a number of comments requesting clarification on the wording of paragraph 4.19 of the CLI Guidance. We also received differing views on the time needed to implement this change.

---

[1] Stakeholder responses to our consultation on the potential introduction of CLI authentication. Ofcom, 2023. _Consultation: Calling Line Identification (CLI) authentication - a potential approach to detecting and blocking spoofed numbers._

**What we have decided – in brief**

We have decided to go ahead with our proposal to update the CLI Guidance - in particular paragraph 4.19 - to reflect that we expect providers to identify and block calls from abroad that use a UK telephone number as a Presentation Number, except in a limited number of legitimate use cases. We have however addressed a number of stakeholder concerns around the wording in paragraph 4.19 of the CLI Guidance and have made some additional changes to provide further clarity.

We have decided to give providers six months to implement the changes. Therefore, the updated CLI Guidance will come into effect from 29 January 2025.

The overview section in this document is a simplified high-level summary only. The decisions we have taken and our reasoning are set out in the full document.

# 2. Background

2.1   Tackling scams is a priority for Ofcom. Fraud accounts for over 40% of all reported crime in England and Wales, which results in significant financial and emotional harm to victims.[2] Data from UK Finance suggests that 16% of cases of Automatic Push Payment (APP) fraud originated from telecommunications in 2023, accounting for a disproportionately high (43%) share of overall losses.[3]

2.2   Scammers use a technique known as CLI spoofing to create a trusted persona to mislead the recipient of the call about their identity, so that their calls are more likely to be answered. Consumers are more likely to answer calls from an unknown UK number than from an unknown international number or a withheld number.[4] Misuse or spoofing of CLI can also lead to a reduction in trust in telephone calls, which may mean that even legitimate calls may be declined. Businesses may then face greater challenges in contacting consumers for legitimate purposes.

2.3   Our strategy to tackle telecoms scams is to:[5]

   i)   **disrupt scammers**, including through strengthened rules and guidance;
   ii)  **collaborate and share information** with stakeholders, including Government, industry, law enforcement, regulators and consumer groups; and
   iii) **educate consumers** and raise awareness of how to avoid scams.

## Use of spoofing in scam calls

2.4   A common tactic used by scammers is to 'spoof' telephone numbers, to make their calls appear to be from a trusted person, organisation or country, so that their calls are more likely to be answered.[6] A spoofed number on a call display could be a random series of digits, or it could mimic the number of a real company or person who has nothing to do with the actual caller.

2.5   The misuse of CLI data, and spoofed Presentation Numbers in particular, can lead to significant harm for consumers. As we noted in the 2023 CLI Authentication Consultation, CLI spoofing can be used by scammers to mislead the recipient of a call about their identity in order to encourage them to give away sensitive information or money.[7] As such, successful scams, especially multichannel scams (scams in which contact is made with the consumer via more than one form of communication), can result in significant financial

---

[2] Ofcom, 2024. *Calling Line Identification (CLI) authentication assessment and future roadmap*, para 2.11.
[3] UK Finance, 2024. *Annual Fraud Report*, p. 43.
[4] Ofcom, 2024. *Experiences of Suspicious calls, texts and app messages 2024*, slides 17-20. 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
[5] Ofcom, 2022. *Policy Positioning Statement: Tackling scam calls and texts*.
[6] The use of spoofed numbers has also made it harder to detect and block such calls and to trace perpetrators.
[7] Ofcom, 2023. *Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers*.

losses. In addition to financial harm, telecoms scams can cause significant emotional and psychological harm.

2.6    Misuse or spoofing of telephone numbers can lead to wider harms too. It can cause a reduction in trust in telephone calls more generally, which would be detrimental to UK consumers and businesses. Any loss of trust in communications services may result in legitimate communications being ignored, blocked or not received.

# Rules for the use of CLI data

2.7    We set out the requirements for the display of CLI data in the General Conditions of Entitlement (GCs), under GC C6.[8] This is accompanied by the Guidance on the provision of Calling Line Identification facilities and other related services (the CLI Guidance), which sets out what is expected of providers in order to demonstrate compliance with GC C6.[9] As set out below, in our February 2022 consultation (the February 2022 Consultation) we proposed changes to the wording of this guidance.[10]

**Figure 1: Presentation Number and Network Number**
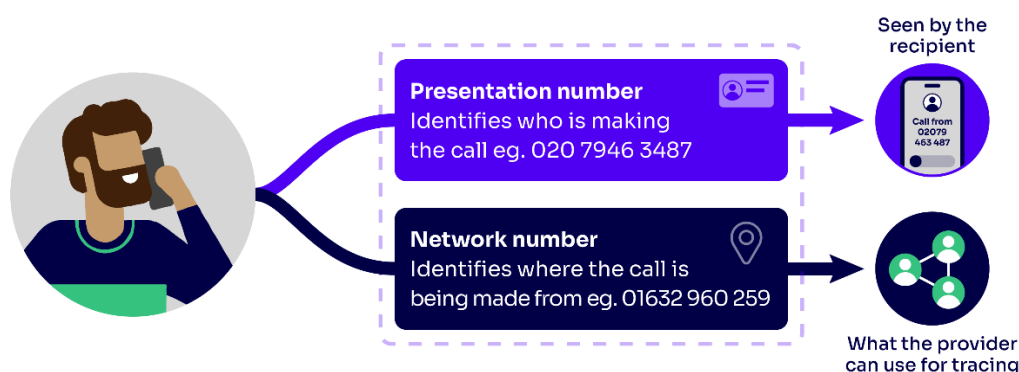


2.8    The telephone number, also known as CLI data, includes both information that identifies the caller and a privacy marking, which indicates whether the number can be shared with the recipient of the call. CLI data can give the recipient of a call information about the identity of the party making the call, which can help them to decide whether they wish to answer or return it. As illustrated in Figure 1, 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.

2.9    In most cases, the two numbers are the same; however, there are scenarios where a legitimate caller may wish to display a different number from the line that they are calling

---

[8] Ofcom, General Condition C6. *General Conditions of Entitlement.*
[9] Ofcom, 2024. *Guidance on the provision of Calling Line Identification (CLI) facilities and other related services.*
[10] Ofcom, 2024. *Consultation: Tackling scam calls – updating our CLI Guidance to expect providers to block more calls with spoofed numbers*, paras 3.1 - 3.8.

from, for example where a call centre may make calls on behalf of a number of different businesses, or businesses which may wish to display a single number for outbound calls.

## History of CLI Guidance

2.10    The rules for the provision of CLI facilities and the display of CLI were introduced in GC C6 in 2017, as a part of our review of the GCs. The rules apply to all providers of Number-based Interpersonal Communications Services and Public Electronic Communications Networks (PECNs) over which Number-based Interpersonal Communications Services are provided.[11] We published a version of the CLI Guidance to support GC C6 in 2018.[12]

2.11    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.[13]

2.12    In February 2022, we consulted on proposals to modify GC C6.6 to require providers to take all reasonable steps to identify and block calls with CLI which do not uniquely identify the caller. We also consulted on making changes to the CLI Guidance. In November 2022 we published a statement (the November 2022 Statement) which included a decision to update our CLI Guidance to confirm that communications providers are expected to identify and block calls from abroad which are spoofing a UK CLI as Network Number, except in a limited number of use cases:[14]

- 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

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

2.13    In our November 2022 Statement, we explained that we would expect the UK network that first receives calls from an international network to understand the types of calls that are connecting into their network, so that calls from organisations that can legitimately use a

---

[11] In our statement on *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.
[12] Ofcom 2018. *Statement: Guidelines for Calling Line Identification Facilities.*
[13] Ofcom, General Condition C6. *General Conditions of Entitlement.*
[14] A full list of the changes to the CLI Guidance from the November 2022 Statement can be found in Section 4 of the statement. *Improving the accuracy of Calling Line Identification (CLI) data.*

UK CLI as a Network Number are separated into a route that is not blocked and calls where the source of the call is unclear are separated into another route.[15] Calls from UK users roaming abroad will enter the UK with a +447 Network Number. We therefore expect international gateways currently have a general exception for calls with Network Numbers that start +447. Calls to a mobile user who is roaming in the UK will be made to a special range of numbers so we expect providers to have a general exception for calls to this range of numbers too.[16] Calls from abroad using other UK Network Numbers may require the provider first receiving the call in the UK to understand whether the caller has the right to use those numbers. If an international gateway provider is not in a position to check, or does not want the responsibility of checking, the validity of the CLI of a call entering the UK network, the call may need to be directly connected to a UK network, rather than use an international gateway.

2.14 This change came into force on 15 May 2023 (six months after the publication of the November 2022 Statement).

2.15 In response to the February 2022 Consultation, some stakeholders expressed concern that there was a potential loophole by which overseas callers could make calls to UK recipients using a UK CLI as a Presentation Number and using a different number (an international number or mobile number) as a Network Number. In our November 2022 Statement, we noted our understanding that, based on information provided by BT Group, nearly all calls with UK CLIs entering BT Group's international gateways have the same number for both the Network Number and Presentation Number. Therefore, at that time, we considered that blocking calls with a UK CLI as a Network Number would lead to fewer scam calls being connected. However, we agreed that this measure could be circumvented by scammers and said that we would consider consulting on blocking calls from abroad which use UK CLI as a Presentation Number.[17]

## Developments since our November 2022 Statement

2.16 Scammers continually adapt their tactics and calls spoofing a UK CLI from abroad remain a problem. In April 2023, we published a consultation inviting views on the potential introduction of a system known as CLI authentication (the 2023 CLI Authentication Consultation), discussing approaches based on the STIR standards which had already been implemented in the US and Canada.[18]

2.17 In February 2024, we published our assessment of stakeholder responses. We noted that, although CLI authentication could be an effective tool in preventing some harmful calls from spoofed numbers, our assessment concluded we should not proceed with CLI

[15] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.139.
[16] These are the Mobile Station Roaming Number (MSRN) ranges. They are numbers used by providers to allocate to callers roaming in the UK.
[17] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.156.
[18] Ofcom, 2023. *Consultation: Calling Line Identification (CLI) authentication – a potential approach to detecting and blocking spoofed numbers*. In this document we explained that the standards-based approach for CLI authentication is made up of the Secure Telephony Identity Revisited (STIR) and Signature-based Handling of Asserted information using toKENs (SHAKEN).

authentication at this time.[19] Stakeholders indicated that calls with UK numbers entering the UK from abroad remained a problem, and they suggested that we should prioritise blocking solutions and extend our guidance to include Presentation Numbers as well as Network Numbers.[20]

2.18    Responses to the 2023 CLI Authentication Consultation also indicated there was a need to be able to distinguish between (i) calls that are from UK callers roaming abroad phoning back into the UK and (ii) calls from abroad that are spoofing UK mobile numbers. We have therefore begun to explore options to address the issue of spoofed UK mobile numbers, including measures introduced by other jurisdictions, and will assess the anticipated benefits and challenges.[21] If we are able to identify a potential solution to validate legitimate roaming calls, we will consider consulting on these options in due course.

**International developments**

2.19    Many other countries have introduced similar measures to identify or block international calls that use numbers from their national number ranges. Many of these rules do not distinguish between Network Numbers and Presentation Numbers. These include rules for:

- Blocking international calls with numbers from their national number ranges (excluding calls to users roaming in that country) by Finland[22], Lithuania[23], Malta[24] and Türkiye.[25]

- Identifying calls using numbers from their national number ranges and requiring the withholding of these numbers to the recipient of the call (international roaming calls are exempt) by Germany[26] and Switzerland.[27]

- Ireland[28] published a consultation on international call blocking measures in 2023.

## Ofcom's role in managing telephone numbers

2.20    Ofcom administers the UK's telephone numbers. In the ITU-T E.164 format, these numbers start with +44. 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 of Jersey, Guernsey and the Isle of Man to use numbers from the +44 UK Country Code.[29]

---

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

[20] Ofcom, 2024*. Calling Line Identification (CLI) authentication assessment and future roadmap,* para 3.19.

[21] Ofcom, 2024. *Reducing scam calls from abroad which spoof UK mobile numbers.*

[22] Traficom's Regulation 28 on the interoperability of communications networks and services. From 2 October 2023 operators must in addition block calls when the number is a Finnish mobile number which is not roaming.

[23] TN-347 Lithuania's Communications Regulatory Authority's decision on rules on the use of communications numbers.

[24] MCA, 2024. *Decision Notice: Preventative measures to mitigate CLI spoofing and vishing scams.*

[25] BTK, 2018. *Procedures and principles regarding the use of Caller Line Information (CLI).*

[26] Bundesnetzagentur, 2021, Telecommunications Modernization Act 2021.

[27] Swiss Federal Authorities, 2020. *Telecommunications Services Ordinance*. Switzerland asks their providers to co-ordinate with each other to delete the number or to block the call.

[28] ComReg, 2023. *Consultation on combatting Nuisance Communications*.

[29] The Bailiwicks of Jersey and Guernsey and the Isle of Man are constitutional dependencies of the British Crown (the Crown Dependencies). The Crown Dependencies have their own telecommunications legislation and communications regulators.

# Our consultation

2.21    Our consultation ran from 1 February until 28 March 2024. In the consultation document, we outlined our proposal to update our CLI Guidance to confirm that we expect providers to identify and block calls from abroad which are spoofing UK Presentation Numbers except in a limited number of legitimate use cases. For simplicity in this document, we refer to this as "Presentation Number blocking". This proposal considered:

- responses from providers to our 2023 CLI Authentication Consultation which supported +44 Presentation Number blocking at international gateways as a possible alternative measure to CLI authentication;[30]

- stakeholder responses to our February 2022 Consultation on improving the accuracy of CLI data that maintained that Presentation Numbers could still be spoofed and therefore needed to be blocked;[31]

- current examples of providers already blocking UK Presentation Numbers from abroad;

- direct or indirect evidence of potential harm from spoofing UK Presentation Numbers; and

- international context and developments in this area.

2.22    Specifically, we proposed to update the text in paragraph 4.19 of our CLI Guidance so that UK networks receiving such calls from abroad would be required to block calls with UK CLIs except in a number of legitimate use cases. We said that providers would be expected to adopt the updated guidance in order to demonstrate their compliance with GC C6.6.

2.23    The changes we consulted on making were set out in the table below (with our proposed changes in bold):

| Previous version of paragraph 4.19 | Proposed version of paragraph 4.19 |
|---|---|
| 4.19    As the CLI represents the origin of a call, calls from abroad should not use UK CLI as a Network Number, except in a limited number of use cases:<br><br>- UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range;<br>- Calls to a mobile user who is roaming in the UK;<br>- Where the traffic has originated on a UK network; | 4.19    As the CLI represents the origin of a call, calls from abroad should not use UK CLI as a Network Number **or as a Presentation Number**, except in a limited number of use cases:<br><br>- UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range;<br>- Calls to a mobile user who is roaming in the UK;<br>- Where the traffic has originated on a UK network; |

[30] Ofcom, 2023. *Consultation: Calling Line Identification (CLI) authentication – a potential approach to detecting and blocking spoofed numbers*.
[31] Ofcom, 2022. *Consultation: Improving the accuracy of Calling Line Identification (CLI) data*.

| | |
|---|---|
| • Where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.<br><br>Except in these use cases, calls from abroad using UK CLI should be blocked. | • Where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.<br><br>Except in these use cases, calls from abroad using UK CLI should be blocked. |

2.24    We said that we consider that it is important the CLI Guidance is updated so that Presentation Number blocking is co-ordinated between all relevant providers and a deadline is set by which this blocking should be in place. Otherwise, scammers may continue to exploit loopholes and connect their calls through routes that do not block the use of a UK CLI as a Presentation Number for calls from abroad. Therefore, this measure is only fully effective if all networks who accept calls from abroad into UK networks identify and block these calls.

2.25    We noted that the following exceptions in the existing version of paragraph 4.19 would continue to apply:

a)    calls from abroad with +447 numbers, so that calls from UK mobile users roaming abroad are not blocked. Therefore, this would apply to calls from outside the UK using a UK geographic or non-geographic number.
b)    calls to a mobile user who is roaming in the UK.
c)    where traffic has originated on a UK network.
d)    where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.

2.26    We received written responses from 16 stakeholders.[32] We have published all non-confidential responses on our website.[33] We had further engagement with some stakeholders to seek further detail on some of the comments they shared on our proposals and this is reflected in Section 3 which sets out the stakeholder responses.

## Structure of this document

2.27    In Section 3 we discuss stakeholders' comments on our consultation and our response, including in relation to (i) our proposed change to paragraph 4.19 of our CLI Guidance; (ii) the potential impact of our proposal; and (iii) our proposed implementation timeframe. We also set out our decisions. Finally, we set out other policy suggestions raised in stakeholder responses which we do not consider will affect the decision in this statement but may be relevant to our wider telecoms scams programme.

2.28    Annex A1 sets out our legal framework, Annex A2 sets out the changes we have made to the CLI Guidance in full and Annex A3 discusses other policy suggestions raised by

---

[32] These respondents were: BT, CCUK, Comms Ombudsman, FCS, Magrathea, NICC, Sky, TalkTalk, Telecom2, Three, UKCTA, UK Finance, VMO2, Vodafone and two individuals.
[33] *Statement: Tackling scam calls – expecting providers to block more calls with spoofed numbers.*

stakeholders that are not relevant to this statement but may be relevant to our wider telecoms scams programme.

# 3. Stakeholder Responses and our Decision

## Key themes of the responses

3.1     All respondents agreed with the principle that blocking more calls from abroad with a Presentation Number as UK CLI would help to protect UK consumers from scam calls. All respondents, apart from Three, also agreed with our proposed approach of expecting providers to block such calls except for specified legitimate use cases. Three suggested a variation to our proposal which would allow providers to either block such calls or anonymise the caller ID.[34]

3.2     While generally agreeing with our proposal, various respondents also raised wider concerns about the meaning of the existing terminology used in paragraph 4.19 of our CLI Guidance, including terms such as "abroad", "overseas" and "UK network".[35] They requested that Ofcom should clarify what is meant by this wording, and they proposed changes to the wording in paragraph 4.19.

3.3     Some respondents also commented on the potential impact of our proposal, in particular on small businesses, cloud calling services, and transit carriers. Some respondents said that we needed to allow stakeholders longer to implement the change and to ensure that it is effectively communicated to affected businesses.

3.4     In the rest of this section, we first address Three's comment on the substance of our proposal and its suggestion that we should add "or anonymised" to the wording of paragraph 4.19, so that calls spoofing UK CLI from abroad would be anonymised and not blocked.

3.5     We then address the requests for clarification of the wording in paragraph 4.19 as well as the comments on the potential impact of our proposal. Our final decision is set out towards the end of this section, including implementation timings.

## Blocking calls from abroad using UK CLI

### What we said

3.6     We proposed that, apart from the exceptions set out in paragraph 2.25 above, calls from abroad using UK CLI should be blocked.

### Stakeholder comments

3.7     While some respondents made suggestions on the specific wording of the proposed change, all respondents, apart from Three, agreed with the overall approach of expecting

---

[34] Three response to the 2024 consultation, p.2.
[35] BT, NICC, VMO2, TalkTalk, Vodafone, Sky.

providers to block these calls unless for a specified legitimate use case.[36] We discuss the drafting suggestions in paragraphs 3.19 - 3.60 below. UKCTA noted that we had considered industry views and chosen not to implement the CLI authentication STIR/SHAKEN method at this time.[37] UKCTA also said that our consultation proposal would be a more effective, feasible and technically achievable alternative.

3.8     Magrathea acknowledged the significant amount of work done by the NICC N-CLI Task Group[38] to explore legitimate use cases that would be impacted by the proposed changes to CLI blocking measures.[39] It said that this work, along with the proposed guidance for implementation of CLI blocking measures, appeared to satisfy most of the scenarios that could potentially cause concerns for its clients. Moreover, the exceptions would serve to ensure that our guidance would not impede the variety of valid scenarios that currently support international trade and cross-border flexibility to a number of communications providers.

3.9     VMO2 agreed that the proposed change would have a positive impact on consumers by reducing the number of scam calls which they receive. However, it indicated that the eventual policy goal should be to have no exceptions to blocking rules, as these could quickly become targets for continued spoofing by scammers.[40]

3.10    Three proposed that we should add "or anonymised" to the wording of paragraph 4.19, so that it would read "Except in these use cases, calls from abroad using UK CLI should be **blocked or anonymised**". Three said it believes that anonymising spoofed calls would remove the motivation for scammers to spoof the CLI. This is because an end user would see "private number" or "no caller ID" on their device rather than a spoofed number pretending to come from a legitimate organisation.[41]

3.11    An individual respondent said that, while the proposed update to our rules represented "real progress", a fundamental problem would still exist in relation to "Number Withheld" calls. The respondent said that these calls were a fundamental source of scams, fraud and phishing, and were extremely frustrating and irritating for the recipient. The respondent suggested that "number withheld calls" should be made illegal and not processed/connected.[42]

## Our response

3.12    We welcome stakeholders' general support for Presentation Number blocking. We recognise that Three's suggestion of including the option to anonymise as well as to block

---

[36] FCS, UKCTA, Communications Ombudsman, Sky, Telecom2, BT, Magrathea, NICC, UK Finance, CCUK, Three, Talktalk, Vodafone, VMO2, two consumers (Name withheld 1, Name withheld 2).

[37] UKCTA response to the 2024 consultation, p.3. UKTCA (The UK Competitive Telecommunications Association) is a trade association promoting the interests of competitive fixed-line telecommunications market.

[38] The Nuisance Call and CLI Task Group. This is the NICC Task Group responsible for technical industry standards for the implementation of the CLI Guidance.

[39] Magrathea response to the 2024 consultation, p.1.

[40] VMO2 response to the 2024 consultation, p.2.

[41] Three response to the 2024 consultation, p.2.

[42] Name withheld 2 response to the 2024 consultation, p.2.

calls could offer some benefits, although we note that other respondents did not propose this option. It may, in some cases, and as Three suggests, remove the incentive for scammers to spoof CLI.[43]

3.13 Although anonymisation of CLI data would prevent scammers from displaying a UK number when calling from abroad, it would also have drawbacks. In particular, consumers would still be at risk, as some people may still answer anonymised scam calls even if the number is withheld.[44] Moreover, if answered, scammers may still be able to convince the recipient of the call that they are calling from the UK. If scammers make many more calls withholding their number, consumers may also associate calls with withheld CLIs as unwanted calls. This may lead to legitimate calls with withheld CLIs not being answered.[45]

3.14 Scammers are quick to adapt their approaches. Where there are different actions taken by providers to combat scam calls, they are likely to seek routes with the weakest protections. Allowing inconsistent anonymisation could create new loopholes which scammers could in turn exploit, if they knew that calls could be anonymised rather than blocked.

3.15 By making call blocking optional and allowing for an alternative action, Three's proposal could lead to lower volumes of calls being blocked overall, which could also reduce the volume of legitimate calls being blocked (known as 'over-blocking').

3.16 However, we consider that the risk of over-blocking under our proposed approach is limited. In our November 2022 Statement, we noted that BT, who had already introduced blocking of calls from abroad with UK CLI as Presentation Numbers in addition to Network Numbers, said that they had received very few complaints of calls from abroad with UK CLI that had been blocked in error.[46] More information on the impact of over-blocking for businesses can be found at paragraphs 3.84 - 3.95.

3.17 We have therefore decided that Three's proposal risks being ineffective in addressing the harm caused by Presentation Number spoofing and we will continue to focus our approach in paragraph 4.19 on *blocking* calls from abroad with a UK CLI as a Presentation Number.

3.18 In relation to the individual respondent's proposal to block all withheld calls, we agree that calls coming from withheld numbers can be a source of scams. The Privacy and Electronic Communications Regulations 2003 (PECR) generally requires providers to give their customers (other than those making calls for direct marketing purposes) the right to withhold their number in order to give callers the option to protect their identity when making a call. However, PECR also requires providers to give their customer a simple way to reject calls with withheld numbers - this is called Anonymous Call Reject. Consumers

---

[43] Ref to options in mobile CFI which have gateway withholding CLI.
[44] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 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
[45] There are legitimate reasons why a caller may wish to withhold their CLI for a call. For example, doctors or hospitals may withhold their CLI for privacy purposes.
[46] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.140.

already have the right to request that calls with withheld numbers are automatically blocked.[47]

# Specific design of 4.19

3.19 Some stakeholders also provided comments on the proposed wording of paragraph 4.19.

## Clarification of the guidance

### Stakeholder comments

3.20 Several stakeholders asked for clarity on the type of calls that must be blocked and which calls may fall into a legitimate use case. In particular, they asked for clarification on the terms and phrases used in paragraph 4.19 and in our consultation, including "UK networks"[48], "networks outside the UK"[49], "overseas"[50], "abroad"[51] and "UK CLI".[52]

3.21 BT commented that the lack of common definitions might lead to misunderstanding or misrepresentation of the circumstances in which calls originating outside the UK should be blocked.[53]

3.22 Vodafone noted its view that that there is currently no consistent definition of what constitutes an overseas network and there was uncertainty around the treatment of such networks. It noted the view that it was dangerous to rely on international gateways to determine whether to exempt individual upstream networks, saying that this would put international gateway providers in the position of assessing the nature of an upstream carrier's business, in particular legitimacy of its traffic. Vodafone suggested that international gateways which have a less robust interpretation of the rules could secure a competitive advantage by taking a relatively lax interpretation to the rules to attract more traffic.[54]

3.23 Vodafone also asked about the level of evidence which we would expect to see in order to support the assessment of the upstream network's business, and observed that this measure would only be as strong as its weakest link. More generally, it asked Ofcom to play a more active part in the process and to clarify whether a given network/international gateway meets the criteria of UK PECN/S.[55] It said that this must be addressed in order for blocking to be effective, and suggested that the technical measures sub-group could be a suitable forum for sharing this intelligence.[56] Vodafone also emphasised the need for

---

[47] The ICO are responsible for the enforcement of PECR. They have published guidance on the use of CLI from a privacy perspective. Guide to PECR: Line Identification (CLI).
[48] Responses to the 2024 consultation: NICC, p.1; BT, p.2; VMO2, p.3.
[49] Responses to the 2024 consultation: NICC, p.1; BT, p.2.
[50] Vodafone response to the 2024 consultation, page 3.
[51] Responses to the 2024 consultation: NICC, p.1; BT, p.2; VMO2, p.3.
[52] Talktalk response to the 2024 consultation, p.2.
[53] BT response to the 2024 consultation, p.2.
[54] Vodafone response to the 2024 consultation, p.3.
[55] Public Electronic Communications Networks/Services.
[56] This is the Strategic Working Group established by Ofcom in 2015 to work with major providers on initiatives to reduce the impact of nuisance and scam calls.

consistent implementation of our proposal across the industry for it to be effective in protecting consumers. It highlighted the specific difficulty for collective agreements between operators: if they agreed on whether a specific upstream network operator should be exempt from having its traffic blocked, there is a risk that this would be perceived as cartel-like behaviour.[57]

3.24   NICC considered that the guidance, in particular paragraph 4.19 (and related clauses), were open to interpretation which could provide opportunities for scam calling from abroad using spoofed UK numbers. NICC suggested amending paragraph 4.19 to refer to "calls from an international interconnect" rather than "calls from abroad". It also suggested definitions for the terms "UK Network", "Domestic Interconnect" and "International Interconnect".[58]

3.25   In further conversations with members of the NICC N-CLI Task Group, we have identified that there may be a difference of interpretation between some stakeholders as to which provider should be considered the provider which first receives these calls from a non-UK network (in particular, whether an international gateway could be considered a provider subject to GC C6.6). They also indicated that some international gateway providers may not be in a position to check, or want the responsibility of checking, the legitimacy of traffic.

3.26   VMO2 noted its view that the terms "overseas" and "UK" were no longer clear in modern networks, and suggested that each scenario would need to be considered in terms of how calls are transiting in terms of "national interconnects" and "international interconnects". It suggested replacing the term "abroad" with the term "international networks".[59]

3.27   TalkTalk suggested that the term "UK CLI" should be defined as "CLI that belongs to the UK numbering plan and which has been allocated to/adopted by a UK public electronic communications provider and/or network". They commented that this would help define the rationale for both the call block and for applying an exception.[60]

## Our response

3.28   We note the comments around the clarity and specificity of the requirements set out in this section of the CLI Guidance. We also recognise that the way in which calls are initiated and can be routed has become increasingly complex and can involve many parties, some of which will be based outside of the UK.

3.29   As a general observation, whether a provider falls within the scope of our CLI rules in GC C6 will depend on (1) whether the nature of the service it provides falls within the definitions in GC C6.1; and (2) whether there is a territorial connection with the UK, for example, because the provider is providing services to customers in the UK. A provider does not need to be based in the UK to be subject to our rules.

3.30   More specifically, our CLI Guidance notes that the obligation to check the validity of the CLI of a call entering the UK network from outside the UK falls to the provider at the first point

[57] Vodafone response to the 2024 consultation, p.4.
[58] NICC response to the 2024 consultation, p.1.
[59] VMO2 response to the 2024 consultation, p.4.
[60] Talktalk response to the 2024 consultation p.2.

of ingress to the UK.[61] This provider will differ depending on the way in which a call is routed into the UK in a particular scenario. Some responses to our consultation have also indicated that it may not always be clear to the various providers involved in bringing a call into the UK, which provider is required to check the validity of the CLI, in particular where an international gateway provider is involved. This may create uncertainty and could result in a situation where no provider checks the validity of the CLI, for example, because there is an expectation another provider will carry out the check.[62]

3.31 In principle, this check may be carried out by an international gateway provider or a provider that receives a call into the UK via a direct route. To provide certainty to stakeholders where a call has entered the UK network through an international gateway provider, we expect the UK provider that first receives the call from the international gateway provider to reassure themselves that the relevant checks have taken place (for example, by ensuring that there are appropriate contractual arrangements in place with the international gateway provider to carry out the relevant checks).[63] [64] While we do not expect UK providers to check the validity of the CLI for each call that enters their network from outside the UK, we do expect the UK provider that first receives a call from a non-UK network or from an international gateway provider to ensure they have appropriate systems and processes in place to be able to demonstrate that calls entering the UK are from a trusted source and fall within the relevant exception in our CLI Guidance. As indicated in our November 2022 Statement, a non-UK network routing calls with a UK CLI into a UK network may prefer to connect directly to a UK network that can separate out the calls which fall into the legitimate use cases into a route that is not blocked.[65]

3.32 Our CLI Guidance is intended to provide practical guidance to help secure compliance with GC C6. In response to Vodafone's suggestion for Ofcom to clarify whether a given network meets the criteria of a UK PECN/S, we do not consider it necessary to introduce new definitions. We also do not consider it necessary or appropriate to identify specific networks that should be classified as a UK network or an international network as this can depend on the nature of the service a network is providing and whether there is a territorial connection with the UK in a particular scenario.

---

[61] See, for example, para 4.16 of our CLI Guidance as well as paras. 4.102, 4.139, 4.142, 4.146 and 4.151 of our November 2022 Statement.

[62] For example, an international gateway provider may incorrectly consider they are not subject to GC C6.6; they may not know they are acting as international gateway provider that is bringing calls into the UK; or they may not be in a position to check, or want the responsibility of checking, the legitimacy of traffic. If the provider first receiving a call from an international gateway provider expects the international gateway provider to check the CLI of a call, or otherwise treats the traffic from an international gateway provider as domestic traffic, there is a risk that the call is connected without there being an assessment of the risk that the CLI of the call may have been spoofed.

[63] For the avoidance of doubt, where an international gateway provider is used to bring calls into the UK, there is no expectation that providers receiving the call from another UK network (that is not the first provider to receive the call from an international gateway provider), will need to carry out their own checks with the international gateway provider.

[64] We have decided to clarify this in a footnote at para 4.19 of our CLI Guidance.

[65] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.139.

3.33    We agree that our CLI Guidance could provide further clarity to ensure consistent implementation across industry. Taking into account stakeholders' comments, we have decided to replace references to "abroad" and "overseas" with "outside the UK", "UK network" and "non-UK network". We have also explained what we mean by "UK customer" and make additional changes to the wording to provide further clarity on which calls may fall into a legitimate use case. We discuss in paragraph 3.56 which networks would be responsible for checking the CLI of a call entering the UK network from outside the UK. Further, we have decided to separate out the legitimate use cases applying to a UK CLI being presented as a Network Number and a UK CLI being presented as a Presentation Number. In our November 2022 Statement, we provided examples of legitimate use cases of UK CLI as a Network Number and we do not consider that we need to change the scenarios in which these apply.[66]

3.34    We note the comment that international gateway providers may interpret the rules in different ways to secure a competitive advantage. As we expect the provider first receiving a call from an international gateway provider to reassure themselves whether the relevant checks have been made, calls with spoofed UK Presentation Numbers should be identified and blocked. This should therefore remove the significant discretion to decide what traffic is and is not legitimate based on the international gateway provider's commercial incentives.

3.35    As explained in paragraph 2.20 above, providers in the Crown Dependencies use +44 numbers from the UK's National Telephone Numbering Plan. Calls from the Crown Dependencies fall into a legitimate use case for use of +44 numbers from outside a UK network. In our November 2022 Statement, we explained that most calls from the Crown Dependencies of Jersey, Guernsey and the Isle of Man using +44 numbers from the UK's National Numbering Scheme will not be affected by this blocking, as these calls enter the UK network via a national interconnect.[67] In response to stakeholders' comments on the clarity of paragraph 4.19, we have, where appropriate, decided to add references to Crown Dependency networks to ensure that providers are clear on both the type of calls that must be blocked and which calls may fall into a legitimate use case.

3.36    In response to TalkTalk's suggestion of a definition for "UK CLI", we have added a definition of UK CLI as "CLI associated with a telephone number identified in the National Telephone Numbering Plan". We disagree that the definition should also refer to the number which has been allocated to/adopted by a UK public electronic communications provider and/or network. The requirements for blocking calls are set out in GC C6.6(a), which states that:

>    "Regulated Providers must … take all reasonable steps to identify calls, other than calls to Emergency Organisations, in relation to which the CLI Data provided is invalid, does not uniquely identify the caller, or does not contain a Telephone Number that is dialable."

3.37    Paragraph 4.10 of the CLI Guidance explains further that where a UK number is used, a valid number is one which must be a number designated as a Telephone Number available for

---

[66] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data,* paras 4.145-4.149.

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

allocation in the National Telephone Numbering Plan and be shown as allocated in the National Numbering Scheme. An invalid number is one which does not belong in a valid range, and therefore this is included separately in GC C6.6(a).

## Calls with a CLI from the +447 range

3.38    The first legitimate use case in the version of paragraph 4.19 we consulted on referred to "UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range".

### Stakeholder comments

3.39    We did not receive any comments on this legitimate use case although, as explained above, we did receive general requests for clarification on the wording in paragraph 4.19, including terms such as "overseas".

### Our response

3.40    As explained in paragraph 3.33 above, we have decided to replace the reference to "overseas" and instead refer to "non-UK networks". We have also decided to explicitly refer to Crown Dependency networks and more clearly explain the purpose of the exception.

3.41    Taking into account our comments above, we have decided to amend the wording of this legitimate use case in a new paragraph 4.19A to refer to "calls with a CLI from the +447 range. This is to ensure calls from UK (and Crown Dependency) mobile users roaming on a non-UK (or non-Crown Dependency) network making calls back to +44 numbers are not blocked". Annex A2 below sets out the changes we have made to the CLI Guidance in full.

3.42    We are concerned that some scam calls which are received by UK consumers may come from scammers who are spoofing +447 (UK mobile) numbers, and we are investigating whether we should change our rules, or consider other measures, to fix this issue. We have therefore published a call for input 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.[68]

---

[68] Ofcom, 2024. *Call for Input: reducing scam calls from abroad which spoof UK mobile numbers*

## Mobile user roaming in UK

3.43    The second legitimate use case in the version of paragraph 4.19 we consulted on referred to "calls to a mobile user who is roaming in the UK".

### Stakeholder comments

3.44    NICC suggested a change to clarify that paragraph 4.19 relates to calls from a UK PECN to a non-UK mobile user who is roaming in the UK.[69] TalkTalk suggested that this use case should be for calls that originate from a UK network calling an international mobile network whose subscriber is roaming within the UK.[70]

### Our response

3.45    We do not think it is necessary to add further clarification as the network receiving the call from outside the UK will not necessarily know whether the call has originated in the UK. We have, however, moved the clarification footnote that these calls can be identified as they are calls to the Mobile Station Roaming Number (MSRN)/International Roaming Number (IRN) ranges into the main body of the guidance.

3.46    We have also decided to amend the wording of this legitimate use case in a new paragraph 4.19A to explicitly refer to the Crown Dependencies so it now refers to "calls to a mobile user who is roaming in the UK (or Crown Dependencies). These are calls to numbers within the Mobile Station Roaming Number (MSRN)/International Roaming Number (IRN) ranges". Annex A2 below sets out the changes we have made to the CLI Guidance in full.

## Traffic originating on a UK network

3.47    The third legitimate use case in the version of paragraph 4.19 we consulted on referred to calls "where the traffic has originated on a UK network".

### Stakeholder comments

3.48    NICC and TalkTalk both suggested an addition to clarify that the call should only be allowed if the UK PECN on ingress can trust the traffic has reliable means to distinguish the traffic from calls with spoofed UK CLI.[71]

### Our response

3.49    As we explained in our February 2022 Consultation (where we originally proposed blocking of calls with UK Network Numbers), we expect providers to liaise with their international interconnecting partners to ensure that calls that have a legitimate reason to use a UK CLI as a Network Number can be routed through a recognisable route and these calls are not blocked.[72] We also expect providers to have processes in place with their international interconnect partners to identify calls that can use UK CLI legitimately and differentiate these from calls that are spoofing UK CLI.[73] In practice, we expect these calls to be connected directly to a UK network that can segment the legitimate calls into a route that is

---

[69] NICC response to the 2024 consultation, p.1.
[70] Talktalk response to the 2024 consultation, p.2.
[71] Responses to the 2024 consultation: NICC, p.1; TalkTalk, p.2.
[72] Ofcom, 2022. *Consultation: Improving the accuracy of Calling Line Identification (CLI) Data,* para 4.30
[73] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) Data*, para 4.146

not blocked, although as noted in 3.31 above, these calls may also be connected via an international gateway provider, where they are able to check the validity of the CLIs associated with these calls. As these calls have originated on a UK network, they should have UK CLI as a Network Number and may also have a UK CLI as a Presentation Number. We agree with the suggestion from NICC and TalkTalk and we have amended the wording in this part of the guidance to indicate that these calls should not be blocked where the provider can demonstrate that the traffic has originated on a UK (or Crown Dependency) network.

3.50    Taking into account our comments above, we have decided to amend the wording of this legitimate use case in a new paragraph 4.19A to refer to "where the CP can demonstrate the traffic has originated on a UK (or Crown Dependency) network, then onward routed outside the UK (or Crown Dependencies) before then re-entering through a UK (or Crown Dependencies) network. This includes calls originating on nodes or cloud services located in the UK (or Crown Dependencies)". Annex A2 below sets out the changes we have made to the CLI Guidance in full.

## UK customers on overseas nodes or cloud services

3.51    The fourth legitimate use case in the version of paragraph 4.19 we consulted on referred to calls "where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services".

### Stakeholder comments

3.52    NICC suggested deleting this exception, noting its view that a provider which uses an overseas node or cloud services for the provision of services to UK customers is considered a UK PECN and therefore did not constitute an exception.[74]

3.53    NICC also subsequently queried the reference to "UK customer", in particular whether this meant customers located in the UK or customers that are UK entities.

3.54    TalkTalk asked for further clarification on the basis of its view that mainstream cloud services are often hosted within EU zones and could be considered international. It suggested that a UK PECN using cloud nodes for hosting services should be considered to fall under the governance of that UK PECN and treated as a domestic interconnect.[75]

### Our response

3.55    We disagree with NICC's suggestion of deleting this measure. As explained in paragraph 3.29, a provider will fall within the scope of GC C6 if the service it provides falls within the definitions in GC C6.1 and there is a territorial connection with the UK (for example, because the provider is providing services to customers in the UK). Importantly, a provider may be based outside of the UK and considered a non-UK network, but still be subject to GC C6; this will depend on the nature of the service the network is providing and whether there is a territorial connection with the UK in a particular scenario. Even if a non-UK network is considered subject to GC C6, that does not make it a UK network - rather, it

---

[74] NICC response to the 2024 consultation, p.1.
[75] Talktalk response to the 2024 consultation, p.2.

means it is subject to, and must comply with, the relevant rules in GC C6. Any provider bringing calls into the UK will ultimately be doing so from a non-UK network. Calls brought into the UK via a node or cloud service hosted outside of the UK should therefore be treated as calls entering the UK network from outside the UK. For that reason, we consider it important to retain this exception.

3.56     As explained in paragraph 3.30, the obligation to check the CLI of a call entering the UK network from outside the UK falls to the provider at the first point of ingress into the UK. This provider will differ depending on the way in which a call is routed into the UK in a particular scenario and may be an international gateway provider or a provider that receives a call into the UK via a direct route. As explained above, to provide certainty to stakeholders where a call has entered the UK network through an international gateway provider, we expect the UK provider that first receives the call from the international gateway provider to reassure themselves that the relevant checks have taken place (for example, by ensuring that there are appropriate contractual arrangements in place with the international gateway provider to carry out the relevant checks).[76] While we do not expect UK networks to check the validity of the CLI for each call that enters their network from outside the UK, we do expect the UK provider that first receives a call from a non-UK network or from an international gateway provider to ensure they have appropriate systems and processes in place to be able to demonstrate that calls entering the UK are from a trusted source and fall within the relevant exception in our CLI Guidance. As indicated in our November 2022 Statement, a non-UK network routing calls with a UK CLI into a UK network may prefer to connect directly to a UK network that can separate out the calls which fall into the legitimate use cases into a route that is not blocked.[77]

3.57     We disagree with TalkTalk's suggestion that cloud services hosted within EU zones by a UK PECN should be treated as a domestic interconnect. These services hosted in EU zones are outside of the UK network and therefore interconnects from these nodes into a UK network should be treated as an international interconnect. As noted above, a non-UK network can be subject to GC C6 but that does not make it a UK network.

3.58     Taking into account the suggestions from NICC and TalkTalk in relation to the third exception (relating to traffic originating on a UK network), we have however decided to amend this exception to say we expect these calls should not be blocked where the provider can demonstrate that the call is being made by a UK customer.[78] One way in which providers can demonstrate this for calls which use UK CLI as a Presentation Number is by seeking assurance from the non-UK network that the caller is using a CLI that they have

---

[76] For the avoidance of doubt, where an international gateway provider is used to bring calls into the UK, there is no expectation that providers receiving the call from another UK network (that is not the first provider to receive the call from an international gateway provider) will need to carry out their own checks with the international gateway provider.

[77] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.139.

[78] In this context, UK customer means a customer that has been allocated a number with the relevant CLI or is otherwise using a CLI that they have permission to use (either because they have been directly assigned that number or has been given permission by a third party who has been assigned that number). In both cases, the customer will be using a number that they have permission to use and it should not therefore be a spoofed number. See also paragraph 4.13 of our CLI Guidance.

permission to use (either because they have been directly assigned that number or has been given permission by a third party who has been assigned that number). For calls using a UK CLI as a Network Number, providers will need to seek assurance that the caller is using a number that has been allocated to the originating CP or one that has been ported into the originating CP's network.[79]

3.59    Therefore, we have decided to amend the wording of this legitimate use case in new paragraphs 4.19A and 4.19B to refer to "where the CP can demonstrate the call is being made by a UK (or Crown Dependency) customer but has originated on a non-UK (or non-Crown Dependency) network. This includes traffic that is hosted on nodes or cloud services outside the UK (or Crown Dependencies)". To provide further clarity for stakeholders, we have also decided to add the examples of ways in which providers can demonstrate a call is being made by a UK customer in paragraph 3.58 above. Annex A2 below sets out the changes we have made to the CLI Guidance in full.

3.60    More generally to help clarify the requirements for calls with UK CLI as a Network Number and as a Presentation Number, we have decided to list the exceptions separately. The exceptions in paragraph 4.19A of the CLI Guidance relate to calls by a UK mobile user roaming on a non-UK network or that originate on UK networks. These will have a UK CLI as a Network Number. Paragraph 4.19B sets out the exceptions for calls from a UK user which have originated on a non-UK network. These calls should have a UK Presentation Number but a non-UK number as a Network Number.

# Impact assessment

3.61    In the paragraphs below, we set out the stakeholder responses to our impact assessment in relation to our proposals for Presentation Number blocking. Taking into account these responses, we have assessed the impact on consumers, providers and businesses.

## Impacts on consumers

### What we said

3.62    We expected our proposal to benefit consumers through reducing the number of scams calls that consumers receive with spoofed numbers. Our proposal was intended to remove a means by which scammers can spoof a UK geographic or non-geographic number when making calls from abroad. This was designed to make it more difficult for scammers to mislead consumers and enable better identification and blocking of scam calls. We expected this to reduce both the financial as well as non-financial impacts on consumers, such as emotional and psychological harm.

### Stakeholder comments

3.63    The consumer benefits of our proposal were widely recognised by respondents, who agreed that our intervention will limit the detrimental impact of scams. The Communications Ombudsman, FCS, and VMO2 suggested that our proposal would help provide greater

---

[79] As set out in paragraphs 4.12 – 4.13 of our CLI Guidance.

confidence for consumers that they are being protected by their communications providers.[80] In particular, VMO2 referred to the importance of supporting consumers and operators in order to maintain trust.[81] CCUK highlighted a growing lack of trust in using the telephone.[82]

3.64    BT confirmed that when it started blocking UK presentation numbers at the international gateway, the impact was immediate and significant, e.g. up to one million calls per day were prevented from entering their network in the first month after implementation.[83]

3.65    Vodafone pointed out that scammers adapt relatively quickly, but while the intervention might not stop scammers from succeeding, it would likely disrupt their business model if implemented effectively. It also emphasised the need for consistent implementation of our proposal across the industry for it to be effective in protecting consumers and emphasised that without clearer definitions of which providers are expected to do what, the effectiveness of our proposals will be determined by the "weakest link", i.e. the international gateway provider which has the least restrictive blocking policy.[84]

### Our response

3.66    We welcome stakeholders' agreement with the analysis of impacts on consumers that we outlined in our consultation. As set out in paragraphs 3.132 - 3.133 below, over the coming months we will conduct a stakeholder engagement programme, particularly focused on smaller providers and call centre end users who may be affected.[85] We expect the amended wording of 4.19 presented in this statement along with the proposed consumer and operator engagement programmes to support consistent and wide implementation of our proposal.

3.67    We explain our response to Vodafone's comment regarding the role of international gateways in paragraphs 3.32- 3.34.

## Impacts on telecoms providers

### What we said

3.68    While we expected that some providers would incur costs when implementing our proposal to block calls from abroad with a UK Presentation Number, we did not expect these costs to be unduly onerous. We also expected that costs will be at least partly offset by a benefit of fewer customer complaints, improved prospects for tracing suspicious calls, and any additional revenue from business customers abroad who may need to directly connect into the UK network.

---

[80] Responses to our 2024 consultation: Communications Ombudsman, FCS, p.2, VMO2, p.2.
[81] VMO2 response to the 2024 consultation, p.2.
[82] CCUK response to the 2024 consultation, p.2.
[83] BT response to the 2024 consultation, p.3.
[84] Vodafone response to the 2024 consultation, pp.2-3.
[85] For example, we aim to engage with industry through our Strategic Working Group, through telecoms membership bodies such as CCUK and FCS, and also to liaise with wider relevant business groups whose members may be affected by this work, such as Data and Marketing Association and the Call Centre Management Association.

3.69    We considered the impact on different providers that may be affected by our proposal:

   a)   providers that first receive scam calls from abroad into the UK network;
   b)   networks abroad that connect calls from abroad with a UK CLI as a Presentation Number into a UK network; and
   c)   cloud voice providers.

3.70    We explained that providers that first receive calls into the UK network would need to work with their international interconnect partners to ensure that any calls with UK Presentation Numbers fall within a legitimate use case. This would require process changes with associated costs that may differ between providers, but we did not expect these to be unduly onerous. We also anticipated an additional source of revenue for these providers, as callers from abroad who can legitimately use a UK CLI may need to pay for a direct connection to the provider to ensure that their calls are not blocked.

3.71    With respect to networks abroad, we recognised that they may incur additional costs to connect their calls into the UK, to ensure that legitimate calls that comply with our updated CLI Guidance are not blocked. We noted that some costs are likely to be passed on to businesses who make use of communication services from these providers.

3.72    We said that cloud voice providers would need to ensure that the calls from UK users with a UK CLI as Presentation Number are not blocked. We did not expect significant additional costs for cloud voice providers, who connect their calls from an IP network into the UK telephony network.

## Stakeholder comments

3.73    The majority of responses did not raise specific concerns about the impact on providers.[86] Telecom2 said that it and its clients have suffered reputational damage due to calls with spoofed numbers and anything that reduces that would be welcome.[87] Magrathea responded that, with exceptions in place to support services such as cloud hosting and international call centres working on behalf of UK business, it does not foresee any major challenges to implementation.[88] VMO2 confirmed that from a technical perspective, the proposed change aligns with its current thinking regarding enhancing the blocking of both Presentation and Network Numbers at international gateways.[89]

3.74    CCUK pointed out that depending on where an operator sits in the value chain, the impact of our proposal could be disproportionately large. CCUK members are faced with technical challenges that could result in the loss of legitimate business, or the inadvertent blocking of genuine calls.[90] In a similar vein, FCS highlighted that the changes would affect cloud/SIP providers and transit carriers more than the traditional networks, urging us to give greater

---

[86] Apart from the comments set out in paras 3.20 - 3.22.
[87] Telecom2 response to the 2024 consultation, p.2.
[88] Magrathea response to the 2024 consultation, p.2.
[89] VMO2 response to the 2024 consultation, p.2.
[90] CCUK response to the 2024 consultation, p.2.

consideration to alternative voice solutions.[91] CCUK also requested that we make available research establishing the likely cost and impact, particularly on cloud providers.[92]

3.75    Vodafone's comment referenced in paragraph 3.23 emphasised that the positive impact of our new rules would depend on consistent adoption by the operators in scope.

## Our response

3.76    We consider that the assessment of impacts on providers included in our consultation was broadly accurate. While most traditional network operators will experience a limited impact from our proposals, we recognise that some providers in the value chain might be affected more, in particular:

a)  international gateway providers;
b)  transit carriers; and
c)  cloud/SIP providers.

3.77    Calls are generally brought into the UK via an international gateway provider or a direct route. UK networks will therefore need to work with any international interconnect partners to ensure only legitimate calls are brought into the UK.[93]

3.78    We recognise that in some cases the international gateway provider may not be in a position to check, or want the responsibility of checking, the legitimacy of traffic coming into the UK.[94] In those cases, providers serving UK customers who wish to legitimately use UK Presentation Numbers may decide to connect calls to a UK network directly and bypass international gateways.

3.79    If providers serving UK customers using UK Presentation Numbers decide to use direct routes that bypass international gateways, we recognise that international gateway providers may lose some of the revenue that they traditionally derived from routing these calls into the UK. However:

a)  Some of that revenue loss will be associated with scam calls that spoofed UK numbers, which we do not consider appropriate to take into account as an adverse impact.
b)  For the remaining legitimate traffic, the adverse impact is mitigated in two ways:

i)   International gateway providers that play other roles in the value chain may benefit to the extent they may also act as a provider involved in connecting calls into the UK using direct routes.
ii)  As referenced in paragraph 2.19 above, we understand that other countries have proposed or implemented rules analogous to ours, so international gateway

---

[91] FCS response to the 2024 consultation, p.2.
[92] CCUK response to the 2024 consultation, p.3.
[93] In response to Vodafone's concerns, we have explained in para 3.29 above that a provider will fall within the scope of GC C6 if the service it provides falls within the definitions in GC C6.1 and there is a territorial connection with the UK, for example, because the provider is providing services to customers in the UK. We have made clarifications to the wording of paragraph 4.19 of the CLI Guidance, as well as the legitimate use cases, as set out in paras 3.28 - 3.60 above.
[94] In other cases, the provider that first receives a call into the UK may also operate the international gateway that brings the call into the UK.

> providers may have to make appropriate changes to their business models and processes regardless of any action we take.

c) Finally, we note that these providers can continue to earn revenue associated with any calls which do not use UK CLI as a Presentation Number, which are unaffected by this change.

> We do not therefore expect our new rules to have very material adverse impacts on international gateway providers.

3.80    As indicated in our consultation, there may be some process changes for providers that currently first receive calls from an international gateway provider. Where calls coming into the UK using a UK Presentation Number continue to be routed via international gateways, providers that first receive calls from those international gateway providers will need to ensure they have appropriate systems and processes in place to be able to demonstrate that calls entering the UK are from a trusted source and fall within the relevant exception in our CLI Guidance. As explained in paragraph 3.31 above, this is likely to involve the UK provider that first receives the call from the international gateway provider reassuring themselves that the relevant checks have taken place (for example by ensuring there are appropriate contractual arrangements in place with the international gateway provider to carry out the relevant checks). We note that providers should have already made similar systems and process changes for the implementation of the blocking of international calls with UK CLIs as Network Numbers. However, as stated in our consultation, there may be an additional source of revenue for providers that currently first receive calls from an international gateway provider, as they could potentially charge more for direct routes that bypass international gateways.

3.81    With respect to transit carriers acting as intermediaries between networks (as mentioned by FCS), we consider that transit carriers handling calls with UK Presentation Numbers between networks outside the UK would lose business, as these calls will be more likely to connect to the UK directly. We consider that domestic UK transit carriers would not be impacted directly by our proposals, because these carriers are not considered providers that first receive calls into the UK network and hence are not required to check the validity of the CLI of such calls.

3.82    With respect to cloud and other alternative voice providers, we remain of the view that the impact is limited. In our November 2022 Statement, we found providers had the capability to route at least a significant proportion (if not all) of their calls with a UK CLI as a Network Number directly to a UK network. We concluded that such networks typically are able to ensure that legitimate calls are not blocked at the international gateway. We consider that the same is true of calls with UK CLI as Presentation Number.[95] The findings from our post-consultation informal engagement with the trade bodies representing a variety of providers, as well as discussions with regulators from other countries which introduced analogous measures, were consistent with our assessment that these providers should generally have the capability to implement our proposals.

---

[95] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.148.

3.83    To address the comments on the need for consistent adoption of our new rules by the operators in their scope, we have made various clarifications to the wording in paragraph 4.19. We also plan to further communicate these rules to the industry through an outreach programme as set out in paragraphs 3.132 - 3.133 below.

## Impacts on businesses

### What we said

3.84    As scam calls result in significant financial harm for victims, as well as wider harm to businesses, we set out our expectation that the updated CLI Guidance would be beneficial to legitimate businesses. Spoofing a firm's number can lead to direct costs for the business to deal with complaints and can also cause reputational harm for the organisation that has been impersonated. These harms and costs would be reduced by preventing scammers based abroad from spoofing these numbers, as it would provide greater protection for businesses from impersonation attempts. This would also improve trust in calls that display a UK geographic or non-geographic number and therefore help businesses as a greater proportion of their attempted calls may be answered.

3.85    In addition, UK businesses who use calling services from abroad, for example offshore call centres and those that have employees based abroad, may be affected by this change. Where they can legitimately use a UK Presentation Number for calls into the UK, they may need to change the ways their calls are routed to ensure they are not blocked. There may be incremental costs associated with this, as they may no longer be able to route the call via the cheapest international routes into the UK. We expected any incremental cost incurred by individual businesses to be relatively small, noting some call centres and businesses may have already made changes to the way they route calls into the UK following our changes on blocking international calls with UK CLI as Network Numbers. We also expected that any such impact would mostly affect large UK businesses, with small UK businesses less likely to be affected.

3.86    With regard to any adverse impacts on businesses due to inadvertent blocking of legitimate calls, the blocking carried out voluntarily by BT Group indicated that this risk is low. BT Group noted in its response to the 2023 CLI Authentication Consultation that where they engaged with their provider customers, with rare exceptions, the calls were unlikely to be legitimate traffic.[96]

3.87    We also recognised that a bulk of the costs imposed on the networks abroad will be passed onto their business customers, namely the cost that these networks will incur to connect their calls into the UK and ensure that legitimate calls (that comply with our updated CLI Guidance) are not blocked.

### Stakeholder comments

3.88    While most of the responses did not raise any specific concerns about impacts on businesses, several respondents highlighted potential adverse effects of our proposals.

---

[96] BT, 2023. Response to CLI authentication consultation, p.5.

3.89    UKCTA, Vodafone, and CCUK pointed out the risk that our proposals would impact
        legitimate users of communications services, e.g. UK businesses that use offshore call
        centres for outbound calling that present as UK-based numbers.[97] UKCTA asserted that
        while the proposals would effectively block scam calls, they would also block many
        legitimate business calls.[98] FCS added that businesses and their operators might need to
        organise different routing into the UK, as they did for Network Number blocking.[99] In a
        similar vein, Vodafone said that our proposals would dictate that enterprises with such a
        model need to connect their call centre to a UK network utilising a long-lining approach
        such as a SIP trunk, rather than egressing calls to their local overseas network. Blocking
        legitimate calls could cause an issue within businesses and for their respective markets.[100]
        UKCTA and CCUK also pointed out that there is huge complexity in this market and changing
        this guidance, and the proposed workaround to enable legitimate business cases to
        continue, could be a huge cost ultimately to the end consumer or the service provider. They
        suggested further analysis of the market and the possible businesses affected to fully
        understand the possible effects of these changes.[101]

3.90    Vodafone and CCUK were also concerned about the impact on call centres providing
        services to multiple smaller UK businesses and those using cloud services which, by default,
        will need to implement special measures to continue providing these services and still
        comply with GC C6.[102] Vodafone also raised concerns about call centres commissioned to
        provide temporary campaign-based outbound calling and about secondary routing for blue
        chip enterprises (i.e. overflow and disaster recovery options). In this context, they also
        highlighted the significant amount of Government-funded outbound calling that was routed
        via overseas networks during the COVID pandemic as an example.

3.91    To ensure this does not have an adverse and costly effect on those businesses, UKCTA and
        Vodafone suggested that we proactively widen the outreach and communication
        programme and request information from those businesses which will be most affected by
        this change.[103] UKCTA also said that providers will warn their customers as soon as possible
        that this will be implemented, but many businesses may need to change their business
        models or adapt in other ways.

3.92    Vodafone also suggested caution in relying on the experience of BT in the UK presentation
        number blocking.[104] While BT's blocking might have had little impact on legitimate callers,
        this might no longer be true in case when all international gateway providers took the same
        approach. Vodafone suggested that upstream carriers with legitimate +44 Presentation
        Number CLI traffic might have routed the calls to alternative UK international gateway
        providers to avoid BT's blocking and ensure the calls are terminated.[105]

---

[97] Responses to the 2024 consultation: UKCTA, p.3; Vodafone, p.2; CCUK, p.2.
[98] UKCTA response to the 2024 consultation, p.4.
[99] FCS response to the 2024 consultation, p.3.
[100] Vodafone response  to the 2024 consultation, p.2.
[101] Responses to the 2024 consultation: UKCTA, p.3; CCUK, p.2.
[102] Responses to the 2024 consultation: Vodafone, p.2; CCUK, p.2.
[103] Responses to the 2024 consultation: Vodafone, p.3; UKCTA, p.4.
[104] Referenced in paragraph 3.16.
[105] UKCTA response to the 2024 consultation, p.4.

**Our response**

3.93    We acknowledge that larger businesses may be more likely to already have the necessary arrangements in place to comply with our rules on blocking calls from outside the UK with a UK number as a Presentation Number except in legitimate use cases. Therefore, the impact on the smaller businesses might be proportionately greater, if they or their international interconnect providers have to invest in administrative or process changes to ensure that legitimate calls are not blocked. We consider that small businesses that wish to make legitimate calls using UK Presentation Numbers will generally be able to continue doing so, by using a third-party service provider that has the necessary direct connection arrangements in place.

3.94    We recognise that this may entail an incremental cost which may be partly or fully passed on to end customers. As discussed in paragraphs 3.123 - 3.133 below, we also consider that our timeframes allow sufficient time for different kinds of businesses to make any necessary changes.

3.95    With respect to blocking of legitimate calls, this will not occur where providers and businesses route their calls appropriately to comply with the legitimate use cases. We consider that our CLI Guidance (with the clarifications we have made) includes appropriate exemptions to allow a comprehensive set of legitimate use cases to continue, including for the short-term calling campaigns and secondary routing. We also note the previous experience with blocking calls with UK Network Numbers, when only a small number of calls were blocked in error and these were quickly resolved.[106] In addition, our outreach programme outlined in paragraph 3.132 - 3.133 will support operators and businesses in ensuring that this routing is completed by our implementation date.

---

[106] Ofcom, 2022. *Statement: Improving the accuracy of Calling Line Identification (CLI) data*, para 4.140.

## Impacts on Crown Dependencies

### What we said

3.96    We did not expect any further impacts on calls from the Crown Dependencies of Jersey, Guernsey and the Isle of Man who also use CLI from the +44 range.

### Stakeholder comments

3.97    We did not receive any comments about the impact of these changes on the Crown Dependencies.

### Our response

3.98    As we explain in paragraph 3.35 above, we have decided to add a clarification to the relevant section of the CLI Guidance to make it clear that calls from the Crown Dependencies are exempt from Presentation Number blocking. As this clarification was previously in our November 2022 Statement, our policy position has remained the same. We are adding this clarification to the CLI Guidance so that the scope of blocking of international calls using +44 numbers is clear.

## Equality impact assessment and Welsh language impact assessment

3.99    Our duties under the Equality Act 2010 and the Northern Ireland Act 1998 require us to consider whether our proposals would have a particular impact on persons sharing protected characteristics.

### What we said

3.100    We said that overall, we believe that this proposed change to the CLI Guidance is justified and proportionate, removing a loophole through which scammers can spoof a UK geographic or non-geographic number when making calls from abroad.

3.101    On the impact on persons sharing protected characteristics, we said in our consultation that we considered our proposals would be likely to have a particularly positive impact on groups of persons that may be more susceptible to scam calls (such as more vulnerable or older persons). We did not identify any adverse impacts on specific groups of persons that are likely to be affected in a different way to the general population.

3.102    On the impact on the Welsh language, we said that our proposals would affect the telephone number consumers would see calling them and we did not therefore consider our proposals would have any impact on our Welsh language obligations.

3.103    We provided a detailed discussion of these issues in Annex 2 of the consultation.[107]

---

[107] Ofcom, 2024. *Consultation: Tackling scam calls – updating our CLI Guidance to expect providers to block more calls with spoofed numbers.*

### Stakeholder comments

3.104    All stakeholders that commented on the Equality Impact Assessment agreed with our approach.[108]

3.105    On the Welsh language impacts, all four stakeholders that commented agreed with our approach.[109]

### Our response

3.106    We remain of the view that the change proposed will not have an adverse impact on specified groups or on Welsh language.

## Our decision – summary

3.107    As explained above, there was general support for the blocking of calls from outside the UK with a UK CLI as a Presentation Number. We continue to believe that our intervention will achieve our objective of reducing the number of scams calls from outside the UK reaching UK consumers (and be more effective in doing so than an approach that also allows the anonymisation of such calls, as suggested by Three). We have listened to stakeholders' concerns around the clarity and specificity of the wording in the CLI Guidance and decided to make various additional changes to the wording to provide further clarity on the type of calls that must be blocked and which calls may fall into a legitimate use case. We have also clarified the circumstances in which providers can be subject to GC C6 and which provider is responsible for checking whether a call falls into a legitimate use case.

3.108    We recognise that the blocking of calls from outside the UK with a UK CLI as a Presentation Number will have an impact on providers and businesses, although the nature and extent of that impact will depend on the size and type of services currently offered by the affected stakeholder. For example, some providers may benefit from the use of more direct routes into the UK, while some businesses might incur higher cost of arranging these routes. Overall, we consider the benefits to UK consumers and businesses of effectively disrupting further scams outweigh any potential implementation costs and we have not identified any less intrusive way to achieve our objective. We also consider any impacts to be mitigated by our proposed implementation timeframe (see paragraphs 3.123 - 3.133 below) and plan to communicate our proposals to the providers and affected businesses through an outreach programme. We therefore consider our intervention to be proportionate.

3.109    For all the reasons set out above, we have decided to proceed with our proposal to amend the CLI Guidance to expect providers to block calls with UK CLI as a Presentation Number except for specified legitimate use cases, subject to the various clarifications outlined above.

3.110    The updated text of paragraph 4.19 is set out in Annex A2, alongside the proposal from our February 2024 consultation.

---

[108] Responses to our 2024 consultation: BT, p.5, Name Withheld 1, p.2, Telecom2, p.2, Three, p.2, TalkTalk, p.3, UK Finance, p.5.

[109] Responses to our 2024 consultation: BT, p.5, FCS, p.3, Telecom2, p.3, TalkTalk, p.3.

3.111    As noted above, providers will be expected to adopt the updated guidance in order to demonstrate their compliance with GC C6.6. We recognise that implementing such measures may be harder for providers with certain business models and have considered this further in our decision on implementation timings below.

# Implementation timings and communications with stakeholders

## What we said

3.112    We said that we consider this to be a small change. In order to protect consumers in good time, while also allowing sufficient time for providers to make necessary changes to their systems, we proposed that the change would take effect six months after the publication of the statement.

## Stakeholder comments

3.113    Seven respondents directly supported the proposed implementation period of six months.[110] One respondent said we should move more quickly[111] and three respondents said a longer implementation period was required.[112] Other respondents provided more general comments on implementation challenges without identifying a specific time period they considered necessary.[113] Some respondents commented that a six month timeframe was feasible or committed to aiming for implementation within six months if required.

3.114    More specifically, UKCTA said its members will work on implementing this solution and hope to meet a six-month deadline.[114] In our engagements with UKCTA, it has said that to ensure the requirements do not have an adverse and costly effect on those businesses, Ofcom needs to widen the communication programme and request information from those businesses who will be most affected by this change.

3.115    Vodafone said that it considered six months to be sufficient to make necessary changes to the gateways in its network. Vodafone also noted the value of having a relatively narrow implementation window, both to provide more certainty for legitimate users and to avoid a situation where scammers could move between different providers who did not implement early. Vodafone did however add that it could not speak for offshore call centres. Although Vodafone supported a six-month implementation period, it noted that providers typically have a network freeze period around the Christmas period which can extend between the week prior to Black Friday until the new year.[115]

3.116    UK Finance said that we should make the change more quickly. It proposed a three-month implementation period to mitigate the harm to potential victims and provided some evidence of the impact of a longer implementation period. It argued for the use of a

---

[110] A consumer, TalkTalk, Vodafone, BT, Telecom2, Sky, UKCTA and Magrathea supported six months.
[111] UK Finance response to the 2024 consultation, p.4.
[112] Responses to the 2024 consultation: CCUK, p3; FCS, p.3; Three, p.2.
[113] Responses to the 2024 consultation: Magrathea, p2; VMO2, p3; Vodafone, p.4.
[114] UKCTA response to the 2024 consultation, p.4.
[115] Vodafone response to the 2024 consultation, p.4.

nimbler process to make changes, saying that the regulatory process from pre-consultation work to implementation timeline, is extensive and onerous. [116]

3.117　Other respondents argued that more than six months may be necessary for implementation. FCS highlighted that implementing Presentation Number blocking may be more difficult for some types of providers, particularly cloud providers. FCS also noted that enterprise customers may have to organise different routing into the UK, as they did for Network Number blocking. Some FCS members have said that this may require longer than a six month implementation period.[117]

3.118　Three said that it was reviewing the options of implementing the proposed changes set out in the consultation with its suppliers, and requested that the timeframe for implementation be extended to nine months.[118]

3.119　CCUK argued for a twelve-month implementation period, saying that six months does not account for certain use cases and may lead to the blocking of legitimate calls. It also said that for providers relying on third parties to manage switching equipment, requests to modify CLI management can take time to schedule. In addition, enterprise customers may need to seek new commercial and technical arrangements outside of any existing contracts in place, which, CCUK said, could have significant time implications.[119]

3.120　We asked CCUK to provide specific examples of the types of calls that would be affected. CCUK subsequently provided two common scenarios:

- An employee of a UK corporation working outside the UK who needs to call clients using their VoIP system, presenting a UK number assigned to their employer. CCUK noted that the proposed rules would require the employer to establish a segmented route to carry these calls.

- A UK entity uses the services of a global cloud communications provider, with an app initiating calls. The call may or may not reside on UK servers, which will call on global communications API endpoints sitting on global cloud services based outside the UK. Therefore, the call origination will be with a cloud service provider outside the UK, although the call will present a valid UK CLI. CCUK noted that this scenario would impact many major UK businesses and brands with significant traffic volumes and the costs of arranging segmentation at this scale would be considerable.

3.121　CCUK also said that many providers are currently consumed with trying to deliver gaining provider-led switching, Voice over IP migration and addressing Telecoms Security Act compliance measures. It said that they simply do not have resources to quickly divert to this issue and that our proposed change does not provide sufficient notice.[120]

3.122　VMO2 said that although it agrees with the proposed solution in principle, it is difficult to assess how long implementation would take with the information currently available.

---

[116] UK Finance response to the 2024 consultation, p.4. It estimated that 50% of impersonation related scams/cases are enabled by telecommunications and would result in 4,250 cases in the additional 3 months.
[117] FCS response to the 2024 consultation, p.3.
[118] Three response to the 2024 consultation, p.2.
[119] CCUK response to the 2024 consultation, p.3.
[120] CCUK response to the 2024 consultation, p.3.

VMO2 noted that a full assessment of timeframes would depend on the full scope of any directive issued by Ofcom. Based upon that, VMO2 said it would request Ofcom remains flexible and works with providers to foster a pragmatic approach to implementation following the publication of any statement.[121]

## Our decision

3.123   We note that stakeholders have expressed a range of views. The most common response was to support six months, with others arguing for a shorter or longer implementation timeframe.

3.124   We recognise the arguments for a shorter implementation window. In particular, the longer implementation takes, the longer that consumers may be exposed to preventable scam calls. We also note Vodafone's point on the benefits of having a short implementation window, to avoid scammers being able to exploit routes with weaker protections against scam calls during implementation.

3.125   On the other hand, we recognise that for the change to be implemented effectively, affected stakeholders need sufficient time. Although we consider it to be a small change, we recognise that some of the changes will need to take place over a period of time, for example to complete administrative changes with suppliers.

3.126   Having followed up with respondents for specific examples of use cases that would require more than six months, we do not think there are any new scenarios that had not been factored into our consultation position. On the further examples provided by CCUK:

- In the use case for a UK employee making calls from outside the UK, we would generally expect the business's provider to already have the capability to recognise when the call is being made by a UK customer who is outside the UK and to segment these calls into a route that is not blocked.

- For the UK entity using the services of a global cloud communications provider, as we explain in paragraph 3.82 we expect cloud voice providers to have the capability to route their calls in a way that their calls with UK CLIs are not blocked.

3.127   To CCUK's point that six months creates an excessive burden in the context of its members currently working through other regulatory work[122], we consider that this is a small change for providers which will deliver tangible protections for consumers. We also note that the changes identified by CCUK have not all been mandated by Ofcom, or have different implementation deadlines.[123]

---

[121] VMO2 response to the 2024 consultation, p.3.

[122] It cited, for example, one Touch Switching, PSTN Switch off and TSR implementation.

[123] For example, One Touch Switching has been a requirement for residential providers since 3 April 2023 – because of industry delays, residential providers are preparing to launch this on 12 September 2024. For PSTN switch off, this process has been led by industry and Ofcom has therefore not set deadlines. Providers have set out their own timescales, depending on how many PSTN lines they have and their customer base. Under the Telecommunications (Security) Act 2021 (TSA), public telecoms providers are required to have measures in place to identify and reduce the risks of security compromises, as well as preparing for any future risks.

3.128    We have also considered relevant precedent. For example, our change to the CLI Guidance announced in 2022 took effect six months after the statement was published, in order to allow providers sufficient time to make the necessary technical changes.[124] These changes came into force in May 2023, and in summer 2023 we asked ten providers if they had implemented these changes. Most of the providers we engaged with were able to make the changes within the six-month implementation period and those that could not meet the implementation period were able to implement the changes soon afterwards.

3.129    To provide further context, we have engaged with international regulators on their approach to implementation timelines for similar regulatory changes and note similar changes have been implemented in similar or shorter periods. For example:

- In Finland, similar changes were announced in May 2022 and took effect in July 2022. Last year Traficom, the Finish communications regulator, said that its change had been "functional and effective".[125]

- In Lithuania, changes were announced in July 2023 and took effect from 1 November 2023.[126]

3.130    Taking into account the written responses to our consultation as well as follow-up conversations with stakeholders that raised concerns, we do not consider it appropriate to allow more than six months for stakeholders to implement our proposal. We have sought specific examples of factors that would require longer to implement, and have not seen any evidence to suggest that Presentation Number blocking cannot be implemented in six months. We consider there are significant benefits to consumers in a shorter implementation period and note that similar proposals (both within and outside the UK) have been implemented in the same or shorter timeframes. We do however recognise that a shorter implementation period may raise challenges for stakeholders, particularly due to the Christmas network freeze period cited by Vodafone.

3.131    For the reasons set out above, we have decided to procced with our proposal for the change to take effect in six months, from 29 January 2025.

3.132    To support effective and widespread implementation, we also consider there will be value in conducting further stakeholder engagement to support industry. Therefore, over the coming months we will conduct a proactive stakeholder engagement programme,

The Electronic Communications (Security Measures) Regulations 2022 (the Regulations) made under the TSA set out specified measures that providers must take and the Secretary of State has published the Telecommunications Security Code of Practice (the Code) to provide guidance for large and medium sized public telecoms providers whose security is most crucial to the effective functioning of the UK's telecoms critical national infrastructure. We note that while the overarching duties in the TSA apply to all public telecoms providers, micro-entities are exempt from the Regulations and the security measures set out in the Code do not apply to smaller, Tier 3 providers. Ofcom's compliance monitoring programme has been designed to gather information from Tier 1 and Tier 2 providers in accordance with the measures and timelines set by Government in the Code, with Tier 1 providers subject to a more intensive level of regulatory oversight.

[124] Ofcom 2022, *Statement: Improving the accuracy of Calling Line Identification (CLI) data.*

[125] Traficom, 22 November 2023.

[126] TN-347 Lithuania's Communications Regulatory Authority's decision on rules on the use of communications numbers.

particularly focused on smaller providers, to remind them of our rules around the provision of accurate CLI information with calls.

3.133    In response to some of the specific points raised on implementation timings, we aim to engage with industry through our Strategic Working Group, through telecoms membership bodies such as CCUK and FCS, and also to liaise with wider relevant business groups whose members may be affected by this work, such as Data and Marketing Association and the Call Centre Management Association.

# A1. Legal Framework

A1.1    This annex provides an overview of the main UK legislative provisions relevant to numbering and this statement.

A1.2    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).

## General duties

A1.3    When making the decisions in this statement 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.

A1.4    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 persons with disabilities, 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.[127] Additionally, Ofcom must have regard to the interests of those consumers in respect of, among other things, quality of service.[128]

A1.5    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).

A1.6    We have also had regard to the Government's Statement of Strategic Priorities in accordance with section 2B of the Act, particularly the Government's commitment to safeguard the interests of telecoms consumers by ensuring they are better protected.

A1.7    Lastly, in accordance with section 108 of the Deregulation Act 2015, we have had regard to the importance of promoting economic growth by exercising our regulatory functions in a way that ensures that regulatory action is taken only when it is needed, and any action taken is proportionate.

## Our functions and powers relating to telephone numbers

---

[127] Section 3(4) of the Act. 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.

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

A1.8    Ofcom also has a general duty under section 63 of the Act in carrying out its telephone numbering functions to, among other things:

- 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
- encourage efficiency and innovation for that purpose.

A1.9    Section 4 of the Act requires us, when carrying out our functions, such as our numbering functions, to act in accordance with the six requirements for regulation which include to promote the interests of all members of the public in the United Kingdom. We consider that this requirement is of particular relevance to the matters under review and that no conflict arises in this regard with any of our general duties in section 3 of the Act.

## Impact assessment

A1.10    Section 7 of the Act requires us to carry out and publish an assessment of the likely impact of implementing a proposal which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities.

A1.11    More generally, impact assessments form part of good policy making and we therefore expect to carry them out in relation to a large majority of our proposals. We use impact assessments to help us understand and assess the potential impact of our policy decisions before we make them. They also help us explain the policy decisions we have decided to take and why we consider those decisions best fulfil our applicable duties and objectives in the least intrusive way. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our proposed decisions.

A1.12    We included our impact assessment in section 3 of our consultation published on 1 February 2024.[129] Taking into account responses to our consultation, we have decided to proceed with our proposal to amend the CLI Guidance to expect providers to block calls with UK CLI as a Presentation Number except for specified legitimate use cases (with various clarifications to the specific wording in our CLI Guidance).

A1.13    In Section 3 of this statement we consider stakeholder comments related to our impact assessment and explain why we still consider that the impact assessment supports our decision to proceed with this change.

A1.14    In summary, we recognise that the blocking of calls coming into the UK with a UK CLI as a Presentation Number will have an impact on providers and businesses, although the nature and extent of that impact will depend on the size and type of services currently offered by the affected stakeholder. For example, some providers may benefit from the use of more direct routes into the UK, while some businesses might incur higher cost of arranging these routes. Overall, we consider the benefits to UK consumers and businesses of effectively disrupting further scams outweigh any potential implementation costs. We have not identified any less intrusive way to achieve our objective and we consider implementing our proposal to be proportionate. We also consider any impacts to be mitigated by our

---

[129] Ofcom, 2024. *Consultation: Tackling scam calls – updating our CLI Guidance to expect providers to block more calls with spoofed numbers*

proposed implementation timeframe and plan to communicate our proposals to the providers and affected businesses through an outreach programme.

## Equality impact assessment

A1.15    We have given careful consideration to whether our decision will have a particular impact on persons sharing protected characteristics (broadly including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. This assessment helps us comply with our duties under the Equality Act 2010 and the Northern Ireland Act 1998.

A1.16    When thinking about equality we think more broadly than persons that share protected characteristics identified in equalities legislation and think about potential impacts on various groups of persons (see paragraph 4.7 of our impact assessment guidance).

A1.17    In particular, section 3(4) of the Act also requires us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:

- the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;

- the needs of persons with disabilities, older persons and persons on low incomes; and

- the different interests of persons in the different parts of the UK, of the different ethnic communities within the UK and of persons living in rural and in urban areas.

A1.18    We examine the potential impact our policy is likely to have on people, depending on their personal circumstances. This also assists us in making sure that we are meeting our principal duty of furthering the interests of citizens and consumers, regardless of their background and identity.

A1.19    By reducing the number of scam calls coming into the UK, we consider that our decision is likely to have a particularly positive impact on groups of persons that may be more susceptible to scam calls (such as more vulnerable or older persons). We have not identified any adverse impacts on specific persons with protected characteristics that are likely to be affected in a different way compared to the general population.

## Welsh language impact assessment

A1.20    The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. Ofcom is required to take Welsh language considerations into account when formulating, reviewing or revising policies which are relevant to Wales (including decisions which are not targeted at Wales specifically but are of interest across the UK).

A1.21    Where the Welsh Language Standards are engaged, we consider the potential impact of a policy decision on (i) opportunities for persons to use the Welsh language; and (ii) treating

the Welsh language no less favourably than the English language. We also consider how a decision could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A1.22    Our decision will affect the telephone number consumers will see calling them and we do not therefore consider our decision will have any impact on our Welsh language obligations. We expect our decision to have a positive impact on all UK customers including Welsh language speakers by disrupting scams and reducing customers' exposure to scam calls. This should minimise the anxiety and emotional distress experienced by victims, including Welsh language speakers.

# A2. Changes to the CLI guidance

A2.1    In our February 2024 consultation, we proposed to update paragraph 4.19 of the CLI Guidance to the following:

> 4.19   As the CLI represents the origin of a call, calls from abroad should not use UK CLI as a Network Number or as a Presentation Number, except in a limited number of use cases:
>
> •       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;
> •       Where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.
>
> Except in these use cases, calls from abroad using UK CLI should be blocked.

A2.2    Having considered the feedback from stakeholders (particularly their concerns around the clarity and specificity of the wording in the CLI Guidance), and for the reasons set out in Section 3 above, we have updated paragraph 4.19 of the CLI Guidance to the following (with changes in bold):

> 4.19   As the CLI represents the origin of a call, calls from **outside the UK (or Crown Dependencies)** should not use UK CLI as a Network Number **or as a Presentation Number**, except in **the** limited number of use cases **identified below**. [130]
>
> **4.19A  Calls from outside the UK (or Crown Dependencies) can present a UK CLI as a Network Number in the following situations:**
>
> •       calls with a CLI from the +447 range. **This is to ensure calls from** UK **(and Crown Dependency)** mobile users roaming **on a non-UK (or non-Crown Dependency) network** making calls back to **+44** numbers **are not blocked**;
> •       Calls to a mobile user who is roaming in the UK **(or Crown Dependencies)**. These are calls to numbers within the Mobile Station Roaming Number (MSRN)/International Roaming (IRN) ranges;[131]

---

[130] **As noted in paragraph 4.16 of the CLI Guidance, for calls originated on networks outside the UK, the responsibility to check the validity of the CLI Data falls on the CP at the first point of ingress to the UK network. This check may be carried out by an international gateway provider or a provider that receives a call into the UK via a direct route. Where a call has entered the UK network through an international gateway provider, we expect the UK provider that first receives the call from the international gateway provider to reassure themselves (for example, via appropriate contractual arrangements) that the international gateway provider has carried out the relevant checks. For further details, please see also paragraph 3.31 of our Statement on Presentation Number Blocking. Ofcom, 2024.** *Statement: Tackling Scam Calls: Updating our CLI Guidance to expect providers to block more calls with spoofed numbers*

[131] A list of these number ranges can be made available on request by email to siwg@ofcom.org.uk. CPs who have such numbers can also submit their number ranges for inclusion using the same email address.

- where **the CP can demonstrate** the traffic has originated on a UK **(or Crown Dependency)** network, **then onward routed outside the UK (or Crown Dependencies) before then re-entering through a UK (or Crown Dependencies) network. This includes calls originating on nodes or cloud services located in the UK (or Crown Dependencies);** or
- where **the CP can demonstrate**[132] the **call is being made by a UK (or Crown Dependency) customer but** has originated **on a non-UK (or non-Crown Dependency) network. This includes traffic** that **is** hosted on nodes or cloud services **outside the UK (or Crown Dependencies)**.

**4.19B    Calls from outside the UK (or the Crown Dependencies) can present a UK CLI as a Presentation Number in the following situation:**

- **where the CP can demonstrate**[133] **the call is being made by a UK (or Crown Dependency) customer but has originated on a non-UK (or non-Crown Dependency) network. This includes traffic that is hosted on nodes or cloud services outside the UK (or Crown Dependencies).**

**4.19C    Some calls may have a UK CLI as both the Network Number and the Presentation Number, in which case all of the use cases will apply.**

**4.19D    Except in these use cases, calls from outside the UK (or Crown Dependencies)** using UK CLI should be blocked.[134]

A2.3    We have also added a definition of UK CLI into the updated CLI Guidance document, in Section A1.

**UK CLI:** CLI associated with a telephone number identified in the National Telephone Numbering Plan.

A2.4    The full revised CLI Guidance can be found here: Annex 2: Guidance on the provision of Calling Line Identification facilities and other related services.

---

[132] **See footnote 130 above. One way in which CPs can demonstrate this legitimate use case applies for calls which use UK CLI as a Network Number is by seeking assurance that the caller is using a number that has been allocated to the originating CP or one that has been ported into the originating CP's network. See also paragraph 3.58 of our Statement on Presentation Number Blocking. Ofcom, 2024.** *Statement: Tackling Scam Calls: Updating our CLI Guidance to expect providers to block more calls with spoofed numbers*

[133] **See footnote 130 above. One way in which CPs can demonstrate this legitimate use case applies for calls which use UK CLI as a Presentation Number is by seeking assurance from the non-UK network that the caller is using a CLI that they have permission to use (either because they have been directly assigned that number or has been given permission by a third party who has been assigned that number). See also paragraph 3.58 of our Statement on Presentation Number Blocking. Ofcom, 2024.** *Statement: Tackling Scam Calls: Updating our CLI Guidance to expect providers to block more calls with spoofed numbers*

[134] The NICC has published guidance in ND1447 about blocking **calls from abroad using UK CLI**.

# A3. Other policy suggestions out of the scope of our consultation

A3.1    Stakeholders commented on other measures to disrupt scams. While we welcome the feedback, we do not consider that these comments affect our decision in this statement. We have nonetheless provided responses below and identified other relevant workstreams.

## DNO list

### Stakeholder comments

A3.2    UK Finance said that the DNO list should become mandatory. It also said that higher-risk numbers linked to impersonation scams (e.g. regulators, county courts, business accounts) should be proactively onboarded to the list. Furthermore, UK Finance said that further overlay services should be utilised to limit calls that slip through gaps due to the technical limitation across some areas of the infrastructure. They also said there should be controls around the claims to numbers, which could potentially extend to stating the types of controls institutions such as banks would want on these numbers.[135]

### Our response

A3.3    Information about adding numbers to the DNO list is available on our website.[136] We welcome submissions from stakeholders, particularly those whose numbers are at high risk of being spoofed and where spoofing has the potential to cause significant consumer harm. At present, it is difficult to set out other controls that providers can have on CLI, particularly where they do not have a commercial relationship with the company making the calls. However, as we set out in our CLI Guidance, the originating provider should ensure that the number that is presented with the call is from a number range that has been allocated to that provider or seek assurance from their customer that they have permission to use that number.

A3.4    We welcome the support of those from other sectors to raise awareness of this list with other organisations within their sectors and consider that they are in a better place to do so through their existing contacts. We will also raise this with our industry stakeholders so that they can also share this with relevant customers.

---

[135] UK Finance response to the 2024 consultation, p.4.
[136] Ofcom, 2023. *Submitting numbers to the 'Do Not Originate' list (ofcom.org.uk).*

# Mobile roaming

## Stakeholder comments

A3.5    UK Finance, VMO2, UKCTA and Sky highlighted the importance of this work.

A3.6    VMO2 said that its overall view was that the goal should always be to eventually achieve a position of having 'no exceptions', as any exception would quickly become known to spoofers/scammers, with the numbers then becoming the target for continued spoofed call ingress. VMO2 said that it is aware that, in order to achieve this goal, a solution for +447 must be defined, noting Ofcom's work in this area.[137]

A3.7    UK Finance proposed that it would be beneficial (where technically possible) to require ingress carriers to confirm (if not done already) with UK Mobile Operators that the mobile number was indeed registered with the operator as being out of the UK. UK Finance added that calls that are routed into the UK from abroad, and cannot be verified as truly registered as roaming, should be either blocked or have the Network CLI amended to a specific Ofcom range to allow consuming parties to make risk-scored decisions about whether to accept the call, or to place it into a higher risk category. UK Finance noted that this would be problematic without appropriate verification services offered by UK Mobile Operators, or the underlying network operator.[138]

A3.8    UKCTA said that it supports Ofcom in identifying the different options to ensure that legitimate roaming calls are not being impacted by any potential interventions.[139]

A3.9    Sky highlighted the importance of being able to distinguish between calls that are from UK callers roaming abroad, and said that it would continue to engage with NICC to manage further changes in this space.[140]

## Our response

A3.10   We agree that this is an important area of work and have published a call for input on spoofed UK mobile numbers alongside this statement. [141]

# Common numbering database

## Stakeholder comments

A3.11   Magrathea said the introduction of a common numbering database (CDB) would significantly improve what tools telecommunications providers can use in relation to number management and CLI handling. Magrathea said that this, combined with general improvements in data management, should bring about some improvements in how industry manage bad actors and share information.[142]

---

[137] VMO2 response to the 2024 consultation, p.2.
[138] UK Finance response  to the 2024 consultation, p.3.
[139] UKCTA response to the 2024 consultation, p.3.
[140] Sky response to the 2024 consultation, p.2.
[141] Ofcom. 2024. *Call for Input: reducing scam calls from abroad which spoof UK mobile numbers*
[142] Magrathea response to the 2024 consultation, p.2.

A3.12    FCS said that it believes that the CDB could aid compliance and reduce scam calls and suggested that Ofcom reviews its approach to the CDB. FCS highlighted that NICC has already specified a CDB definition, but further work is required before implementation.[143]

A3.13    One consumer said that they would like Ofcom to consider making the telecommunications companies responsible for registering *all* telephone numbers to an individual or organisation so that in the event of scamming or other illegal activities the "owner" can be sanctioned (blocked).[144]

## Our response

A3.14    As we explained in our 2022 CLI Authentication consultation, establishing a common numbering database would be a significant programme of work.[145] Industry would need to agree on the requirements, design and architecture of the database and a funding and administration model would also be needed. It would also require further work to populate the database with initial data, as there is currently no centralised source of up to date information about telephone number use in the UK. The work required to ensure that the database contains accurate information on telephone numbers is likely to be a complex and resource-intensive process. Instead, we are focusing our efforts on more targeted initiatives to target specific types of CLI spoofing, such as our decision on blocking calls from outside the UK presenting a UK CLI as a Presentation Number and exploring ways to identify calls from UK users roaming abroad, to further limit the spoofing of +447 numbers from abroad.

# CLI authentication

## Stakeholder comments

A3.15    A number of stakeholders noted their support of our approach to CLI authentication, as set out in our February 2024 statement.[146] UK Finance noted its disappointment at the move away from CLI authentication at the moment. UK Finance said in the absence of CLI authentication, there needs to be a more robust and layered approach to the controls being required to protect the public from the harm caused by call spoofing.[147]

## Our response

A3.16    As we set out in our February 2024 assessment of CLI authentication, although we believe CLI authentication has the potential to be an effective tool in preventing some harmful calls from spoofed numbers, we did not think we should proceed with CLI authentication at this time. This was because CLI authentication on its own would not adequately address the risk of calls from abroad spoofing UK numbers and calls from overseas with international numbers are unlikely to be fully verified. We also thought that CLI authentication would be complex, costly and time-consuming to implement. Instead, and as discussed in this document, we have focus on initiatives which will seek to address the

---

[143] FCS response to the 2024 consultation, p.2.
[144] Name withheld 1 response to the 2024 consultation, p.2.
[145] Ofcom, 2022. *Consultation: Calling Line Identification (CLI) authentication: A potential approach to detecting and blocking spoofed numbers.*
[146] Ofcom, 2024. *Calling Line Identification (CLI) authentication assessment update and future roadmap.*
[147] UK Finance response to the 2024 consultation, p.1.

harm in the near term, including further work to explore the blocking of calls from abroad spoofing a UK mobile number[148] and our enforcement programme on phone and text scams.[149] interpreta

# Checks on the use of numbers

## Stakeholder comments

A3.17    UK Finance noted that if criminals are unable to leverage vulnerabilities they will migrate to acquiring or taking over existing legitimate services. They urged Ofcom to reconsider their previous recommendations in response to the consultation on the "Good practice guide to help prevent misuse of sub-allocated and assigned numbers".[150]

## Our response

A3.18    We encourage providers to carry out the relevant due diligence checks. As we set out in the Good Practice Guide, providers should know who they are sub-allocating or assigning numbers to.[151]  We also request information from applicants to assess their eligibility to be allocated telephone numbers directly from Ofcom.

# Call tracing

## Stakeholder comments

A3.19    UK Finance said that due to privacy restrictions, albeit important, the threshold for law enforcement to trace a call is too high. Furthermore, ideally, there would need to be the ability to harvest data attached to the calls to show the VoIP provider and the source of the call itself, e.g., IP address. UK Finance argued for enhanced capability for providers to support institutions such as banks in investigating fraud attacks. UK Finance said that this could include the capability, in conjunction with Ofcom, to be able to bring a 'fraud investigation' ticket to the supplying provider. Then for them to be required to investigate this and any upstream providers to be compelled as part of their licence to investigate and supply data back down to enable an organisation to understand/investigate where attacks are originating.[152]

A3.20    UKCTA said that it strongly supports our proposal to explore enhanced call tracing solutions in order to identify and tackle fraudulent calls at the source.[153]

---

[148] Ofcom. 2024. *Call for Input: reducing scam calls from abroad which spoof UK mobile numbers*
[149] Ofcom, 2024. *Enforcement programme into phone and text scams*.
[150] UK Finance response to the 2024 consultation, p.3.
[151] Ofcom, 2022. *Good practice guide to help prevent misuse of sub-allocated and assigned numbers (the Good Practice Guide).*
[152] UK Finance response to the 2024 consultation, p.4.
[153] UKCTA response to the 2024 consultation, p.3.

### Our response

A3.21    We are currently exploring suitable approaches for call tracing as well as the associated enforcement options that may apply.  We shall provide an update in due course.

## Monitoring service provider traffic and better collaboration between sectors

### Stakeholder comments

A3.22    Magrathea noted that it is championing a new initiative, raised in February 2023 with the ICO, whereby carrier networks could use Telephone Preference Service (TPS) data to retrospectively monitor service provider traffic, enabling rapid investigation of potential bad behaviour. Magrathea said that although this is not something that will solve the problems by itself, it would be another tool to tackle scams. Magrathea said it is now apparent that regulatory and government support will be required to bring about the changes needed to allow the ICO to support this initiative.[154]

A3.23    UK Finance noted that they saw a need for further incentivisation on telecoms to encourage further behaviour change as well as increased transparency. They noted a fundamental need for a more equitable approach to collaborative mitigation, explaining that where there had been solutions between financial services and telecoms, paywalls have been put in place.[155]

### Our response

A3.24    We agree that collaboration and information sharing between stakeholders including Government, industry, law enforcement, regulators and others is important to tackle the threat of scams. We promote collaboration in a number of ways, including hosting the Strategic Working Group to share data. As described above, we intend to engage further with industry to support implementation of our new Presentation Number blocking rules and our wider work on CLI. We also welcome discussion of further initiatives with stakeholders, recognising the benefits of having a range of tools to tackle scam calls.

## SMS measures

### Stakeholder comments

A3.25    BT highlighted its rollout of a new SMS anti-spam filter which it says has blocked more than 285m scam texts, leading to an 85% overall reduction in EE customers reporting spam messages to BT.[156]

A3.26    UK Finance noted that the spoofing of brands on SMS continues to impact businesses not onboarded to the Mobile Ecosystem Forum (MEF) SenderID Registry, resulting in additional victims and money flowing to criminals. It said that the SenderID Registry needs to be mandated for all SMS suppliers.[157]

---

[154] Magrathea response to the 2024 consultation, p.2.
[155] UK Finance response to the 2024 consultation, p.3.
[156] BT response to the 2024 consultation, p.2.
[157] UK Finance response to the 2024 consultation, p.3.

## Our response

A3.27    Alongside this statement, we have published a Call for Input on mobile messaging scams.[158] This sets out the evidence we have reviewed on the scale and nature of messaging scams, as well as measures being taken to prevent them in the UK and internationally. The Call for Input includes discussion on measures to filter SMS messages and to protect Sender IDs. We aim to provide an update on our work on messaging scams by Spring 2025, including a view whether further act

---

[158] Ofcom, 2024. *Call for input: Reducing mobile messaging scams*.