Calling Line Identification (CLI) authentication assessment and future roadmap

Welsh overview available

Published 1 February 2024

Contents

Section

1. Overview

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

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

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

1.3 In April 2023, we consulted on a possible approach that could enable providers to detect and block calls from spoofed numbers more comprehensively.[1] This would involve the network originating the call, where technically possible, confirming the validity of the caller's telephone number before passing that confirmation to the network of the person receiving the call. This would mean that the person receiving the call would be assured that an incoming call is legitimate. We referred to this as 'Calling Line Identification (CLI) authentication'.

1.4 The April 2023 consultation did not make any specific proposals for the introduction of CLI authentication. Instead, we sought views from stakeholders on our initial thinking about how CLI authentication could work and the extent to which other measures could be sufficient in addressing the problem of number spoofing. We invited comments from stakeholders both to enable us to assess the workability of our proposals, and to enable us to formulate detailed proposals for implementation, in the event that we considered such proposals to be appropriate.

1.5 We have assessed the workability of CLI authentication, taking into account responses to our consultation. We have particularly considered:

- the potential effectiveness of CLI authentication in preventing scams;
- how CLI authentication would be monitored and enforced; and
- barriers to the implementation of CLI authentication.

1.6 Although, overall, we believe that CLI authentication has potential to be an effective tool in preventing some harmful calls from spoofed numbers, our **assessment is that we should not proceed with CLI authentication at this time.** This is because:

- Calls arriving from overseas displaying international numbers are unlikely to be fully verified. This is because overseas operators are not obliged to follow our rules on verification. To help address this issue, we proposed a process called 'gateway

[1] Ofcom, 2023. Calling Line Identification (CLI) Authentication: a potential approach to detecting and blocking spoofed numbers.

attestation' which would mean that, although the number associated with the call itself could not be verified, it would be possible to identify the operator who first introduced the call into the UK public telephone network. However, there is a risk that this approach is unlikely to sufficiently hinder scam calls that originate overseas, undermining the effectiveness of CLI authentication.

- CLI Authentication on its own would not adequately address the risk of calls from abroad spoofing UK mobile numbers. This means there would be a need for a complementary process, running alongside CLI authentication, to ensure that calls from abroad displaying UK mobile numbers are from genuine UK roamers. Without this process, CLI authentication alone would not adequately address the problem of inbound calls spoofing UK mobile numbers.
- CLI authentication would be complex, costly and time-consuming to implement. We believe that alternative measures may have the potential to reduce number spoofing effectively and more quickly.

1.7 Given the scale of harm from spoofed scam calls, we will progress a series of initiatives which will seek to address this harm in the near term. These are set out below.

Summary of initiatives

- **Updating our guidance to block calls with spoofed UK geographic and non-geographic Presentation Numbers.** We already require operators to identify calls from abroad which are spoofing UK geographic and non-geographic Network Numbers and to block them. We are proposing to update our rules to require blocking of calls from abroad which spoof UK geographic and non-geographic Presentation Numbers (the number that the call recipient sees) and have published a consultation in parallel with this update.[2]

- **Exploring the blocking of calls from abroad spoofing a UK mobile number**: There is a need to be able to distinguish between calls that are from UK callers roaming abroad phoning back into their home country and calls that are spoofing UK mobile numbers. We have therefore begun to explore the available options for identifying genuine mobile roamers, including measures introduced by other jurisdictions, and will assess the anticipated benefits and challenges. If we are able to identify a potential solution to validate legitimate roaming calls, we will consult on these options in due course.

- **Monitoring compliance with our rules under an enforcement programme.** We have opened an enforcement programme focused on identifying and preventing individual telecoms providers who allow scam and spoofed voice calls to enter the UK's telephony system.[3] This will include making use of our good practice guide, which was introduced to set out our expectations on the steps we expect providers to take to help prevent the misuse of telephone numbers.[4] As the guide has been in place for over a year, one of the aims of this enforcement programme will be to see how well this guide has been implemented.

- **Exploring enhanced call tracing solutions.** The ability to quickly identify the source of fraudulent calls is key to reducing the impact of scams. We will continue to work with

[2] Ofcom, 2024. Consultation: Tackling scam calls – expecting providers to block more calls with spoofed numbers.

[3] Ofcom, 2024. Enforcement programme into phone and text scams.

[4] Ofcom, 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

industry to improve call tracing processes to help speed up the process of identifying operators who are allowing the origination and/or transit of fraudulent traffic.

- **Industry and international monitoring.** We will monitor the impact of industry's own voluntary measures on scams and actively participate in international bodies to explore cross-border coordination to block scam calls.

1.8 We may still choose to re-examine CLI authentication at a later date, especially if our initiatives and industry measures do not result in a timely reduction in scam calls.

1.9 Our consultation to further tightening our rules to block calls with spoofed UK geographic and non-geographic numbers will close on 28 March 2024. In the meantime, we will progress all other initiatives.

2. Background

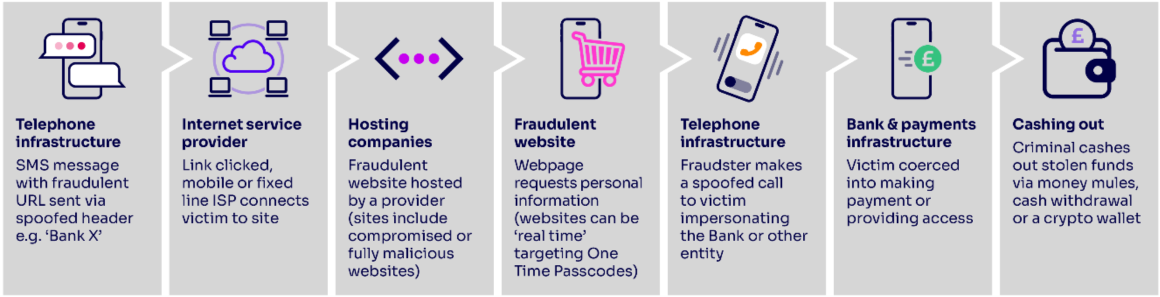
2.1 In our April 2023 consultation, we set out the scope and scale of the harm caused by scams which are facilitated by phone calls. We noted the increasing complexity of scams, which may involve more than one communication channel, and the financial and emotional impact of scams on individual and business consumers. In this section, we provide an update on the evidence base for the harm caused by scams, particularly scam calls, and we set out our strategic objectives for tackling scams more broadly. We also provide an update on international and other developments that have taken place since we published our April 2023 consultation.

How scams happen and why they are becoming more complex

2.2 In our April 2023 consultation, we explained that voice calls are one of a range of channels which are used by scammers to manipulate people into divulging personal details or transferring money.[5] Other tactics can include the use of text messages, email, fake websites, and social media posts, to obtain personal details and passwords which are then used to trick the victim into authorising payments.

2.3 While the majority of scams start online, phone calls can play a significant role even where first contact is made through other means. For example, a malicious SMS or email might lead the recipient to a fraudulent website (used to obtain information about the victim) and the scammer may then contact the victim by phone (e.g. impersonating their bank) to request a payment.[6]

Figure 1: An illustrative fraud chain


Telephone infrastructure
SMS message with fraudulent URL sent via spoofed header e.g. 'Bank X'
Internet service provider
Link clicked, mobile or fixed line ISP connects victim to site
Hosting companies
Fraudulent website hosted by a provider (sites include compromised or fully malicious websites)
Fraudulent website
Webpage requests personal information (websites can be 'real time' targeting One Time Passcodes)
Telephone infrastructure
Fraudster makes a spoofed call to victim impersonating the Bank or other entity
Bank & payments infrastructure
Victim coerced into making payment or providing access
Cashing out
Criminal cashes out stolen funds via money mules, cash withdrawal or a crypto wallet

Number spoofing, which can enable successful impersonation, is a significant driver of scam calls

2.4 Modern telephony systems allow a caller to modify or hide the phone number that the caller is calling from, through the data that is attached to each call, which is known as Calling Line

[5] Ofcom, April 2023. CLI Authentication Consultation, paragraphs 3.28 – 3.30.

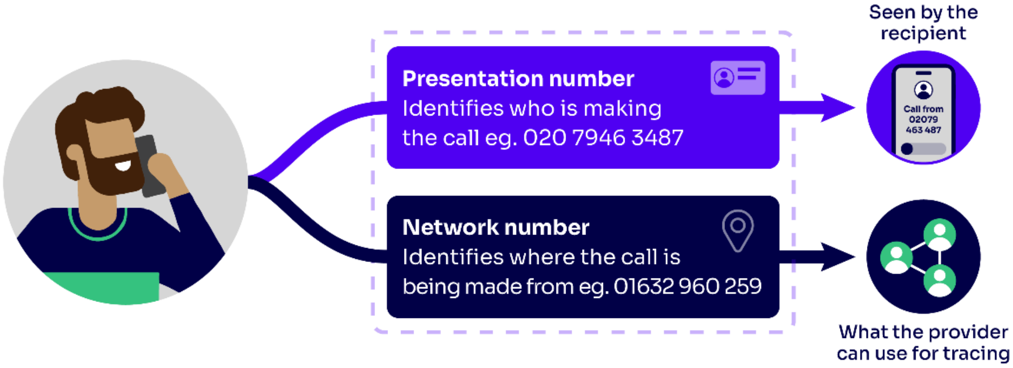
[6] Frontier Economics 2022. Frontier Economics, 2022. Tackling Fraud and Scams: An Ecosystem-Wide Approach, pp. 13-14.

Identification (CLI) data. There can be legitimate and beneficial reasons for businesses to use this technology.

2.5 CLI data refers to the contents of the signalling messages, which are used between providers and/or between a provider and an end user, to signal the point of origin of the call and/or the identity of the calling party. This includes any associated privacy markings, which indicate whether the number can be shared with the recipient of the call or whether it is withheld.

2.6 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.[7]

Figure 2: Presentation Number and Network Number


Seen by the recipient
Presentation number
Identifies who is making the call eg. 020 7946 3487
Call from 02079 463 487
Network number
Identifies where the call is being made from eg. 01632 960 259
What the provider can use for tracing

2.7 The Presentation Number can help recipients decide if they wish to answer the call (or return a missed call), or not (for example, it may indicate that it is a family member calling, or a child's school).

2.8 In most cases, the Presentation Number will be the same as the Network Number, but in some calls it will be different. Examples of legitimate reasons why a caller would choose to display a phone number (the Presentation Number) different to the Network Number include:

- call centres making calls on behalf of one or more different businesses;
- businesses or public bodies that wish to display a common contact number (e.g. a freephone number that customers may use to call back) for calls made from different locations; and
- professionals who wish to display a business number when calling from a private line.

Misuse of CLI data contributes to the prevalence of scam calls

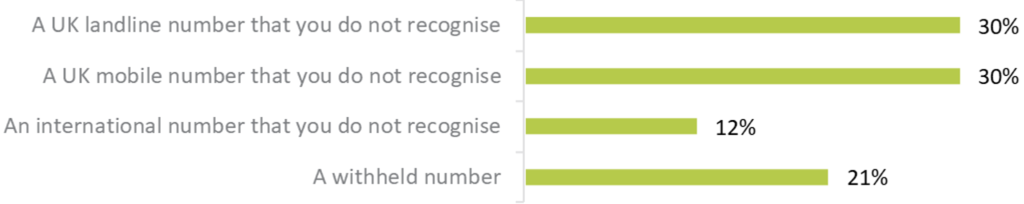
2.9 However, because phone calls enable high-quality one-to-one interactions, scammers can go to great lengths to pretend to be from well-known organisations.[8] They may make use of number spoofing to add to the apparent legitimacy of the scam call.

[7] Presentation and Network Number are legacy terms which typically correlate to the FROM and P-Asserted-Identity header field (RFC 3325) in SIP respectively. The legacy terms are used in this document to aid readability.

[8] Communications Consumer Panel (CCP), December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, Table 52.

2.10 Our 2022 consumer research showed that mobile users (and landline users with a handset that features a caller display) who at least sometimes look at the caller's number before deciding whether to answer a call are markedly more likely to answer calls when they recognise the number displayed.[9]

Figure 3: Likelihood of answering calls from different types of numbers



Source: Ofcom CLI and Scams Consumer Research 2022. Figures reflect the percentage of respondents answering 4 or 5 on a scale from 1 (very unlikely) to 5 (very likely).
Base: All who always/usually/sometimes decide whether to answer by looking at the number on the handset, N=1869.

Scam calls result in significant harm to consumers

2.11 As noted in our April 2023 consultation, fraud is a complex and widespread source of acute consumer harm, and accounts for over 40% of all reported crime incidents in England and Wales.[10] While online fraud, particularly fraudulent advertising, accounts for the majority of scams by volume, scams originating on telecommunications networks tend to be higher value overall.[11] There is evidence that the financial and emotional harm caused to individual victims is substantial. Scams also harm businesses and the wider economy.

Many consumers continue to be affected by scam calls

2.12 For many consumers, phone calls continue to be an important method of contacting friends and family, supplementing and enriching other methods (such as messaging).[12] Phone calls are also an important tool for businesses.

2.13 In 2024, we conducted research to inform our understanding of suspicious calls, texts and online activity. Our research found that suspicious calls affect the majority of internet users in the UK, and that at the time the research was conducted in January 2024:

- 24% of those with a mobile phone claimed to receive a suspicious call either every day or at least once a week; and

[9] Ofcom CLI and Scams Consumer Research 2022, Data Tables, table 49.
[10] UK Finance, 2023. Annual Fraud Report, p.3.
[11] More than 200,000 cases of authorised push payment (APP) fraud were reported in 2022. Push payment fraud is a scam in which a victim is tricked into making bank transfers to an account pretending to be a legitimate payee. These cases led to financial losses of £485m; while only 18% of those cases originated via telecommunications networks (voice calls or SMS), these accounted for an estimated 44% of the total losses. UK Finance, 2023. Annual Fraud Report, pp.47 – 49.
[12] Futuresight research commissioned for Ofcom, 2020. Declining Calls and Changing Behaviour. The report notes that "Like face-to-face communication, voice communication was regarded universally as fundamental. It was seen, across the sample, as essential in itself, as a primary method of communication and means of contact, but also as a primary means to supplement, qualify and enrich message communication", p.28.

- 27% of landline users claimed to receive a suspicious call either every day or at least once a week.[13]

2.14 The prevalence of scam calls and other unwanted calls leads to many calls going unanswered. Our 2022 research into suspicious calls and texts found that a majority of consumers do not always answer the phone, even when they could easily do so.[14] When asked for the reason for not answering, the top option selected by those respondents was "I don't want to deal with marketing calls/ spam/suspicious callers".[15] Where this leads to calls being declined even when they are legitimate, it may undermine the effectiveness and efficiency of the telephony system.

Scam calls can have a significant financial and emotional impact on victims

2.15 In our April 2023 consultation, we detailed the financial impact of scam calls, and the wider impact and harm on individuals and businesses from scam calls. We also explained the harm caused by other types of unlawful calls such as unlawful nuisance calls and malicious calls.[16]

2.16 Successful scams can cause significant financial and emotional harm, while even attempted scams are annoying and can cause substantial anxiety for recipients. Scams also impose costs on the wider economy, including the resources spent by businesses to support customers that fall victim to fraud.

2.17 Individual financial losses from scams involving voice calls can vary significantly from case to case. The Communications Consumer Panel (CCP) conducted research in 2020 which estimated a median loss of around £300 among victims of scam calls, with 28% of victims having lost more than £500.[17] Although financial losses typically affect victims of scams in the first instance, some will receive reimbursement at the expense of financial institutions. UK Finance estimates that around 66% of the losses to Authorised Push Payment (APP) fraud across all communications channels, in cases which were assessed and closed in 2022, were returned to victims.[18] Significant financial losses are therefore still borne by the victims of these scams.

2.18 Businesses are also significantly affected by scams. In 2022, APP scams which targeted non-personal or business accounts constituted only 3% of all successful APP scams (6,729 out of 207,372 cases), but they accounted for 16% of losses in terms of value.[19]

[13] Ofcom 2024. Ofcom joint online, calls and texts fraud research 2024, slide 8.

[14] Ofcom 2022. Ofcom CLI and Scams Consumer Research 2022. (60% of landline users and 70% of mobile users.) table 5/table 28.

[15] Ofcom 2022. Ofcom CLI and Scams Consumer Research 2022. (Chosen by 69% of these landline users and 74% of these mobile users.) table 9 / table 31.

[16] Ofcom, April 2023. CLI Authentication Consultation, paragraphs 3.50 – 3.66.

[17] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, pages 4 and 10.

[18] UK Finance, 2023. Annual Fraud Report, p.51. Authorised push payment (APP) fraud is a scam in which a victim is tricked into making bank transfers to an account pretending to be a legitimate payee. APP scams tend to fall into eight categories: malicious payee (purchase scam, investment scam, romance scam and advance fee scam) and malicious redirection (invoice and mandate scam, CEO fraud, impersonation: police/bank staff and impersonation: other).

[19] UK Finance, 2023. Annual Fraud Report, p.47.

Wider impact of scam calls

2.19 For consumers who fall victim to a scam, there may be a need to spend time and money to put their affairs in order, report the crime and seek compensation. Direct financial losses can also have knock-on impacts; for example, research shows that victims may lose some or all of their savings, go into debt, or lack money for essentials.[20]

2.20 Scams and their repercussions can also lead to emotional harm. Research by the European Commission has suggested that this occurs in 79% of cases,[21] while research by the CCP also identified common feelings of embarrassment, loss of self-belief, anger, anxiety, isolation and helplessness.[22] A study commissioned by Which? found evidence of significant harm to a victim's wellbeing, which is estimated to outweigh the financial loss on average.[23]

2.21 For businesses or other organisations impersonated by scammers, scam calls could entail both reputational impacts and financial costs of dealing with customer cases or implementing measures that seek to prevent fraud.[24] For example, banking and payments organisations are investing in various measures to reduce the impact of fraud, including security systems, training and customer education campaigns.[25]

Our aims and objectives in tackling scams

2.22 Given the pace at which scammers change their tactics, we understand that it will not be possible to stop all scams reaching consumers, and there is no single intervention or measure which will eliminate scam calls completely. As we set out in our February 2022 statement, our strategy to counter scam calls seeks to make it harder for scammers to operate at every stage of the value chain.[26] We aim to achieve this by focusing on three key areas of intervention:

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

[20] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, pp.11–13.

[21] Ipsos for the European Commission, 2020. Survey on "scams and fraud experienced by consumers".

[22] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, p.3 and pp.10–13.

[23] Which? and Simetrica Jacobs, 2022, Scams and subjective wellbeing. The study estimates that the harm to each victim's wellbeing can be valued as £2,509 on average, with a 95% confidence interval of £438 to £4,732. Note that this average reflects all types of scams and may include scams not enabled by telephone.

[24] Survey evidence shows that, of those consumers who know they got a call from someone impersonating a legitimate business, 22% reported having decreased trust in the security of that business. Hiya, State of the Call 2022.

[25] UK Finance Press Release, Cross-sector action needed as criminal gangs steal more than £1.3 billion - Notes to Editor, point 4.

[26] Ofcom, 2022. Tackling scam calls and texts: Ofcom's role and approach.

- **Informing consumers:** We are working to help consumers to avoid scams by raising awareness and understanding, so that people can more easily spot and report them.

We have developed and implemented a range of measures to help combat scam calls

2.23 We have worked with industry and government stakeholders to develop and implement several measures to make it harder for scammers to succeed across the scams value chain, and to reduce scam calls and texts.

"Do not originate" list

2.24 We have worked with UK Finance and the Strategic Working Group (SWG) to develop the "Do Not Originate" (DNO) list.[27] This is a list of numbers which consumer-facing organisations (for example, banks and government bodies) make available for people to call them on, but which are not used by the organisation to make outgoing calls. These numbers are sometimes spoofed by scammers claiming to be calling from the organisation they are imitating. They are frequently found on, for example, the reverse of bank cards.

2.25 In 2019, we began sharing this DNO list with telecommunications providers, intermediaries, and other relevant stakeholders (for example, call blocking and filtering services) so that outgoing calls appearing to be from these numbers could be blocked. Since 2019, we have received increasing volumes of requests for numbers to be added to the list. Organisations with numbers on the list, such as HMRC, have reported decreased volumes of impersonation scams using their numbers.[28]

2.26 We updated our guidance for submitting numbers in 2022, to clarify use of the scheme and to provide further information on its limitations.[29]

Improving the accuracy of CLI

2.27 We have introduced new rules and guidance to require providers, where possible, to detect and block spoofed numbers and to make it harder for scammers to access valid numbers.[30] While we expect these changes to have an impact on the capability of scammers to reach victims, the extent of this impact is limited by technical factors. These requirements took effect on 15 May 2023.

Detecting and blocking spoofed numbers

2.28 Our rules already required originating providers to ensure that accurate CLI data was provided with a call. Transit and terminating providers are expected to check that the number provided with a call is from a valid number range. However, changes in technology have made it easier for scammers to manipulate this data to spoof numbers. This includes scammers who are based abroad using spoofed numbers to make it look like they are calling from the UK.

[27] Further information on the role of the SWG can be found in paragraph 2.7 of Tackling scam calls and texts: Ofcom's role and approach.
[28] HMRC, June 2019. Controls prevent phone fraudsters spoofing HMRC.
[29] Ofcom, February 2022. Submitting Numbers to the 'Do Not Originate' list.
[30] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data.

2.29 While not all spoofed numbers can be detected, some are easier to spot. This might be because they are numbers that have not been allocated for use to anyone or where a UK number has been used, in some situations, in a call which originated abroad. We therefore strengthened our rules and guidance, so that providers do more to block spoofed numbers, by modifying our General Condition (GC) C6.[31] We have added the requirement for providers to identify and block calls where the CLI does not "uniquely identify the caller", where this is technically feasible.[32] Spoofed numbers, even when they appear valid and dialable, will not uniquely identify the caller because the person spoofing the call does not have authority to use the number.

2.30 Without CLI authentication, it is not possible for providers to validate every individual CLI. However, in our November 2022 Statement, we noted that there are technically feasible steps that can be taken by transit and terminating providers to check whether a number can be used for outbound calls, for example using the DNO list and checking whether a number has been allocated for use.

2.31 We have also issued revised guidance on how providers could validate the telephone numbers of a call.[33] This guidance includes:

- clarifying that the format of a CLI should be a 10- or 11-digit number;
- making use of information that identifies numbers which should not be used as CLI, such as Ofcom's numbering allocation information and the DNO list;
- identifying calls originating abroad that do not have valid CLI and blocking them;
- identifying and blocking calls from abroad spoofing UK CLI (discussed below); and
- prohibiting the use of 09 non-geographic numbers as CLI.

Blocking of international calls with UK Network Numbers

2.32 In 2021, the NICC published industry guidance aimed at UK operators that receive calls with a UK CLI (as a Network Number) from a non-UK interconnect.[34] The guidance (ND1447) identified the limited number of legitimate use cases where a UK CLI may be used as a Network Number from abroad and encouraged operators to block other calls coming from abroad displaying a UK number, potentially with the intention of misleading UK consumers and thus increasing the likelihood that they answer the call.

2.33 We also made changes to our rules and guidance on the provision of CLI facilities more generally. These changes included the addition of an expectation in our guidance that telecoms providers should block calls from abroad which use a UK CLI as a Network Number, except in a number of specified use cases, referring to the examples set out in ND1447. The limited exceptions include calls from UK mobile users roaming overseas when making calls back to UK numbers.

2.34 We recognise that the implementation of ND1447 and the associated changes to our CLI guidance, while important interventions in tackling number spoofing, do not address all potential scam call scenarios. For example:

[31] Ofcom, General Conditions of Entitlement, Condition C6.

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

[33] Ofcom, November 2022. Statement: Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

[34] NICC, April 2021. Guidance on blocking of inbound international calls with UK Network Number as CLI ('ND1447'). The NICC is the UK telecommunications network and service interoperability standards body.

- Scammers calling from abroad could bypass this measure by using a UK CLI as a Presentation Number, or by using a mobile CLI (these are exempted from blocking due to the need to allow for mobile roaming by UK residents while abroad).
- Although UK providers are required to comply with GC C6.4 and to ensure that the caller is using a number which they have permission to use, some CPs may be non-compliant and permit spoofing on their network. As noted above, it is not currently possible to validate every individual CLI and therefore some calls with spoofed CLI can still be connected to the recipient.
- Scammers calling from abroad may seek to bypass this measure by routing calls via interconnect points that are supposed to be used exclusively for domestic interconnects (that is between providers within the UK for the transit of domestic calls), in a way that does not enable them to be readily identified as an international call.). This means that some international calls that should have been blocked could potentially be allowed to enter the provider's network through these routes.

Research into the impact of voice scams

2.35 We will continue to conduct research into the incidence and effects of call and text scams to help us monitor the impact of work that we and others are doing, including where to focus our efforts as scammers evolve their tactics. Our research will also continue to inform further work to raise awareness of scams and the steps people can take to protect themselves.

International and other developments

2.36 In the April 2023 Consultation we summarised various international developments that sought to provide a mechanism by which the terminating network can have assurance that the CLI data received, along with a call, has been input by a known party, and has not been tampered with in transmission. In particular, we highlighted how the US and Canada had introduced a standard known as SHAKEN/STIR.[35]

2.37 Since publishing the April 2023 Consultation, we have seen the following developments which are directly related to CLI authentication:

- In the USA, the Federal Communications Commission (FCC) has adjusted its rules relating to CLI authentication. This includes extending traceback provisions, introducing a Do Not Originate list, and requiring terminating providers to offer analytics-based blocking solutions.[36] In addition, according to a consultancy, the FCC now requires "non-gateway intermediate providers that receive unauthenticated calls directly from an originating provider" to add their own authentication, before passing the call further into the network.[37]

[35] SHAKEN/STIR refers to a set of standards collectively known as Secure Telephone Identity Revisited (STIR)108 has been developed to support the conveyance of the information along with the call109 b) A framework for deployment of STIR known as 'Signature based Handling of Asserted information using toKENs' (SHAKEN).

[36] FCC, April 2023. Combatting Illegal Robocalls Factsheet.

[37] See press release from Award Consulting, March 2023. You may need to update your Robocall Mitigation Plan - Award Consulting.

- In June 2023, the Irish telecoms regulator, the Commission for Communications Regulation (ComReg), said that they would not be proposing to adopt the STIR/SHAKEN model of CLI authentication. This was announced as part of a broader consultation on measures to address calls from spoofed numbers and text message scams.[38]
- In France, the formal deadline for implementing SHAKEN/STIR passed in June 2023. However, media reports have indicated that the rules will not currently be enforced, thereby allowing more time for implementation.[39]
- Internationally, the i3 forum-led "One Consortium" Initiative has been established, with the goal of ’of restoring trust in international communications’.[40] This consortium is still in the planning stage of activity.

2.38 There have also been some significant developments in relation to countering scam calls within the UK:

- In May 2023 the UK Government launched its Fraud Strategy, which aims to reduce fraud by 10% in 2024 from 2019 levels, and will be delivered in partnership with government departments, government agencies, law enforcement, and private sector stakeholders.[41] The strategy will focus on blocking scams at source, identifying scammers, and, where possible, pursuing them regardless of jurisdiction.
- Since May 2023, UK operators who sub-allocate numbers to business customers must carry out appropriate due diligence checks to understand the customer to which they intend to make an allocation and to minimise the risk of number misuse. Such checks should also make it easier to trace the user of a number that is associated with specific scam calls. This is important because the UK has a very long tail of operators who “lease” numbers from other operators, and identifying the current user of a number is not straightforward.[42]

[38] Commission for Communications Regulation, June 2023. Consultation on combatting Nuisance Communications. Specifically, ComReg highlighted that they would not adopt the STIR/SHAKEN model of CLI and it requires the adoption of IP-based networks to work. ComReg noted they may revisit the use of STIRSHAKEN, particularly if their other proposed interventions fail to deliver in a timely and effective fashion. (paragraphs 4.49 – 4.54).

[39] Commsrisk.com, December 2023, French Telcos Are Breaking the Law Today, and STIR/SHAKEN Is to Blame.

[40] See https://i3forum.org/restore-trust.

[41] See https://www.gov.uk/government/publications/fraud-strategy.

[42] Ofcom, February 2022. Statement: Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

3. Calling Line Identification authentication: our assessment

Introduction: the 2023 CLI authentication consultation

3.1 In April 2023, we issued a consultation inviting views on the potential introduction of CLI authentication to UK networks (‘the 2023 consultation’).[43] We noted that the emergence of CLI authentication in other countries, and the fact that UK providers are moving from Public Switched Telephone Network (PSTN) services to Voice over IP (VoIP) to carry calls, meant that there was an opportunity to consider whether CLI authentication could result in a reduction in the volume and impact of scam calls in the UK.

3.2 In our consultation we explained that CLI authentication seeks to overcome the lack of assurance with the information associated with a call by ensuring that the provider placing that call onto the phone network (the originating provider) has attested that the information associated with that call, including the telephone number, is legitimate. Conversely, where the originating provider is unable to attest the numbers associated with the call, this will act as an alert to the terminating provider.

3.3 CLI authentication needs both to reliably identify the originating provider (authentication) and confirm that the originating provider has satisfied itself that the customer originating the call can legitimately associate a specific telephone number with that call (attestation).

3.4 Our suggested approach to how CLI authentication might operate in the UK would lead to originating providers attesting that the numbers used by their customers (for almost all +44 calls) are legitimate, to ensure that the terminating provider accepts the call and passes it to their customer. In the absence of this attestation, terminating providers would not be expected to accept and connect the call by default.

3.5 We recognised that there would be certain circumstances where, although attestation would be desirable, it may not be possible, and there will be a need to connect legitimate calls which may not have attestation. However, connecting calls without attestation creates the risk of loopholes that could be exploited by scammers. Therefore, our view of how CLI authentication could work sought to balance the need to connect legitimate calls with the need to minimise any gaps in the system. We sought stakeholders’ views on the completeness, workability and potential effectiveness of our suggested approach.

3.6 Our April 2023 consultation did not make any specific proposals for the introduction of CLI authentication. Instead, the document sought views from stakeholders on our initial thinking about how CLI authentication could work if implemented in the UK, and the extent to which other measures could be sufficient in addressing the problem of number spoofing.

[43] Ofcom, 2023. Consultation: Calling Line Identification (CLI) authentication – a potential approach to detecting and blocking spoofed numbers. Subsequent references are to this publication.

3.7 In the consultation we invited comments from stakeholders specifically on:

- the extent to which our suggested approach to CLI authentication could have a material impact on reducing scams and other unwanted calls, i.e. how effective CLI authentication could be in preventing scams;
- whether any additional measures could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions;
- whether stakeholders agreed with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication; and
- the feasibility and workability of our proposals.

3.8 This section considers stakeholder responses to the April 2023 Consultation. In particular, we consider stakeholder responses on:

- the effectiveness of CLI authentication in preventing scams;
- how CLI authentication would be monitored and enforced; and
- barriers to the implementation of CLI authentication.

3.9 At the end of this section, we set out our assessment of the workability of CLI authentication in light of these responses and, where relevant, other market developments.

Stakeholder responses: the effectiveness of CLI authentication

3.10 Our 2023 consultation set out a suggested approach to call authentication and number attestation. It proposed the introduction of technical measures for digitally signing information associated with each call, and an associated process for ensuring that providers originating calls take steps to verify that their customers use numbers for which they have permission from the range holder to use. The process we suggested also included steps for providers that are acting as 'gateways' for calls into the UK from abroad.

3.11 We sought feedback from stakeholders as to the feasibility of our suggested approach and whether other steps or measures should be considered to make this approach more effective.

3.12 Consumer organisations and wider stakeholders outside of the telecoms sector generally responded favourably to our suggested approach to CLI authentication. For example, the Consumer Communications Panel (CCP) said that 'The Panel advocates for strong action against scams and number spoofing and our response is in support of Ofcom's proposals'.[44] However, telecoms industry stakeholders raised concerns about the potential effectiveness of CLI authentication, as set out below.

3.13 We have grouped stakeholder responses by reference to the following topics:

- calls with UK geographic and non-geographic telephone numbers entering the UK from abroad;
- calls with international telephone numbers entering the UK from abroad;
- calls with UK mobile numbers entering the UK from abroad; and
- calls from the Crown Dependencies.

[44] Communications Consumer Panel response to the 2023 CLI authentication consultation, p.1.

Calls with UK geographic and non-geographic telephone numbers entering the UK from abroad

3.14 In our April 2023 consultation, we proposed that the issue of scams calls made by overseas scammers spoofing UK geographic and non-geographic numbers could be addressed by a process described as 'gateway attestation'. This would mean that, when a gateway provider received a call from abroad without attestation, it could add its own authentication information to the call. This would allow other providers to reliably identify the gateway provider, and therefore identify who first introduced the call into the UK public telephone network.

3.15 We explained that a gateway provider who introduces harmful calls from outside the UK would be readily identified, as some of these calls would lead to complaints raised with terminating providers by end users. In turn, the terminating provider can report the gateway provider using the authentication information provided within the attestation passport.

3.16 Stakeholders agreed that calls with UK geographic and non-geographic telephone numbers entering the UK from abroad remained a problem but felt that other measures, including those described at paragraphs 2.23 – 2.34 which Ofcom has already introduced, may be equally or more effective compared to CLI authentication.

3.17 For example, in its response to the CLI authentication consultation, TalkTalk noted that 'when investigating known scam calls, including those captured by our Security team, we discovered that the vast majority entered our network from international carriers' and that since 'TalkTalk first started blocking international calls using UK Network Numbers (apart from +44 mobile calls), we saw around a 60% reduction in calls to our contact centres'.[45]

3.18 TalkTalk were concerned about the effectiveness of our proposals to use gateway attestation, explaining that gateway attestation 'only tells the terminating network which Communications Provider was used to admit the call into the UK network. This gives no indication of whether the CLI used is valid or not, and therefore would not prevent an international scam call from reaching a UK consumer'.

3.19 Other stakeholders suggested that we prioritise our blocking solutions and extend our guidance to include Presentation Numbers as well as Network Numbers. For example, in its response to the CLI authentication consultation, the NICC suggested prioritising blocking solutions, and specifically extending our guidance to include Presentation Numbers. The NICC, said that 'blocking of +44 Presentation Numbers at international gateways would strengthen (or provide an alternative to) the suggested approach, and we believe that it should be considered'.[46]

3.20 Similarly, Three said that the limitations of CLI authentication mean that Ofcom should 'consider strengthening existing measures to tackle CLI spoofing', and it gave the examples of 'expanding ND1447' to a) 'block UK Fixed Line Presentation Numbers at International Gateways' and b) 'block UK mobile numbers at International Gateways based on Roaming status lookup on MNO databases' as a higher priority.[47]

[45] TalkTalk response to the 2023 CLI authentication consultation, p.2.

[46] NICC response to the 2023 CLI authentication consultation, p.2. The NICC is s a technical forum for the UK communications sector that develops interoperability standards for public communications networks and services in the UK.

[47] Three response to the 2023 CLI authentication consultation, p.2.

Calls with international telephone numbers entering the UK from abroad

3.21 In our April 2023 consultation we recognised that calls that bear international telephone numbers could not be blocked by gateway providers as it would, in effect, potentially prevent legitimate calls from overseas arriving in the UK from individuals and businesses outside the UK.

3.22 Instead, we suggested that gateway attestation would be possible for international calls. We noted that:

- we would expect the gateway provider to record which provider they received the call from; and
- where technically feasible, the gateway provider should confirm that the numbers being presented by the overseas provider were currently in use by the relevant overseas provider.[48]

3.23 However, we also recognised the extent to which this is possible might be dependent on the existence and capability of common numbering databases in other countries and we acknowledged this would not be possible in a significant proportion of cases.[49]

3.24 Stakeholders agreed that verification of international calls would not be possible in a significant proportion of cases. For example, Warwick University research team noted that 'expecting the originating provider or the international gateway to fully attest if a caller is authorised to use a number without having the relevant cross-provider user information is not realistic'.[50]

3.25 In its response, BT Group noted that the approach of relying on gateway attestation of international calls, followed by traceback and enforcement, could still enable significant amounts of scam traffic to enter into the UK, and that enforcement action in these circumstances would only be taken after the scammers had contacted their victim. BT Group claimed that this would represent a poor outcome for consumers.[51]

3.26 Furthermore, the likelihood of having a coordinated international approach to CLI authentication has reduced since publication of our consultation, as at least one other regulator has now ruled out implementing CLI authentication in the near term and has instead prioritised other measures to counter scam calls.[52] This means that the possibility of gateway providers being able to confirm that the numbers being presented by the overseas provider are being correctly used remains limited.

Calls with UK mobile numbers entering the UK from abroad

3.27 In our April 2023 consultation we noted that when a call enters the UK from abroad bearing a UK mobile telephone number there are often a limited number of checks the provider

[48] Ofcom, April 2023. CLI Authentication Consultation, paragraphs 5.43 – 5.44.
[49] Ofcom, April 2023. CLI Authentication Consultation, footnote 152.
[50] Warwick University research team response to the 2023 CLI authentication consultation, question 5.2.
[51] BT Group response to the 2023 CLI authentication consultation, paragraph 2.11.
[52] Commission for Communications Regulation, June 2023, Consultation on combatting nuisance communications, paragraphs 6.142. 'ComReg also set out its preliminary view that STIR/SHAKEN is not a valid regulatory option for the purpose of this consultation, and consequently is not considered further at this time'. See https://www.comreg.ie/publication/consultation-on-combatting-nuisance-communications.

bringing it into the UK (the gateway provider) or the terminating provider can conduct to determine if the number presented is legitimate.

3.28 We noted that some countries are examining the implementation of a country 'roaming' database (that is, a database continuously updated by mobile operators indicating whether a particular mobile number is registered as being abroad). Such a database may help distinguish between calls that are from national callers abroad phoning back into their home country and calls that are spoofing mobile numbers.

3.29 We therefore invited stakeholder views on the feasibility and effectiveness of a mobile roaming database, either on its own or in conjunction with the CLI authentication approach set out here in the consultation.[53]

3.30 Some stakeholders said in response that a mobile roaming database would be necessary to avoid CLI authentication being undermined due to the loophole opened by scammers based overseas spoofing UK mobile numbers. For example, Jersey Telecom noted that 'the current loophole of Mobile numbers being excluded from this screening could be reduced through a look-up to validate whether the caller is roaming. This option may prove simpler to implement than STIR/SHAKEN, and may not be reliant on the move to SIP for all providers'.[54]

3.31 Since we published our April 2023 consultation, additional evidence of the risk of scammers using spoofed mobile numbers has emerged. As part of our voice scams monitoring activity, we have observed that scammers appear to be modifying their tactics, increasingly making calls from abroad using spoofed UK mobile numbers. Our observations have been supported by stakeholder responses. For example, in its response to the CLI authentication consultation, BT Group noted that 'while difficult to verify, we strongly suspect that the gradual reduction in the numbers of overseas invalid and spoofed CLI calls being blocked by BT after July 2022 was due, in part, to scammers switching to mobile UK CLIs'.[55]

Calls from the Crown Dependencies

3.32 In our April 2023 consultation, we explained that there is an arrangement for the 'Crown Dependencies' of Jersey, Guernsey and the Isle of Man to use numbers from the UK's +44 UK Country Code. However, because the Crown Dependencies are not part of the UK and are not subject to our regulation, there is a risk that legitimate calls originating from the Crown Dependencies and displaying +44 numbers would not be attested, and would therefore be blocked by terminating providers. The alternative, that +44 numbers used by callers in the Crown Dependencies continue to be used for calls to the UK without attestation, would create a loophole which scammers may look to exploit.[56]

3.33 In the April 2023 consultation we identified three options to minimise such a loophole:

- The CLI Authentication Administrator could accept members from outside the UK, and therefore providers operating in the Crown Dependencies could join the CLI Authentication Administrator and develop the ability to attest their own calls. We explain the role of Administrator below.

[53] Ofcom, April 2023. CLI Authentication Consultation, paragraphs 5.41.

[54] Jersey Telecom response to the 2023 CLI authentication consultation, p.3.

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

[56] Ofcom, April 2023. CLI Authentication Consultation, paragraphs 5.50.

- Providers operating in the Crown Dependencies could work with their (UK-based) national interconnect partners so that the UK partner could fully attest calls originating in the Crown Dependencies and entering the UK public telephone network.
- Calls arriving from the Crown Dependencies are given gateway attestation only, by the gateway provider introducing the call into the UK, in a similar way to other international calls arriving from abroad.

3.34 We also noted that, in relation to option a) accepting members from outside the UK, a different enforcement regime could be required, as these providers do not fall under our jurisdiction. We also considered whether the Administrator itself might be allowed to suspend or expel non-UK providers from membership in the event of serious non-compliance.[57]

3.35 In response, Jersey Telecom expressed support for the first option (accepting members from outside the UK), stating its belief that 'opening access to the UK CLI Authentication Administrator would not only satisfy the requirements of the Crown Dependencies, but would also facilitate some of the other problematic use cases where calls are potentially originating from outside of the UK, including non-UK based call centres'.[58]

Stakeholder responses: how CLI authentication would be monitored and enforced

3.36 In our April 2023 Consultation, we explained that a trusted third party or an 'Administrator' would be required, so that originating providers could register and provide the necessary certification information, and so that terminating providers could obtain necessary information from a central body to verify the digital signatures for each received call.[59]

3.37 Our expectation was that the Administrator would play a central role in monitoring the operation of the rules supporting CLI authentication, identifying where issues arose and taking action to ensure the effectiveness of CLI authentication by its members. We noted that we would be able to take enforcement action in the event of non-compliance with the Administrator's rules, and that we would be likely to prioritise enforcement where non-compliance compromised the effectiveness of the scheme or otherwise caused or created a risk of material consumer harm.

3.38 We sought feedback from stakeholders to understand whether they agreed with the approach outlined for the monitoring and enforcement of the rules about CLI authentication. Stakeholder responses focused on:

- the role of the Administrator and how an attestation regime might be policed to ensure compliance with the rules, together with the potential impact of CLI authentication on enforcement against scam and nuisance calls more widely; and
- improvements to call traceability.

[57] Ofcom, April 2023. CLI Authentication Consultation, paragraph 6.18.
[58] Jersey Telecom response to the 2023 CLI authentication consultation, p.3.
[59] Ofcom, April 2023. CLI Authentication Consultation, paragraph 5.22.

The role of the Administrator and Enforcement of a CLI authentication regime

3.39 Some stakeholders expressed concerns about the proposed role and structure of the Administrator. For example, Vodafone and UKCTA expressed the view that it was not appropriate for responsibility for implementation of the CLI Authentication Administrator to be passed to industry in the UK, and noted that, under the consultation proposals, 'in the case of a dispute about the identity of the originator, a complainant may claim the Authentication Administrator is acting anti-competitively'.[60] [61]

3.40 A Warwick University research team also suggested that it was 'unclear how [the] administrator will be chosen and managed', and that there would be a 'clear conflict of interest' if 'all UK providers are "trusted third parties" for themselves'.[62] Warwick University research team also noted the view that, if UK providers had the power to suspend or expel non-UK providers through the administrator, this would be 'detrimental to competition' and would represent 'a clear conflict of interest for UK providers to be law enforcers'.[63]

3.41 Stakeholders also expressed concerns about inequalities between UK and non-UK members when it came to enforcement of the regime. This is because in our April 2023 Consultation we noted that, in relation to accepting members from outside the UK, a different enforcement regime could be required, as these providers do not fall under our jurisdiction. We also considered whether the Administrator itself might be allowed to suspend or expel non-UK providers from membership in the event of serious non-compliance.[64]

3.42 Jersey Telecom expressed concerns about this proposal. It explained that 'whilst taking the grave nature of serious contravention in mind, [suspension or expulsion] could be materially damaging to our subscribers and the Crown Dependencies themselves. Instead, Jersey Telecom would propose that the Administrator should establish a similar reporting regime with the Crown Dependency regulatory bodies such that these bodies can take equivalent actions to OFCOM within the Crown Dependencies'.[65]

Improvements to call traceability

3.43 In the April 2023 Consultation, we also highlighted issues regarding call tracing. We noted that the ability to trace quickly and simply where scam or nuisance calls have originated from and, by extension, to identify the party which is making them, is a major challenge.[66]

3.44 This means that currently, when a complaint is made about the content of a call or where there is a pattern of suspicious calls, the terminating provider can usually identify the upstream provider who passed the call to them, but cannot necessarily directly identify which provider originated the call or how it entered the UK network.[67]

3.45 We explained that, in order to identify the originating provider, or the entry point into the UK network, it is necessary to trace the call back through the call routing, starting with the

[60] Vodafone response to the 2023 CLI authentication consultation, p.6.

[61] UKCTA response to the 2023 CLI authentication consultation p.4

[62] Warwick University research team response to the 2023 CLI authentication consultation, p.2.

[63] Warwick University research team response to the 2023 CLI authentication consultation, pp.3-4.

[64] Ofcom, April 2023. CLI Authentication Consultation, paragraph 6.18.

[65] Jersey Telecom response to the 2023 CLI authentication consultation, p.5.

[66] Ofcom, 2023. CLI authentication consultation, p.55.

[67] Ofcom, 2023. CLI authentication consultation, p.56.

provider that passed the call to the terminating provider and working back from there until the call originator is identified. However, each call can be carried over the networks of multiple telecoms providers that accept and pass traffic on to the terminating provider, which delays the process. The call tracing process is also dependent on the co-operation of the providers involved, including responding to requests promptly. Call tracing is a time-consuming and resource-intensive task for both enforcement agencies and providers.

3.46 Call tracing is also hampered by the data retention practices of providers, who may only retain call records for a few days. Call tracing requests must be made quickly if they are to be successful. For scam calls originating overseas, where the call traverses networks in multiple jurisdictions, overseas providers may take longer to respond to tracing requests, or ignore them completely, reducing the likelihood of the originating provider being successfully identified.[68]

3.47 We suggested that CLI authentication could enable a different and more effective approach to call tracing. We noted that an attestation passport, where used, would immediately verify the originating provider and eliminate the need to check back through the records of providers to trace the call. In the event of a gateway-attested call, the attestation passport would immediately identify the gateway provider that injected the call into the UK network, or that added the passport to an unattested call.[69]

3.48 Many stakeholders acknowledged the issues we identified in relation to call tracing. Some noted that, although CLI authentication could facilitate better call tracing, it would face limitations and therefore it would be better to focus on less resource and cost-intensive initiatives.

3.49 The NICC, for example, agreed that 'CLI authentication could make call tracing easier than it is today', but observed that 'in the international case it would only identify the UK gateway network'. The NICC also suggested that 'it would be better to focus on easier methods to give the same information (Call Traceback and/or mobile roaming checks)'.[70]

3.50 TalkTalk said that 'Ofcom should consider what could be achieved using call traceback solutions without the introduction of CLI authentication'. It also argued 'that call traceback combined with effective enforcement and the other measures highlighted may be a more effective and cost-efficient option than CLI authentication'.[71]

3.51 TalkTalk went on to say that 'we agree that CLIA could make call tracing easier, but it is a very expensive and time-consuming method of achieving this outcome and it has potential limitations. Separate call traceback solutions should be considered alongside other measures, rather than implementation of CLI authentication'.[72]

3.52 BT Group also suggested that it would be more cost-effective instead to use a new Traceback mechanism which is being considered by several CPs (BT Group, Vodafone, TalkTalk, Gamma and Virgin Media O2) in conjunction with the NICC, which it noted 'would need to extend to the wider community of voice service providers across fixed and mobile networks'.[73] BT Group also noted its view that there is 'sufficient common ground amongst

[68] Ofcom, 2023. CLI authentication consultation, p.56.

[69] Ofcom, 2023. CLI authentication consultation, p.56.

[70] NICC response to the 2023 CLI authentication consultation, p.2.

[71] TalkTalk response to the 2023 CLI authentication consultation, p.4.

[72] TalkTalk response to the 2023 CLI authentication consultation, p.5

[73] BT Group response to the 2023 CLI authentication consultation, paragraphs. 3.9-3.10.

the major operators' to initiate a work programme focusing on 'options for blocking UK mobile CLIs originating overseas and which are not roaming'.[74]

3.53 A Warwick University research team suggested that Ofcom might prioritise 'introducing a Service level agreement (SLA)-backed process for CPs to trace calls back to the originating UK network or International Gateway'.[75]

3.54 Although UK Finance acknowledged questions about how call tracing should be implemented was not within '[its] sector's expertise', they did highlight that currently the opportunity to take spoofed calls intelligence forward is not leveraged within the spoofed calls environment in the same way as spoofed SMS messages, due to the tracing constraints on spoofed calls.[76]

Stakeholder responses: barriers to the design and implementation of CLI authentication

3.55 In the April 2023 Consultation, we set out our initial views on how CLI authentication could be implemented in the UK as a regulatory requirement. We considered timeframes and the tasks that would be required to implement CLI authentication.

3.56 In considering timeframes, we explained that CLI authentication standards have been developed to operate in IP networks, and we assumed that CLI authentication, if introduced, would be present only on IP networks. This was because our expectation was that the vast majority of legacy networks in the UK will have been decommissioned and replaced by IP networks by the end of 2025. We did not envisage that it would be practical to implement CLI authentication prior to this date due to the complexity of introducing CLI authentication on legacy networks that were soon to be decommissioned.

3.57 We also set out the tasks that all telecom providers in the UK would need to follow in order to integrate CLI authentication capability into the UK telecoms network.

3.58 In response to the April 2023 consultation, some stakeholders noted that successful implementation of CLI authentication would be difficult because of additional resource constraints, particularly on smaller providers.

3.59 Additionally, some providers said that they could struggle to implement CLI authentication in parallel with other regulatory requirements. For example, the Communications Council UK (CCUK) noted that changes to the switching regime, implementation of the requirements of the Telecommunications (Security) Act 2021, and preparations for a potential duty for providers to report suspicious traffic to the Information Commissioner, were already areas of focus for the UK telecommunications industry.[77]

3.60 The CCUK also noted that the industry-led closure of the traditional copper network (PSTN) and the switch to IP-based services would have 'a significant knock-on effect'. The CCUK said that these demands are placing 'significant strain on the resources of telecommunications providers'.[78]

[74] BT Group response to the 2023 CLI authentication consultation, paragraph 4.12.

[75] Three response to the 2023 CLI authentication consultation, p.2.

[76] UK Finance response to the 2023 CLI authentication consultation, p.3, q 6.1

[77] Communications Council UK response to the 2023 CLI authentication consultation, pp.4 – 5.

[78] Communications Council UK response to 2023 CLI authentication consultation, p.4.

3.61 The NICC also said that ‘resource contention from projects such as Telecoms Security Requirements (TSR) compliance, legacy network switch-off, mobile 3G switch-off, and the skills shortage in the telecommunications industry’ should be taken into account.[79]

3.62 Some stakeholders said that the proposals in the 2023 Consultation were likely to be expensive, and that this could have different levels of impact on different kinds and sizes of providers. UKCTA, for example, said that ‘the disproportionate investments in equipment and technology [if a country were to mandate STIR/SHAKEN] may drive some enterprise providers out of business and increase the barriers [to] entry for new providers’. UKCTA also suggested that ‘if STIR/SHAKEN or CLI authentication is mandated, small providers would face a costly and resource-intensive mandate to implement such an intervention, without commensurate benefit’.[80]

Our assessment

3.63 As we set out in our April 2023 Consultation, while CLI authentication offers some advantages over other interventions to prevent number spoofing (for example, greater automation and a speedier process for identifying bad actors), it is not a ‘catch all’ solution, and it cannot address the risk of harm from spoofed calls completely.

3.64 We have considered stakeholder responses to the April 2023 Consultation and their views on to the extent to which CLI authentication could address the risk of harm from spoofed calls.

3.65 Telecoms industry stakeholders in general raised more concerns about the effectiveness of CLI authentication than other stakeholders. We have focused our assessment on three key issues which industry stakeholders have raised, and which we believe could have a material impact on the effectiveness of CLI authentication. These are:

- the risk that there would be over-use of gateway attestation, which could lead to an over-reliance on enforcement to rectify, and which would require significant enforcement resources to address;
- the issue of identifying genuine UK mobile roaming traffic in the context of other calls entering the UK which are spoofing UK mobile numbers; and
- the proportionality of the proposed solution, noting its complexity, cost and time to implement.

The risk of over-use of gateway attestation and reliance on enforcement

3.66 As we explained in the April 2023 Consultation, we would only be able to place CLI authentication requirements on UK operators. This means that calls arriving from overseas displaying international numbers could not be fully authenticated unless the international operators were also obliged to adopt similar rules.

3.67 Our April 2023 consultation suggested that this could be addressed by a process described as ‘gateway attestation’. This would mean that when a gateway provider received a foreign-numbered call from abroad without attestation it could add its own authentication

[79] NICC response to the 2023 CLI authentication consultation, p.3.

[80] Communications Council UK response to the 2023 CLI authentication consultation, p.5.

information to the call allowing other providers to reliably identify the gateway provider, and therefore identify who first introduced the call into the UK public telephone network.

3.68 However, it is now clear that widespread international adoption of CLI authentication is unlikely to happen in the near-term. Gateway attestation would therefore become the de-facto approach for international calls. This could allow significant amounts of scam traffic to enter into the UK.

3.69 We also noted in our April 2023 consultation that providers may need to rely on gateway attestation for domestic calls in the event of a system outage.[81] We explained that, if a provider discovers that attestation is absent and can satisfy themselves as to the reason that the call does not have attestation, it should follow a similar process to that of a gateway provider and add gateway attestation to the call. This would allow other providers in the call's journey to know who had added attestation to the call, and also to see that the number could not be fully attested.

3.70 In the April 2023 consultation, we explained that a gateway provider which introduced harmful calls from outside the UK could be readily identified, as some of these calls would lead to complaints raised with terminating providers by end users. Similarly, providers who added gateway attestation to domestic calls could also be identified. In turn, the terminating provider could report the gateway provider using the authentication information provided within the attestation passport.

3.71 Investigating individual use of gateway attestation to determine whether it is justified could require significant resources. Furthermore, action in these circumstances could only be taken after the call had been made and potentially allowed scammers to contact victims, leading to the very harm the remedy seeks to address and undermining the effectiveness of CLI authentication.

3.72 In summary, as stakeholders have noted, gateway attestation could be used frequently and it will not always be clear whether the use is appropriate. We accept that the risk of over-reliance on gateway attestation under our suggested approach remains, and has the potential to compromise the effectiveness of CLI authentication in terms of preventing scam calls.

The issue of identifying genuine UK mobile roaming traffic terminating in the UK

3.73 In the April 2023 Consultation, we considered the potential need for a complementary process to authenticate calls from UK mobile numbers arriving from abroad that are genuinely from UK roamers.

3.74 We accept that, without a process to authenticate calls from UK mobile numbers roaming abroad running alongside CLI authentication, CLI authentication would not adequately address the problem of inbound calls spoofing UK mobile numbers. This is because UK mobile calls entering via gateway providers could not be fully authenticated and hence may be simply allowed through. This would undermine the benefits of CLI authentication. In addition, there are unresolved complications relating to identifying mobile calls from the

[81] Ofcom, 2023. CLI Authentication Consultation, p.51.

Channel Islands. Channel Island operators do not fall within our regulatory remit, despite being entitled to use UK numbers.

Proportionality

3.75 Many stakeholder responses highlighted that many of the benefits offered by CLI authentication could be achieved by other measures more quickly, more easily, or at lower costs. Stakeholders said that these other actions should be prioritised over CLI authentication.

3.76 Stakeholders have also highlighted the potentially significant resource and cost impacts to communications providers, particularly the impact that these proposals could have on the ability of smaller operators to implement the proposals in the near term.

3.77 We accept that CLI authentication would be a complex, costly and time-consuming exercise, and that its effectiveness could be compromised by the complexities outlined in this document. We believe that alternative measures have the potential to reduce number spoofing more quickly, and are likely to be more proportionate compared to the proposed CLI authentication process.

Conclusion

3.78 For the reasons set out above, we have decided that, although CLI authentication has the potential to be an effective tool in preventing scam calls from spoofed numbers, our assessment is that we should not proceed with CLI authentication at this time.

4. Our future work plan

Introduction

4.1 The previous section considered stakeholder responses to the 2023 Consultation and set out our assessment of the workability of CLI authentication as it stands today. In summary, we have decided that, although CLI authentication has the potential to be an effective tool in preventing some scam calls from spoofed numbers, we should not proceed with CLI authentication at this time.

4.2 However, given the scale of harm which scam calls pose, we will progress a series of initiatives which will seek to address this harm in a shorter timeframe. In addition to these initiatives, we will continue to assess developments in the market and their impact on scams, as well as actively participating in the work of international bodies to explore cross-border scam prevention. These initiatives are:

- further tightening of our rules to block calls with spoofed UK geographic and non-geographic numbers;
- exploring the blocking of calls from abroad which are spoofing a UK mobile number;
- Monitoring compliance with our rules under an enforcement programme;
- exploring enhanced call tracing solutions; and
- continuing to monitor Industry and international developments.

4.3 We may still choose to re-examine CLI authentication at a later date, especially if our initiatives and industry measures do not result in a reduction in voice scams.

Further updates to our guidance on blocking calls from abroad with spoofed UK geographic and non-geographic numbers

4.4 As set out in our 2023 CLI authentication consultation, and above in Section 2, we already require operators to identify geographic and non-geographic calls from abroad which are spoofing a UK geographic and non-geographic network number and to block them unless a legitimate use case applies.

4.5 We are now proposing further enhancement of our guidance for providers on what we expect them to do to comply with the rules in GC 6.6.[82] This would include identifying and blocking calls from abroad which are spoofing UK Presentation Numbers, except for a limited number of legitimate use cases.

4.6 We have therefore published a consultation on the further tightening of our rules to require blocking of spoofed UK geographic and non-geographic Presentation Numbers from abroad, except where the operator is assured that the originator of that call has a legitimate reason for using a UK number.[83]

[82] See GC 6.6, Ofcom's General Conditions of Entitlement.

[83] Ofcom, 2024. Consultation: Tackling scam calls – expecting providers to block more calls with spoofed numbers.

Exploring the blocking of calls from abroad spoofing a UK mobile number

4.7 There is a potential risk of scammers spoofing UK mobile numbers because they are seeking to circumvent our existing rules on blocking calls from abroad which are displaying UK geographic and non-geographic numbers. In light of this risk, we think it is appropriate to explore options for blocking calls from abroad which are spoofing UK mobile numbers.

4.8 Responses from stakeholders to the CLI authentication consultation, together with international developments more broadly, indicate that there is a need to be able to distinguish between calls that are from UK mobile users roaming overseas and making calls to UK numbers, and calls that are spoofing UK mobile numbers. There are different ways in which this could be achieved: for example, legitimate roaming calls could be distinguished by routing calls to the caller's home network in the UK for validation, or by checking incoming calls against a register or database of numbers which are identified as roaming.

4.9 We have therefore begun to explore available options for identifying mobile roamers and distinguishing between legitimate calls and scammers who are spoofing UK mobile numbers. This includes assessing technical solutions, the anticipated benefits and challenges, and identifying any similar measures which are being introduced in other jurisdictions. We will continue to participate in the NICC N-CLI Task Group which is examining these issues. If we are able to identify a potential solution to validate legitimate roaming calls, we will consult on these options in due course.

Monitoring compliance with our rules under an enforcement programme

4.10 We have opened an enforcement programme focused on identifying and preventing individual telecoms providers who allow scam and spoofed voice calls to enter the UK’s telephony system. This will include making use of our good practice guide, which was introduced to set out our expectations on the steps we expect providers to take to help prevent the misuse of telephone numbers. As the guide has been in place for over a year, one of the aims of this enforcement programme will be to see how well this guide has been implemented.

Exploring enhanced call tracing solutions

4.11 We are now working with industry to improve the existing call tracing process. An improved process will help speed up the process of identifying operators who are allowing the origination and/or transit of fraudulent traffic. In the absence of CLI authentication, the ability to quicky identify the source of fraudulent calls could offer tangible incremental benefits to help reduce scams.

Continue to monitor industry and international developments

4.12 Industry is currently implementing its own voluntary measures, some of which seek to address a broader set of issues than spoofing. We will monitor the impact of these voluntary measures. In addition, we will actively participate in international bodies to explore the potential for cross-border coordination to counter voice scams.