Ofcom
making communications work
for everyone

Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers

Welsh overview available

CONSULTATION:

Publication date: 28 April 2023
Closing date for responses: 23 June 2023

Contents

Section

1. Overview 1
2. Introduction 4
3. The harm caused by number spoofing 8
4. Regulatory and market context 24
5. Our view of how CLI authentication could work 39
6. Enforcement 52
7. Implementation 58
8. Proposed framework for impact assessment 62

Annex

A1. Additional Information on STIR/SHAKEN and international implementations 68
A2. Responding to this consultation 78
A3. Ofcom's consultation principles 81
A4. Consultation coversheet 82
A5. Consultation questions 83
A6. Glossary of terms 84

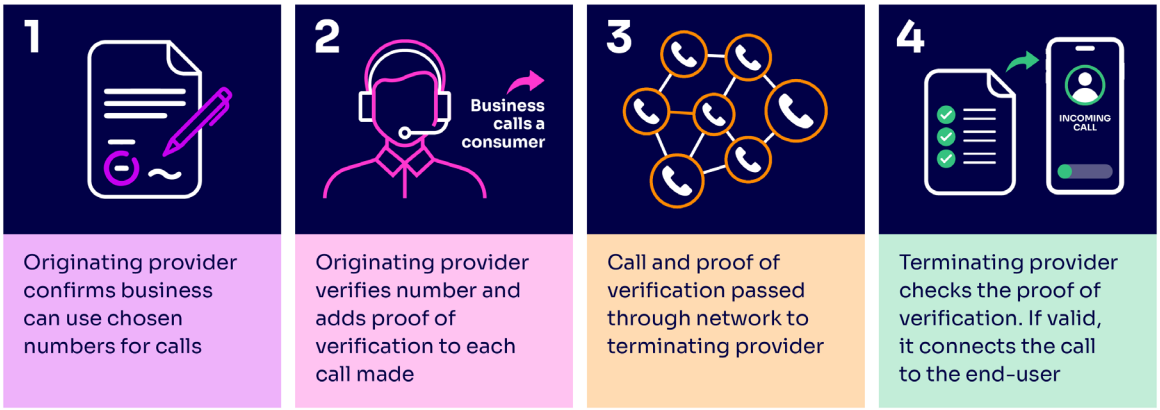
1. Overview

Protecting consumers from harm is a priority for Ofcom and we are concerned about the problem of scams facilitated by phone calls. 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.

Ofcom has already taken a number of steps to reduce scam calls and texts. We have recently strengthened our rules requiring telecoms providers to detect and block spoofed numbers where possible, and published related guidance and a separate good practice guide to help prevent scammers accessing valid phone numbers. Some providers are implementing additional measures which could also be effective in reducing scam calls.

However, over the longer term, it would be possible for providers to implement processes that detect and block spoofed numbers more comprehensively. These would entail the network originating the call, where technically possible, confirming the validity of the caller's telephone number before passing it to the network of the person receiving the call. We refer to this as 'Calling Line Identification (CLI) authentication'. Figure 1 shows how this would work for a business, although the same principles would apply to all calls.

Figure 1: CLI authentication



In this document, we are inviting stakeholders' views on our initial thinking about how CLI authentication might work in the UK and the extent to which actions providers are already taking are likely to address the problem of number spoofing. We are not making any proposals for specific regulatory interventions at this stage.

If our provisional view following this consultation is that there is a case for requiring the implementation of CLI authentication, we will publish a full assessment of the likely impact and our proposals for the regulatory rules that would be needed.

What we are proposing

Scam calls and texts are widespread, with our research finding that suspicious calls affect the vast majority of people in the UK, and the use of number 'spoofing'- where the identity of the caller is disguised - is a frequent factor. Victims of a scam can suffer significant financial and emotional harm, and scams also impose costs on the wider economy.

We already have initiatives in place to reduce scam calls and texts. These are being implemented now and offer some immediate benefits to consumers. However, although these interventions will hinder specific scam methodologies, scammers can and do change their methods in order to circumvent them.

Industry initiatives such as call filters, phone apps and blocklists help to address the challenge to some extent, but these are likely to be insufficient in tackling the problem of number spoofing. For example, some solutions may rely on consumer adoption and are unlikely to become ubiquitous. Even when used, technical limitations can make them less effective in preventing scams. While other initiatives to combat scam calls are planned or in early stages of implementation by individual providers, it is unclear at this stage how successful they will be. Scammers may also seek to bypass any measures introduced, requiring a more comprehensive solution. We therefore foresee that further regulatory intervention might be needed.

In 2019, as part of our consultation on promoting trust in telephone numbers[1], we considered CLI authentication, although having taken account of the consultation responses, we decided not to pursue CLI authentication at that time. Since then, we have observed the experiences of other countries which have started to introduce approaches to CLI authentication, and the NICC (an industry group) has further considered how CLI authentication might be introduced in the UK. We also note that UK providers are moving to using Voice over IP to carry calls, a significant system change which allows for new approaches to countering scam and nuisance calls. As a result, now is the right time to look again at the potential role of CLI authentication in tackling spoofed calls.

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 in order 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.

We recognise that there will 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 seeks to balance the need to connect legitimate calls with the need to minimise any gaps in the system. We have also considered how the attestation regime might be policed to ensure compliance with the rules. We seek stakeholders' views on the completeness, workability and potential effectiveness of these suggestions.

[1] Ofcom, 2019. Promoting trust in telephone numbers.

Finally, if introduced, CLI authentication may lead to easier detection of regulatory breaches and scam callers through more rapid identification of the originating provider of a call. This may make it easier for Ofcom, other regulators and law enforcement to pursue those responsible for making scam calls.

We do not make any specific proposals for the introduction of CLI authentication in this consultation. Instead, in this document we are seeking views from stakeholders on our initial thinking about how CLI authentication could work and the extent to which other measures may be sufficient in addressing the problem of number spoofing.

Next steps

We invite responses by **23 June 2023**.

2. Introduction

2.1 There has been an increase in scam calls and texts in recent years, which reflects a general increase in fraudulent activity in the UK, and their use is now widespread. Our research has found that suspicious calls and/or texts affect the vast majority of people in the UK. Successful scams can cause significant financial and emotional harm, but even attempted scams are annoying and can cause anxiety for recipients. Scams also impose costs on the wider economy, including the resources spent by businesses to support those customers that fall victim to fraud.

2.2 Ofcom has been working for a number of years to reduce unwanted calls. The initial focus of our work was on nuisance calls but the nature of the problem has been changing, and our work has increasingly focused on scam calls. We set out in our February 2022 policy positioning statement[2] the key elements of our response to scam calls. These are:

- We aim to **disrupt scams** by making it harder for scammers to use communications services to reach consumers. We are strengthening our rules and guidance, while at the same time supporting providers to develop their own technical solutions to detect and prevent scam traffic.
- Scams are increasingly complex, often involving different companies and sectors. So, a coordinated approach is vital to ensure more scam attempts are blocked or disrupted. We **collaborate and share information** as appropriate, including with Government, regulators, law enforcement and consumer groups.
- Given the pace at which scammers change their tactics, we understand that it will not be possible to protect consumers from all scam activity. We are working to **help consumers avoid scams** by raising awareness so consumers can more easily spot and report them.

2.3 We already have some initiatives in place to reduce scam calls and texts and have recently strengthened our rules and published guidance for providers to detect and block spoofed numbers, and a good practice guide to help prevent scammers accessing valid phone numbers. [3]

2.4 There are, in addition, a variety of measures that are being implemented by some providers which could be effective in reducing scam calls; and we seek stakeholder views on their likely impact and the extent to which they will stop number spoofing and scam calls more broadly.

2.5 These measures should help to bring some immediate benefits to consumers but over the longer term, it would be possible for providers to implement processes that detect and block spoofed numbers more comprehensively. We refer to this as 'CLI authentication'.

[2] Ofcom, 2022. Tackling scam calls and texts: Ofcom's role and approach.
[3] Number spoofing is sometimes used to describe legitimate use cases, however throughout this consultation, we refer to it as a practice utilised by scammers for malicious purposes.

Ofcom's duties and powers

2.6 The proposals explored in this document reflect Ofcom's duties in sections 3 and 4 of the Communications Act 2003 (the Act). These include our principal duty in section 3(1), in carrying out our functions:

a) to further the interests of citizens in relation to communications matters; and

b) to further the interests of consumers in relevant markets, where appropriate by promoting competition.

2.7 We have also had regard to the matters in section 3(4) of the Act so far as they appear relevant, including:

a) the desirability of ensuring the security and availability of public electronic communications networks and services;

b) the desirability of preventing crime and disorder; and

c) the extent to which, in the circumstances of the case, the furthering or securing of the matters mentioned in section 3(1) is reasonably practicable.

2.8 In accordance with section 3(3) of the Act, we have had regard to our regulatory principles of being transparent, accountable, proportionate, consistent and targeting our actions only at cases where it is needed. As required by section 2B(2)(a) of the Act, we have also had regard to the UK Government's Statement of Strategic Priorities for telecommunications, management of radio spectrum and postal services.

2.9 Ofcom has powers under section 45 of the Act to set General Conditions (GCs) applying to telecoms providers (or a specified category of providers). The matters which may be the subject of a General Condition are set out sections 51, 52, 57, 58 or 64 of the Act and include conditions which:

a) protect the interests of end-users of public electronic communications services;[4]

b) impose requirements on a provider, in specified circumstances, to block access to telephone numbers or services in order to prevent fraud or misuse;[5]

c) regulate the use by a communications provider, for the purpose of providing an electronic communications network or electronic communications service, of telephone numbers not allocated to that provider;[6] and

d) impose restrictions on the adoption of telephone numbers by a communications provider, and on other practices by communications providers in relation to telephone numbers allocated to them.[7]

[4] Section 51(1)(a) of the Act.
[5] Section 51(2)(f) of the Act.
[6] Section 58(1)(b) of the Act.
[7] Section 58(1)(c) of the Act.

Our policy objectives

2.10 Reflecting our duties, we have developed a set of policy objectives to guide our work in this area. We also intend to use these policy objectives to provide a framework for our impact assessment, should we decide to proceed with detailed proposals for implementing CLI authentication.

a) **Objective 1: Reducing the harm caused by scam, nuisance and other harmful phone calls.** Phone calls can facilitate scams, nuisance and be used for other criminal and/or malicious activities. Such calls harm both recipients and legitimate businesses. The measures explored in this consultation are intended to reduce these harms, for instance by requiring communications providers to block calls with spoofed numbers and making it easier to take enforcement action against those making harmful calls. This is our primary objective.

b) **Objective 2: Supporting legitimate phone calls taking place.** Phone calls offer a convenient, instant and near universal means of communications. They are important to both consumers (e.g. to speak to friends and family), organisations (e.g. to speak to medical professionals) and businesses (e.g. to contact, and be contacted by, existing and potential customers). The potential measures outlined in this consultation may help increase trust in the UK telephony system, and could potentially support additional calls taking place: for instance if recipients are more likely to answer calls because they are less worried that it might be a scam or a nuisance caller.

c) **Objective 3: Limiting the costs incurred by legitimate businesses.** In considering the development of possible measures on CLI authentication we recognise they are likely to result in additional costs for communications providers, which could be passed on to their customers. We will consider the potential cost implications as part of the development of any new regulatory requirements.

This document

2.11 This document sets out our initial thinking on how CLI authentication could work if it were to be introduced in the UK and gives an overview of the regulatory requirements that we envisage would underpin implementation. We are inviting comments from stakeholders to enable us to assess the workability of our proposals; and to enable us to formulate detailed proposals for implementation, should we consider that to be appropriate.

2.12 Any such detailed proposals would be set out in a second consultation, which we would expect to publish in 2024, together with our impact assessment and our proposed modifications to the General Conditions.

2.13 This document is structured as follows:

a) Section 3 describes the nature and size of the problem of number spoofing, and scam and nuisance calls more broadly;

b) Section 4 considers the extent to which existing or planned measures by Ofcom and industry may address the problem adequately;

c) Section 5 outlines our initial thinking on how CLI authentication could be implemented in the UK;

d) Section 6 sets out our suggested approach to monitoring and enforcement;

e) Section 7 gives an overview of the main steps that would be required to implement CLI authentication;

f) Section 8 outlines the framework that we would expect to use to assess the impact of the measure, should we go on to develop detailed proposals.

3. The harm caused by number spoofing

3.1 Harmful calls, such as scam calls and nuisance calls, are commonplace in the UK. These calls can harm the consumers and organisations directly affected. They can cause both financial losses and non-financial harms, such as emotional and psychological impacts. The prevalence of harmful calls can weaken trust in the telephone service, potentially leading to further harms if this results in legitimate calls going unanswered.

3.2 Spoofing is a common tactic used by scammers. In this context, spoofing refers to callers hiding their identity by causing a false or invalid phone number to be displayed when making calls. As well as being used to deceive victims, for instance by impersonating trusted organisations, spoofing also makes it more difficult to trace perpetrators.

3.3 In this section, we describe the extent of spoofing as part of harmful calls in the UK, examining the harm to different stakeholders. We discuss the following issues:

a) The importance of phone calls to UK consumers and businesses.

b) The legitimate reasons why callers may change the phone number displayed to recipients.

c) The risk of misuse of numbers for illegitimate purposes (i.e. spoofing).

d) The harm caused by scam calls and nuisance calls.

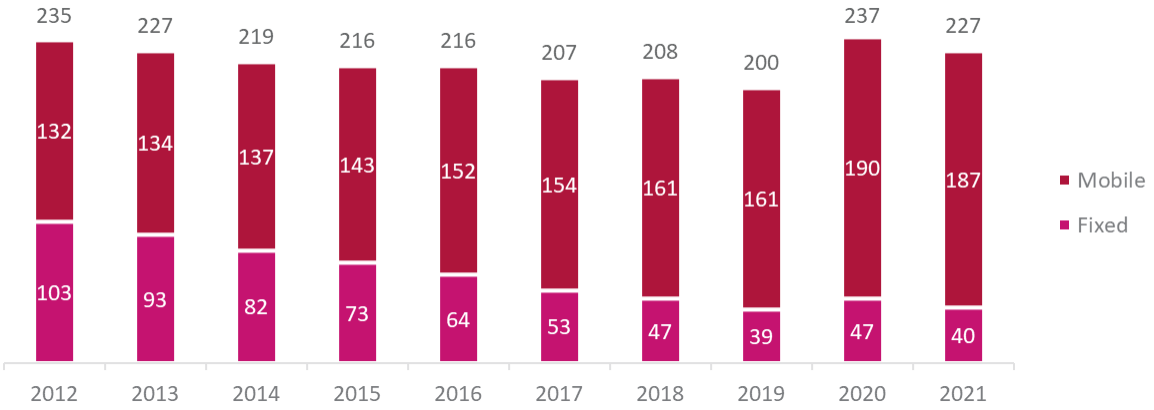
The importance of phone calls

3.4 For many consumers and businesses, phone calls continue to be a fundamental tool for contacting friends, family, patients, customers or suppliers.

3.5 Notwithstanding the emergence of over-the-top services for instant messaging and calls, the total volume of phone calls in 2021 was 227 billion minutes, which is broadly in line with the level seen ten years ago, as shown in Figure 2.[8]

[8] Wholesale Voice Markets Review. See Wholesale Voice Markets Review 2021-26 - *Use of mobile, fixed and over the top voice services all saw increases as a result of the Covid-19 pandemic, p14-15*. .

Figure 2: Total volume of outgoing phone calls (billion minutes)



Source: Ofcom Communications Market Report 2022

3.6 There has been substitution from fixed to mobile telephony over time, but both channels remain widely used. In 2022, 63% of UK households had a landline while 97% of UK households had a mobile phone.[9] Each fixed connection saw an average of 104 outgoing call minutes per month in 2021, rising to 196 minutes for each mobile subscription.[10]

3.7 For many consumers, phone calls continue to be a primary method of contacting friends and family, supplementing and enriching other methods (such as messaging).[11] Phone calls are also an important tool for businesses. For example, 50% of SMEs surveyed in our 2022 SME Communications research reported that a fixed phone was 'absolutely vital' or 'very important' to their organisation, while 83% of SMEs did so for mobile phones.[12]

Legitimate reasons for changing the number displayed to recipients

3.8 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 Identification (CLI) data. As discussed below, there are many legitimate and beneficial reasons for businesses to do this.

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

[9] Ofcom Technology Tracker 2022.
[10] Ofcom Communications Market Report 2022.
[11] 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", p28.*
[12] SME Communications Experience Research 2022.

3.10 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.[13]

Figure 3: Presentation Number and Network Number

3.11 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). Our 2022 consumer research found that 93% of mobile users who ever answer their calls said they at least sometimes look at the number displayed on their handset to decide whether to answer a call.[14] Additionally, most landline users who have a caller display facility said they at least sometimes decide whether to answer a call by looking at the number displayed on the handset (91%).[15]

3.12 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:

a) Call centres making calls on behalf of one or more different businesses;

b) 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

c) Professionals who wish to display a business number when calling from a private line.

3.13 CLI data can also be used for other purposes, such as call tracing to identify the source of unwanted calls, or as a reference to help identify the location of a caller in emergency situations. To be effective, CLI data must accurately identify the caller, including through a Presentation Number that the caller has authority to use as a number which they have

[13] 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.
[14] Ofcom CLI and Scams Consumer Research 2022, Data Tables, table 34.
[15] Ofcom CLI and Scams Consumer Research 2022, Data Tables, *77% of landline users have caller display*, table 10.

been assigned or have been given permission to use by a third party who has been assigned the number.

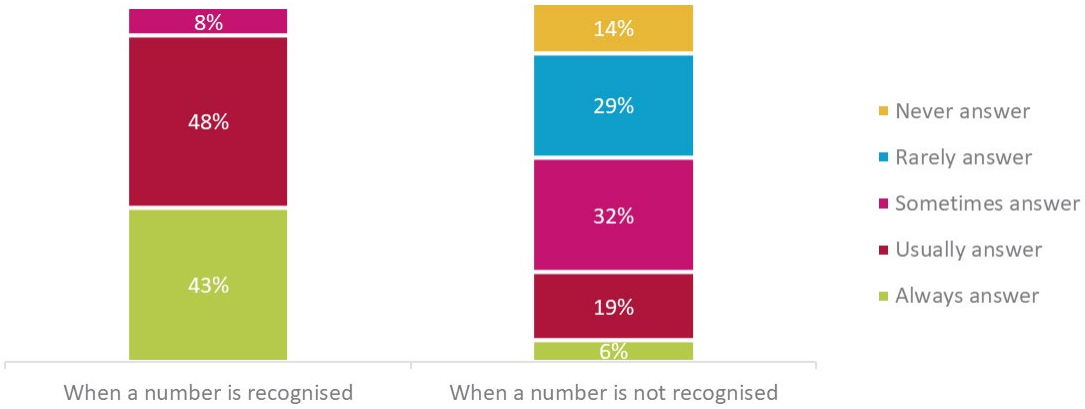
3.14 CLI data may be incorrectly set at source or be lost or corrupted as the call traverses multiple networks. Therefore, there may be legitimate reasons why CLI data may not be available or correct when it is received by the terminating provider.

Misuse of CLI data

3.15 Some callers misuse CLI data, causing a false or invalid Presentation Number to be displayed when making calls. These spoofed calls are used frequently by scammers.

3.16 A spoofed number on a call display can mimic the number of a real company or person that is known to the recipient, but who has nothing to do with the actual caller. Our 2022 consumer research has shown 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.

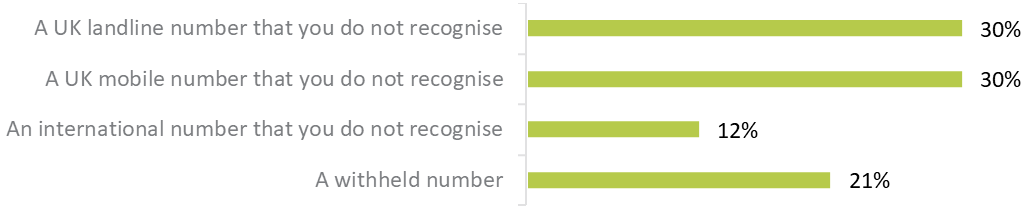
Figure 4: Propensity to answer mobile when a number is or is not recognised



Source: Ofcom CLI and Scams Consumer Research 2022. 'Don't know' responses excluded.
Base: mobile users who always/usually/sometimes decide whether to answer by looking at the number, N=1751.

3.17 Scammers based abroad sometimes seek to spoof UK CLIs when making scam calls to UK consumers, as this might mislead the recipient to believe that a call is from a legitimate source and make them more likely to answer it. As shown in Figure 5 below, consumers are more likely to answer calls from an unknown UK number than from an unknown international number or a withheld number.

Figure 5: 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.

3.18 The use of spoofed numbers also makes it harder to detect and block any unlawful calls, or to trace perpetrators when evidence of a potential scam is reported. In this way, spoofing can limit the effectiveness of enforcement as a deterrent. Even where perpetrators are eventually caught, the delays involved in tracing spoofed numbers can mean that action is taken only after significant harm has already occurred.

3.19 As there is currently no reliable and efficient way to identify all instances of spoofing, there is a lack of comprehensive data on the volume of spoofed calls taking place. However, a 2022 report by the House of Lords Fraud Act 2006 and Digital Fraud Committee concluded that "number spoofing is prolific in the UK".[16]

3.20 A recent case study gives an indication of the scale of spoofing in the UK:

[16] House of Lords Fraud Act 2006 and Digital Fraud Committee, 2022. Fighting Fraud: Breaking the Chain.

Operation Elaborate[17]

In November 2022, the UK's biggest ever fraud operation brought down a criminal group running an online service – iSpoof – that enabled number spoofing. Criminals paid a monthly subscription in Bitcoin to use the service to attempt to steal personal information, impersonating trusted organisations such as banks. The service had additional features like Interactive Voice Response (IVR) call handling with custom hold music and call centre background noise. Victims contacted would be instructed to share six-digit banking passcodes with the scammers, allowing them to access their bank accounts.

The service (which was created in December 2020) facilitated around 10 million spoofed calls between June 2021 and July 2022, of which three and a half million were reportedly made in the UK, with 350,000 calls lasting more than one minute. Losses of around £48 million have been reported, though the full amount is believed to be higher due to under-reporting.

The harm caused by scam calls

3.21 Scam calls primarily aim to defraud consumers, by tricking them into revealing personal details or making a payment to the scammer. We use the term 'scam calls' to mean all such attempted calls, whether or not they are successful in defrauding the recipient.

3.22 As we discuss below, there is evidence that the financial and emotional harm caused to victims is substantial, with other harms also potentially affecting consumers, businesses and the wider economy.

Many consumers are affected by scam calls

3.23 Scam calls are commonplace in the UK. Our 2022 research found that consumers frequently receive calls they consider to be suspicious.[18] Specifically, we found that:

a) 40% of those with a mobile phone had received at least one suspicious call in the last 3 months; and

b) 53% of landline users had received at least one suspicious call in the last 3 months.[19]

3.24 Hiya's Global Call Threat Report, which analyses a sample of calls observed during Q4 of 2022 on the Hiya Voice Security Network, estimates that the rate of fraud calls in the UK is

[17] Action Fraud, 2022. More than 100 arrests in UK's biggest ever fraud operation.
[18] These statistics are intended to give a sense of the prevalence of suspicious calls. However, not all calls considered suspicious by the recipient are necessarily unlawful or harmful; some of these might be legitimate, lawful calls. Similarly, there could be unlawful or harmful calls that the recipient has not identified as suspicious, including where spoofing has been used to mislead the recipient.
[19] Ofcom CLI and Scams Consumer Research 2022. *Percentages refer to respondents who receive at least one live voice call or recorded message,* Q28 responses.

the highest among European countries for which data is available (though this data is not necessarily representative of all calls taking place).[20]

3.25 Our research suggests that the volume of scam calls has increased over time. Between 2013 and 2019, we conducted an annual survey asking participants to complete a diary about the unwanted calls they received.[21] One of the questions captured respondents' understanding of the product or service being promoted in an unwanted call. In 2019, a quarter of calls where a product or service was identified, were thought by the respondents to be scams. This was up from 2% in 2016 and 4% in 2017.[22]

3.26 The increase in scam calls is part of a more general rise in fraud in the UK. Fraud comprised 41% of all reported crime against individuals in England and Wales for the year ending June 2022, compared with 30% for the year ending March 2017.[23] A European Commission study in 2020 estimated that 67% of UK consumers had experienced some form of fraud in the past two years, which was the third highest level among 30 countries.[24]

3.27 The prevalence of scam calls and other unwanted calls leads to many calls going unanswered. Our research found that a majority of consumers do not always answer the phone, even when they could easily do so.[25] 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".[26] Where this leads to calls being declined even when they are legitimate, it may undermine the effectiveness and efficiency of the telephony system.

Scammers use phone calls alongside other channels of communication

3.28 Phone calls are one of a range of channels used by scammers to manipulate people into divulging personal details or transferring money.[27] Based on the Office for National Statistics' Crime Survey for England and Wales, in fraud cases with direct contact between the offender and the victim,[28] online/email channels are the most common method used by scammers for first contact, followed by phone calls.[29] A separate survey of fraud victims by Which? found that, in around one-fifth of cases, respondents reported being first contacted by phone call.[30]

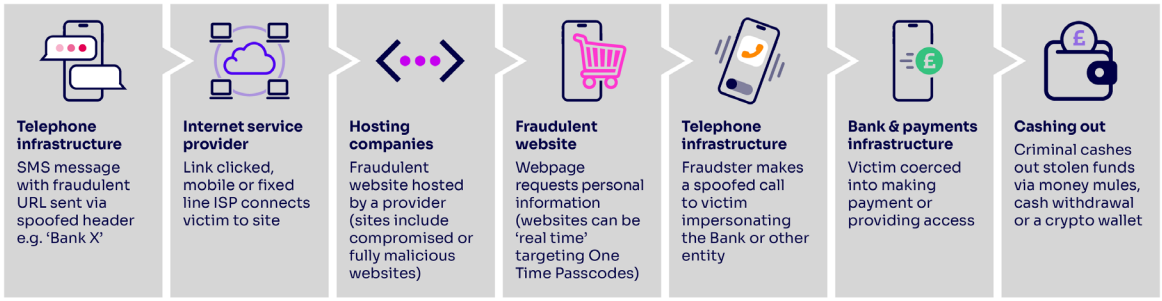
---

[20] Hiya, 2022. Global Call Threat Report Q4 2022.
[21] Note that the survey was not carried out in 2018 and it has been paused since 2019.
[22] Ofcom and Ipsos Mori, January/February 2019. Landline Nuisance Calls W6. *Note that this is the participant's understanding of the product or service being promoted and may not reflect the actual reason for the call.*
[23] National Audit Office, 2022. Progress combatting fraud.
[24] Ipsos for the European Commission, 2020. Survey on "scams and fraud experienced by consumers".
[25] Ofcom 2022. Ofcom CLI and Scams Consumer Research 2022 - *60% of landline users and 70% of mobile users.*
[26] Ofcom 2022. Ofcom CLI and Scams Consumer Research 2022 - *Chosen by 69% of these landline users and 74% of these mobile users.*
[27] UK Finance 2021. The Annual Fraud Report: The Definitive Overview of Payment Industry Fraud In 2021, page 7.
[28] Note that many incidents of fraud (for example, where hacking is involved), do not involve contact. Such incidents are outside of scope for the purposes of this document.
[29] ONS Crime Survey for England and Wales 2019/20. Note that this question has not been asked in more recent waves of the survey.
[30] Which? Money, September 2022 issue, Investigations: Fraud.

3.29 Scams can involve a number of different channels. Thus, 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.[31]

3.30 An illustrative fraud chain using multiple communication channels is illustrated below.

Figure 6: An illustrative fraud chain



Source: House of Lords Fraud Act 2006 and Digital Fraud Committee, 2022, Fighting Fraud: Breaking the Chain.

Scammers rely on successful imitation, often enabled by spoofing

3.31 A survey of scam victims by Which? found that, where scams originated via phone call, spoofing was reported to have been used in the majority of cases.[32] Spoofing is often used for impersonation scams in particular, where scammers claim to be from legitimate organisations to try to trick people into giving away personal details or making a payment.

3.32 Separate research by Which? describes how scammers succeed by creating a credible and trusted persona, which relies on two tactics: imitation and building a relationship.[33] Previous research commissioned by the Consumer Communications Panel (CCP) found that phone calls – by enabling high-quality one-to-one interactions – were often used for intricate scams where scammers would go to great lengths to pretend to be from well-known organisations.[34]

3.33 Scammers imitate a variety of trusted organisations as part of different types of scams. Many of these are authorised push payment (APP) scams, which involve tricking a victim into authorising a payment to an account controlled by a criminal. Examples include:

[31] Frontier Economics 2022. Frontier Economics, 2022. Tackling Fraud and Scams: An Ecosystem-Wide Approach, p.13- 14.
[32] Which? Money (Chiara Cavaglieri), September 2022 issue, On the hook.
[33] Which?, 2022. The psychology of scams.
[34] CCP December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, page 10.

a) Impersonating the police or the victim's bank, claiming that there has been fraud on the victim's account, and that they need to transfer funds to a 'safe account'. In fact, the criminal controls the recipient account and steals the transferred funds.[35]

b) Impersonating a utility company, telecoms provider or government department and requesting payment of fictitious fines, overdue tax or erroneous refunds.[36]

3.34 In other cases, impersonation is used for unauthorised fraud, where customer details are stolen and used to make unauthorised payments. Examples include:

a) Claiming to represent the victim's bank and requesting to connect to the victim's computer to cancel a fictitious fraudulent transaction. Victims are asked to download a remote access tool, which is used to steal information or funds.[37]

b) Impersonating organisations such as HMRC or e-commerce companies to trick victims into giving away personal information, such as login details.[38] Stolen details are then used to access online accounts and make unauthorised transactions.

3.35 Scammers are also known to adapt their scam call tactics to exploit major events and other societal trends. For instance, during the Covid-19 pandemic, scammers would claim to be calling from the Government, GP surgeries, the NHS, or even the World Health Organisation about the Coronavirus.[39] Recently, scammers have been calling consumers about cost-of-living rebates or discounts, impersonating local councils, phone providers, banks, the police or the Department for Work and Pensions.[40]

3.36 Scammers are also known to take advantage of the latest technological innovations. The adoption of number-spoofing software is itself an example. In the future, technological developments may offer new opportunities for scammers to deceive victims, such as generating synthetic media in the form of voice cloning in order to impersonate others.[41] To date such scams are not thought to be widespread, but they may become more common as commercial software becomes more widely available and easy to use.

3.37 Two real-world examples – first reported by Which? and by the House of Lords Fraud Act 2006 and Digital Fraud Committee – illustrate how scammers use spoofed numbers to reach and mislead consumers in practice.

---

[35] UK Finance, The Definitive Overview of Payment Industry Fraud In 2021, page 64.
[36] UK Finance, The Definitive Overview of Payment Industry Fraud In 2021, page 66.
[37] Action Fraud, 06 April 2022. More than £50 million lost to remote access tool scams last year.
[38] UK Finance 2021. The Annual Fraud Report: The Definitive Overview of Payment Industry Fraud In 2021, page 40. *Note that emails or text messages are also used to this end*
[39] Ofcom, 2022. Coronavirus scam calls and texts, 31 March 2022. See also Europol, 2020. Pandemic profiteering; and UK Finance, Fraud – The Facts 2021.
[40] MoneySavingExpert, 2022. Warning: Three cost of living scams to watch out for as scammers try to exploit the crisis; Action Fraud, 2022. Criminals are using the cost of living crisis to scam the public – don't become a victim.
[41] FTC, 2023. Scammers use AI to enhance their family emergency schemes and Washington Post, 2023, They thought loved ones were calling for help. It was an AI scam.

Aliyah, student, 19.

Aliyah had just finished her first year of university. She was called from a landline number with a familiar area code. After initially ignoring the call, the number called again and Aliyah answered. She recalls the conversation as follows:

'Hi, I just want to let you know we're from [Aliyah's university bank branch]. Please can you confirm that the number that we're calling is legitimate?'

Bearing in mind I go to university in [place]. He even told me to go on the website to check it was that number. I did that and it was the number, so nothing really screams, you know, that 'this is fake' because that was the actual number that was calling me… he said: *'this may be very unexpected, but we have had somebody come into our bank claiming to be you opening a new bank account.'*

The scammer successfully convinced Aliyah that it was the bank calling by using number spoofing. Pressured by the scammer to quickly 'protect' her money, Aliyah sent £1,000 to what she thought was a 'safe' account owned by the police.

Source: Which?, 2022, The psychology of scams

Paul, mid-70s, pensioner.

Paul is a pensioner in his mid-70s who suffers from a history of heart attacks. His income outside savings is a state pension of £817. He fell victim to a sophisticated malicious misdirection APP scam that cost him £65,000. The fraud used number spoofing with the bulk of the interaction being conducted by phone.

Initially, Paul received a text message claiming to be from Royal Mail. Because he was expecting a delivery, Paul did not consider the text unusual and paid a redirection fee of £2.99 using his debit card. Two days later, he received a spoofing call claiming to be 'Clive' from his bank's fraud department.

Through sophisticated social engineering techniques, the scammer convinced Paul that he needed Paul to assist him in catching other alleged scammers at the bank, asking him to transfer money to 'dummy accounts'. By the end of this process, the scammer had stolen £65,000.

Paul eventually received full compensation following a Financial Ombudsmen review, but he describes how the effects of the scam are longstanding:

"I feel that the scam of which I am a victim was extremely sophisticated—they played on my anxiety and this whole experience has left me feeling violated. It's as if someone took control of my brain and manipulated me."

Source: House of Lords Fraud Act 2006 and Digital Fraud Committee, 2022, Fighting Fraud: Breaking the Chain.

The direct financial losses from scam calls can be substantial

3.38 Successful scams can result in significant financial losses. In the context of this consultation, it is relevant to consider the financial losses associated with scams that use spoofed phone calls. Below we outline some measurement challenges and summarise relevant evidence to give a sense of the broad magnitude of financial losses.

3.39 Financial losses from scams involving phone calls can vary significantly from case to case. Research by CCP in 2020 estimated a median loss of around £300 among victims of scam calls, with 28% of victims having lost more than £500.[42] In a minority of cases, individuals lose much larger sums, as shown in Paul's case study above and other similar cases.[43] The average loss from those who reported being scammed by users of spoofing website iSpoof is believed to be £10,000.[44]

3.40 Financial losses typically affect scam victims in the first instance, although some will receive reimbursement at the expense of financial institutions. For example, UK Finance estimates that 60% of losses from APP scams are reimbursed,[45] meaning that significant financial losses are still borne by the victims.

3.41 When seeking to quantify the total financial losses caused by all scam calls, there are some intrinsic challenges because:

a) evidence in relation to economic crime is generally affected by under-reporting, the hidden nature of the activities in question, and the use of multiple indicators or definitions by different stakeholders;[46] and

b) scams can involve a combination of communication channels (which may include spoofed phone calls and/or non-spoofed phone calls) and the available evidence on financial losses does not typically isolate the exact amounts associated with scams that use spoofed phone calls.

3.42 Nevertheless, available data can provide a reasonable indication of the likely order of magnitude of financial losses, particularly in relation to APP fraud.

3.43 UK Finance estimates that losses from impersonation APP scams[47] – a subcategory of APP scams – have increased in recent years. Based on the most recent 12 months of available data, annualised losses can be estimated as £187m.[48]

---

[42] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, page 4 and 10.
[43] Action Fraud, 06 April 2022. More than £50 million lost to remote access tool scams last year; Which? Money, December 2022 issue, Investigations: Number Spoofing, p16.
[44] Action Fraud, 2022. More than 100 arrests in UK's biggest ever fraud operation.
[45] UK Finance, 2022. 2022 Half Year Fraud Update.
[46] See for example, NAO, 2022. Progress combatting fraud.
[47] UK Finance defines impersonation APP scams to include those based on impersonating the police, banks, or other organisations such as utility companies, communication service providers or government departments.
[48] UK Finance, 2022. 2022 Half Year Fraud Update.

Table 1: UK Finance estimates for impersonation APP scams[49]

	H1 2020	H2 2020	H1 2021	H2 2021	H1 2022
Total cases[50]	15,183	25,722	32,163	23,470	21,257
Total losses	£57.2m	£89.4m	£118.6m	£96.4m	£90.5m

3.44 Not all impersonation APP scams necessarily involve phone calls. UK Finance's analysis of a sample of impersonation APP scams found that all of them originated by phone call or text message,[51] with more recent indicative estimates suggesting that four in ten of these scams may originate via phone call.[52]

3.45 Given the above and the fact that phone calls may be used in a scam even where first contact is via text message, we believe it is reasonable to expect that around half of impersonation APP scams may involve phone calls. Among those scams, based on evidence previously presented in this section we believe it is reasonable to expect that a majority involve spoofed phone calls.[53]

3.46 Across other categories of APP scams[54], between 2% and 9% of cases have been estimated to originate via phone call or text message.[55] The annual loss from these types of APP scams is estimated as £329.4m.[56]

3.47 Aside from APP scams, phone calls can facilitate unauthorised fraud, such as remote banking fraud, where customer details are stolen and used to make unauthorised payments.[57] The annual loss from remote banking fraud is estimated as £227.2m.[58]

3.48 Since March 2022, UK Finance has observed a marked increase in scammers using phone calls to trick someone into providing security credentials, which the scammers then use to

[49] Figures include the categories 'Impersonation: police / bank staff' and 'Impersonation: other'
[50] Each case refers to one card or account being defrauded. For example, if a fraud was carried out on two cards, but they both belonged to the same individual, this would represent two cases, not one.
[51] UK Finance, Over two thirds of all app scams start online – new UK Finance analysis.
[52] Based on statement from UK Finance to Ofcom, March 2023. This is based on closed scam cases on an industry case management platform (BPS) and subject to limitations: not all relevant instances of fraud are reported; data is collected based on the victim's understanding of the scam; it is input manually and may be restated by UK Finance members.
We also note that other data suggests that, for scams in general, origination via phone call is prevalent. For example, In a Which? survey, first contact was reported to be via phone call in 21% of cases, compared to 10% for text messages (Which? survey of 1,008 scam victims). Crime Survey data indicates that, for fraud in general and for banking and credit card fraud specifically, first contact via phone call is more commonly reported than via text (ONS Crime Survey for England and Wales 2019/20). CCP research found that consumers reported higher general exposure to scams via phone calls than via text (CCP December 2020, Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?)
[53] In particular, the Which? survey of scams victims, which found that spoofing was used in most scams originating via phone call (Which? Money (Chiara Cavaglieri), September 2022 issue, On the hook).
[54] These are: investment, romance, purchase, invoice and mandate, and advance fee APP scams.
[55] UK Finance, Over two thirds of all app scams start online – new UK Finance analysis.
[56] Based on data for the most recent available 12 months at the time of writing (H2 2021 and H1 2022). UK Finance, 2022 Half Year Fraud Update.
[57] UK Finance 2021. Fraud – The Facts 2021, p45.
[58] UK Finance, 2022. 2022 Half Year Fraud Update. *Based on data for the most recent available 12 months at the time of writing (H2 2021 and H1 2022).*

process card transactions.[59] This follows the introduction of Strong Customer Authentication, which entails additional steps for consumers to confirm their identity before making transactions.[60] One tier-one bank estimates that phone calls were used as an enabler in the majority of unauthorised push payment scams recorded on its case management system from Jan-Mar 2023, equating to more than 1,000 cases.[61]

3.49 In summary, estimates of financial losses typically do not isolate the exact amounts associated with scams that use spoofed phone calls. However, we believe that – as an indication of order of magnitude – the total losses from scams using spoofed phone calls could plausibly be in excess of £100m annually. This is based on a range of evidence and taking into account that fraud is generally under-reported.

Scam calls cause wider harm to consumers, businesses and society

3.50 As well as the direct financial losses discussed above, scam calls cause substantial harm to different parties.

3.51 **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.[62]

3.52 Scams and their repercussions can lead to emotional harm, which occurs in 79% of cases according to research by the European Commission.[63] Research by CCP identifies common feelings of embarrassment, loss of self-belief, anger, anxiety, isolation and helplessness.[64] A study commissioned by Which? finds evidence of significant harm to victim's wellbeing, which is estimated to outweigh the financial loss on average.[65]

3.53 Scam calls do not only harm the victims who are defrauded. Our research suggests suspicious calls can cause negative feelings such as anger, anxiety, distress, frustration, irritation, and vulnerability, even among those not caught out by scams. People worry that they, or their family and friends, might fall victim in the future.[66]

3.54 Such feelings may lead many consumers to avoid answering calls at least some of the time. They then risk missing useful or important calls from friends, relatives, or legitimate organisations, which may result in emotional distress or financial costs.

---

[59] This is classed as unauthorised fraud, because the scammers are processing the transaction.
[60] UK Finance. Strong Customer Authentication.
[61] Based on a statement from UK Finance to Ofcom, March 2023.
[62] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, see pages 11-13 which also include some individual stories.
[63] Ipsos for the European Commission, 2020. Survey on "scams and fraud experienced by consumers".
[64] CCP, December 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, page 3 and pages 10-13 which includes individual stories.
[65] 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.
[66] Ofcom, September 2021. Scams Research Chart pack - *Answers to Q7: How, if anything, does receiving these suspicious messages/calls make you feel? Base: All who have received a suspicious message/call, n=1738.*

3.55 **For businesses or other organisations** impersonated by scammers, scam calls could entail reputational impacts[67] and other costs of dealing with customer cases or implementing measures that seek to prevent fraud. For example, banking and payments organisations are investing in various measures, including security systems, training and customer education campaigns.[68]

3.56 For businesses more generally, the adverse impact of scam calls (and other unlawful calls) on trust in telephone services is significant. For example, the prevalence of scam calls means that consumers are more reluctant to answer calls in general, this weakens the effectiveness of phone calls as a customer service or sales tool. Organisations may then face greater challenges in reaching consumers for legitimate purposes, requiring additional time, effort and cost.

3.57 **For providers** specifically, there may be adverse impacts from any lack of trust in the telephone system, as this would be expected to reduce telephone usage, negatively affecting provider revenues.

3.58 There may also be costs for providers from dealing with customer queries or complaints related to scam calls, where consumers get in touch with their provider responsible for terminating the call. Some providers also incur costs for voluntary measures which seek to tackle scam or nuisance calls on their networks (this is discussed further in Section 4).

3.59 In the various cases where scam calls may entail additional costs for businesses, consumers will ultimately be worse off if the costs are partly or fully passed through into higher prices.

The harm caused by other types of unlawful calls

3.60 As well as scam calls, there are other types of calls that are unlawful and liable to cause harm. These include unlawful nuisance calls and malicious calls, as discussed below.

3.61 There are various different types of unlawful nuisance calls, including:

a) Live telesales calls and automated marketing calls that do not comply with the Privacy and Electronic Communications (EC Directive) Regulations 2003, enforced by the Information Commissioner's Office (ICO). Examples include calls to numbers registered with the Telephone Preference Service (TPS), certain calls about claims management services or pensions, and automated marketing calls without consent.[69]

b) Other calls that amount to a misuse of the telephone service under the Communications Act 2003, enforced by Ofcom. These include attempted marketing calls that result in abandoned calls, where a connection is terminated by the caller

[67] 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.
[68] UK Finance Press Release, Cross-sector action needed as criminal gangs steal more than £1.3 billion - *Notes to Editor, point 4.*
[69] For further information, see ICO's rules for organisations for telephone marketing.

soon after the call is answered, or silent calls, where the recipient hears nothing upon answering the call and cannot establish if anyone is at the other end.[70]

3.62 Nuisance calls are commonplace, though they have declined over time. Our research suggests that volumes of nuisance calls may have peaked in 2015, where the number of nuisance calls to the average landline user was estimated as 8.3 in a four-week period, falling to 5.8 in 2019.[71] A more recent third-party estimate suggests nuisance call volumes (across both landlines and mobile) of 4 billion for 2022.[72]

3.63 Complaints about nuisance calls to Ofcom and the ICO have also fallen over time. This may reflect decreasing volumes of nuisance calls, but might also be influenced by other factors, such as changes in how consumers respond to nuisance calls.[73]

3.64 Unlawful nuisance calls do not necessarily rely on the impersonation tactics used by scam calls. Nevertheless, perpetrators sometimes make use of spoofing because:

a) It makes call tracing much more difficult and can therefore reduce the likelihood of being caught. For example, the ICO estimated, based on 2015 data, that around 13% of complaints it receives relate to spoofed calls, leading to "a disproportionate amount of time" spent on identifying the organisation responsible.[74]

b) It may improve the likelihood of a successful call connection – for example, by displaying a number with the recipient's local area code.[75]

3.65 Nuisance calls do not typically result in financial losses, and they may not have the same severe emotional and psychological impacts of some scam calls. However, nuisance calls can still lead to significant harms, such as:

a) Annoyance, inconvenience, and anxiety for consumers. Our research has consistently found over several years that around 80% of landline owners find nuisance calls to be annoying, while between 5%-11% find them to be distressing.[76]

b) Harm to all telephone users and to providers, resulting from tendencies to avoid picking up calls due to the possibility of receiving nuisance calls, leading to some legitimate calls not being answered.

3.66 In addition to scam and nuisance calls, harm may also be caused by malicious calls, such as calls involving threats, abuse, blackmail or hoaxes. These calls are likely to cause distress and disruption to victims. It is possible that spoofing could be used by perpetrators of

[70] For further information, see Ofcom's Guide on Abandoned and silent calls and Ofcom's Persistent Misuse Policy Statement, 2016.
[71] Ofcom and Ipsos Mori, January/February 2019. Landline Nuisance Calls W6.
[72] Green Smartphones, 2022. Study: Brits Will Receive 4.03 Billion Nuisance Calls This Year.
[73] For instance, the propensity to complain may fall over time if some consumers might adapt by simply ignoring calls from unfamiliar numbers, instead of registering complaints
[74] ICO response to DCMS consultation on requiring direct marketing callers to provide CLI.
[75] ICO. ICO monetary penalty notice issued to Making it Easy Ltd, p13.
[76] Ofcom and Ipsos Mori, January/February 2019. Landline Nuisance Calls W6, page 38. This landline nuisance calls research has been carried out in 2013, 2014, 2015, 2016, 2017 and 2019.

malicious calls, but there is a lack of evidence regarding the overall prevalence of malicious calls, the harm caused and the role of spoofing.

The potential need for further measures to tackle harmful calls

3.67 The evidence summarised in this section points to a significant problem of scam and nuisance calls, with spoofing being a key tool used to mislead consumers. As well as the direct harm caused to the consumers and organisations affected, the use of spoofing makes it more difficult to trace perpetrators and weakens trust in numbers.

3.68 There is a risk that harmful calls will be an enduring problem in the future. As mobile phone ownership is ubiquitous and landlines are still used by a significant share of the population, phone calls appear likely to remain a cheap and convenient way for scammers and nuisance callers to reach large numbers of people. Moreover, the high-quality one-to-one interactions enabled by phone calls – as opposed to emails or text messages, for example – will continue to be attractive to perpetrators who seek to persuade, manipulate or pressurise victims through social engineering tactics. The effectiveness of these tactics could be enhanced by new technologies, such as voice cloning to impersonate individuals.

3.69 Against this backdrop, we are considering whether and what further measures are needed to reduce the incidence and impact of harmful calls. In the next section we outline the regulatory measures and industry initiatives that are in place to tackle harmful calls, with a particular focus on reducing the prevalence of number spoofing. We consider whether these measures and initiatives may be sufficient to address the problem fully; or whether other interventions may be necessary such as CLI authentication, which we explore in subsequent sections.

Consultation question

Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

4. Regulatory and market context

4.1 In view of the prevalence and harm they cause, both Ofcom and the industry are working to tackle scam calls in general, and number spoofing in particular. In this section we provide an overview of regulation and guidance we have put in place and summarise the actions industry has taken or intends to take in the near future. We explain that while these initiatives are welcome, there may still be a risk of scammers exploiting some gaps in the measures taken to continue to spoof numbers. Given this context, we explain why the introduction of new CLI authentication requirements merits fresh examination, as a potentially more comprehensive means of combatting the problem of number spoofing.

Our wider work to tackle scam and nuisance calls

4.2 We have been working to reduce the harm to consumers from nuisance calls since 2015. Our initial focus was on silent and abandoned calls which were identified as causing the most harm to consumers at the time. We were able to successfully reduce the prevalence of nuisance calls by requiring CLI data to be sent alongside a call and requiring providers to block calls with invalid CLIs, where feasible.[77] [78]

4.3 In 2015, we established a Strategic Working Group (SWG) with major telecoms providers who submit monthly data on the nuisance calls which we collate and share a summary with members of the group.[79] The data is also used to inform our enforcement work. Our work was complemented by the ICO's powers to fine nuisance marketing callers and the establishment of an opt-out for consumers from marketing calls via the ICO-managed Telephone Preference Service. This work has helped to reduce the number of silent and abandoned calls reaching consumers.[80]

4.4 Over time we have observed the nature of the harm has been shifting from nuisance calls towards scam calls, the use of spoofing and, more recently, scam texts.[81] Moreover, wider public awareness of scam calls and texts has increased, partially due to high-profile pandemic-related scams, e.g. fraudulent offers of testing and vaccination services. This has made the issue even more of a focus for government, regulators and consumer groups, all of whom are looking at improved methods of tackling scams, with Ofcom and the telecoms sector being considered as part of that solution.

[77] GC C6 specifies the rules around Calling Line Identification.
[78] Ofcom, 2018. Guidance on CLI Facilities, paragraph 3.41.

[79] The current membership is AQL, BT (which includes EE), Colt, Gamma, KCOM, Sky, TalkTalk, Three, Virgin Media O2 and Vodafone.
[80] This is supported by a reduction in our complaints data, where consumer complaints about silent and abandoned calls fell between 2015 and 2020.
[81] Ofcom and Ipsos Mori, Landline Nuisance Calls W6, Jan/Feb 2019. *Scam texts have become increasingly common, with our latest research finding that 71% of those surveyed thought they had received a suspicious text. Our nuisance calls research in 2019 indicated that an increasing number of calls were thought to be scam calls. One in four of the calls recorded by panellists were thought to be for scams, up from very few in previous years.*

4.5 In 2022 we published a series of consultations and statements which explained our role and approach to tackling scams.[82] These publications included:

a) the publication of a good practice guide to help prevent scammers accessing valid phone numbers;

b) updates to our scheme to protect legitimate numbers that are most likely to be spoofed by scammers; and

c) updates to strengthen our rules and guidance for providers to detect and block spoofed numbers.

Good practice guide to help prevent scammers accessing valid phone numbers

4.6 Ofcom is responsible for the administration of the UK's phone numbers under the Communications Act 2003. In carrying out our telephone numbering functions, we have a general duty to ensure that the best use is made of phone numbers and to encourage efficiency and innovation for that purpose. Providers are subject to Ofcom's General Conditions, including General Condition B1, which includes requirements to ensure numbers are used effectively and efficiently.

4.7 We found that there was considerable variation in how providers manage numbers, including their due diligence checks before transferring numbers to other providers, resellers and end users; processes for ensuring customers use numbers in compliance with the General Conditions; and how they respond to reports of misuse. Without appropriate processes in place for managing numbers, there is greater risk that numbers may be misused, for example to facilitate scams. We therefore published a good practice guide which sets out the steps that we expect providers to take to help prevent valid numbers being misused, including to facilitate scams.

Updating our scheme to protect legitimate numbers that are most likely to be spoofed by scammers

4.8 Consumers may be more likely to trust a call coming from a number associated with a known organisation. In some cases, scammers may deliberately change their number to hide their identity or mimic the number of a legitimate business, e.g. a bank, in order to mislead the consumer.

4.9 Some telephone numbers that are assigned to a business or organisation may never be used by that organisation to make outgoing calls. This may be the case where the number is reserved for inbound calls only (e.g. the number on a bank card which is reserved for consumers to report problems to their bank). Any outgoing calls appearing to originate from these numbers are likely to have been spoofed and not be a genuine call from the organisation.

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

4.10 We therefore worked with the SWG and UK Finance to develop the Do Not Originate (DNO) list which we began sharing with providers in 2019. The DNO list includes those numbers that consumer-facing organisations, e.g. banks and government bodies, make available for people to call them on but which are not used by the organisation to make outgoing calls.

4.11 These numbers are sometimes spoofed by scammers, claiming to be calling from that organisation. This can be a particularly effective tactic for scammers, as these numbers can appear on legitimate correspondence, for example on bank cards or statements, or as results from online searches for bank numbers. The DNO list is shared with telecoms providers, their intermediaries and interested parties like call blocking or filtering services, who can block outgoing calls from numbers on the list.

4.12 As the DNO list has become more widely known, we have received higher volumes of requests for numbers to be added. To maintain the effectiveness of the list in its current form, in 2022 we updated our guidance for submitting numbers and added information to our website to explain the purpose of the list and explained the benefits for private and public sector organisations and their customers/users.[83]

4.13 The DNO list has been shown to be an effective tool in combating scam calls using spoofed numbers. Organisations with numbers on the list have reported decreases in impersonation scams using their numbers. For example, HMRC reported a significant reduction in spoofed calls as a result of its inbound-only numbers being added to the DNO list.[84]

4.14 However, adding a number to the DNO list does not guarantee that all call attempts will be blocked. Whilst the majority will be, technical constraints may mean that a small number of calls are still connected. These constraints relate to the technology available on the networks involved, the route the call takes across networks and whether the providers of the networks are able to make use of the full DNO list.

4.15 Additionally, while the DNO list is effective in protecting the most commonly spoofed numbers and thus stopping some scam calls reaching consumers, we have observed scammers attempting to bypass it, sometimes successfully, by making use of numbers adjacent to those numbers protected by the list.[85]

4.16 Finally, because it is not possible to distinguish between a legitimate outbound call and a spoofed outbound call, all outbound calls from numbers on the DNO list will be blocked where technically feasible. Therefore, any number an organisation (or individual) may legitimately use to make outgoing calls should not be added to the DNO list and there is a risk that these numbers will be used for spoofing. This introduces complexities and limitations to the DNO list and is a barrier to its comprehensive effectiveness.

---

[83] Ofcom, February 2022. Guide for organisations: Submitting numbers to the 'Do Not Originate' list.
[84] HMRC, June 2019. Controls prevent phone fraudsters spoofing HMRC.
[85] For example, in the 'iSpoof' scam, scammers changed the last digit of the CLI when posing as a bank representative, thereby bypassing the DNO list, and leading some consumers to be scammed. See Daily Mail, 24 November 2022. Dozens arrested in UK's biggest ever-fraud probe.

4.17 Therefore, although the DNO list has proved effective in preventing some cases of number spoofing, it should be regarded as one part of a suite of actions that need to be taken to protect the public from scam calls.

Updates to strengthen our rules and guidance for providers to detect and block spoofed numbers

4.18 In 2022 we 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.[86] These changes will help prevent harm to consumers, in particular by increasing the blocking of spoofed numbers. This will have the dual benefit of reducing the number of scam calls that are connected and making it harder for scammers to make their calls appear legitimate.

4.19 Our rules already required originating providers to ensure that accurate CLI data is 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.

4.20 While not all of these 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 a call which originated abroad. We therefore strengthened our rules and guidance so that providers do more to block spoofed numbers. The blocking of international calls with UK network numbers is discussed further below.

4.21 We modified our General Condition (GC) C6[87], to add the requirement for providers, where technically feasible, to identify and block calls where the CLI does not "uniquely identify the caller".[88] This requirement takes effect on 15 May 2023, but we expect all providers to have started work already to implement these changes in order to meet this deadline.

4.22 Providers are required to validate that the telephone number is dialable for calls that originate on or enter their networks, to ensure that all providers involved in the transmission of a call play a part in identifying calls that do not comply with the requirements set by GC C6, and in preventing these calls from being connected to the called party.

4.23 We provided revised guidance as to how providers could validate the telephone numbers of a call. This guidance included:

a) clarifying that the format of a CLI should be a 10- or 11-digit number;

[86] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data.
[87] General Conditions of Entitlement, Condition C6.
[88] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data.

b) 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;

c) identifying calls originating abroad that do not have valid CLI and blocking them;

d) identifying and blocking calls from abroad spoofing UK CLI (discussed below); and

e) prohibiting the use of 09 non-geographic numbers as CLI.

Blocking of international calls with UK Network Numbers

4.24 In 2021, the NICC[89] published industry guidance aimed at UK operators that receive calls with a UK CLI (as a Network Number) from a non-UK interconnect.[90] The guidance (ND1447[91]) 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 as having originated in the UK, potentially with the intention of misleading UK consumers and thus increasing the likelihood that they answer the call.

4.25 As part of our 2022 updates to strengthen our rules and guidance for providers to detect and block spoofed numbers, we made changes to our rules and guidance on the provision of CLI facilities.[92] These changes included adding an expectation in our guidance that telecoms providers should block calls from abroad that 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. These new requirements will come into force in May 2023, though some providers have already taken steps to implement the NICC guidance.

4.26 The implementation of ND1447 and the associated changes to our CLI guidance, while an important intervention in tackling number spoofing, does not address all potential scam call scenarios.

4.27 For example, scammers calling from abroad may seek to bypass this measure by withholding their number, 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).

4.28 Furthermore, this measure only addresses calls using a UK CLI when originating calls from outside the UK. Although all networks in the UK are required under GC C6 to check that the caller has permission to use that CLI (and therefore spoofing should not occur for calls originated within the UK) we recognise there are barriers to effectively checking and enforcing GC C6 fully. These barriers include, for example, the difficulties in tracing the origination of the call. So, in practice there are likely to be some scammers who are

[89] The NICC is the UK telecommunications network and service interoperability standards body.
[90] In 2020, TalkTalk had earlier prepared a report on the prevention of number spoofing for discussion within the NICC. The report explored a number of methods to prevent calls with spoofed UK CLIs which originate from abroad reaching UK consumers.
[91] NICC, April 2021. Guidance on blocking of inbound international calls with UK Network Number as CLI ('ND1447').
[92] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data.

operating within the UK and originating scam calls using UK numbers, and hence other measures may be needed to stop these calls.

4.29 Finally, ND1447 has only been applied on international interconnects, that is, connections to other providers from whom international calls are expected to be received. UK providers often have other interconnect points for domestic calls where ND1447 does not apply, hence potentially allowing some international calls that should have been blocked to enter the provider's network through these routes.

4.30 As indicated in our November 2022 Statement, we are monitoring the impact of this blocking measure. We will proactively assess the risk of scammers modifying their tactics in response, including with a view to potentially consulting on blocking calls from abroad using UK CLI as a Presentation Number if appropriate.

Government initiatives to reduce scams and number spoofing

4.31 The Home Office is currently developing a new Fraud Action Plan which is likely to include actions focused around preventing scams reaching consumers; empowering the public to spot and avoid attempted scams; and increasing the detection of those responsible for scams. The Home Office has also reconstituted the Joint Fraud Taskforce (JFT), a partnership between government, the private sector and law enforcement to tackle fraud collectively and which now includes Ofcom as a member.[93] The JFT will monitor the delivery of voluntary commitments made by industry, with the aim of addressing fraud enablers in key sectors.

4.32 Commitments by telecoms providers are contained in a Home Office developed Telecoms Fraud Sector Charter[94] and there are similar charters for the retail banking and accountancy sectors. Via the sector charter, fixed and mobile telecoms providers have committed to identify and implement techniques to block scam calls and share data on the source of these calls across the sector. They have also committed to work with banks to tackle identity theft affecting customers and subscription fraud and support the banking industry by providing real-time checking to tackle SIM swap and MNP fraud.

Industry initiatives to reduce number spoofing

4.33 Telecoms providers are undertaking a significant amount of work to tackle scam calls and texts, including some pursuing initiatives that are specifically designed to reduce the incidence of number spoofing. We outline some of these measures below.

Additional measures implemented by telecoms providers

4.34 Telecoms providers are taking steps to reduce scam calls by applying some of the following measures:

[93] For more information about the membership and sector-based charters, see the webpage Joint Fraud Taskforce.
[94] UK Government, 2021. Fraud sector charter: telecommunications.

a) As outlined above, providers are implementing initiatives to meet (and in some cases exceed) the forthcoming changes to our regulatory requirements. This includes:

   i) number blocking of malformed and invalid CLI based on the Ofcom Numbering Plan;

   ii) number blocking based on a variety of blocklists, such as the DNO list and the providers' own blocklists;

   iii) international call blocking as set out in ND1447 (some providers are blocking calls from abroad that have UK Presentation Numbers, in addition to blocking calls with UK Network Numbers).[95]

b) Use of network monitoring tools to help identify suspicious call traffic patterns. These tools analyse a variety of metrics such as volume of calls, call duration, call answer rate, calls from numbers not allocated or in use, calls to invalid destinations as well as time of day when these calls were placed, to identify scam campaigns and assess whether to block certain phone numbers.

c) Making call screening facilities available to customers, with products such as BT's Call Protect[96], TalkTalk's CallSafe[97] and Sky's Talk Shield[98]. These facilities allow end users to reject withheld numbers, create a personal blocklist, block incoming calls from automated callers, flag suspicious calls and / or redirect calls to voicemail.

d) Working with the banking industry to introduce a pilot scheme called 159, a memorable short code phone service that connects the retail banking customers directly with their bank, should they receive an unexpected or suspicious call on a financial matter.

4.35 Additionally, in January 2023, EE announced that it has partnered with Hiya, a call analytics company, to implement network-wide call protection for EE Mobile and BT Digital Voice customers.[99] The service will launch on the BT and EE networks later in 2023, with the aim of helping to prevent scam and nuisance calls by labelling and blocking spoofed numbers.

4.36 BT's network will check calls in real time using the Hiya Protect service. This will screen numbers and provide additional information that may either be presented to the end user's handset as a warning or in some cases the call will be diverted to a junk voice mailbox.

4.37 EE / BT anticipate the Hiya partnership will help to reduce the thousands of weekly calls that come into its call centres from customers reporting attempted scams, [✂].[100]

4.38 Meanwhile, one provider says it is considering the introduction of a reputation service which would interface with enterprises (such as banks) and allow them to indicate when

[95] Telecoms providers' responses to 2022 Ofcom information requests, answers to question 3.
[96] BT, BT Landline features.
[97] TalkTalk, About CallSafe.
[98] Sky, Sky Talk Shield.
[99] EE, 2023. EE secures latest partnership on its mission to eradicate scam calls.
[100] BT's responses of 6 February 2023 and 20 February 2023 to Ofcom's information request of 23 January 2023.

they have made a call to that provider's numbers, hence allowing the provider to allow/block calls from their CLIs as appropriate. However, the deployment timeline in the UK has not been finalised.[101]

4.39 In addition, we understand that Virgin Media O2 is in discussions with a vendor on implementing an enhanced nuisance call blocking solution into their network. Integration in the O2 Mobile platform may occur later this year. Extension of this solution to the Virgin Media fixed network in the future is under exploration, which would replace or complement the existing 'filtering and blocking solution' that is already in place.[102]

Commercially available products to reduce scam calls

4.40 In addition to measures introduced by telecoms providers, there are several commercial products available to consumers and / or businesses.[103] These options tend to be preventative in nature and help consumers to reduce their exposure to scam and nuisance calls. These product options include:

a) Landline devices: These 'plug-in' handsets, which consumers can purchase and install at home, offer embedded call blocking functionality and specialised call blocking services for landline phones. The devices collect information about incoming and outgoing calls by observing the behaviour of the caller and receiver of the call and use this information to identify nuisance calling numbers.

b) Call screening applications for smartphone devices: These apps perform multiple functions, from caller identification to spam labelling or number blocking. Consumers can download these apps for free (with premium features behind a paywall) or purchase handsets with these features preinstalled. These apps rely on crowdsourced data by collecting real-time feedback from user reports and using it to assess calls in real time.

c) Branded caller ID services: These services enable businesses to display their company name, logo and reason for calling on the call recipient's handset.

These industry measures are welcome but may be insufficient

4.41 It is encouraging that telecoms providers and other third-party services are taking steps to tackle scam calls and are considering other future investments in this space. While some initiatives will take time to evaluate, there is already some evidence of measures having an impact - for instance, BT Group says it is blocking up to 7m international scam calls which are spoofing UK-based numbers each month.[104]

[101] [✂]
[102] Virgin Media O2 meeting with Ofcom, 23 February 2023.
[103] For example, trueCall, Truecaller, Hiya and Google's Verified Calls service are examples of some of these products.
[104] BT Group, Data & AI driven fraud protection, presentation to BT Group event on 13 March 2023.

4.42 However, there are likely to be limitations on the scope and effectiveness of industry-led measures, which may mean they are insufficient in tackling the problem of number spoofing.

4.43 We understand that blocklists developed by telecoms providers may have technical limitations. For example, one provider [✂] said the more telephone numbers are added to their call blocking tool, the more ineffective it gets as it was not initially built to hold increasingly large quantities of telephone numbers.[105] Furthermore, scammers tend to cycle through number ranges and only use numbers for a limited period of time. By the time a number is added to a blocklist, scammers are likely to have moved on to spoofing other numbers. This is turn can cause further detriment for consumers, if their legitimate numbers are spoofed by scammers, and they receive queries from recipients about calls they didn't make.

4.44 Commercial propositions for consumers, such as call filtering, can give consumers more information about incoming calls, potentially influencing their behaviour (such as declining to answer the call or being wary about the caller). However, these options are not ubiquitous and currently require consumer action, such as downloading (and sometimes paying for) an app, or purchasing an appropriate device. Our 2022 research found that 27% of landline users and 25% of mobile users reported that they are using a call screening or blocking service.[106] These products also rely on crowdsourced data which is not always representative (we have heard from legitimate organisations whose calls are being marked as a potential scam), and options for landline customers are limited.

4.45 The recently announced network-level partnership between BT / EE and Hiya to inform customers of potential scam calls is a positive development. While already also available as a consumer app and as a feature on some mobile phone handsets[107], the integration of a call analytics service into a major provider's network means it will have access to network data which is likely to enhance its call analytics capability. But the extent of its effectiveness in reducing scam and nuisance calls in future is not yet clear, nor the extent to which it, or similar approaches, will be adopted by network providers. Only BT / EE have confirmed it will be available to their customers [✂]. Additionally, other networks may develop alternative proprietary approaches (such as verifying a caller's identity), which may raise questions regarding interoperability.

4.46 At this stage our view is that these industry initiatives, while very welcome, may not provide a sufficiently comprehensive and standardised response to scam calls which deploy number spoofing, especially as scammers adapt their techniques as technologies to detect and prevent scams develop.

[105] [✂] response to Ofcom's information request of 31 August 2022.
[106] Ofcom, CLI and Scams Consumer Research 2022.
[107] Hiya's description of the Samsung Smart Call function.

International developments

4.47 As previously set out, the purpose of CLI authentication is 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.

4.48 This requires two high level components;

a) A method through which to convey this information along with the call;

b) A framework of tools, processes, and governance to support multilateral interworking of a) above.

4.49 Internationally a standards-based approach has been adopted to achieve this (as will be outlined further in the following section):

a) 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 call[109]

b) A framework for deployment of STIR known as 'Signature based Handling of Asserted information using toKENs' (SHAKEN)[110].[111]

4.50 In the US:

- In June 2019, the Federal Communications Commission (FCC) published a Notice of Proposed Rule Making that initially requested operators to voluntarily introduce STIR/SHAKEN by the end of 2019.[112] In March 2020, due to limited voluntary adoption, the FCC mandated that all operators should adopt the STIR/SHAKEN framework for IP based voice networks.[113]
- The deadline for implementation for all operators (except for the smallest), was 30 June 2022.[114]

4.51 In Canada:

- In December 2019[115] the communications regulator, Radio-television and Telecommunications Commission (CRTC) set a deadline of 30 November 2021 for implementation of CLI authentication.[116] This is utilising STIR and an implementation of SHAKEN modified for Canada.[117]
- In July 2022, the Secure Telephone Identity Governance Authority (STI-GA) and the Canadian Secure Token Governance Authority (CST- GA) signed a memorandum of

[108] STIR is primarily defined by the Internet Exchange Task Force (IETF).
[109] Initially specified to support Voice over IP (VoIP), work is ongoing to also support PSTN technologies.
[110] SHAKEN is primarily defined by Alliance for Telecommunications Industry Solutions (ATIS).
[111] SHAKEN was defined for the US but has been closely followed in Canada and formed the basis in France.
[112] FCC, 2022. Advanced Methods To Target and Eliminate Unlawful Robocalls, Call Authentication Trust Anchor.
[113] FCC, 2020. Report and Order: Call Authentication Trust Anchor.
[114] FCC, 2022. FCC Reminds Small Providers of June 30 STIR/SHAKEN Deadline.
[115] CRTC, 2019. Compliance and Enforcement and Telecom Notice of Consultation CRTC 2019-404.
[116] CRTC, 2021. Compliance and Enforcement and Telecom Decision CRTC 2021-123.
[117] CRTC Interconnection Steering Committee Network Working Group, 2021. STIR/SHAKEN Guidelines.

understanding (MoU) to coordinate efforts between the two countries, including STIR/SHAKEN interworking.[118]

4.52 In France:

- In July 2019, the communication regulator, Autorité de Régulation des Communications Electroniques (ARCEP) published a decision to amend the French numbering plan to include several measures, including introduction of a CLI authentication mechanism to protect users against fraud and theft.[119] The deadline for introduction of authentication is 25 July 2023.
- The French approach is based on STIR/SHAKEN.

Other international approaches to tackling number spoofing

4.53 In Finland the approach being taken is twofold.[120] Finnish operators and service providers receiving incoming international traffic to Finland (international gateways) must block:

a) traffic where the CLI is obviously not correct or where numbers belong to Finland's dialling plan (with some limited exceptions);

b) from 2 October 2023; traffic where the CLI is a mobile number belonging to Finland's numbering plan in cases where the number holder is not roaming (abroad).

4.54 The blocking of mobile calls will be achieved through the introduction of a common database where any operator can check whether any subscriber is roaming or not.

4.55 Meanwhile, in Germany, new regulations for improved protection against number spoofing came into force on 1 December 2022.[121] Providers of publicly available telecommunications services must now have the technical means in place to ensure that:

a) calls that falsely display the emergency call numbers 110 or 112, premium rate numbers that begin with (0)900 or (0)137, or numbers for directory enquiries or short code services will not be connected;

b) international calls coming from networks outside of Germany do not display a German telephone number as the presentation number. In such cases the caller's number must be withheld. This does not apply to mobile numbers in international roaming.[122]

4.56 For both Finland and Germany, no data is yet available to assess the relative effectiveness of these regulatory approaches. In the German case there is an expectation there will be an increase in the number of anonymous calls delivered to consumers.

[118] CST-GA. MoU to Collaborate in the Fight to Mitigate Illegal Robocalling.
[119] ARCEP, 2019. Decision No. 2019-0954 amending the decision establishing the national numbering plan and its management rules.
[120] Traficom, 2022. Recommendation to telecommunications operators on detecting and preventing caller ID spoofing.
[121] Bundesnetzagentur, 2022. Improved protection against telephone number manipulation.
[122] German mobile operators must support "home routing" to display CLI for their users when roaming outside of the country. This routes incoming calls from roaming users back to their home mobile operator, allowing the operator to confirm the user is roaming and permit the display of their CLI.

4.57 We will continue to monitor international developments in relation to CLI authentication and alternative measures to tackle number spoofing adopted by other regulators. We would welcome input from stakeholders on the effectiveness of measures taken to tackle number spoofing in other jurisdictions, and whether there are differentiating factors that might be relevant to assessing the effectiveness of similar measures in the UK.

The need for further action to tackle number spoofing

4.58 Our regulatory interventions so far, alongside the actions and initiatives of telecoms providers and other organisations, have been designed to tackle some of the main known methods used by scammers, and, as we have noted, there is some evidence they are having a positive effect. However, the extent of these benefits is uncertain and some potential spoofing scenarios (such as scam calls originated in the UK or mobile roaming calls) are not specifically targeted by these initiatives.

4.59 There are also technical feasibility barriers which limit the effectiveness of current efforts to tackle scams. This is because the ability for a provider to recognise and prevent unlawful calls relies on limited information: the dialled number, the Presentation and Network Numbers (CLI) associated with the call, and, where relevant, the details of the provider with whom they interconnect. As there is a risk the CLI can be manipulated at source by a technically sophisticated scammer, or in transit between networks, CLI data will continue to be potentially unreliable. Similarly, the complex nature of interconnection between providers means that it is unlikely that a UK provider terminating a call can be sure that the intermediate organisations passing calls have all conducted the necessary due diligence on their customers and interconnect partners.

4.60 While some commercial approaches seek to introduce additional information – such as crowd-sourced data to assess, on a real-time basis, whether a call is a potential scam, or to offer incentives to businesses to effectively give recipients confidence about the validity of their numbers – in order to be fully effective, these solutions would need to become ubiquitous, and they are far from that today. This is because they require adoption from both end users (to possess a suitable handset and download the software/app),and for almost all businesses to participate. Additionally, there is little independent oversight of the accuracy of this information, which could lead to erroneous/malicious marking of calls as potentially being scams.

4.61 Furthermore, as we have seen from the implementation of other measures to tackle scam calls and texts, scammers will likely seek to find ways to bypass the measures introduced.

The potential role of CLI authentication

4.62 Therefore, over the medium term, there may be a need for more comprehensive processes to detect and block calls from +44 spoofed numbers across the telecoms industry. CLI authentication could provide a more comprehensive solution. It would entail the introduction of technical standards, so that the network originating the call is able to

confirm the authenticity of the caller's telephone number before passing it to the network of the person receiving the call.

4.63 CLI authentication offers the opportunity to introduce additional information into the call set up network signalling associated with a call – information that can reliably identify the originating provider. Potentially, this could be information that all network providers would be expected to provide and for which manipulation or forgery would be difficult.

4.64 CLI authentication could represent a marked improvement in the information made available to providers, allowing them to make better decisions about whether to pass a call on to their customers. But to take advantage of this facility providers would need to invest in additional systems and processes to access and verify this information. Further, providers that originate calls would need to create and introduce the new information that would be associated with a call to allow the terminating network to have confidence about who has provided this information.

4.65 CLI authentication information could be regarded as complementary to existing measures to counter scams. For example, crowd-sourced data can identify some scam calls even if the numbers being used are not being spoofed.

4.66 As we discuss in Section 6 below, the introduction of CLI authentication may also facilitate more effective and efficient enforcement since it will assist more rapid identification of the person or network responsible for a harmful call, whether or not the number is legitimate.

4.67 Taken together, the blocking of spoofed calls and the facilitation of more effective enforcement has the potential to significantly reduce the volume and effectiveness of scam and nuisance calls that use +44 numbers.

4.68 We therefore consider that it is the right time to consider, in principle, the introduction of CLI authentication, taking advantage of the maturing standards, system availability and implementation learnings and experiences that now exist.

Our 2017 and 2019 consultations

4.69 We first considered CLI authentication as part of our consultation on the guidance on CLI facilities in 2017.[123] This was before the STIR standard was finalised at the international level, and therefore feedback from respondents reflected the early stages of developing approaches to CLI authentication. We subsequently published a statement[124] concluding that given developments and consultation responses, we did not expect CLI authentication to be ready in the UK for at least another three years. We also stated that implementation of CLI authentication would need to be supported by the migration of the majority of voice services to an all-IP platform. We said we would consult again when it was clearer how CLI authentication might be implemented in the UK.

[123] Ofcom, 2017. Consultation: Guidelines for CLI facilities.
[124] Ofcom, 2018. Statement: Guidelines for CLI facilities.

4.70 In 2019, as part of a broader consultation on promoting trust in telephone numbers,[125] we reconsidered CLI authentication, recognising that, while the solution would not prevent all scam and nuisance calls, it had the prospect of making a significant contribution to providing assurance about the identity of the caller.

4.71 At that time, NICC had published a report on how STIR could be implemented in the UK.[126] NICC's main recommendation was that the solution for UK implementation would require a database of numbers assigned for usage and their respective networks (i.e. a common numbering database). It said without such a database the approach would be of limited value since this would only provide a pointer back to the network that originated a call, rather than whether they had any rights to use the associated CLI. NICC also noted that populating such a database would be a significant undertaking in terms of scale and ensuring the integrity of the data.

4.72 In the 2019 consultation,[127] we explored a number of wider issues including:

a) The possible use of blockchain to reduce scam and nuisance calls: at that time, we were at a 'proof of concept' stage in assessing whether distributed ledger (blockchain) technology could provide the basis for establishing a common numbering database.

b) The timeline for implementation of CLI authentication, based on the migration to IP: we said that STIR could only be implemented effectively in standards-compliant IP networks, and therefore would only have a beneficial impact once a significant proportion of traffic is originated and carried on such networks. This suggested that implementation could potentially start around 2022 and would grow over time until PSTN switch-off was complete around 2025.

4.73 We published stakeholder responses to the consultation and below we briefly summarise the responses.

4.74 Industry responses at the time were broadly supportive of CLI authentication and more specifically STIR as a method to reduce nuisance and scam calls. However, several providers, industry bodies and associations noted that implementation of STIR would not eliminate scam calls as they said it would not resolve the issue of spoofed calls originating from abroad.

4.75 Vodafone raised concerns about STIR being a "large sledgehammer to crack the wrong nut", but said that, given the US deployment, it would be sensible for the UK to follow international standards. Tata and iconectiv also said that since other countries have implemented STIR, it would be a sensible approach for the UK.

4.76 Having conducted further analysis into the feasibility of blockchain and given our and industry's priorities during the Covid-19 pandemic, we decided not to pursue further consideration of the proposals in the 2019 consultation at that time.

---

[125] Ofcom, 2019. First consultation: Promoting trust in telephone numbers.
[126] NICC, 2018. Report into implementation of Secure Telephone Identity Revisited (STIR) in the UK. See, in particular, page 31.
[127] Ofcom, 2019. First consultation: Promoting trust in telephone numbers.

Industry suggestions to address number spoofing

4.77 A few alternative measures were suggested in responses to our 2019 consultation including:

a) Magrathea suggested greater monitoring of adherence to CLI guidelines;

b) the Mobile Ecosystem Forum suggested stronger business processes (or "know your customer" checks) in number allocations for both fixed and mobile numbers;

c) Virgin Media argued that, if end users of a Type 5 Presentation Number[128] were made more accountable by Ofcom, the benefits would come quickly and at a much-reduced cost for telecoms providers.

4.78 In addition, TalkTalk's subsequent report on the prevention of number spoofing identified some possible limitations with the adoption of STIR, claiming that it would not solve the problem of internationally spoofed UK Presentation Numbers, and claimed that it would only really add value for calls within the UK. [129]

4.79 As we have outlined in this section, we subsequently advanced a number of initiatives to tackle scam and nuisance calls, including in partnership with the industry. With the migration to IP networks now in progress, we consider that now is the right time to reassess the case for CLI authentication as a potentially more comprehensive response to tackling number spoofing, which we explore in more detail in subsequent sections.

Consultation question

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

[128] Presentation Numbers that identify separate groups of callers behind a private network switch wishing to send different outgoing CLIs. A typical scenario is a call centre making calls on behalf of more than one client.
[129] TalkTalk, 2020. Prevention of UK Number Spoofing (unpublished).

5. Our view of how CLI authentication could work

5.1 In the previous section we explained how we already have some initiatives in place to reduce scam calls. We set out how we have recently strengthened our rules requiring telecoms providers to detect and blocked spoofed numbers where possible, and published related guidance and a separate good practice guide to help prevent scammers accessing valid phone numbers. These are being implemented now and offer some immediate benefits to consumers. However, although these interventions will hinder specific scam scenarios, scammers can and do change their methods in order to circumvent them.

5.2 We also explained that industry initiatives such as call filters, phone apps and block lists often rely on consumer adoption and handset compatibility, and that even when used, technical limitations can limit their effectiveness in preventing scams. While other initiatives to combat scam calls are planned or in early stages of implementation by individual providers, it is unclear at this stage how successful they will be. We therefore foresee that further regulatory intervention might be required to prevent harmful spoofing and the harm caused by spoofing-enabled scams.

5.3 In this section we set out measures that we consider would make it harder for calls from spoofed numbers to be delivered to UK numbers. We explain what CLI authentication is, describe the technical detail of how it could work in the UK, highlight where different treatment might be appropriate and outline how it could be effective to address number spoofing.

5.4 We are inviting views from stakeholders as to whether the proposals we have set out provide a feasible and credible means to counter spoofing and thereby reduce scams and other illegitimate calls.

5.5 The methods discussed in this section are based on the STIR standards, which have already been implemented in the US and Canada, and to a lesser extent, the associated SHAKEN framework (see Annex 1 for further information).[130]

The purpose of call attestation

5.6 As discussed in Section 3 the CLI data associated with a call, in particular the 'Presentation' and 'Network' Numbers, can be omitted, lost or manipulated either at source or in transit between the caller and called party. If the Presentation Number is manipulated, this may mean the number on a caller display mimics the number of a real company or person that

[130] STIR/SHAKEN is the set of standards which is being used for CLI authentication in the US and Canada. See FCC, Combating Spoofed Robocalls with Caller ID Authentication. STIR is a set of standards that describe the mechanics of CLI authentication signalling. See IETF, Secure Telephone Identity Problem Statement and Requirements: RFC 7340. SHAKEN is a framework which defines the use of STIR and other elements to make up a complete ecosystem as defined by the Alliance for Telecommunications Industry Solutions (ATIS) in a number of standards including ATIS, ATIS 1000074: Signature-based Handling of Asserted information using toKENs (SHAKEN).

is known to the recipient, although that company or person has nothing to do with the actual caller. Alternatively, it can mean that the Network Number (received by the recipient's network provider) may not correctly identify the network that placed the call onto the public telephone network. We refer to this as 'spoofing' and the numbers used in this scenario as 'spoofed numbers'. This lack of assurance as to the validity of the Presentation Number and Network Number can undermine trust in the phone network as well as offering a pathway for scammers to operate.

5.7 Call attestation 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. [131] 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; we discuss the action that we consider it should take as a result in paragraphs 5.17-5.20 below.

5.8 Therefore, call attestation both needs 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).

5.9 This authentication and attestation information can then be passed to the network receiving the call (the terminating provider) which as a result will know the information associated with that call, including the telephone number, is legitimate. [132] The terminating provider is able to validate the information it receives in what we refer to as an 'attestation passport '.[133] [134] As a result, customers can have greater confidence that the number displayed accurately identifies the caller.

5.10 In turn, the absence of an attestation passport enables the terminating provider to identify and block spoofed calls, removing the scammer's ability to hide the network that they are using to make calls and / or use numbers which they are not permitted to use, to hide their identity or pretend to be someone else.

[131] The specific numbers and other information that forms part of the technical authentication process would largely be a matter for industry to agree. We note that in the 2020 technical report by the NICC on STIR implementation, it was the originating provider's 'P-Asserted-Identity' (Network Number) that was proposed to be included in the secure PASSporT, although this may be revised in future publications. See NICC, 2020. Report into implementation of Secure Telephone Identity Revisited (STIR) in the UK (NICC ND1522V2.1.1).

[132] Several pieces of information are passed to the terminating provider along with the call; the key ones being the caller's telephone number and a confidence level associated with the legitimacy of the caller's telephone number (attestation).

[133] To note, we use the term passport in the descriptive sense, and do not follow precisely the technical definition of Personal Assertion Token (PASSporT), a token object that conveys cryptographically signed information about the participants involved in communications, as described in the STIR specification.

[134] We expect information to be signed using cryptographical methods.

Our envisaged approach to call attestation

5.11 The rest of this section sets out how we envisage a call attestation regime could operate in practice in the UK.

5.12 Because not all calls originate within the UK, our envisaged call attestation approach will need to also account for calls entering the UK for which no attestation has been supplied and where confirmation of originating network or number cannot be provided.

5.13 Therefore, we consider both intra-UK calling (i.e. where both originating and terminating providers are within the UK), and other scenarios, in particular international calls to UK customers. The responsibilities of the key organisations involved are discussed along with relevant expectations and incentives to ensure that the proposed approach works as envisaged. We avoid, where possible, specific technical details as relevant standards and systems continue to evolve.

5.14 The actions a terminating provider might take drive the incentives of the originating provider to comply with the process. We therefore first consider the role of the terminating provider, the information that might be available to them, and what actions they might take as a result of this information. We then consider the actions of originating and gateway providers that introduce calls onto the public telephone network and how they would generate information to associate with their calls to steer the actions of the terminating provider. Finally, we consider how exceptions to the proposed approach may arise and their potential mitigations.

The role of the terminating provider

5.15 The principle of call attestation expects all calls made over the public telephone network to be accompanied by an attestation passport transmitted alongside the call. All terminating providers must inspect the attestation passport accompanying each incoming call's set-up protocols and signals to verify that it has the correct authentication credentials and that the call has originated from an identified network.[135] [136]

5.16 Additional measures may be taken by the terminating provider to confirm that numbers associated with the call, in particular the Presentation Number, are being used legitimately. This may be achieved using a common numbering database (which is discussed further below), or through other means, such as number allocation records from Ofcom[137] or through its own databases and systems.

5.17 If the inspection of the attestation passport (and any other associated checks) is successful, the terminating provider connects the call and provides the Presentation Number to the end user (unless the caller has requested it to be withheld). However, if the checks fail for

[135] A terminating provider can receive a call either directly from the originating provider or via an intermediary or transit provider.
[136] To prevent these credentials from being manipulated, copied or forged by others, these credentials would need to be digitally signed.
[137] Ofcom's webpage on Telecoms numbering.

any reason, then the terminating provider would need to take a different approach. We consider that there are three broad options for terminating providers in this situation:

a) Prevent the call from reaching the end user (i.e. block the call).[138] Potentially the terminating provider might notify the caller of this, for example via playing a message indicating the call was unsuccessful.

b) Divert the call to a junk voicemail system so that the end user can listen to any message and decide whether to call back. However, this may lead to consumer dissatisfaction as they have to call their voicemail to listen to a message they potentially didn't want to receive, as well as offering an opportunity for scammers to leave a voice message which may mislead the end user.

c) Pass the call to the end user but alert them that the inspection of the attestation passport was unsuccessful and therefore the Presentation Number has not been verified.

5.18 We consider the blocking of calls that have not been successfully authenticated to be the optimal outcome for securing end-user protection from harmful calls. This is because alternative approaches, such as alerting the called party that the call does not have verified attestation through an audio announcement before the call is connected or displaying a warning message on the called party's handset, are in our view unlikely to provide sufficient protection to consumers and may be technically complex. Displaying a warning message could require compatible handsets, while our research indicates that a quarter of end users with call screening services still answer a call despite knowing it to be suspicious, limiting the effectiveness of this approach. [139]

5.19 We also consider that the blocking of unverified calls will provide an incentive for originating providers to satisfy themselves that the customer making the call can legitimately associate a specific Presentation Number with that call and therefore the call can be attested. Other approaches may not have sufficient incentives to ensure attestation is carried out for all calls.

5.20 Under a regulatory scheme for the implementation of CLI authentication, we anticipate that action by terminating providers to prevent calls without verified authentication from being connected would be underpinned by a regulatory measure, such as a modified General Condition or updated guidance to the existing relevant General Conditions.

The role of the originating provider

5.21 Originating providers will need to attest each and every call originated on their network. This will require them to satisfy themselves that the customer originating the call can legitimately associate a specific Presentation Number with that call and then authenticate this information with their own identity. This can then be passed across the public telephone network as a completed attestation passport. If an originating provider fails to

[138] General Condition GC C6.6 may apply in such circumstances.
[139] Ofcom, 2021. Scams research 2021, slide 28.

associate an attestation passport with a call, the call would be blocked by the terminating provider.

5.22 In practice we envisage a system of digitally signed authentication credentials associated with each outbound call during call setup. Digital signatures are used as they cannot be easily manipulated by intermediate networks between the originating provider and terminating provider. A trusted third party would be needed with which originating providers can register and provide the necessary certification information and from which terminating providers can obtain necessary information to verify the digital signatures for each received call. In this consultation we shall use the term CLI Authentication Administrator (or simply the 'Administrator') to describe this entity.[140]

5.23 The CLI Authentication Administrator will need to perform a number of functions, including the critical function of the certificate authority, the trusted holder of certification information associated with each registered originating provider. This is discussed further below.

5.24 Because of the expectation that digitally signed authentication credentials would be used, and these could only be issued by a CLI Authentication Administrator, every originating provider in the UK would need to register with the Administrator who would hold the information necessary to independently verify the originating provider's credentials. Consequently, a terminating provider receiving a call can verify the attestation passport by using the information held by the Administrator.

5.25 Finally, because of the need for all UK providers to coordinate with the CLI Authentication Administrator in order to successfully originate and terminate calls, we would expect this entity to be a body of which all UK providers would be members. The membership rules of the Administrator, which in a regulatory scheme we would expect to be subject to approval by Ofcom, would include the processes that providers must follow for the operation of the authentication system (including how digital signatures will operate).

The verification of calling party numbers

5.26 In the approach described above, only calls where the originating provider has associated an attestation passport which has been validated by the terminating provider would be presented to call recipients. While the authentication provided in an attestation passport ensures the originating provider can be identified, it does not, in itself, confirm that the originating provider has legitimately associated a specific Presentation Number with that call (i.e. the attested number). We therefore expect that further actions are taken by the originating provider and for it to be satisfied that its customer has the necessary permissions to use the number associated with the call.

[140] This entity will include the roles such as that of STI-CA, STI-PA and STI-GA as described in the SHAKEN framework. See ATIS, 2017. ATIS-1000074: Joint ATIS/SIP Forum Standard – Signature-based Handling of Asserted information using toKENs (SHAKEN).

5.27 We recognise that although originating providers may have a strong incentive to ensure that calls are attested so that they are not blocked by the terminating provider, there may be less incentive for the originating provider to conduct sufficient due diligence on whether its customer can legitimately associate a specific Presentation Number with that call.

5.28 We therefore consider that our approach requires an additional expectation that originating providers check the validity of the numbers used by their customers for outbound calls and satisfy themselves that the numbers associated with the call are not being misused. These checks should include the correct use of Network Number, and where the Presentation Number is different to the Network Number, that the customer has the necessary permissions to use the number.[141]

5.29 If the originating provider is unable to satisfy themselves about the legitimacy of the numbers being used, they must not attest that call.[142] Where a customer provides proof of permission to use specific numbers, we envisage that the originating provider would need to record this proof and take any necessary steps to verify that the permission is genuine.

5.30 An originating provider that fails to conduct these checks could be identified as some calls they incorrectly attest may come from spoofed numbers, leading to complaints raised with terminating providers by end users. In turn, the terminating provider can report the originating provider using the information provided within the attestation passport. We would expect the CLI Authentication Administrator to collate such reports and where appropriate pass this information to Ofcom and other authorities for possible enforcement. We discuss this further in Section 6.

5.31 We believe that the incentives placed on the originating provider to correctly attest each call would be strong. This is because if the originating provider fails to correctly attest a call, either the call will be blocked, or this may be discovered after the call has been passed to the end user. Therefore, in normal practice no call should be passed from a UK-based originating provider which has not been fully attested, and therefore no UK originated call should be blocked by a terminating provider.

The potential use of a common numbering database

5.32 We consider that the creation and use of a common numbering database could play a role in CLI authentication by offering an additional mechanism to allow terminating providers to check that numbers are being used appropriately before passing calls to their customers. We note that such a database may serve many purposes for providers and the associated

[141] Ofcom, 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers, Annex 2, para 3.1. - 3.4 and Ofcom, 2022. Updated guidance on the provision of Calling Line Identification facilities and other related services, Annex 2 para 4.13.

[142] While the STIR standard allows for a third category of attestation ('partial'), we do not consider that it is necessary given our proposed expectations on originating operators not to attest calls for which they are not satisfied that its customer has the relevant permissions.

industry (such as to facilitate porting, routing and number management), but these are out of scope of our discussion in this document.

5.33 In the context of CLI authentication the purpose of a common numbering database would be to provide independent confirmation that the numbers associated with the call are valid and the originating provider is able to legitimately attest them. Specifically, a common numbering database would be used firstly to confirm that the Network Number associated with the call is allocated to and in use by the originating provider and has been verified through the call attestation process.

5.34 Secondly, this database could additionally be used to verify that the Presentation Number[143] displayed to the end user is being used correctly and potentially offer the originating provider confirmation that a number it is being asked to attest is assigned to a specific organisation. The extent to which this might be possible would depend on the degree to which a common numbering database can record not only the provider to whom a number has been allocated but also the end-user organisation that the provider has given permission to use that number.[144] This therefore depends on the specific database architecture, its granularity, the frequency at which information is updated and who has permission to enter the updates. [145]

5.35 At this stage, we do not have a strong view as to whether the creation of a common numbering database either for Network Numbers only, or Network and Presentation Numbers, should form a necessary part of the overall call attestation process. We acknowledge that the creation and maintenance of the database would be likely to require significant time and resources and note that the specific design of any database and the frequency and granularity of updates would materially affect both its effectiveness and its costs. We also recognise that a common numbering database could potentially be introduced at a later stage, following the introduction of CLI authentication.

5.36 In summary, the inclusion of a common numbering database to complement the proposed authentication process would offer additional information to industry and hence reduce the opportunities for spoofing. This would reduce consumer harm, lessen the frequency of terminating providers reporting issues to the CLI Authentication Administrator, and ultimately would likely lessen the need for potential enforcement action by Ofcom and other authorities. However, we recognise that there are likely to be significant costs associated with securing these potential benefits.

5.37 We discuss the implementation of any potential common numbering database in Section 7.

[143] Presentation Number or SIP 'From' header.

[144] In general, for calls from residential lines the Presentation Number will be the same as the Network Number. Business organisations often use different Presentation Numbers to assist customers and consumers call back to dedicated operators.

[145] Because Presentation Numbers can be ported across providers, a common numbering database would need to be regularly updated to ensure it reflects accurate information. We do not explore how frequently this may need to happen in this document.

Calls entering the UK from abroad

5.38 Up to this point we have been considering the scenario whereby a call originates and terminates within the UK between UK providers. Although this scenario will likely cover the majority of calls received in the UK, when a call enters the UK from abroad the originating provider will not be obliged to provide attestation under our proposed approach.[146]

5.39 Calls entering the UK from abroad fall into two categories:

a) calls that bear international telephone numbers e.g. standard international calls arriving in the UK from individuals and businesses outside the UK.

b) calls that bear UK telephone numbers – calls arriving from abroad but that appear to be originating from a caller in the UK.

5.40 Considering the second category, calls that bear UK telephone numbers, we recently set out legitimate use cases where calls from abroad with UK CLI as a Network Number might be expected. [147] These were:

a) UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range;[148]

b) calls to a mobile user who is roaming in the UK;

c) where the traffic has originated on a UK network[149]; or

d) where the traffic has originated from UK customers that are hosted on overseas nodes or cloud services.[150] [151]

5.41 When a call enters the UK from abroad bearing a UK mobile telephone number there are often a limited number of checks the provider bringing it into the UK (the gateway provider) or the terminating provider can conduct to determine if the numbers presented are legitimate. As noted in Section 4, some countries are examining the implementation of a national '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. We

[146] Interworking, or the mutual recognition of CLI authentication between countries may be possible in future.
[147] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data.
[148] Current international mobile roaming over 2G and 3G networks allows for the UK registered number to be used, so calls back into the UK would bear UK numbers, despite being carried by international networks. As the timescales for 2G/3G network retirement are dependent on the evolution of mobile networks around the world, it is likely that these calls will continue to arrive in the UK for the foreseeable future, although diminishing in numbers.
[149] In some cases, traffic originated on a UK network may be routed out of the UK and back in again.
[150] This includes calls from international call centres making calls legitimately on behalf of UK businesses and therefore using appropriate non-geographic (e.g., '0800') numbers to identify the business on whose behalf the calls are being made. Such calls may traverse a number of intermediate networks before interconnecting with a UK network.
[151] As discussed in our November 202 statement, Improving the accuracy of Calling Line Identification (CLI) data, calls from UK customers hosted on an overseas node should be routed over a pre-agreed interconnect. We also indicated that callers from abroad could also continue to use a UK CLI as a Presentation Number provided that the Network Number identifies the source of the call, for example by using a number from the country where the call has originated. However, situations may still arise whereby legitimate calls enter the UK without being routed over a pre-agreed interconnect.

invite stakeholder views as to the feasibility and effectiveness of this approach, either on its own or in conjunction with the CLI authentication approach set out here.

5.42 In line with our recent Statement on improving the accuracy of Calling Line Identification (CLI) data, we expect calls from abroad with UK CLI as a Network Number that do not meet the legitimate use cases to be blocked by the gateway provider. However, for calls entering the UK and bearing international telephone numbers, gateway providers cannot block them, as it would in effect potentially prevent legitimate calls from overseas to the UK.

5.43 However, the gateway provider when receiving a call from abroad without attestation could add its own authentication 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. This would be case regardless of whether the call bears an international telephone number or a UK telephone number.

5.44 Although the gateway provider may not be able to fully attest the numbers that accompany the call, it could provide an alternative type of attestation, which we refer to as 'gateway attestation', which would allow the terminating provider to know how the call arrived into the UK, and that it was not possible to fully attest the number.

5.45 As part of the gateway attestation process, 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 are currently in use by the relevant overseas provider.[152]

5.46 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. We would expect the CLI Authentication Administrator to collate such reports and where appropriate pass this information to Ofcom.

5.47 We therefore suggest that proposing an additional gateway attestation level combined with the ability to identify the gateway who received the call may reduce the risk of calls originating overseas being used for scams.

5.48 Should we proceed with detailed proposals for a regulatory scheme which includes gateway attestation, it is likely that we would expect the rules of the Administrator to prohibit the use of gateway attestation by providers for calls made by their own customers irrespective of location. This is to prevent the use of gateway attestation as a default option where the provider is unable or unwilling to conduct the necessary due diligence on the correct use of numbers by its customers.

[152] The extent to which this is possible may be dependent on the existence and capability of common numbering databases in other countries and we acknowledge this will not be possible in a significant proportion of cases.

Calls from the Crown Dependencies

5.49 In the CLI statement 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.[153] Ofcom allocates numbers directly to providers that operate in the Crown Dependencies. We noted that most calls from the Crown Dependencies using +44 numbers enter the UK network via a national interconnect and therefore calls originating from the Crown Dependencies would not be impacted by our November 2022 CLI guidance.

5.50 However, because the Crown Dependencies are not part of the UK and not subject to our regulation, there is a risk 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 can continue to be used for calls to the UK without attestation, would create a loophole which scammers may look to exploit.

5.51 When looking at how to minimise such a loophole, we have identified three options:

a) 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. This is not a matter that Ofcom could mandate so our expectation is that this would be done on a voluntary basis by the providers operating in the Crown Dependencies, unless regulators in the Crown Dependencies were to mandate membership.

b) Providers operating in the Crown Dependencies could work with their (UK-based) national interconnect partners so that the UK partner can fully attest calls originating in the Crown Dependencies and entering the UK public telephone network. This would require systems to be put in place, so the UK provider is able to verify with the Crown Dependency provider that the caller in the Crown Dependency has the right to use the numbers.

c) 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 calls arriving from abroad. We would expect providers to identify legitimate calls from Crown Dependency number ranges and ensure that these are not blocked. However, although a less onerous option, this could result in such calls being at greater risk of being blocked if UK providers identified patterns in calls coming from a Crown Dependency that would indicate they were suspicious. This option could still allow +44 spoofed numbers to enter the UK.

[153] Ofcom, November 2022. Statement: Improving the accuracy of Calling Line Identification (CLI) data, paragraph 4.114.

Technical failures

5.52 The scenarios thus far considered assume that the systems required by the originating provider to support CLI attestation are working as expected. We recognise however that there may be occasions where for reasons beyond the provider's reasonable control an originating provider is unable to provide attestation but is still able to originate a call. Alternatively, the originating provider may have attested the call, but this attestation has been lost as the call traversed intermediate networks.

5.53 In such circumstances we would expect the provider who discovers attestation is absent to make efforts to contact the originating provider to understand why they are being passed calls without attestation and record that reason. If the provider who discovers that attestation is absent cannot satisfy themselves to the legitimacy of the reason for non-attestation, they should neither attest that call nor pass it to another provider or their own customers.

5.54 If, however, the provider who discovers attestation is absent can satisfy themselves to the reason the call does not have attestation it should follow a similar process to that of a gateway provider and add gateway attestation, which would allow other providers in the call's journey to know who had added attestation to the call and that the number could not be fully attested.

5.55 In order to ensure that gateway attestation is used appropriately, we suggest that the provider who discovers attestation is absent should report to the Administrator any instances where it has received a call from another UK provider that is without attestation. We would expect the CLI Authentication Administrator to collate such reports. If a pattern emerges from such reports which raises questions about why an originating provider has passed calls without attestation, it may be appropriate for the administrator and potentially Ofcom to take further action. (See paras 6.14-6.19.)

5.56 In circumstances where the terminating provider is unable to check the validity of the attestation passport due to its own technical failure, it should ensure it does not default to blocking all calls it receives. Reasonable steps should be taken to protect against such failures, and we envisage that the terminating provider should record details of failures, and report to the Administrator.

5.57 It should be noted that calls to the emergency services should not be blocked or otherwise impaired by operators even if they do not have authentication information. Therefore, even in the event of a systems failure that prevents authentication from taking place, calls to the emergency services should be unaffected.

The role and functions of the CLI Authentication Administrator

5.58 In the description of the call attestation process above, we have already referred to some potential functions of the CLI Authentication Administrator. A proposed governance framework for the Administrator is described in Section 7; here we summarise a number of

technical functions that could be carried out by or on behalf of the CLI Authentication Administrator.[154]

5.59 First, as explained at paragraphs 5.22-5.25 above, the Administrator would hold certification credentials of all UK providers[155] so that terminating providers can use these credentials to identify the network that inserted the call into the UK public telephone network.

5.60 Second, the Administrator could be responsible for the creation and management of the underlying systems that store and make available digital signature credentials of providers in a secure and reliable manner.[156]

5.61 Third, the Administrator could have oversight of the process to 'onboard' new providers onto the systems which support the attestation process. This may include any relevant checks and other due diligence to ensure that provider information is accurate and complete. While we envisage that the criteria for membership of the CLI Authentication Administrator would seek to avoid creating any disproportionate barriers to entry, we do expect some level of checks to take place to identify, for example, organisations creating unnecessary accounts for testing purposes.

5.62 Fourth, the Administrator could be involved in the recording and monitoring of call attestation statistics from providers.[157] We have described above how the monitoring of attestation is important as it incentivises compliance with the process.

5.63 Fifth, the Administrator could have the ability to conduct audits and inquiries into the systems and processes of providers with respect to CLI authentication, either in response to specific complaints or issues, or as part of monitoring of compliance with its rules. This is explored further in Section 6.

Summary

5.64 The section has outlined, at a high level, a suggested approach to call authentication and number attestation. It proposes 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.

5.65 The process we suggest also includes steps for providers that are acting as 'gateways' for calls into the UK from abroad. We seek feedback from stakeholders as to the feasibility of

[154] Given the various functions considered, it is uncertain if these will all be conducted by a single entity. Observations on the relevant organisational structures adopted in other countries suggest that some functions may be undertaken by multiple organisations.

[155] This includes gateway providers. Additionally, originating providers will be classified as a terminating provider when receiving a call and vice versa.

[156] Any system would likely need to have high availability to ensure credentials are available on demand from terminating providers wishing to verify authentication records. It should also have the necessary security to prevent the modification or deletion of these records.

[157] This could include calls without attestation and a breakdown of calls that have full and gateway attestation and may be recorded in real time or through bulk data transfer from providers.

the approach and whether other steps or measures should be considered to make this approach more effective.

Consultation questions

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.

Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?

6. Enforcement

6.1 The previous section set out our suggested approach to how CLI authentication might operate in the UK. We explained that under our suggested approach, originating providers attest the numbers used by their customers (for almost all +44 calls) if they are satisfied that they are legitimate; on receipt of the attestation, 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 terminate the call by default.

6.2 We recognised that there will 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, because connecting calls without attestation creates the risk of loopholes that could be exploited by scammers, our expectation is that the rules that will support attestation will need to balance the need to connect legitimate calls with the need to minimise any exploitable loopholes.

6.3 This section considers how the attestation regime might be policed to ensure compliance with the rules. We first discuss our approach to the enforcement of attestation rules. We then consider the potential impact of CLI authentication on enforcement against scam and nuisance calls, and improvements to call traceability.

Our approach to enforcement of the attestation rules

6.4 Should we choose to proceed with detailed implementation proposals, we would expect to set out in a subsequent consultation proposed modifications to the General Conditions that would allow this regime to function. In this consultation we have not made specific proposals, but instead set out the regulatory structure that we envisage could form the basis of modified General Conditions that we would propose.

6.5 This regulatory structure would:

a) require providers to establish and be a member of of the Administrator, the body which would carry out the functions described in this Section and Section 5.

b) require the Administrator to have membership rules, subject to the approval of Ofcom, which would govern the implementation and operation of CLI authentication; and

c) require members to comply with the membership rules of the Administrator.

6.6 We suggest that the membership rules would have to address:

a) how the attestation regime would work, including how to handle calls without attestation, what would be considered incorrect attestation, and when issues should be reported to the Administrator;

b) how the Administrator would monitor the operation and compliance with its membership rules; and

c) what measures could be taken against a provider in the event of a failure of its authentication processes, including for example, an action plan for improvement or referral to Ofcom for consideration of enforcement action for non-compliance under the General Conditions;

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

6.8 We outlined in Section 5 some examples of reporting to the Administrator by providers, for example that a provider who discovers attestation is absent should report to the Administrator any instances where it has received the call from another UK provider. We would expect the Administrator to collate such reports and pass, where appropriate this information to Ofcom for possible enforcement.

Types of infringement

6.9 Under our proposals, the enforcement approach differentiates between:

a) inadvertent or irregular infringements of the rules; and

b) more persistent or serious infringements.

Inadvertent infringements

6.10 There are a variety of reasons why providers may inadvertently breach the rules. For example, providers may have systems and processes that are still being developed to check a customer's right to use a number, so that they may fail to pick up when a customer is misusing a number and as a result fully attest a call incorrectly. Technical failures, such as system outages, could also occur and result in an originating provider being unable to attest calls. We outlined in Section 5 some of the potential steps that providers might need to take in the event of such failures.

6.11 Such inadvertent transgressions would be detected through the regular monitoring and reporting mechanism set out by the Administrator and shared with Ofcom on request. Persistent issues could be dealt with through, for example, recommended improvements to providers' processes.

More persistent or serious infringements

6.12 There may also be examples of more persistent non-compliance or serious breaches of the rules. In such cases, the conduct of the provider may have serious consequences in terms of the effectiveness of the scheme or actual or potential material consumer harm. We would expect such cases to be identified through reporting and monitoring by the Administrator. In addition, we would expect other information from terminating providers

about suspicious activity that they have identified on their network to help the Administrator to identify potentially problematic providers. In the event of such suspicions, we envisage that the Administrator would be able to conduct inquiries where these issues arise to assess whether breaches of its membership rules have occurred.

Supervisory measures and escalation to Ofcom

6.13 In order to allow the Administrator to distinguish inadvertent or irregular infringements of the rules from cases of persistent non-compliance or serious breaches, we would expect providers to be open with the Administrator about the actions they have taken to ensure compliance, for example, the checks they have carried out to ensure the legitimate use of numbers and how they have evaluated the effectiveness of their action. We would expect providers to engage constructively with the Administrator to resolve any issues.

6.14 However, where the Administrator considers that a provider is not taking appropriate action to comply with its rules, it will be able to intervene.

6.15 One potential action the Administrator may consider in these circumstances would be to place a provider into a period of enhanced monitoring and supervision. Such a step would give the provider the opportunity to make any improvements necessary to its processes, enable the Administrator to share good practice from across the sector and gain confidence that the provider will be consistently following the rules when they exit the period of enhanced monitoring. We would expect that providers would have a duty under the membership rules to cooperate with the Administrator and implement with any directions it may give.

6.16 If improvements are not forthcoming, the Administrator could refer the matter to Ofcom. We would then consider whether to open an investigation into the provider's compliance with the General Conditions. More generally, where issues come to our attention in relation to operation of CLI authentication, whether as a result of information provided by the Administrator or otherwise, we will consider whether the matter could be resolved by the Administrator under its rules or whether formal enforcement action under the General Conditions is appropriate. We would expect to work closely with the Administrator, particularly during the initial period when the scheme becomes operational, to ensure a coherent approach to the oversight and enforcement of the new regime.

6.17 Because Ofcom is responsible for the regulation of communications providers under the Act, including the enforcement of their obligations under the General Conditions, we do not consider that it would be appropriate for the Administrator to have powers under its rules to impose sanctions on its UK members in the event of non-compliance, such as penalties or suspension or expulsion.

6.18 We consider the position would be different for non-UK providers, which have become voluntary members of the Administrator (assuming the Administrator makes this possible under its rules) in order to ensure the acceptance and termination of their attested calls. Such providers do not fall under the jurisdiction of Ofcom. Accordingly, it would not be possible to refer such providers to Ofcom for formal enforcement action and therefore an

alternative form of enforcement action would be needed. We envisage that in such circumstances, the membership rules might allow the Administrator to suspend or expel non-UK providers from membership in the event of serious non-compliance, to protect the integrity of the CLI authentication regime.

Enforcement against scam and nuisance calls

6.19 We believe the rules outlined in Section 5 could be effective in substantially reducing the spoofing of +44 numbers in telephone calls. However, some scam and nuisance calls will continue to be connected. For example, scammers may decide to make calls with numbers that they legitimately control, rather than spoofing numbers. This would enable them to make fully attested calls which would be connected by default. Effective enforcement action against scammers and nuisance callers therefore remains an important part of our approach.

6.20 The Administrator would have no remit over the content of calls. Enforcement in relation to the content of calls would be a matter for Ofcom or other enforcement bodies, depending on the particular issue, as set out below.[158]

Action by Government and other regulators in relation to scams and nuisance calls

6.21 The ICO regulates the use of live and recorded marketing calls and has powers to take enforcement action against people who make unlawful live and recorded marketing calls. The ICO also manages the Telephone Preference Service, which enables consumers to opt out of receiving marketing calls. The ICO has worked jointly with Ofcom on tackling nuisance calls since 2013.

6.22 Fraud, which includes scam calls, is a priority for Government and law enforcement bodies, given the scale of the issue and the increase in this type of activity. A number of other regulators are also undertaking work to tackle other aspects of scams, including the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR).

Call traceability

6.23 A major challenge today for any enforcement body is 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.

6.24 Ofcom is responsible for the administration of the UK's phone numbers under the Communications Act 2003. Providers who have been allocated numbers by Ofcom are able

[158] Ofcom, February 2022. Tackling scam calls and texts: Ofcom's role and approach - *Where telephone numbers or services have been misused, Ofcom can request that providers block access to those numbers or services, and Ofcom can withdraw number allocations if the numbers have been used to cause harm and the provider has not taken adequate steps to prevent this. Under sections 128 to 130 of the Communications Act 2003, Ofcom can take enforcement action against a person who has persistently misused a communications network or service, which may include where communications services are persistently used to facilitate scams. For an overview of other bodies with responsibilities in this area.*

to sub-allocate those numbers to other providers and resellers or assign them to end users. Sub-allocated numbers may be further sub-allocated or assigned, and other providers may manage connectivity on the sub-allocatee's behalf.

6.25 Customers may also port numbers when they switch providers to enable them to continue using the same number with a different provider. As a result, the provider who was originally allocated the number is often no longer in control of the number. There is no central record of where such changes have taken place and which provider is the current controller of a number.

6.26 As a result, when a complaint is made about the content of a call or where there is a pattern of suspicious calls, the terminating provider can normally identify the upstream provider who passed them the call but cannot necessarily directly identify which provider originated the call or how it entered the UK network.

6.27 In order to identify the originating provider, or the entry point into the UK network, it is necessary to trace back through the call routing, starting with the 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 onto the terminating provider, which delays the process.[159] This process is also dependent on the co-operation of the providers to respond to requests in a timely way and is a time-consuming and resource-intensive job for both enforcement agencies and providers.[160]

6.28 Call tracing is also hampered by the data retention practices of the providers, who may only retain the call records for a few days. Therefore, call tracing requests must be made promptly to be successful. Furthermore, for scam calls originating overseas, where the call traverses networks in multiple jurisdictions, overseas providers could ignore or take longer to respond to tracing requests, reducing the likelihood of the originating provider being successfully identified.

Improvements to current call tracing process

6.29 CLI authentication could enable a different and substantially more effective approach to call tracing. The attestation passport 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.

[159] In the US, most illegal calls often contain between 5-8 hops for a single call. See USTelecom – The Broadband Association. Traceback 101.

[160] The NICC has standard guidelines for the call tracing process. See Guidelines for the Tracing of Calls Across and Between Networks. Ofcom, 2019. Guidance on the provision of Calling Line identification facilities.

6.30 This would enable enforcement agencies to take more timely action and refocus resources away from the task of tracing calls through multiple providers as well as reducing the number of traceback requests providers would receive.

Consultation questions

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?

7. Implementation

7.1 This section sets out our initial views on how CLI authentication could be implemented in the UK as a regulatory scheme. It begins by outlining our views on timeframes, before describing the key tasks that would be required to implement CLI authentication.

7.2 As explained above, if we decide to propose the introduction of CLI authentication, we will set out our proposed approach to implementation in detail in a further consultation. However, our initial view is that our proposals would provide scope for providers to collectively develop aspects of the regime, where they are best placed to do so.

Timeframes

7.3 CLI authentication standards have been developed to operate in IP networks, and we have assumed that CLI authentication, if introduced, would be present only on IP networks. This is because our expectation is that the vast majority of legacy networks in the UK will have been decommissioned and replaced by IP networks by the end of 2025, and do not envisage 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.

7.4 As we have explained, in a regulatory scheme we would need to carry out a further consultation on the detailed regulatory requirements for the introduction of CLI authentication and then publish a final statement confirming our decision, providing telecoms providers with a reasonable period to implement CLI authentication in accordance with our decision. We recognise providers would need sufficient time to procure and develop technical systems, to establish the Administrator (as discussed in Section 6) and to trial operational processes. We consider that the time needed for these steps would be broadly consistent with the migration to IP services set out above.

Key implementation tasks

7.5 At a high level, the implementation of CLI authentication would require:

a) integration of CLI authentication capability within telecoms networks;

b) a governance framework, including robust cryptographic key and certificate management and the establishment of the CLI Authentication Administrator, the body which would carry out the functions described in Sections 5 and 6;

c) if included as part of the regime, the establishment of a common numbering database to provide independent confirmation that numbers associated with calls have been attested correctly (as described in Section 5); and

d) development and approval of the Administrator's rules, setting out operational requirements in relation to, by way of example, attestation, how to handle calls without attestation and "exception handling" for failures.

Integration of CLI authentication capability within telecoms networks

7.6 Originating providers would need an authentication service, namely the capability to add attestation passports to calls. Providers could decide whether to set up their own authentication service or outsource this capability to a third party who would carry this out on their behalf. The authentication service would also require processes and tools to securely manage the creation and secure storage of information relating to the creation of certificates.

7.7 Terminating providers would need a verification service to check attestation passports. The service would allow the terminating providers to retrieve information with which to verify the authenticity of the CLI authentication.

Governance framework

7.8 In Sections 5 and 6, we discussed the functions that we propose would be carried out by the CLI Authentication Administrator. We envisaged that these would be carried out by a body which would be established by telecoms providers, and of which those providers would be members.[161]

7.9 The Administrator would need to be established, or an appropriate existing body to perform the role would need to be identified. As part of this, details of the funding and administrative arrangements for the Administrator would need to be agreed. Our expectation at this stage is that these would be matters for telecoms providers to seek to agree collectively.

7.10 The Administrator would then need to decide on policies relating to its functions and put in place the systems to carry out the technical functions outlined in section 5. These policies and systems would govern matters such as the issuing of certificates to telecoms providers.

7.11 Providers would then need to register with the Administrator and interfaces would need to be set up to enable the creation of certifications by originating providers and the verification of attestation passports by terminating providers.

7.12 It is important to agree and define a robust approach to how the 'trust service' for digital certificates would be designed, as this is complex to set up and requires a constant level of maintenance by skilled practitioners.

Common numbering database

7.13 If included as part of the regime, we consider that establishing a common numbering database would be a significant programme of work that would need to be taken forward during the implementation period for CLI authentication unless it was developed at a later stage, following the introduction of CLI authentication.

[161] However, in principle these functions could be carried out by more than one body.

7.14 The requirements, design and architecture would need to be decided, and we anticipate that these would be best agreed by telecoms providers, if possible. We are aware that the NICC Standards CDB Task Group has been examining the design and specification of a UK common numbering database and expects to publish its findings later this year.[162]

7.15 Once the requirements and design have been decided, a funding and administration model would be needed. Given the current industry activity around the design and specification of a common numbering database, we believe that decisions regarding the most effective funding and administration model would also likely be best agreed by the telecoms industry, which might also include issuing and awarding a tender for the database development.

7.16 There is currently no centralised source of information about number use in the UK. Ofcom allocates numbers in large blocks to telecoms providers, and we hold information about number range holders (i.e. the providers to whom blocks of numbers are allocated).[163] Those providers then give numbers to their customers and/or sub-allocate to other telecoms providers and resellers in a complex chain of number distribution. Numbers are ported between providers and range holders sometimes host their number allocations on another provider's network. We do not hold any of this information beyond details of our primary allocation to the range holder.

7.17 Establishing the database would therefore require telecoms providers to populate it with initial data according to the agreed specifications. This may include information on whether a number range has been adopted, hosted on another network, whether individual numbers within an allocated block have been sub-allocated and if those numbers are in use. This is likely to be a complex and resource-intensive process. It would be essential that the data held in the database is accurate, otherwise legitimate calls may be blocked and the purpose of the database would not be achieved.

7.18 Industry would need to agree processes for updating and amending the database on an ongoing basis following its establishment, including criteria setting which entities would have permission to enter updates. Additionally, the development of a common numbering database would require interfaces between providers and the database, to allow entries to be updated and queried.

7.19 As discussed in Section 5, a common numbering database might not be an essential element of the CLI authentication process. However, we recognise that many countries have such databases, given the wider benefits (such as to facilitate porting, routing and number management) that they offer. It is therefore possible that if we decided to introduce CLI authentication but without the requirement to introduce an associated common numbering database, telecoms providers may choose to establish such a

[162] NICC Standards

[163] Ofcom is required (under s.56(3) of the Act) to keep day to day records of telephone numbers allocated in accordance with the National Telephone Numbering Plan. This is known as the 'National Numbering Scheme'. We update this information weekly on our website here. This information is limited to the data that Ofcom holds and includes the number range, its status (e.g. allocated, protected etc.), the range holder's name, digit length and date of allocation.

database in the future for their own purposes, which could contribute to any CLI authentication approach adopted.

Consultation questions

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?

8. Proposed framework for impact assessment

8.1 If we proceed to a second consultation, we will include an assessment of the impact of any proposed intervention. As part of this, we would expect to gather further information on the scale and nature of the expected impacts of an intervention, including any costs that providers may need to incur.

8.2 In this section we identify, in general terms, the factors that we would be minded to consider as part of an impact assessment. We first discuss the counterfactual and then we discuss how we intend to assess the impacts of any proposed intervention, relative to the counterfactual, with respect to each of our objectives.

The counterfactual

8.3 We intend to assess the impacts of any proposed intervention around CLI authentication by comparing the potential outcomes following this intervention against the outcomes in an alternative scenario in which the intervention does not take place (referred to as the counterfactual).

8.4 As explained in Section 7, any implementation of CLI authentication would be unlikely to be mandated before the end of 2025. The impacts may be felt for many years after implementation. When considering the counterfactual, we are thus minded to look forward several years into the future. We anticipate that this exercise will be subject to considerable uncertainty.

8.5 Although we have not yet assessed the counterfactual in detail, in broad terms we expect that harmful calls will continue to be a problem in the future, to some degree. This reflects the following expectations:

a) Phone calls will continue to be widely and frequently used by consumers and businesses for the foreseeable future. Therefore, and because of the high-quality interactions enabled by phone calls, they are likely to remain an attractive communications channel for scammers and nuisance callers. See Section 3 for further discussion of these issues.

b) Recent regulatory interventions and market developments will not fully address the problem. Although these developments should bring about improvements, they are subject to certain exceptions and other limitations or challenges. See Section 4 for further discussion of these issues.

Factors that indicate the extent to which intervention would achieve Ofcom's objectives

Ofcom's proposed objectives

8.6 We have structured the proposed impact assessment framework around our policy objectives. As set out in Section 2, these are:

a) **Objective 1:** Reducing the harm caused by scam, nuisance and other harmful phone calls (our primary objective).

b) **Objective 2:** Supporting legitimate phone calls taking place.

c) **Objective 3:** Limiting the costs incurred by legitimate businesses.

8.7 We intend to consider the benefits of any intervention to introduce CLI authentication, that is, the extent to which it would achieve Objectives 1 and 2. We will also consider the costs incurred by legitimate businesses (Objective 3) and any other adverse effects. We would then consider whether there is any risk that the costs could ultimately render the intervention disproportionate, given its expected benefits.[164]

8.8 Below we outline some factors that we may need to consider when assessing the contribution to each of these objectives. We expect that it will not be possible to reliably quantify some impacts of our proposals and that we would therefore assess some impacts qualitatively. We also recognise that there is likely to be uncertainty around both the costs and benefits, which we would seek to take into account when reaching an overall view on the proportionality of our proposals.

Objective 1: Reducing the harm caused by scam, nuisance and other harmful phone calls

8.9 We anticipate considering the effectiveness of our proposals in reducing the harm caused to both consumers and businesses by scam calls in particular. In doing so, we expect to consider the extent to which the intervention could reasonably be expected to bring about a reduction in the volume of attempted scam calls, and/or a reduction in the success rate of attempted scam calls.[165]

8.10 We would take into account how scammers might change their use of phone calls in response to the intervention. However, we are not minded to take into account any associated change in the harm caused by other means of communication, such as email, mobile messaging, OTT services etc. We believe this approach would be appropriate because our policy objective is to tackle the harm caused by harmful phone calls. Dealing

[164] In the event that we identified multiple equally effective measures to achieve Objectives 1 and 2, we would consider which of these is likely to be the least onerous.

[165] For instance, this effect might arise if a larger proportion of attempted scam calls are blocked or unanswered, and/or if a smaller proportion of those scam calls that are answered lead to a victim being defrauded.

with the harm caused by other forms of communications is for other Ofcom projects and/or other bodies; it does not form part of our work on CLI authentication.

8.11 In reaching this view, we have had regard to the following considerations:

a) Forecasting any net impact on harm arising across other means of communication would be particularly complex and uncertain. There might be a degree of substitutability **between** phone calls and other means of communication, from a scammer's perspective. That is, scammers could increase their use of other means of communications, if phone calls become a less effective way to reach and to deceive consumers. However, there may also be a degree of complementarity between communication channels. As summarised in Section 3, scams often involve a combination of channels, with phone calls enabling a distinctive form of interaction.

b) In practice, it is not possible to introduce a suite of interventions covering all possible communications channels at once. Regulation often evolves in a more gradual, step-by-step fashion. Regulatory progress could be impeded if an intervention addressing one channel were to be precluded due to the possibility of displacing some scams to other channels, where further effective interventions could occur in the future).

8.12 As well as the impact on scam calls, we also anticipate considering the effectiveness of our proposals in reducing the harm caused to consumers by other types of harmful calls, such as unlawful nuisance calls and malicious calls, for example by making it easier to trace such calls.

8.13 Our initial view of the types of benefits that could arise in relation to Objective 1 is summarised below.

Objective 1: Potential categories of benefits resulting from an intervention

- Reduction in financial losses due to scams. This includes financial losses to institutions that reimburse fraud victims, as well as the financial losses to victims themselves with respect to amounts that are not reimbursed.
- Reduction in emotional and psychological harm to consumers due to falling victim to scams.
- Reduction in emotional and psychological harm to consumers even if not falling victim to scams. For example, anxiety about the possibility of oneself, or one's relatives or friends, being scammed.
- Reduction in other costs and harm for scam victims. For example, time and money spent on reporting fraud, seeking compensation and putting affairs in order; knock-on financial impacts where losses due to scams push victims into debt.
- Reduction in other costs and harms for consumers in general. For example, time and money spent on acquiring call screening tools.
- Reduction in other costs and harms for businesses. For example, cost of investigating reported fraud cases; reputational damage to businesses who are impersonated by scammers; cost of implementing measures associated with scams, such as staff training or consumer campaigns.

Objective 2: Supporting legitimate phone calls taking place

8.14 Our assessment against this objective would consider how the intervention would be expected to affect the number of legitimate calls taking place. Over time, we expect that a reduction in spoofing and in the volume of harmful calls should mean that consumers become less worried about receiving harmful calls. In this case, they may become more likely to answer calls in general, enabling additional legitimate calls to take place.

8.15 We would also consider any risk of a negative impact on this objective, for example if the proposed measures could result in some legitimate calls being blocked.[166]

8.16 Our initial view of the types of benefits that could arise in relation to Objective 2 is summarised below.

[166] For example, due to technical failure or human error as part of a CLI authentication process.

Objective 2: Potential categories of benefits resulting from an intervention

- Benefits to consumers. For example, reduced harm from legitimate and valued communications – potentially including important or useful information – going unanswered.
- Benefits to providers. For example, increase in revenues if higher trust in numbers results in higher volumes of phone calls and minutes.
- Benefits to businesses. For example, lower costs and higher efficiency as part of customer service operations and phone-based sales and marketing activities.

Objective 3: Limiting the costs incurred by legitimate businesses

8.17 We intend to consider the additional costs that legitimate businesses will incur due to our proposals. We expect that this will primarily consist of additional costs that providers would have to incur, under an assumption of reasonable efficiency, to meet the new CLI authentication requirements.

8.18 Our initial view of the types of costs that could arise in relation to Objective 3 is summarised below.

Objective 3: Potential categories of costs resulting from an intervention

- The costs of introducing technical capabilities to authenticate and verify calls, such as updating providers' network functions to support the CLI authentication process.
- The ongoing costs of authenticating and verifying calls, including maintaining network functions such as hardware and software.
- The ongoing administrative cost of providers' record-keeping (e.g. retaining details of unattested calls) and any reporting required for compliance.
- For originating providers, the administrative cost of verifying that callers are permitted to use the Presentation Number and keeping records.
- One-off costs to establish the CLI Authentication Administrator. For example, to set up its rules and governance; to establish relationships with other members and verify their identities.
- Ongoing operating costs of the CLI Authentication Administrator. For example, to administer the issuing of certificates, to monitor reporting submitted by providers and to inquire into cases of suspected non-compliance with its rules.
- One-off costs to establish and populate a common numbering database.
- Ongoing operating costs of a common numbering database. For example, to handle queries as part of the call authentication process; to maintain the database and update its records to reflect new number allocations, sub-allocations and ports.

8.19 It might be that the intervention would also enable or facilitate cost reductions for providers in certain operational areas. For example, there might be a reduced need for providers to maintain the same level of expenditure on other voluntary measures to tackle scam and nuisance calls, or the availability of a common numbering database might

generate efficiencies with respect to call routing and network management. In this case, as part of assessing the intervention against Objective 3 we would be minded to consider the expected net costs incurred, taking into account both the additional costs due to the intervention and any cost savings that could be realised.

8.20 More broadly, we anticipate that CLI authentication could affect costs incurred by other legitimate businesses across economic sectors, for example by reducing costs associated with customer service or reimbursement of scam victims. Given that we are minded to consider such impacts in relation to Objectives 1 and 2, we would not also take them into account in relation to Objective 3, to avoid 'double counting' the benefits of our proposals. However, any other incremental cost impacts on businesses that are not already captured under Objectives 1 and 2 would be considered under Objective 3.

Other adverse impacts

8.21 If any other potential adverse effects of the intervention are identified, such as any risk of unintended consequences, these will also be considered. This will include having due regard to any impact that a proposed intervention could have on competition.

8.22 However, we would not expect to consider the following potential impacts as being within the scope of Objective 3:

a) Any impact of the intervention on consumers, providers or other businesses outside the UK.

b) Any impact on costs incurred by public bodies such as Ofcom, the ICO and the police (for example, enforcement costs in relation to scam and nuisance calls).

Consultation question

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.

A1. Additional Information on STIR/SHAKEN and international implementations

A1.1 This annex provides some additional information on the STIR/SHAKEN standards, as well as outlining the approaches being adopted outside of the UK to address the issue of number spoofing through the use of these approaches.

A1.2 This annex first outlines the key technical features of both STIR and SHAKEN and then discusses how these have been, or are being, implemented in the United States, Canada and France.

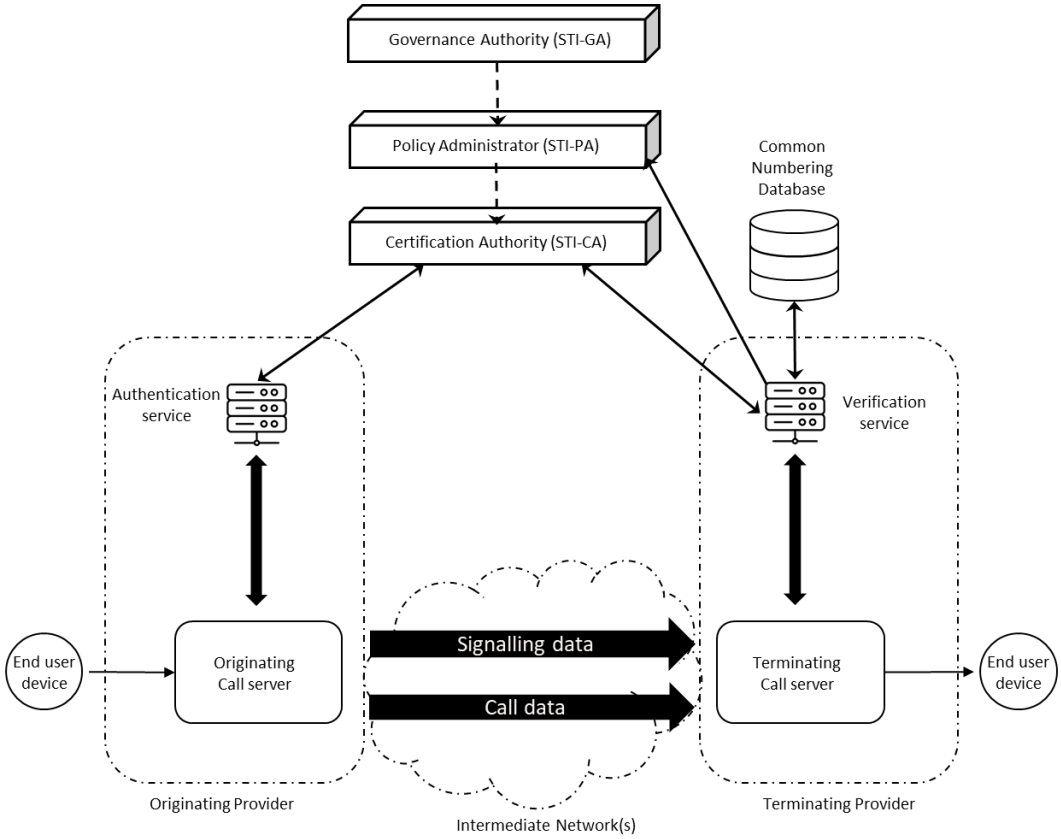
STIR/SHAKEN

A1.3 The standards-based approach adopted for CLI authentication described in the international examples below is made up of Secure Telephony Identity Revisited (STIR), and Signature-based Handling of Asserted information using toKENs (SHAKEN), albeit with some variations as outlined.

A1.4 Figure A.1 below provides an overview of the key elements to enable CLI authentication.[167] The diagram considers the actions and responsibilities of an originating provider; an equivalent process would be followed for a gateway provider. Many steps are omitted for clarity and brevity (such as key management), with the focus on those that relate to caller attestation and authentication only.

[167] The figure is adapted from NICC ND1522 "Report into implementation of Secure Telephone Identity Revisited (STIR) in the UK"

Figure A.1: Overview of key elements to enable CLI authentication



A1.5 The existence and use of a common numbering database is also shown in the diagram although it is not part of the STIR/SHAKEN standards; it is still in scope for consideration for the implementation of CLI authentication in the UK. Moreover, the information available to a terminating provider would depend on the common numbering database data structure.

A1.6 The links shown between elements in the figure show where significant interactions are expected, for example, where the verification service obtains the necessary certification details from the Certificate Authority in order to verify the received call PASSPorT. In practice, terminating providers may also hold local caches of data to improve performance and reliability, therefore data transfer may not take place on a call-by-call basis.

A1.7 The diagram shows the path that a call takes ('Call Data') may differ from the route taken by the data associated with the call ('Signalling Data'). This does not alter the effectiveness of CLI authentication but is highlighted to recognise that different networks and systems may be involved in call setup and conveyance which are not shown in the diagram.

A1.8 Finally, the diagram separates the different governance roles and functions described in the STIR/SHAKEN approach and summarised below. We would consider at a later date how these functions would be conducted were the UK to implement CLI authentication.

Secure Telephony Identity Revisited (STIR)

A1.9 STIR is an Internet Engineering Task Force (IETF) working group responsible for the development of number of RFCs (Requests for Comments) which provide a framework of interconnected standards now commonly referred to as STIR.[168]

A1.10 According to the working group's charter: "The STIR working group will specify Internet-based mechanisms that allow verification of the calling party's authorization to use a particular telephone number for an incoming call". The mechanism for authorisation is described in several RFCs with some of the key ones being RFC 8224[169], RFC 8225[170], RFC 8226.[171]

Signature-based Handling of Asserted information using toKENs (SHAKEN)

A1.11 The Alliance for Telecommunications Solutions (ATIS) and the SIP Forum have a joint Network-to-Network Interface (NNI) Task Force to fully specify an IP communications network-to-network interface between North American service providers. The task force has been working to develop standards to verify and authenticate caller credentials.[172]

A1.12 This has built upon STIR as defined by the IETF and describes the additional elements required to enable an end-to-end solution. The work has been progressed in several phases.[173]

A1.13 Within the SHAKEN framework there are three levels of attestation, as described in the table below:

Table A.1: SHAKEN - different levels of attestation

Attestation	The signing service provider shall satisfy all of the following conditions
A - Full Attestation	I. Is responsible for the origination of the call onto the IP-based service provider voice network. II. Has a direct authenticated relationship with the customer and can identify the customer. III. Has established a verified association with the telephone number used for the call.
B – Partial Attestation	As above for points I, II, for point III;

[168] IETF Secure Telephone Identity Revisited (stir)
[169] RFC 8224 Authenticated Identity Management in the Session Initiation Protocol (SIP) - defines the SIP header used for conveying a signature used for validating the identity and for conveying a reference to the credentials of the signer.
[170] RFC 8225 PASSporT: Personal Assertion Token - defines a method for creating and validating a token that cryptographically verifies an originating identity to be utilised within the SIP header defined in RFC 8225.
[171] RFC 8226 Secure Telephone Identity Credentials: Certificates - describes the use of certificates in establishing authority over telephone numbers to be utilised for implementation of PASSporT as described in RFC 8225.
[172] IP-NNI Task Force
[173] FCC FACT SHEET Call Authentication Trust Anchor Notice of Inquiry – WC Docket No. 17-97

Attestation	The signing service provider shall satisfy all of the following conditions
	III. Has **NOT** established a verified association with the telephone number being used for the call.
C – Gateway Attestation	Has no relationship with the originator of the call (e.g. international gateways).

A1.14 Additionally, a number of governance roles have been defined, as shown in Table A.2[174]:

Table A.2: SHAKEN - Key governance roles defined

Role	Key characteristics
Governance Authority (STI-GA)	Oversight role, one per country or region, defines policies on who can acquire certificates and which entities can manage the PKI and issue certificates.
Policy Administrator (STI-PA)	Policy enforcement role including active list of approved Certificate Authorities in the form of public key certificates for service providers.
Certificate Authority (STI-CA)	Acts as the Root Certificate Authority.

A1.15 The following sections will now outline the status of STIR and SHAKEN in the US, Canada, and France, concluding with a comparison of some of the key characteristics.

International examples of STIR/SHAKEN implementation

United States

A1.16 The Federal Communications Commission (FCC) reported that US consumers receive approximately 4 billion robocalls[175] a month.[176] This has prompted the FCC to make combatting these calls (including those facilitated by number spoofing) a "top consumer priority" and to act, including adopting CLI authentication.

A1.17 U.S. Congress passed the TRACED (Telephone Robocall Abuse Criminal Enforcement and Deterrence) Act in 2019 mandating that by the 30 June 2021 carriers had to adopt the STIR/SHAKEN framework for IP-based network voice calls[177], with smaller providers being

[175] A robocall, a term common to the US, is an automated telephone call which delivers a recorded message, typically on behalf of a political party or telemarketing company.
[176] FCC Robocall Response Team: Combating Scam Robocalls & Robotexts
[177] FCC Report and Order

granted extensions.[178] From June 2021 all providers must certify compliance in a Robocall Mitigation Database[179], through confirmation of implementation of STIR/SHAKEN and/or have instituted a robocall mitigation program to ensure that they are not originating illegal robocalls.

A1.18 FCC rules also mean providers must either upgrade non-IP networks or develop/deploy an equivalent call authentication solution.[180] STIR was chosen to address the authentication requirement and additional work by standards and industry bodies was required to both describe how the STIR standards should be implemented and provide the framework to support the governance, creation, and management of certificates using SHAKEN.

Accompanying capabilities

A1.19 The requirement for STIR included basic Know Your Customer (KYC) requirements. [181] Subsequently, the FCC has looked to strengthen this by additionally requiring gateway providers[182] to 'Know Your Upstream Provider', meaning an onus is put on the gateway provider to "take reasonable and effective steps to ensure that the immediate upstream 'foreign provider' is not using the gateway provider to carry or process a high volume of illegal traffic onto the U.S. network".[183]

A1.20 The introduction of the TRACED Act also included a responsibility for the FCC to issue rules "for the registration of a single consortium that conducts private-led efforts to trace back the origin of suspected unlawful robocalls". A pre-existing industry body, USTelecom who had formed the Industry Traceback Group (ITG) in 2015, was selected.[184]

Current Status and ongoing developments

A1.21 Notwithstanding the requirements of the TRACED Act, robocalls continue to be an issue, increasing in the year to February 2023. While February did see a decrease[185], it is too early to know if this trend will continue. As of March 2023, most calls reach their destination unsigned (72.48%) and full attestation of calls at the originating provider has been "hovering" around 16% for the last 6 months. [186]

A1.22 Several aspects are being worked on to enhance the capabilities of the STIR and SHAKEN framework with the objective of increasing deployments and/or closing loopholes. These include:

---

[178] FCC Combating Spoofed Robocalls with Caller ID Authentication, FCC Reminds Small Providers of June 30 STIR/SHAKEN Deadline
[179] FCC Robocall Mitigation Database. The database includes details of persons responsible and a description of actions taken.
[180] FCC Combating Spoofed Robocalls with Caller ID Authentication
[181] FCC Report and Order
[182] FCC Advanced Methods to Target and Eliminate Unlawful Robocalls
[183] FCC Advanced Methods to Target and Eliminate Unlawful Robocalls
[184] Industry Traceback Group
[185] TransNexus Robocalls down in February
[186] TransNexus STIR/SHAKEN statistics from February 2023

a) Ability for service providers to create certificates for entities who do not themselves have access to generate certificates.[187]

b) Introduction of support for emergency calls and Resource Priority Header (RPH). [188] This has the added benefit of authenticating the legitimate use of RPH as part of the signing.

c) Diverted call support in STIR.[189] Without this, diverted calls currently present a potential mechanism to bypass measures.

d) International attestation and certificate framework.[190] This extends SHAKEN to allow interworking between multiple framework (PKI) realms.

e) Non-SIP ATIS group formed May 2020[191], Non-IP Call Authentication Task Force (NIPCA), which has approved a number of standards to allow for carrying of the Attestation level in signalling[192] and sending of PASSporTs out-of-band. [193]

Canada

A1.23 The Canadian approach is closely aligned to the US with Canada introducing equivalent capability such as the Canadian Secure Token Governance Authority (CST-GA)[194], and the Canadian Certificate Administrator (CCA).[195]

A1.24 Guidelines have been published by the communications regulator, Radio-television and Telecommunications Commission (CRTC) Interconnection Steering Committee in a Network Working Group Report.[196] These guidelines are intended to take the current CRTC directives and review these against the list of available standards. In January 2018, the CRTC issued the 'compliance and enforcement and telecom decision CRTC 2018-32' which mandated the implementation of STIR/SHAKEN to authenticate and verify caller identification information for IP-based network voice calls by 30 November 2021.[197]

Accompanying capabilities

A1.25 The CLI authentication regime relies on existing mechanisms of KYC which is set out as an expectation for originating providers to apply full attestation to a call.

A1.26 With regards to call tracing, an interim process was introduced in February 2019, going live in November 2020.[198] Similar to the US, a serial approach to tracing is taken. The process

[187] ATIS-1000092, SHAKEN: Delegate Certificates
[188] ATIS-1000078, National Security / Emergency Preparedness Priority Service Session Initiation Protocol Resource-Priority Header (SIP RPH) Signing and Verification using PASSporTs
[189] ATIS-1000085, SHAKEN: SHAKEN Support of "div" PASSporT
[190] IPNNI-2022-00011R000.docx, Baseline text for SHAKEN: International Attestation and Certificate Framework
[191] ATIS Launches New Non-IP Call Authentication Task Force | ATIS
[192] ATIS-1000095, Extending STIR/SHAKEN over TDM
[193] ATIS-1000096, SHAKEN: Out-of-Band PASSporT Transmission Involving TDM Networks
[194] Canadian Secure Token - Governance Authority
[195] Compliance and Enforcement and Telecom Decision CRTC 2019-403
[196] CRTC INTERCONNECTION STEERING COMMITTEE NETWORK WORKING GROUP: STIR/SHAKEN Guidelines
[197] Compliance and Enforcement and Telecom Decision CRTC 2021-123
[198] Canadian Traceback Interim Process

begins with the provider which terminated the call and follows the call to the point of ingress where it is then handed over to the next provider and so on until the origination point is found (or records missing or unresponsive provider).

A1.27 This has been refined over time, although the same basic process exists currently. Successful outcomes remain relatively low; in the 4th quarter of 2022, 10% of completed requests (5 of 51) were successful. In most cases, the incomplete tracebacks are due to the call originating from an international communications provider. [199]

Current Status and ongoing developments

A1.28 CRTC is in the process of collating data reported every 6 months by operators as defined in decision 2021-123.[200] Data requested includes statistics on performance, status of general implementations, and work on standards relating to Canadian-specific requirements.

France

A1.29 In July 2019, the communication regulator, Autorité de Régulation des Communications Electroniques (ARCEP) published a decision to amend the numbering plan to include several measures, including introduction of a number authentication mechanism to protect users against fraud and theft.[201] The deadline for introduction of authentication is the 25 July 2023.

A1.30 The French approach differs from the US and Canada where the introduction has been phased, with an initial focus on IP network voice calls; the French approach is to have limited exceptions in the initial phase. Legacy technologies are not excluded from the initial phase but are expected to have been retired prior to implementation of the solution. In addition to this, a common platform is being delivered to provide the capabilities equivalent to the STI-PA and STI-CA (see Table A.3 below).

[199] Quarterly traceback report #4 (TIF 38)
[200] Compliance and Enforcement and Telecom Decision CRTC 2021-123
[201] Arcep Decision No. 2019-0954

Table A.3: French governance roles

Role	Key characteristics
Governance Authority (STI-GA)	Oversight role (APNF and ARCEP); defines policies on who can acquire certificates, rules relating to certificate management including approved and revoked operators.
Policy Administrator (STI-PA)	Platform MAN[202] made up of several logical components that provide the equivalent capability with the addition of a monitoring database for the feedback of traces, incidents, reports and metrics from operators related to the MAN framework.[203]
Certificate Authority (STI-CA)	
Database of Signals and Measurements	

A1.31 French operators and ARCEP have requested the Association de la portabilité des numéros fixes[204] project manage the delivery of the project, called MAN.

A1.32 Accompanying capabilities Call tracing will be supported through the introduction of the Platform MAN. Data collected will support the ability to standardise the approach to call tracing.

Current Status and ongoing developments

A1.33 We understand that work is ongoing in preparation for the introduction in the summer of this year.

International summary comparison

A1.34 Table A.4 summarises some of the key aspects that make up the CLI authentication approaches described above.

Table A.4: International summary comparison

	US	Canada	France
Governance Authority	New legal entity made up of national operators.[205]	New legal entity made up of national operators.[206]	Existing legal entity made up of national operators.[207]

[202] Mécanisme d'authentification du Numéro (MAN): Number Authentication Mechanism
[203] Enterprise Telecom Consultants 2018. Number Authentication: What is the situation in the US? In France.
[204] APNF - Fixed Number Portability Association made up of 9 French operators
[205] US Secure Telephone Identity Governance Authority
[206] Canadian Secure Token Governance Authority
[207] Association de la portabilité des numéros fixes (APNF) - Fixed Number Portability Association, an association made up of operators using numbering resources belonging to the French telephone numbering plan. APNF supports several services including fixed number portability.

	US	Canada	France
Policy Administrator	Commercial entity[208]	Commercial entity[209]	Existing legal entity made up of national operators[210]
Certificate Authority	Commercial entities, 10 Certificate Authorities[211]	Commercial entities, 2 Certificate Authorities[212]	Existing legal entity made up of national operators[213]
Terminating Network - behaviour for unsigned or invalidly signed calls	Communicate information to end-user to allow them to decide. In some cases, disconnect the call.		Disconnect the call (excludes emergency and non-SIP calls) [214] With exceptions of 'Breakable calls'[215]
Number of Attestation Levels	3 (A -Full, B -Partial, and C -Gateway)		1 (not blocked) A attestation[216]
Approach to Legacy networks (TDM)	Work in progress on potential technical alternatives		Legacy networks to be decommissioned by launch date
Call Tracing	Existing legal entity made up of national operators Industry Traceback Group (ITG)[217] Spreadsheet-based form	Process developed by national operators as part of CRTC "Network working group"[218] Spreadsheet-based form	Capability being developed as part of centralised 'MAN monitoring database' Planned API based

[208] iconectiv Authenticate
[209] Neustar Policy Administrator
[210] APNF
[211] US Certificate Authorities
[212] Canada Certificate Authorities
[213] APNF
[214] Enterprise Telecom Consultants 2018. Number Authentication: What is the situation in the US? In France.
[215] Breakable Call exceptions includes emergency calls, potentially any calls in the early stages of introduction, potentially any calls when a failure arises which requires the system to be overridden.
[216] Enterprise Telecom Consultants 2018. Number Authentication: What is the situation in the US? In France.
[217] Industry Traceback Group (ITG)
[218] CRTC Network Working Group: Traceback Documentation

	US	Canada	France
Metrics / Reporting	Metrics Proposed by ATIS[219] No common reporting platform	Metrics (periodic reporting) defined by Network working group.[220] Reports emailed to CRTC, manually collated	Capability being developed as part of centralised 'MAN monitoring database' Planned API based

[219] ATIS STIR/SHAKEN Metrics
[220] CRTC STIR/SHAKEN Guidelines

A2. Responding to this consultation

How to respond

A2.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 23 June 2023.

A2.2 You can download a response form from https://www.ofcom.org.uk/consultations-and-statements/category-2/cli-authentication. You can return this by email or post to the address provided in the response form.

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

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

CLI authentication team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

A2.4 We welcome responses in formats other than print, for example an audio recording or a British Sign Language video. To respond in BSL:

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

A2.5 We will publish a transcript of any audio or video responses we receive (unless your response is confidential).

A2.6 We do not need a paper copy of your response as well as an electronic version. We will acknowledge receipt of a response submitted to us by email.

A2.7 You do not have to answer all the questions in the consultation if you do not have a view; a short response on just one point is fine. We also welcome joint responses.

A2.8 It would be helpful if your response could include direct answers to the questions asked in the consultation document. The questions are listed at Annex 5. It would help if you could explain why you hold your views, and what you think the effect of Ofcom's proposals would be.

A2.9 If you want to discuss the issues and questions raised in this consultation, please contact the CLI authentication team at CLIauthentication@ofcom.org.uk.

Confidentiality

A2.10 Consultations are more effective if we publish the responses before the consultation period closes. In particular, this can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

A2.11 If you think your response should be kept confidential, please specify which part(s) this applies to; and explain why. Please send any confidential sections as a separate annex. If you want your name, address, other contact details or job title to remain confidential, please provide them only in the cover sheet, so that we don't have to edit your response.

A2.12 If someone asks us to keep part or all of a response confidential, we will treat this request seriously and try to respect it. But sometimes we will need to publish all responses, including those that are marked as confidential, in order to meet legal obligations.

A2.13 To fulfil our pre-disclosure duty, we may share a copy of your response with the relevant government department before we publish it on our website.

A2.14 Please also note that copyright and all other intellectual property in responses will be assumed to be licensed to Ofcom to use. Ofcom's intellectual property rights are explained further in our Terms of Use.

Next steps

A2.15 If our provisional view following this consultation is that there is a case for requiring the implementation of CLI authentication, we will publish a full assessment of the likely impact and our proposals for the regulatory rules that would be needed.

A2.16 If you wish, you can register to receive mail updates alerting you to new Ofcom publications.

Ofcom's consultation processes

A2.17 Ofcom aims to make responding to a consultation as easy as possible. For more information, please see our consultation principles in Annex 3.

A2.18 If you have any comments or suggestions on how we manage our consultations, please email us at consult@ofcom.org.uk. We particularly welcome ideas on how Ofcom could more effectively seek the views of groups or individuals, such as small businesses and residential consumers, who are less likely to give their opinions through a formal consultation.

A2.19 If you would like to discuss these issues, or Ofcom's consultation processes more generally, please contact the corporation secretary:

Corporation Secretary
Ofcom
Riverside House
2a Southwark Bridge Road
London SE1 9HA
Email: corporationsecretary@ofcom.org.uk

A3. Ofcom's consultation principles

Ofcom has seven principles that it follows for every public written consultation:

Before the consultation

A3.1 Wherever possible, we will hold informal talks with people and organisations before announcing a big consultation, to find out whether we are thinking along the right lines. If we do not have enough time to do this, we will hold an open meeting to explain our proposals, shortly after announcing the consultation.

During the consultation

A3.2 We will be clear about whom we are consulting, why, on what questions and for how long.

A3.3 We will make the consultation document as short and simple as possible, with an overview of no more than two pages. We will try to make it as easy as possible for people to give us a written response.

A3.4 We will consult for up to ten weeks, depending on the potential impact of our proposals.

A3.5 A person within Ofcom will oversee making sure we follow our own guidelines and aim to reach the largest possible number of people and organisations who may be interested in the outcome of our decisions. Ofcom's Consultation Champion is the main person to contact if you have views on the way we run our consultations.

A3.6 If we are not able to follow any of these seven principles, we will explain why.

After the consultation

A3.7 We think it is important that everyone who is interested in an issue can see other people's views, so we usually publish the responses on our website at regular intervals during and after the consultation period. After the consultation we will make our decisions and publish a statement explaining what we are going to do, and why, showing how respondents' views helped to shape these decisions.

A4. Consultation coversheet

BASIC DETAILS

Consultation title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

CONFIDENTIALITY

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

Nothing ☐

Name/contact details/job title ☐

Whole response ☐

Organisation ☐

Part of the response ☐

If there is no separate annex, which parts? _____

_____

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

DECLARATION

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

Ofcom aims to publish responses at regular intervals during and after the consultation period. If your response is non-confidential (in whole or in part), and you would prefer us to publish your response only once the consultation has ended, please tick here.

Name Signed (if hard copy)

A5. Consultation questions

Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.

Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

Question 6.2: Do you agree that CLI authentication could make call tracing easier and yield benefits in terms of detecting scammers and nuisance callers?

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.

A6. Glossary of terms

Allocate (in relation to phone numbers): 'allocate' generally means allocation of numbers by Ofcom.

Assigned (in relation to phone numbers): where numbers are transferred to end users i.e. individuals and businesses.

Attestation: confirmation of the extent to which a telecoms provider has itself identified and/or authenticated its customer and determined the customer's association to the calling party telephone number.

Attestation passport: Shorthand to mean an approximation of the technical definition of Personal ASSertion Token (PASSporT), a token object that conveys cryptographically signed information about the participants involved in communications.

Authentication service: The originating provider would be responsible for authenticating calls through an authentication service. The authentication service carries out checks to confirm the calling number meets requirements and inserts a SIP identity header which includes the originating provider's signature.

Authorised Push Payment (APP) scam: a type of scam which involves tricking a victim into authorising a payment to an account controlled by a criminal.

Blocklist: a list of phone numbers compiled by the provider or customer. Calls from those numbers are not allowed to reach the recipient.

Calling Line Identification (CLI) data: means the contents of all signalling messages which can be used between telecoms providers and/or between telecoms providers and End-Users to signal the origin of the call and/or the identity of the calling party, including any associated privacy markings.

Certificate: A (digital) certificate, also known as a public key certificate, is a digital document that serves as a means of confidently verifying the identity of an entity. This is utilised by the terminating provider to verify the originating provider (or other attesting provider) and information signed within the attestation passport (PASSporT).

Certificate authority: trusted holder of certification information associated with each registered originating provider

CLI authentication: implementation of standards that make it possible for a provider to add CLI data in such a way that the terminating provider can have confidence the information received was added by the provider and has not been modified in transit.

Consumer: is defined in the General Conditions as meaning any natural person who uses or requests a Public Electronic Communications Service or Bundle for purposes which are outside his or her trade, business, craft or profession.

Customer: is defined in the General Conditions and, in relation to a Communications Provider, means the following (including any of them whose use or potential use of the network or service is for the purposes of, or in connection with, a business): (a) the persons to whom the network, service or Bundle is provided in the course of any business carried on as such by the Communications

Provider; (b) the persons to whom the Communications Provider is seeking to secure that the network, service or Bundle is so provided; (c) the persons who wish to be so provided with the network, service or Bundle, or who are likely to seek to become persons to whom the network, service or Bundle is so provided.

Do Not Originate (DNO) list: a list, set up by Ofcom and UK Finance, of certain telephone numbers used only for inbound calls that would not be used to call consumers.

End user: is defined in the General Conditions and means in relation to a Public Electronic Communications Service or Bundle: (a) a person who, otherwise than as a Communications Provider, is a Customer of the provider of that service or Bundle; (b) a person who makes use of the service or Bundle otherwise than as a Communications Provider; or (c) a person who may be authorised, by a person falling within paragraph (a), so to make use of the service or Bundle.

Gateway provider: the provider bringing a call into the UK public telephone network, but not able to provide full attestation due to not having a direct relationship with the end user.

General Conditions (GCs): conditions set by Ofcom under section 45 of the Communications Act 2003.

Geographic number: a telephone number that is identified with a particular geographic area.

Impersonation scams: where scammers claim to be from legitimate organisations to try to trick people into giving away personal details or making a payment.

Interconnection: the linking (whether directly or indirectly by physical or logical means, or by a combination of physical or logical means) of one Public Electronic Communications Network to another for the purpose of enabling the persons using one of them to be able: (a) to communicate with users of the other one; or (b) to make use of services provided by means of the other one (whether by the provider of that Network or by another person).

Network Number: a telephone number that unambiguously identifies the line identity of the fixed access ingress to or egress from a Public Electronic Communications Network or a subscriber or terminal/telephone that has non-fixed access to a Public Electronic Communications Network.

Non-geographic number: any telephone number other than a geographic number.

Nuisance calls: may include unwanted attempts to promote a product or service, as well as silent and abandoned calls. Nuisance calls are likely to cause annoyance, inconvenience and anxiety to consumers.

Number spoofing: Spoofing is a tactic commonly used by scammers and involves callers hiding their identity by causing a false or invalid phone number to be displayed when making calls. Those making such calls may create a number that appears like a phone number or may even mimic the number of a real company or person who has nothing to do with the actual caller.

Originating provider: provider with a contractual relationship with the originating end user placing a call onto the public telephone network.

Presentation Number: a number nominated or provided by the caller that can identify that caller or be used to make a return or subsequent call. It may not necessarily identify the line identity of the geographic source of the call.

Provider: communications provider, defined in section 405(1) of the Communications Act 2003 as meaning a person who (within the meaning of section 32(4)) provides an electronic communications network or an electronic communications service.

PSTN: Public Switched Telephone Network.

Public Telephone Network: We use this term to describe the aggregate of the UK's telephone networks, including both legacy and IP-based networks.

Range holder: the provider to whom a particular number range or block has been allocated by Ofcom.

Scam calls: calls primarily aimed at defrauding consumers, either by tricking them into revealing personal details or into making a payment.

STIR (Secure Telephone Identity Revisited) /SHAKEN (Signature based Handling of Asserted information using toKENs): STIR/SHAKEN is the set of standards which is being used for CLI authentication in the US and Canada. STIR is a set of standards that describe the mechanics of CLI authentication signalling. SHAKEN is a framework which defines the use of STIR and other elements to make up a complete ecosystem as defined by the Alliance for Telecommunications Industry Solutions (ATIS).

Sub-allocate: where numbers are transferred by a provider to other providers or resellers.

Terminating provider: provider with a contractual relationship with the terminating end user.

Transit provider: a third-party provider which conveys a call in the path between the originating and terminating provider.

Unwanted calls: calls with the potential to cause harm that consumers do not want to receive. These can range from nuisance calls through to scams.

Verification service: Terminating providers would be responsible for verifying calls through a verification service. The verification service checks the contents of the SIP identity header and verifies the originating provider's signature.