Tackling scam calls and texts

Ofcom's role and approach

Tackling scam calls and texts – Welsh overview

POLICY POSITIONING STATEMENT

Publication date: 23 February 2022

Contents

Section

Annex

1. Overview

Protecting consumers from harm is a priority for Ofcom and we are concerned about the growing problem of scams facilitated by calls and texts.[1] During the Covid-19 pandemic, we saw scammers quickly adapting to take advantage of the changing circumstances – for example, sending texts with fraudulent links for booking vaccinations or impersonating delivery companies. We also saw this form of criminal activity becoming increasingly complex, with scammers, based in the UK and abroad, using more sophisticated techniques to trick people.

The use of scam calls and texts is now widespread, with our research finding that suspected scam attempts affect the vast majority of people in the UK. Over the three-month period covered by our survey, we estimated that almost a million people followed the scammers' instructions in a message or call, risking financial loss and emotional distress. Even when not successful, attempted scams are annoying and cause anxiety for recipients. Scams also impose costs on the wider economy, including the resources spent by legitimate businesses to support those customers that fall victim to fraud.

We are committed to working with partners to reduce the harm from scam calls and texts. This document explains the prevalence and changing nature of scams, their impact and the key elements of our response.

- We aim to **disrupt scams** by making it harder for scammers to use communications services to reach consumers. We propose to strengthen 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 will **collaborate and share information** more widely, 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 stop all scams reaching consumers. We are working to **help consumers avoid scams** by raising awareness so consumers can more easily spot and report them.

A significant amount of work is already underway in the telecoms sector to help prevent customers being scammed. For example, mobile network operators either have introduced or are in the process of introducing technology that can detect the key traits of scam texts sent over their networks, allowing them to block more suspicious messages.

It is encouraging that telecoms providers are taking steps to disrupt scams. However, we think there are some areas where more could be done. This document explains our proposals to strengthen the steps providers should take to prevent scammers using communications services to reach consumers. If implemented, we expect these changes would 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.

[1] See Ofcom, March 2021. Ofcom's plan of work 2021/22, page 16.

What we are proposing

We are consulting on two proposals to strengthen our rules and guidance on what providers should do to make it harder for scammers to use communications services to reach consumers:

- **Strengthening our rules and guidance for providers to detect and block 'spoofed' numbers**. 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 phone number that appears like or mimics the number of a real company, such as a bank. Our rules require providers to prevent these calls, where possible. While not all spoofed numbers can be detected, some are easier to spot. This might be because they are numbers that have not been allocated for use to anyone or where a UK number has been used in a call which originated abroad. We are proposing to strengthen our rules and guidance so that providers do more to detect and block the most obviously spoofed numbers.
- **A good practice guide to help prevent scammers accessing valid phone numbers.** Providers allocated numbers by Ofcom may transfer those numbers to other providers or resellers or to customers for their day-to-day use. There is currently considerable variation in the checks that providers do both before and after transferring numbers to prevent misuse. In this guide we set out what we expect providers to do to ensure they know their business customers and how numbers will be used by them. The guide contains processes that should be in place to check customers are using numbers in compliance with our rules, and for responding to reports of misuse. Where these measures are in place, it will be more difficult for scammers to access legitimate telephone numbers to make potentially harmful scam calls.

We are also working on other measures to help tackle scams:

- **Updating our scheme to protect legitimate numbers that are most likely to be spoofed by scammers.** People may be more likely to trust a call coming from a number associated with a known organisation, such as a bank. We worked with UK Finance on a 'Do Not Originate' (DNO) list to record numbers used by these organisations, including banks and government agencies, to receive calls but never to make calls. The list allows providers to check incoming calls against the numbers on the DNO list and block the call. We have updated our guidance for using the list and will consider whether it can be expanded to include numbers from a wider range of organisations.
- Over the longer term, having processes that detect and block spoofed numbers more comprehensively will be important to help tackle scam calls. **We are exploring the introduction of technical standards that make it possible for the network originating the call to confirm the caller's authenticity** before passing it to the network of the person receiving the call, referred to as 'CLI authentication.'[2] We plan to issue a call for inputs in Q4 2022 seeking views on the role of CLI authentication and what would be required to implement the technology across industry.

[2] Calling Line Identification (CLI) is the data that enables identification of the number from which a call could be made or to which a return call could be made.

Next steps

1.1 Our consultations will close on 20 April 2022. Full details on how to respond to these are contained in each of the consultation documents.[3] Following consideration of the consultation responses, we plan to publish our decisions in Autumn 2022.

1.2 We know that scammers will find other ways to reach consumers and no single organisation can solve the problem alone. Alongside our work with providers, we will continue to collaborate with other organisations working to reduce scams as part of a coordinated approach.

1.3 We will carry out follow-up research into the incidence of call and text scams to help us monitor the impact of work that we and others are doing, including where to focus our efforts as scammers evolve their tactics. The research will also inform our continued work to raise awareness of scams and the steps people can take to protect themselves.

[3] Ofcom, February 2022. Improving the accuracy of Calling Line Identification (CLI) data; Ofcom, February 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

2. Background and introduction

2.1 This section explores Ofcom's existing work on unwanted calls, which initially focused on nuisance calls. It also discusses how the nature of the problem has changed with a shift from nuisance calls to scams. Finally, we highlight the need to adapt our response to this changing problem.

Ofcom has been working for a number of years to reduce unwanted calls

The initial focus of our work was on nuisance calls

2.2 Consumers receive a variety of calls and texts that they do not want. These can range from nuisance calls and texts, through to scams. Nuisance calls and texts include unwanted attempts to promote a product or service (marketing calls), as well as silent and abandoned calls. The Information Commissioner's Office (ICO) take the lead on tackling unwanted marketing calls and Ofcom leads on silent and abandoned calls. Scam calls are different from other types of nuisance calls and are primarily aimed at defrauding consumers, either by tricking them into revealing personal details or into making a payment.

2.3 Nuisance calls are often the result of call centres making outbound calls to consumers, usually with the assistance of dialling technology. For example, silent and abandoned calls can result when Automated Calling Systems (ACS) are being used and there is over-dialling which means that call centre agents are busy when the call recipient answers the phone and/or the ACS disconnects the call.[4] Nuisance calls are likely to cause annoyance, inconvenience and anxiety to consumers.

2.4 Through our monitoring of unwanted calls received by consumers and complaints data, we previously determined that, within our remit, silent and abandoned calls were having the most serious harmful effects on consumers. To date we have therefore undertaken a significant amount of work focused on reducing this problem.

Our powers

2.5 Ofcom's principal duty, in carrying out its functions, is to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition. In performing our duties, we are required to have regard to a number of matters, as they appear to us to be relevant in the circumstances, including the desirability of ensuring the security and availability of public

[4] A silent call is where you receive a call, but you cannot hear anything and have no means of knowing whether anyone is at the other end of the line. An abandoned call is one that is terminated when you pick up the receiver. Instead of a person on the other end of the line you hear an information message from the organisation that is trying to call you. See Ofcom, December 2016. Persistent Misuse: A statement of Ofcom's general policy on the exercise of its enforcement powers.

electronic communications networks and services; the needs of persons with disabilities, of the elderly and of those on low incomes; the desirability of preventing crime and disorder; and the opinions of consumers in relevant markets and of members of the public generally.[5]

2.6 In broad terms, Ofcom's powers in this area relate to setting rules around the allocation and use of telephone numbers and what providers should be doing to protect the interests of end-users of public electronic communications services. 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. 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 used to facilitate scams. Further detail of the existing obligations on providers and Ofcom's relevant powers are contained in Annex A1.

Our response to nuisance calls

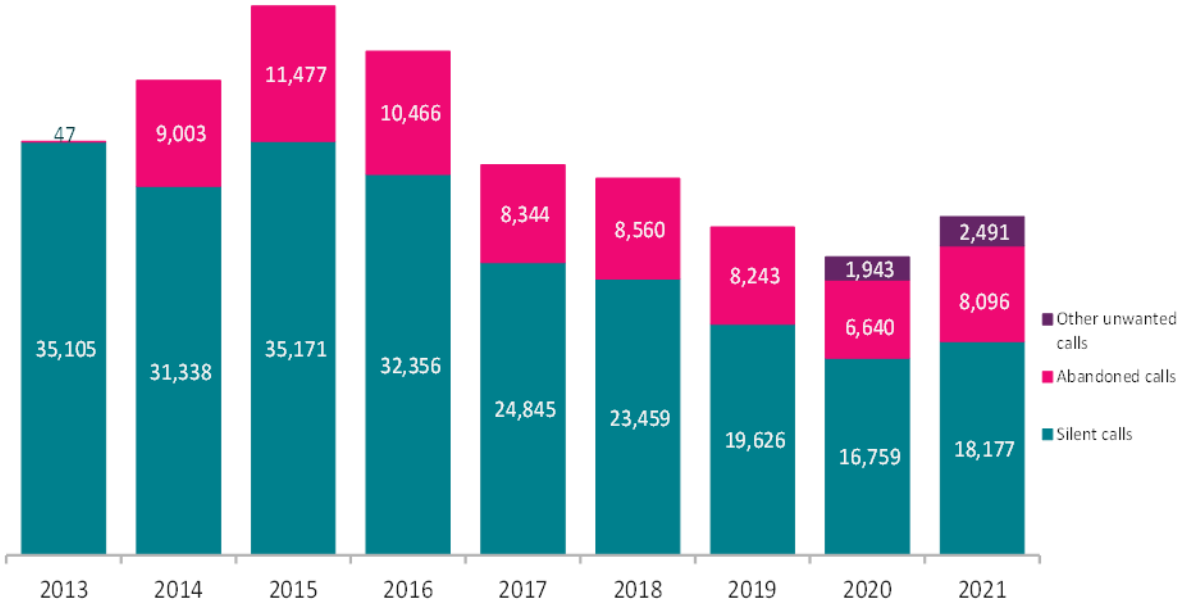
2.7 Using our powers, we introduced a number of measures aimed at reducing the harm from nuisance calls. This included requirements on providers to enable CLI data to be displayed and for providers to block calls with invalid and non-dialable CLI data, where feasible.[6] We also exercised our powers under the Communications Act 2003 to take enforcement action where a person has persistently misused an electronic communications network or service.

2.8 We established a Strategic Working Group (SWG) with nine major providers in 2015 to work on reducing the impact of nuisance calls.[7] Members of this group submit data to us each month on the nuisance calls they receive on a particular day, using specific characteristics developed and agreed by the group. We collate this information and share a summary with members of the group. The data is also used to inform our enforcement work.

2.9 This work has helped to reduce the number of silent and abandoned calls reaching consumers. This is supported by our complaints data, as shown in Figure 1, where consumer complaints about silent and abandoned calls fell between 2015 and 2020. We did, however, see an uptick in complaints in 2021 which we explore further below.

[5] Section 3 of the Communications Act 2003.
[6] GC C6 specifies the rules around Calling Line Identification. More information is provided in Annex A1.
[7] These providers were BT (which includes EE), Gamma, KCOM, Sky, TalkTalk, Telefonica, Three, Virgin Media, and Vodafone. We have since extended membership of this group to eleven other telecoms companies who provide wholesale or business services. Note also that Virgin Media and O2 (Telefonica) have now merged to become Virgin Media O2.

Figure 1: Consumer complaints to Ofcom about silent and abandoned calls, 2013 to September 2021



Source: Ofcom consumer complaints data.

Note: A category for 'other' unwanted calls (i.e. defined as all calls other than silent and abandoned calls) was added in 2020).

We work closely with the Information Commissioner's Office on nuisance calls

2.10 The ICO has powers to take enforcement action against people who make unlawful live and recorded marketing calls, texts and emails. The ICO also manages the Telephone Preference Service, which enables consumers to opt out of receiving marketing calls. Given the complementary nature of our work, since 2013 Ofcom and the ICO have published an annual joint action plan for tackling nuisance calls and messages.[8]

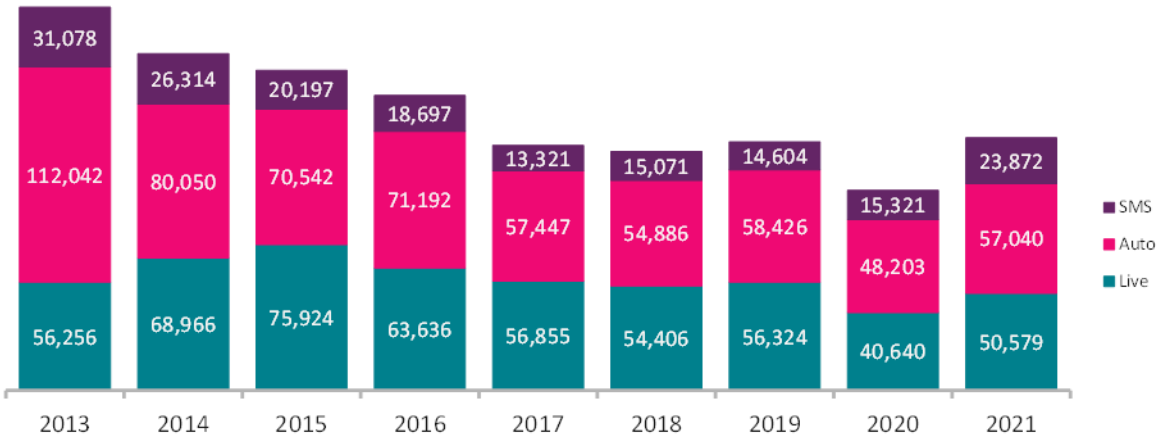
2.11 Looking at trends over the past five years, the ICO reports that its complaint numbers about nuisance calls and text messages have decreased by 22,034 complaints or 14% since 2016, when 153,525 complaints were reported.[9] Despite the drop in complaints during 2020, reporting across the last four years is generally stable, which suggests that whilst the ICO experiences periods of increases in reporting, complaint levels are lower than those seen historically.

[8] The latest report can be found here: Ofcom and ICO, May 2021. Nuisance calls and messages: Update to ICO/Ofcom joint action plan.

[9] Complaint volumes numbers were subject to a particular increase between the end of June 2018 and early August 2019, believed to be caused by increased public awareness of the ICO and therefore increased reporting, following the introduction of strengthened regulations in relation to nuisance call activity and the General Data Protection Regulation (GDPR).

2.12 The ICO's complaints data for live and automated calls and texts between 2013 and 2021 is shown in Figure 2 below.

Figure 2: Complaints to the ICO's Online Reporting Tool (OLRT) about live and automated calls, 2013 to December 2021



Source: ICO, OLRT complaints data.

2.13 In 2021, the ICO received a total of 131,491 complaints about nuisance calls and nuisance text messages. This is a year-on-year increase of 27,327 complaints, or 26%, since 2020, when 104,164 complaints were reported. Much of this annual increase was the result of rising numbers of complaints during the various easings of Covid-19 lockdowns. More detail on the nature of the complaints is included in paragraphs 2.21 and 2.22.

2.14 During the initial period of 2021, complaint numbers had recovered from the drop seen in 2020, and in fact rose to the highest levels seen since 2016. Between January and June 2021, 83,558 complaints were reported, whilst in that same period in 2020, just 38,269 complaints were reported. This represents an increase of 45,289 complaints or a 118% rise.

2.15 Despite the high reporting volumes recorded during the first half of the year, complaint figures actually decreased in the second half of 2021 and were in fact lower than those seen in the latter months of 2020. It is anticipated that these lower reporting levels may continue as we move into 2022, but more data is required to ascertain how many of these trends were impacted by Covid-19.

The nature of the problem is changing, and new responses are required

Unwanted calls are now harder to detect

2.16 In the past, one way to detect potential unwanted calls was to look for a single number being used to make large volumes of short calls. However, those making unwanted calls

are now more likely to change their numbers frequently, only using each number for a brief period. It is also much more likely for a spoofed number to be used. Spoofing involves callers hiding their identity by causing a false or invalid phone number to be displayed when making calls. A spoofed number on a call display can mimic the number of a real company or person who has nothing to do with the actual caller.

2.17 This has made it harder to detect and block unwanted calls. In terms of blocking, the perpetrator is likely to have moved to a new number by the time the issue has been flagged. It also makes it more difficult to trace the perpetrators because the number will not have been assigned to the individual making the calls.

2.18 This trend may have been one of the drivers of the increase in complaints we saw about silent, abandoned and other calls in 2021.[10]

There has also been a shift from nuisance to scam calls, and scam texts have become prevalent

2.19 Between 2013 and 2019, we conducted an annual survey asking participants to complete a diary about the unwanted calls they received.[11] One of the questions asked respondents to record their understanding of the product or service being promoted in an unwanted call. In 2019, a quarter of calls where the product or service was identified were thought, by the respondents, to be scams. This was up from 2% in 2016 and 4% in 2017.[12] In addition, scam texts are now commonly received by consumers. [13] In the following section we talk in more detail about the current impact of unwanted calls and texts on consumers.

2.20 The shift to scam calls and texts is unlikely to be reflected in our own complaints data which relates specifically to silent and abandoned calls, that were previously noted as a particular concern.[14]

2.21 The ICO has reported that over the course of 2021, it continued to see a large volume of complaints concerning scam text messages. Whilst not within the remit of the ICO, it was noted that many of these related to common delivery and banking scams, but also a substantial volume regarding Covid-19 vaccinations and certification passports. Complaint levels regarding Covid-19 across all contact types in 2021 were much higher than those seen in 2020, with this mostly a result of the vaccination rollout. Complaint data has seen a mixture of genuine and scam vaccination messages reported to the ICO, and there has been a rise in nuisance calling by callers purporting to be the NHS exploiting the pandemic

[10] However, it can be difficult to work out what is driving the data given concurrent changes e.g. there were also changes in consumer behaviour such as being more likely to be at home and able to answer calls as a result of the Covid-19 pandemic.
[11] Note that the survey was not carried out in 2018 due to changes in Ofcom regulations and it has been paused since 2019.
[12] 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.
[13] See Ofcom, September 2021. Scams Survey. Suspicious texts were defined in the research as text messages sent to your mobile and an example was given of a recent postal delivery scam.
[14] There is now a category for 'other' unwanted calls (i.e. defined as all calls other than silent and abandoned calls). Consumers are encouraged to report scam calls to Action Fraud who are the reporting body responsible for scam calls.

by asking for vaccination status information before attempting to sell life or health insurance plans.

2.22 The trend towards scam calls and texts has also been raised with us in discussions with providers and has been widely reported by other organisations, including the Government, UK Finance and Which?.[15]

The increase in scam calls and texts reflects a general increase in fraudulent activity in the UK

2.23 The increase in scam calls and texts should be seen in the context of the general increase in fraud incidents across the UK, with fraud now accounting for 40% of all reported crime incidents.[16] In total, there were 5.1 million fraud offences in the year ending September 2021, a 36% increase compared with the year ending September 2019.[17] This included large increases in advance fee fraud, consumer and retail fraud and other fraud. The Office for National Statistics suggested that this may be because fraudsters were taking advantage of behaviour changes related to the Covid-19 pandemic, such as increased online shopping.[18]

2.24 While scams come in many different forms, a number of people are exposed to scams via their communications services. As discussed above, some of these scams are facilitated via calls and texts but can also be initiated via email and through other online services including social media, online messaging apps and search services. This document focuses on scams via calls and text. We are also considering some elements of online fraud that may be captured through new powers under the Online Safety Bill.[19]

There are some existing initiatives in place to reduce scam calls and texts but more needs to be done

2.25 We have previously supported work to tackle scam texts, based on protecting sender IDs. In 2018, mobile providers through Mobile UK and the Mobile Ecosystem Forum (MEF),[20] supported by Ofcom, launched 'SMS PhishGuard'. This initiative developed a SenderID Protection Registry, involving the banking industry and government agencies, where participants could register and protect the message headers used when sending texts to

[15] See Home Office, October 2021. Joint taskforce relaunched to protect against rise in fraud crime; UK Finance, March 2021. Fraud – The Facts 2021, pages 4 and 5; Which?, July 2021. Scams rocket by 33% during pandemic; Which?, September 2021. More than £355m lost to bank transfer scams in the first half of 2021.
[16] Note that these are incidents reported as part of the Crime Survey for England and Wales, rather than police recorded crime. See Office for National Statistics, January 2022. Crime in England and Wales, Appendix tables - year ending September 2021; based on total crime incidents of 12.9 million and 5.1 million incidents of fraud.
[17] Office for National Statistics, January 2022. Crime in England and Wales: year ending September 2021, Section 9. The year ending September 2019 face-to-face Crime Survey for England and Wales (CSEW) data are the latest that are based on a sample that is independent of the year ending September 2021 Telephone-operated Crime Survey for England and Wales (TCSEW) and allow for comparison over time.
[18] Office for National Statistics, January 2022. Crime in England and Wales: year ending September 2021, Section 9
[19] Draft Online Safety Bill.
[20] Mobile UK is the trade association for the UK's mobile network operators: EE, O2, Three and Vodafone. The Mobile Ecosystem Forum (MEF) is a global trade body that addresses issues affecting the broader mobile ecosystem.

consumers.[21] The registry reduces the ability for scammers to send texts impersonating a brand in the message header by providing a check on whether the sender using that sender ID is the registered party. MEF reported in 2021 that there are now more than 70 bank and government brands being protected by the registry, with over 1,500 unauthorised variants being blocked, including 300 sender IDs relating to the Government's coronavirus campaign.[22]

2.26 On scam calls, we worked with the SWG, discussed in paragraph 2.8, and UK Finance to develop the DNO list which we began sharing with providers in 2019. The DNO list includes those numbers that consumer-facing organisations, e.g. provided by UK Finance and government bodies, make available for people to call them on but which are not used by the organisation to make outgoing calls. These numbers are sometimes spoofed by scammers, claiming to be calling from that organisation. This can be a particularly effective tactic for scammers, as these numbers can appear on legitimate correspondence, for example on bank statements or on bank cards. The DNO list is shared with telecoms providers, their intermediaries and interested parties like call blocking or filtering services,[23] who can block outgoing calls from numbers on the list. Organisations with numbers on the list have reported decreases in impersonation scams using their numbers.[24]

2.27 While these solutions have had some positive results, the problem of scam calls and texts continues to evolve, requiring new and updated solutions from Ofcom, the telecoms industry and a number of other organisations. We set out below how we plan to work with those other organisations as part of a joint effort to help tackle scam calls and texts.

Structure of this document

2.28 The remainder of this document is set out as follows:

- Section 3 examines the nature and scale of the use of calls and texts to initiate scams, as well as the impact of scam calls and texts on consumers and the wider economy.
- Section 4 sets out Ofcom's proposed approach for reducing the harm from scam calls and texts.
- Section 5 highlights our next steps, including the consultations we are publishing alongside this document and the date for responding.

2.29 The document also includes the following annexes:

- Annex 1: Ofcom's powers and the obligations on telecoms providers.
- Annex 2: Glossary and abbreviations.

[21] Mobile UK, November 2018. SMS PhishGuard – Upping the ante in the fight against fraud.
[22] Mobile Ecosystem Forum, 2021. Reduce the impact of Smishing & Spoofing by SMS through industry collaboration.
[23] Call blocking or filtering services use technology to block or filter unwanted and nuisance calls on behalf of the consumer, for example via an app or hardware that is installed on a fixed line.
[24] See HMRC, June 2019. Controls prevent phone fraudsters spoofing HMRC.

3. Scam calls and texts and the impact on consumers and the wider economy

3.1 This section examines the current nature of the problem of unwanted calls and texts and attempts to set out its scale. It examines both the available data on how many people in the UK are likely to be affected by scam calls and texts and outlines the potential harmful impacts of these scams.

Understanding the problem of scam calls and texts

Scams initiated via calls and texts are often impersonation scams

3.2 Impersonation scams often begin with a call or text pretending to be from a trusted organisation. The aim is to trick the consumer into giving away sensitive information or making a payment. UK Finance notes the NHS, police and government departments as being prime among the list of trusted organisations impersonated in this way. Other organisations that are commonly impersonated include banks, utility companies, e-commerce firms, delivery companies, and broadband providers.[25]

3.3 According to UK Finance, some common methodologies for carrying out these scams are where the scammer pretends to be:

- police or bank staff claiming there has been fraud on a consumer's account. The consumer is then told to transfer money to a 'safe account', which is actually linked to the scammer;[26]
- from a utility company, communications provider or government department. These scams are likely to request that the consumer makes a payment e.g. pays a fine or overdue tax. Where the scammer is successful in getting payment details these can be used to access the consumer's account or to make unauthorised payments; or
- from a technology company requesting access to the consumer's computer, claiming that they need to help 'fix' a problem.[27]

3.4 UK Finance reported that impersonation scams saw the biggest increase of any scam type, almost doubling in 2020 compared to 2019.[28] These impersonation scams were adapted to take advantage of changing circumstances during the Covid-19 pandemic. For example, scammers used text messages containing fraudulent links for booking vaccinations or purported to be from delivery companies.

[25] UK Finance, March 2021. Fraud – The Facts 2021, page 11.
[26] UK Finance, March 2021. Fraud – The Facts 2021, page 71.
[27] UK Finance, March 2021. Fraud – The Facts 2021, page 72.
[28] UK Finance, March 2021. Fraud – The Facts 2021, page 11.

3.5 Calls and texts are commonly used for impersonation scams because they can reach large numbers of people at relatively low cost. In addition, they can be used by perpetrators who are not located in the UK.

3.6 To trick their victims, impersonation scams often include a number of common features:

- Appearance of legitimacy: scammers will mimic legitimate contacts that a consumer might expect to have. With phone calls, one way to help create the appearance of legitimacy is to use a valid phone number. Another option is to spoof a valid number or one from a trusted organisation.
- Exploiting personal traits: scammers may have already obtained information about the consumer they are contacting.
- Scarcity and urgency: scammers may stress the need to take urgent action or offer something time limited.[29]

3.7 Given our powers in relation to the use of communications services, we focus on where those services are being used to facilitate scams. However, we are aware that there can also be specific vulnerabilities in the communications ecosystem that can be exploited by scammers to cause harm to consumers. One example is SIM-swap fraud where the scammer tricks a mobile provider into providing a new SIM card for an account that does not belong to the scammer. The mobile provider then cancels the victim's existing SIM card and activates the new one which is sent to the fraudster. This may then allow the scammer to access one-time security passcodes for the consumer's personal accounts. Providers are looking into solutions for some of these vulnerabilities and more details on actions being taken are provided in paragraph 4.5.

Scams can be very sophisticated and often involve multiple steps

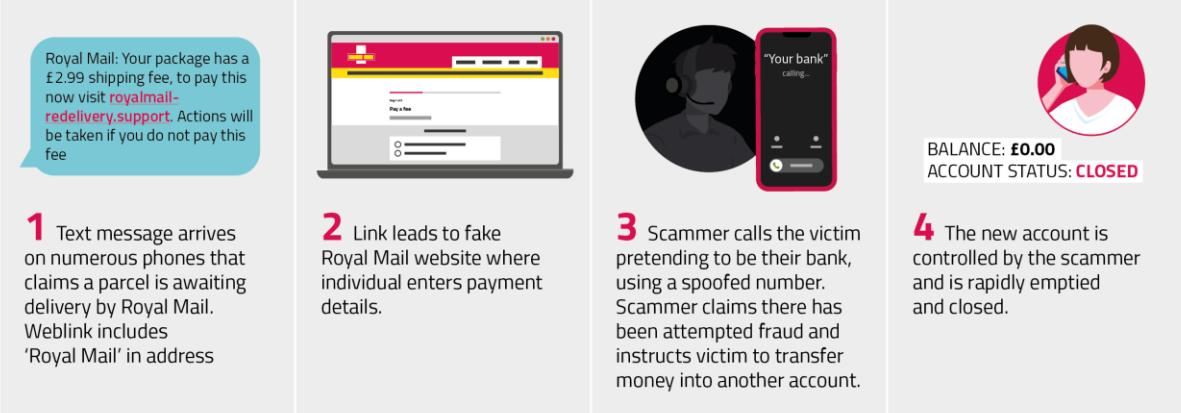
3.8 Understanding how impersonation scams are carried out is important in order for Ofcom and providers to determine how best to disrupt them.

3.9 To highlight the complexities, we set out the steps involved in a recent text scam that claimed to be from a delivery company. This is also illustrated in Figure 3 below:

- The initial text directed the victim to a professional-looking website.
- If the link was clicked, the consumer would be directed to a very convincing fraudulent website where payment and other personal details could be entered.
- The personal details were then used in a follow up call where the victim was asked to transfer money to a different account to avoid 'attempted fraud'.
- The new account was controlled by the scammer.

[29] These criteria draw on those set out by the Communications Consumer Panel in their report on scams, which included: (i) trust and the appearance of legitimacy; (ii) taking advantage of low confidence in technology and exploiting personal traits; (iii) scarcity and uniqueness of product; and (iv) consumer impulses to realise a life-changing dream. See CCP, December 2020. Scammed! Exploited and afraid. What more can be done to protect communications consumers from the ham caused by scams?, page 4.

Figure 3: Example of the steps involved in a recent text scam



3.10 Scams are dynamic in nature, with scammers adapting their tactics and new forms of scams emerging over time. We will conduct regular market research to understand how call and text scams are evolving and whether we need to adapt our response.

3.11 The example above also highlights that the use of communications services is only one part of a scam, so action from Ofcom and providers alone will not fully address the problem. An important part of our work is understanding how our plans for reducing scam calls and texts fit with steps being taken by other organisations and identifying opportunities for collaboration, to make scams harder to perpetrate across the board. Scams of this nature are common in other countries, so we also collaborate with other regulators internationally to share knowledge about our experiences and regulatory approaches. Our collaboration with other organisations is set out in more detail in Section 4 of this document.

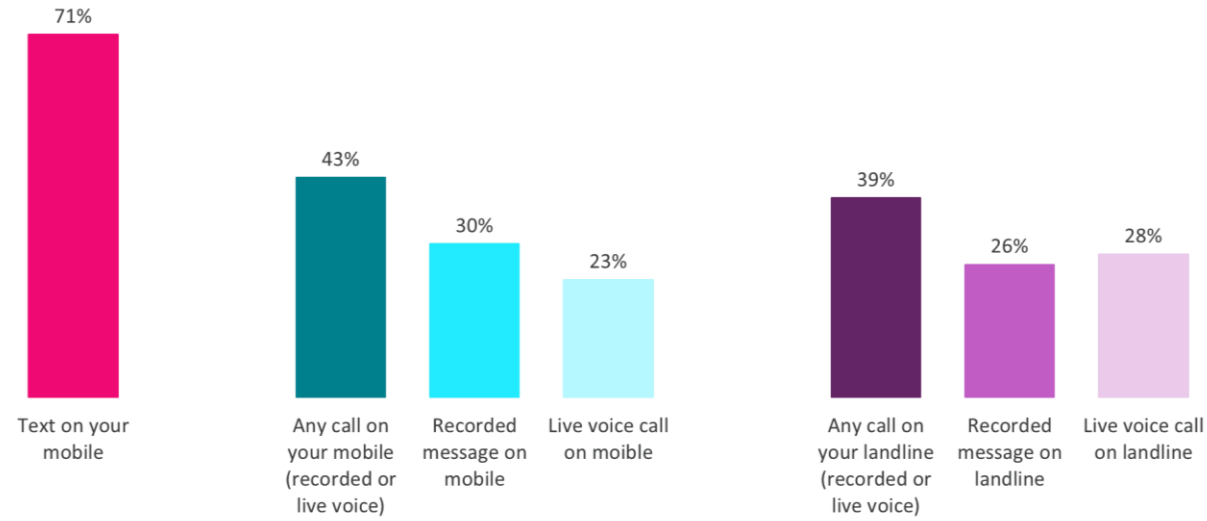
The incidence of scam calls and texts

The majority of adults in the UK are now receiving suspicious calls and texts

3.12 In a recent survey, we found that more than eight in 10 (82%) UK adults said they had received a suspicious message, in the form of either a text, recorded message or live voice call to a landline or mobile, over the past three months.[30] This represents an estimated 44.6 million adults in the UK.[31] Texts are the most common form of suspicious message with seven in 10 people (71% of respondents) reporting that they had received suspicious texts. Reports of suspicious calls were lower but still significant: 43% of respondents reported suspicious calls to their mobiles and 39% to their landlines, as shown in Figure 4.[32]

[30] In our research, 'suspicious calls and texts' were defined as including (i) text messages sent to your mobile; (ii) live voice calls (when you answer your mobile or landline phone and there is a live person on the end of the line who you can have a conversation with); and (iii) recorded messages (when you answer your mobile or landline phone and you hear a recorded message rather than a person on the end of the line). Examples were given of different types of call and text scams.
[31] Ofcom, September 2021. Scams Survey, population estimate confidence interval: +/- 900k.
[32] Ofcom, September 2021. Scams Survey.

Figure 4: Incidence of suspicious calls and texts, September 2021



Source: Scams Research 2021, Yonder.

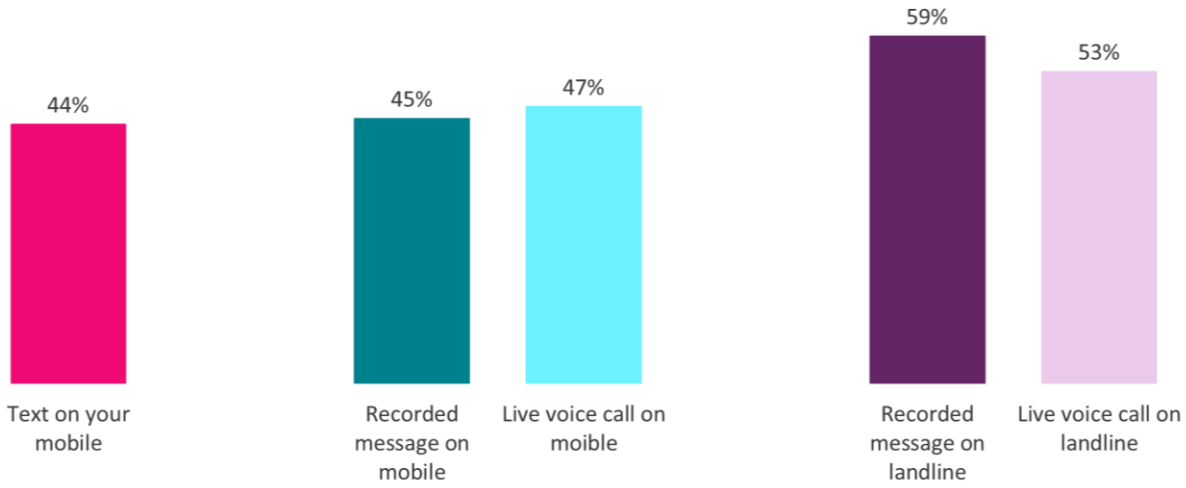
Q1: Thinking about the last three months, have you received any of the following types of suspicious texts or calls on your mobile or landline phone?

Base: All respondents, n=212433

3.13 Suspicious calls and texts are often sent regularly. Our research showed that nearly half (44%) of those who had received a suspicious text over the past three months reported receiving them at least once a week.[34] 45% of those who had received a suspicious recorded message to their mobile over the past three months received them at least once a week and 47% of those who had received at least one suspicious live voice call to their mobile received such messages at least once a week.[35] For landline, the frequency was higher with 59% of those who had received at least one suspicious recorded message over the past 3 months receiving such messages at least once a week, and 53% for live voice calls.[36] This is shown in Figure 5 below.

[33] Incidence, Total: 82%, equating to an estimated 44.6m of the population (+/-900k) / Text: 71%, equating to an estimated 38.8m of the population (+/-1,100k) / Mobile call: 43%, equating to an estimated 23.4m of the population (+/-1,200k) / Landline call: 39%, equating to an estimated 21.3m of the population (+/-1,100k).
[34] Frequency: 20% at least once a week, 19% at least a few times a week, 3% at least once a day, 2% at least several times a day.
[35] Ofcom, September 2021. Scams Survey.
[36] Ofcom, September 2021. Scams Survey.

Figure 5: Proportion of respondents receiving suspicious texts and calls at least once a week, September 2021



Source: Scams Research 2021, Yonder.

Q2a: Thinking about suspicious [text messages/recorded messages/live voice calls], how often have you received these types of message in the last three months?

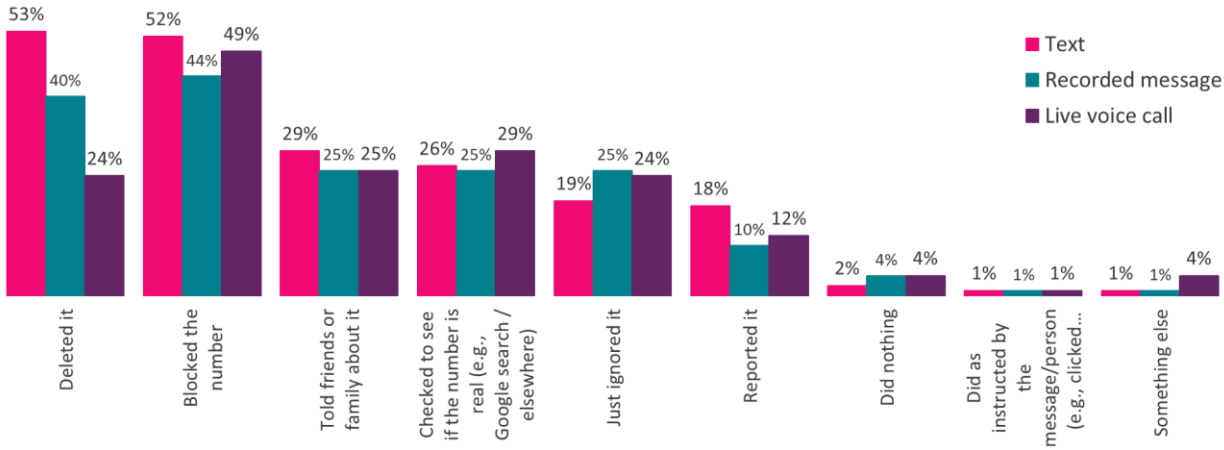
Base: All who have received a suspicious: text in the past three months, n=1519; recorded message on mobile, n=633; live voice call on mobile, n=496; recorded message on landline, n=526; live voice call on landline, n=563

While most block or delete these messages, a small but significant number follow the scammers instructions

3.14 More than half of people who received a suspicious text either deleted the message (53%) and/or blocked the number (52%). Similarly, almost half (49%) of those who received a suspicious live voice call, and more than four in 10 (44%) who received a suspicious recorded message, blocked the number. However, in the three months prior to our survey, 2% of adults who had received some form of suspicious message (text, recorded or live voice call) reported following the scammers' instructions. This is shown in Figure 6 below. The figures suggest that almost a million people followed scammers' instructions in a call or text over this period, risking financial loss and emotional distress.[37]

[37] Ofcom, September 2021. Scams Survey. Population estimate: 900k (confidence interval: +/- 300k).

Figure 6: Actions taken as a result of receiving suspicious calls or messages, September 2021



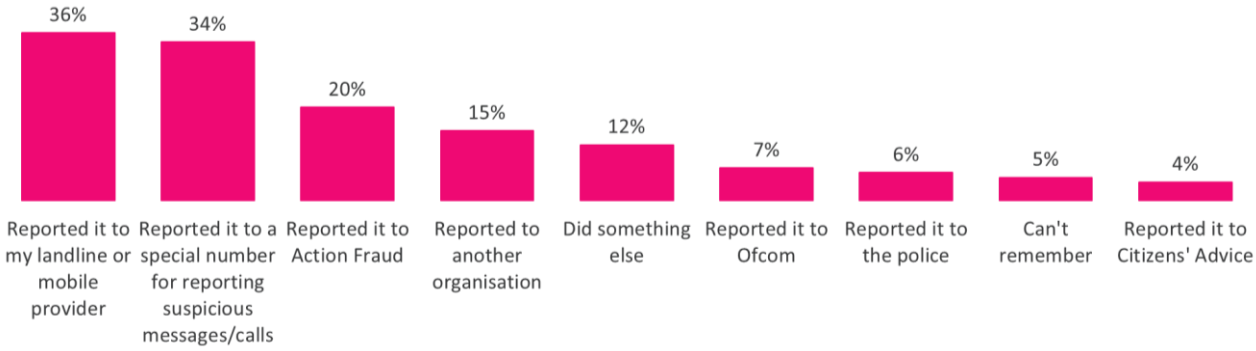
Source: Scams Research 2021, Yonder.

Question: Which, if any, actions have you taken as a result of receiving these suspicious calls/messages? Base: All who have received a suspicious text (n=1519), recorded message (n=917), live voice call (n=842).

People want to report fraudulent activity, but many are not sure how to do it

3.15 Where suspicious calls or texts were reported, the most used routes for reporting were to the person's landline or mobile provider, which was used by almost four in 10 (36%) of those who reported, or to a special number for reporting suspicious calls or texts, which was used by around three in 10 (34%) of those who reported. The next most used reporting route was Action Fraud (20%).[38] However, people were not necessarily immediately aware of where they should report suspicious communications, with 40% having to search for where to report it.[39]

Figure 7: How suspicious messages/calls were reported, September 2021



[38] Ofcom, September 2021. Scams Survey
[39] Ofcom, September 2021. Scams Survey

Source: Scams Research 2021, Yonder.

Q5a: How did you report the suspicious message/call?

Base: All who have reported a suspicious message/call, n=328

3.16 The research also revealed that almost eight in 10 (79%) mobile phone users are not aware of the 7726 number used to report a suspicious call or text – although 81% of mobile and/or landline users agreed that reporting messages is helpful in preventing people being scammed in the future.[40]

Impact on consumers

The direct financial costs from scams can be significant

3.17 The direct financial impact on those consumers who are victims of scams can be significant. Research conducted by the Communications Consumer Panel (CCP) in 2020 found that around two-thirds of people who fell victim to call scams lost more than £100 while 28% lost more than £500. For text scams, the majority (63%) of people who lost money lost up to £100.[41] The research also found that for those aged 65+ who were targeted and scammed, nearly one in two (48%) were scammed via telephone. Where people in that age group lost money, seven out of 10 (70%) lost more than £100 and several in the qualitative sample lost thousands.[42]

3.18 UK Finance estimates that police and bank staff impersonation scams resulted in losses totaling £96.6 million in 2020,[43] while other types of impersonation scams resulted in £53.7 million in losses.[44] Victims of scammers may also have to spend significant time and resources sorting out their affairs (making calls, writing letters) and awaiting compensation, after the fraud has taken place.

Many consumers also report emotional impacts from being scammed

3.19 The costs to individuals will include not only possibly significant, direct financial losses and time and resources, but also anxiety and emotional distress. Some consumers may be older and more vulnerable and find the experience particularly difficult.

3.20 Age UK reported that victims often blame themselves for falling victim to a scam. They can feel ashamed and embarrassed as a result and can feel responsible for the crime even if

[40] Ofcom, September 2021. Scams Survey.
[41] CCP, December 2020. Scammed! Exploited and afraid. What more can be done to protect communications consumers from the ham caused by scams?, page 10.
[42] CCP, December 2020. Scammed! Exploited and afraid. What more can be done to protect communications consumers from the ham caused by scams?,, page 9. Note that this may include scams initiated by means other than call or text.
[43] UK Finance, March 2021. Fraud – The Facts 2021, page 70. Note that the figures reported by UK Finance may include scams initiated via email, as well as call and text.
[44] UK Finance, March 2021. Fraud – The Facts 2021, page 72. Note that the figures reported by UK Finance may include scams initiated via email, as well as call and text.

they took precautionary measures. For older people who are more vulnerable, scams can induce feelings of loneliness, stress and depression.[45]

3.21 The CCP research also reported profound and damaging impacts on consumers, both emotionally and psychologically. Research participants reported being embarrassed at being caught out and also noted a loss of self-belief.[46] Most respondents felt angry that they had been duped. Several were too embarrassed to talk to friends or family, leaving them feeling isolated.[47]

3.22 These emotional impacts were reflected in the comments respondents provided as part of our research. When asked about how receiving suspicious calls and texts made them feel, an example of one participant's concerns is set out below.

> *"I feel more unsure of myself in keeping my personal information safe. I feel under threat. I am not very savvy when it comes to technology and sometimes don't know what to do to avoid scams. I can worry for a while afterwards in case I've reacted in the wrong way or not protected myself adequately. I feel angry and irritated as these types of messages/calls are unwanted."* – Female, 57

There can be negative effects for consumers who receive scam calls and texts, even if they are not caught out by scams

3.23 There are also likely to be wider negative effects on all consumers, including those who are not caught out by scams. Frequent unwanted calls and texts can be annoying, disruptive and waste people's time. Some comments made as part of our research reflect this.

> ***"It makes me feel very uneasy & vulnerable. They are getting more & more frequent & elaborate and I am afraid that one day I may fall for one."*** – Female, 68
>
> ***"I really dislike receiving these suspicious messages and calls. It makes me feel vulnerable and stressed out. I really dislike the idea that these suspicious calls and messages are attempts to trick my family and happen so frequently…It makes me feel annoyed too, at all the time and energy it wastes, trying to defend against it all."*** – Female, 24

3.24 Consumers may stop answering calls (letting them go to 'voicemail' if they have this facility) or may mistakenly ignore or delete genuine text messages. As a result, they may miss useful and important messages from friends, relatives or legitimate companies. This in itself may result in emotional distress or financial costs (such as the loss of a deal that would have benefitted them or missing messages about needing, for example, to update insurance details). Some consumers might spend money on technology to help block

[45] Age UK, 2018. Age UK & Action Fraud to combat scams targeting older Londoners.
[46] CCP, December 2020. Scammed! Exploited and afraid. What more can be done to protect communications consumers from the ham caused by scams?, page 11.
[47] CCP, December 2020. Scammed! Exploited and afraid. What more can be done to protect communications consumers from the ham caused by scams?, page 11.

unwanted calls or pay for services from providers to deliver personalised number blocking. These impacts were also reflected in our research.

> ***"I feel annoyed and harassed. It is difficult to tell whether the people behind these calls are the same. Now, I tend not to answer calls from numbers I do not know, but worry I might miss genuine calls."*** – Male, 37
>
> ***"It's annoying because it means I have to be suspicious of all messages even the legitimate ones"*** – Female, 18
>
> ***"To be honest they are so frequent… that I just hang up and then erase the number. I do feel slightly uncomfortable and I worry that the messages may get more pertinent and realistic so that I may be fooled. But I never answer my landline."*** – Female, 74

Scams also generate costs for the wider economy

3.25 As well as costs to consumers, there are likely to be a variety of wider negative impacts on the economy. Any wider loss of trust and confidence in telephone and text communication services as a result of scams undermines the general value of these services. For example, if consumers are reluctant to accept calls, legitimate businesses derive less value from using the telephone service to contact existing and potential customers.

3.26 Legitimate companies may also need to engage in activities to tackle scams (for example, hiring or training staff, changing communication strategies and potentially investing in technical solutions). They may also compensate customers who have been scammed. This will ultimately result in higher costs and so potentially lower profits and/or higher prices to end consumers.

4. Ofcom's approach to reducing the harm from scam calls and texts

4.1 In this section, we set out the actions we are taking and how we will be collaborating with other organisations to tackle the problem of scam calls and texts. There are three key elements to our approach:

- We aim to **disrupt scams** by making it harder for scammers to use communications services to reach consumers. We propose to strengthen 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 will **collaborate and share information** more widely, 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 stop all scams reaching consumers. We are working to **help consumers avoid scams** by raising awareness so consumers can more easily spot and report them.

Disrupting scams

Providers are taking steps to disrupt scam calls and texts sent over their networks

4.2 We have been engaging with providers to understand the steps they are taking to help prevent consumers being scammed. We have found that there is a significant amount of work already underway, as outlined below.

4.3 For example, mobile network operators either have introduced or are in the process of introducing technology that can detect the key traits of scam texts sent over their networks, allowing them to block more suspicious messages. ("SMS filtering"). Mobile network operators also use details of scam texts and calls reported to the dedicated 7726 number to identify the latest scams.

4.4 Other initiatives to tackle scams have been introduced by some providers. These include volume controls on the number of texts that can be sent in a specified time period; limiting the number of SIM cards that can be sold per transaction via online retailers; and monitoring the volume of calls made from different numbers, as well as other metrics.

4.5 In addition to these individual measures, a group of providers recently became signatories to the Telecommunications Fraud Sector Charter ('the Fraud Charter') which is an industry-led initiative that commits them to working with the Government to reduce the growing

threat of scams/fraud.[48] The Fraud Charter includes a number of actions that signatories have committed to take to reduce the harm from telecoms enabled scams. Examples include:

- Use of real-time checking to tackle SIM swap fraud: providers will supply a real-time check to financial providers of whether a mobile phone has recently been subject to a SIM swap. This will allow financial providers to check for any correlations between suspicious financial activity and the SIM swap, which may indicate an attempted fraud.
- Sector information sharing: providers will share information to help detect and reduce fraud. The aim is for this information sharing to be extended to law enforcement and financial providers.
- Improved support for victims: providers will work with victims' support groups to understand current concerns about victim handling and to identify best practice that could be adopted.

4.6 Charters have also been established by retail banking and accountancy providers. Further detail on the Fraud Charter, actions being supported by Ofcom and the Joint Fraud Taskforce (JFT) which oversees it is set out in paragraph 4.26.

We are proposing to strengthen our rules and provide updated guidance to ensure providers are doing as much as they can to tackle this problem now

4.7 It is encouraging that providers are taking steps to tackle scam calls and texts, e.g. the introduction of SMS filtering. However, we think there are some areas, particularly in relation to detecting and preventing scam calls, where strengthening our rules and guidance will make it clearer to providers what is expected of them. So we are proposing new rules and guidance to require providers to detect and block spoofed numbers and to make it harder for scammers to access valid numbers.[49]

4.8 We consider that these proposals should help prevent harm to consumers, in particular by increasing the blocking of spoofed numbers and inhibiting scammers' access to valid numbers. If implemented, these proposals are likely to 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.

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

4.9 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 phone number that appears like or mimics the number of a real company, such as a bank.

[48] The Telecommunications Fraud Sector Charter can be found here: Fraud sector charter: telecommunications. Signatories to this voluntary charter include BT, EE, Sky, Three, Tesco Mobile, Virgin Media and O2, and Vodafone.
[49] See our consultations: Ofcom, February 2022. Improving the accuracy of Calling Line Identification (CLI) data; Ofcom, February 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

4.10 Our rules already require providers to prevent these calls by sending data alongside every call that helps identify its origin. This is called CLI data. 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.

4.11 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 are proposing to strengthen our rules and guidance so that providers do more to block spoofed numbers. Our proposals have been published alongside this document.[50]

Proposed good practice guide to help prevent scammers accessing valid phone numbers

4.12 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.[51] Providers are subject to Ofcom's General Conditions, including General Condition B1, which includes requirements to ensure numbers are used effectively and efficiently.

4.13 We have found that there is 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. This proposed guide sets out the steps that we expect providers to take to help prevent valid numbers being misused, including to facilitate scams. We are publishing our proposals alongside this document.[52]

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

4.14 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 will have been spoofed and will not be a genuine call from the organisation.

4.15 In 2018, Ofcom and UK Finance began working on the DNO list. We coordinated with providers, the devolved administrations, government agencies and other public sector bodies, to record numbers that were used by those organisations to receive calls but never

[50] Ofcom, February 2022. Improving the accuracy of Calling Line Identification (CLI) data.
[51] Section 63 (General duty as to telephone numbering functions) of the Act.
[52] Ofcom, February 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.

to make calls. 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. It has been shown to be an effective tool in combating scam calls using spoofed numbers.[53]

4.16 As the DNO list has become more widely known, we are receiving higher volumes of requests for numbers to be added. To maintain the effectiveness of the list in its current form, we have updated our guidance for submitting numbers and have added information to our website to explain the purpose of the list and how to get in touch if you think you have numbers that should be added.[54] We will also be looking into expanding the list to include numbers from a wider group of organisations.

We are also considering next steps for a more comprehensive solution to number spoofing

4.17 In addition to the measures above, which we propose can be implemented quickly and offer some immediate benefits to consumers, we consider that CLI authentication could offer a more comprehensive solution to the problem of number spoofing in the longer term. CLI authentication would make it possible for the network originating the call to confirm the caller's authenticity before passing the call between networks. This would help provide consumers with assurance about the identity of the party making the call.

4.18 There are currently technical constraints on providers' ability to confirm that the telephone number included in CLI data is valid and dialable, and that the caller has permission to use the number. In particular, implementation of CLI authentication essentially requires IP networking. This means that full implementation in the UK will not be possible until the mid-2020s when voice services have migrated to IP.

4.19 Given the potential for consumer harm from spoofed CLI data, we are investigating what more could be done to ensure that the data is correct and can be trusted. If providers could do this, it may have a significant impact on preventing scams linked to spoofed numbers. For example, in the US the Secure Telephone Identity Revisited (STIR) standard has been introduced for this purpose. Through this standard, telephone numbers are 'attested' and 'signed' at call origination and 'verified' at call termination. To maximise the benefits of introducing a STIR-based standard, previous work by the NICC[55] recommended that implementation should be accompanied by a common numbering database – i.e. a database of which numbers are assigned for usage on which networks. [56]

4.20 In principle the implementation of CLI authentication supported by a common numbering database and certification authority could reduce the harm from scam calls while modernising the way telephone numbers are managed. However, deciding how this could

[53] For example, HMRC reported a significant reduction in spoof calls as a result of its inbound-only numbers being added to the list. See HMRC, June 2019. Controls prevent phone fraudsters spoofing.
[54] More information about the 'Do Not Originate' (DNO) list is available on our website.
[55] NICC is a technical forum for the UK communications sector that develops interoperability standards.
[56] NICC, 2018. Report into implementation of Secure Telephone Identity Revisited (STIR) in the UK, page 31.

be implemented and defining the necessary technical standards to meet our key policy objectives, will entail a significant amount of work. Therefore, we think it is important that planning for any future changes starts now.

4.21 We are meeting with industry stakeholders to understand their views on the introduction of CLI authentication in the UK and will use insights from these meetings to determine the best way forward. We plan to issue a call for inputs in Q4 2022 seeking views on the role of CLI authentication and what would be required to implement industry wide CLI authentication technology.

Enhancing collaboration and sharing information

4.22 The example of an impersonation scam set out in Figure 3 shows that disrupting access to and the use of communications services by scammers is one way of making scams harder to perpetrate. However, because there are a number of steps involved in a scam (e.g. contacting the consumer, convincing them the scammer is from a legitimate organisation, accessing personal details and using those details to facilitate a payment to the scammer), there are likely to be a number of other interventions that would help to disrupt the scam.

4.23 Not all of these levers sit with Ofcom and a range of organisations have a role to play. Collaboration and coordination are therefore important for maximising the impact of our work to protect consumers from scam calls and texts. We have therefore been working to understand how our plans fit with what others are doing and have looked for opportunities to collaborate.

4.24 An overview of some of the key organisations we collaborate with to help tackle scams is shown in Figure 8 below.

Figure 8: Overview of some of the key stakeholders working to tackle scams

Source: Ofcom.

4.25 In the section below, we set out details of our collaboration with other organisations to help tackle the problem of scams.

Government and law enforcement bodies

4.26 Scams facilitated via calls and texts form part of a wider problem of fraud, which is a priority for Government and law enforcement bodies given concerning increases in this type of activity. We have been working closely with the Home Office, which has overall government responsibility in this area. Ofcom is a member of the recently relaunched Joint Fraud Taskforce (JFT), which includes members from across Government, industry, regulators, law enforcement and victim representatives. The role of the JFT is to monitor the delivery of voluntary commitments made by signatories to the telecoms, retail banking and accountancy fraud sector sectors, as discussed in paragraph 4.5.[57]

4.27 We, along with a range of other organisations, will be supporting providers in delivering some of the actions in the Fraud Charter. This is discussed in more detail in paragraph 4.35 to 4.36.

[57] Home Office October 2021. Joint taskforce relaunched to protect against rise in fraud crime.

Regulators

4.28 There are a number of regulators who have specific areas of responsibility in relation to unwanted calls and texts or scams and with whom we need to coordinate in order to ensure a joined-up response to these issues.

UK

4.29 The ICO leads on tackling live and recorded marketing calls and nuisance text messages and emails (which may sometimes be a pre-cursor to fraud) and has worked jointly with Ofcom on tackling nuisance calls since 2013. During the pandemic, the ICO reported an increase in complaints about nuisance marketing and noted that where they find evidence of fraud, they work closely with Action Fraud, Trading Standards and law enforcement.[58]

4.30 During 2021/22, the ICO issued 26 fines, totalling £2,465,000, to organisations that had made unlawful nuisance marketing calls and/or had sent nuisance text messages or emails. The ICO's most recent work has been focused on three main areas of investigation in relation to unsolicited marketing calls:

- White goods insurance/warranty products.[59] These calls appeared to be fraudulent in nature and targeting elderly and vulnerable individuals with a high level of potential detriment. To date, fines totalling £130,000 plus two Enforcement Notices have been issued to organisations found to have breached the legislation.
- Home improvements/energy saving.[60] These nuisance calls also appear to target the elderly and vulnerable. To date, the ICO has issued fines totalling £452,000 plus three Enforcement Notices.
- Pensions. This investigation is in relation to calls relating to pensions and more recently widened to include investment marketing, as this can be used as a vehicle to encourage the release of monetary assets, including pensions funds. In 2021, the ICO has issued fines totalling £190,000 plus two Enforcement Notices.

4.31 The ICO is working with partner agencies in relation to these nuisance calls. The ICO also leads Operation Linden, a group that includes regulators, consumer groups, trade associations and industry, whose members work together to share their experience of nuisance calls and identify opportunities to tackle them. Minutes and actions from meetings are published on the ICO's website.[61]

4.32 In addition to the ICO, a number of other regulators are undertaking work to tackle scams or related areas of work, including the Financial Conduct Authority (FCA) and the Payment Systems Regulator (PSR).[62] Given the cross-cutting nature of scams, we have been coordinating with other regulators both bilaterally and through existing joint initiatives to

[58] ICO, April 2020. ICO statement on investigating coronavirus scams.
[59] Including fridge freezers and TVs etc.
[60] Including loft insulation, solar panels, windows/double glazing and boiler/heater replacements.
[61] See ICO, Nuisance calls and messages.
[62] The PSR recently consulted on a number of measures to improve scam detection, prevention and, ultimately, victim reimbursement.

consider any opportunities for collaboration. The Digital Regulation Cooperation Forum (DRCF) will also be an important vehicle for regulatory coordination and collaboration on fraud and scams.[63]

International regulators

4.33 The problem of unwanted calls and texts reaches beyond the UK and we have benefitted from sharing our approaches for tackling these problems with regulators in other jurisdictions. Experiences in many of these countries have mirrored those in the UK, indicating that the problem of scam calls and texts is a global one.

4.34 Regulators are implementing a variety of solutions and it is useful to learn from these experiences. For example, in the US the Federal Communications Commission (FCC) has recently implemented a CLI authentication standard[64] and the Australian Communications and Media Authority (ACMA) has introduced a code requiring companies to detect, block and trace scam calls.[65] In addition, many scams that we see in the UK originate outside the UK, making international cooperation even more vital.

Industry collaboration

4.35 In addition to our role on the JFT, Ofcom is collaborating with providers and other organisations to support work under two key actions from the Fraud Charter.

4.36 Through our already established SWG, Ofcom is working with providers on an action to identify and prevent scam calls.[66] Ofcom will be supporting this action through its chairing of the SWG, set out in paragraph 2.8. In relation to calls, many providers are already monitoring indicators for unwanted calls but the criteria being used needs updating to reflect the way in which unwanted calls are now manifesting, as outlined in paragraph 2.16. Further consideration will also be given by the SWG to how relevant data can be shared both within the industry and more widely, for example with law enforcement and the banking sector.

4.37 In response to the launch of the Fraud Charter, the existing cross-industry body, which brought together Ofcom with Mobile UK, mobile providers, the ICO and the National Cyber Security Centre (NCSC), has been reformed as the Messaging Scams Group (MSG) to look at the issue of smishing (text scams), as outlined in the Fraud Charter.[67] The current focus of the MSG is reviewing the use of the 7726 reporting service, which is provided by industry and allows consumers to report suspected scam calls and texts received on their mobiles. The review will consider how 7726 data can be used more effectively against scam texts.

[63] The DRCF was formed in July 2020 by Ofcom, the ICO and the Competition and Markets Authority (CMA). The Financial Conduct Authority (FCA) joined the DRCF as a full member in April 2021.
[64] See Combating Spoofed Robocalls with Caller ID Authentication | Federal Communications Commission (fcc.gov) .
[65] See New rules to detect, trace and block scam calls | ACMA.
[66] See Action (1) in the Fraud Charter.
[67] See Action (2) in the Fraud Charter. Smishing is defined in the charter as where 'Criminals use SMS/text messages to obtain personal information, socially engineer and/or defraud the victim'.

4.38 There are also a number of initiatives that are intended to foster collaboration across organisations and sectors. For example, Ofcom supports Stop Scams UK, a cross-industry group. Stop Scams UK brings together senior experts from the telecoms and financial services sectors to collaborate on technical initiatives which aim to prevent scams. In September 2021, Stop Scams UK and the Global Cyber Alliance launched a UK-wide service, the 159 call service, which is intended to help consumers who think they may have been contacted by a scammer claiming to be from their bank, by providing a safe route through which they can contact their bank.[68] Ofcom has been supporting Stop Scams UK in its use of the 159 short-code.

Helping consumers avoid scams

4.39 Given the pace at which scammers change their tactics, we understand that it will not be possible to stop all scams reaching consumers. We are working to help consumers avoid scams by raising awareness and improving information about scams so consumers can more easily spot and report them.

Raising awareness

4.40 We recently launched a scams awareness campaign with clear advice for consumers on how to respond to suspicious calls and texts, making use of social media and print/broadcast media to reach a broad range of UK consumers. Given the low levels of reporting of scams, we focused on ways to report suspicious activity, with the aim being that this would provide better information for providers and law enforcement to act on. In particular, we promoted the use of 7726 for reporting scam calls and texts to mobiles. Our updated messaging is set out below.

Figure 9: What to do if you receive a suspicious call

[68] See 159 — Stop Scams UK.

Figure 10: What to do if you receive a suspicious text message

Updating consumer advice

4.41 Given the shift from nuisance calls to scam calls, and the significant increase in scam texts, we have also been making updates to the consumer advice on Ofcom's website. This is intended to raise awareness amongst consumers about current scams and how to respond when they receive suspicious communications. We will continue to monitor engagement with our updated advice.

4.42 We are engaging with other organisations such as City of London Police, who are the national policing lead for economic crime, and Which? to understand the latest scam methods so we can keep our advice up to date. We will be carrying out regular research on the incidence of scam calls and texts, and how consumers are responding, to guide our ongoing work and approach to tackling scams.

4.43 We have also assessed the advice about scams that providers currently make available to customers. We found that it commonly includes information on signs of scams, advice on how to avoid and report scams, services offered by the provider (e.g. call-screening and anti-virus software) and links to further resources. However, the content varies between providers and we think customers would benefits from more consistent advice and messaging. We note that signatories to the Fraud Charter will be reviewing the effectiveness of existing awareness measures and will consider using more consistent cross-sector messaging for consumers.

Preventative tools for consumers

4.44 In addition to being aware of scams, there are several preventative tools available for consumers to help reduce their exposure to scams. For example, there are several facilities for screening calls, both for fixed and mobile voice services. Many fixed voice providers already make these kinds of services available, often for free, but take-up has historically been low. People can also make use of landline call blocker services and mobile device solutions offered through operating systems or device manufacturers. We will be considering how to promote awareness of these tools through our consumer advice.

5. Next steps

5.1 Reducing harm from scams is an active part of Ofcom's work and we are constantly reassessing what we can do to protect consumers. It is a complex problem that no single organisation can solve. We will continue to work closely with providers, other regulators, law enforcement and other bodies to identify how best to protect people from scams and prevent them happening in the first place.

5.2 Alongside this policy statement, we have published consultations on:

- Proposals to strengthen our rules and guidance for providers to detect and block 'spoofed' numbers.[69]
- A proposed good practice guide to help prevent scammers accessing valid phone numbers.[70]

5.3 These consultations close on 20 April 2022. We will consider consultation responses carefully and intend to publish statements on our decisions in Autumn 2022.

5.4 We have also added information to our website to explain the purpose of the DNO list and how to get in touch if you think you have numbers that should be added to the list.[71] We will be considering whether the DNO list can be expanded to include numbers from a wider group of organisations.

5.5 In order to monitor the impact of the work that we and others are doing, we plan to carry out follow-up research into the incidence of call and text scams. This will help to inform us about the extent to which our work is helping to protect consumers and areas where more needs to be done.

5.6 These measures should help to bring some immediate benefits to consumers but over the longer term, having processes that detect and block spoofed numbers more comprehensively will be important to help tackle scam calls. We are exploring the introduction of technical standards that make it possible for the network originating the call to confirm the caller's authenticity before passing it to the network of the person receiving the call, referred to as 'CLI authentication.' We plan to issue a call for inputs in Q4 2022 seeking views on the role of CLI authentication and what would be required to implement the technology across industry.

[69] Ofcom, February 2022. Improving the accuracy of Calling Line Identification (CLI) data.
[70] Ofcom, February 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers.
[71] More information about the 'Do Not Originate' (DNO) list is available on our website.

A1. Ofcom's powers and the obligations on telecoms providers

General duties

A1.1 Ofcom's principal duty, in carrying out its functions, is to further the interests of citizens in relation to communications matters and to further the interests of consumers in relevant markets, where appropriate by promoting competition. In performing our duties, we are required to have regard to a number of matters, as they appear to us to be relevant in the circumstances, including the desirability of ensuring the security and availability of public electronic communications networks and services; the needs of persons with disabilities, of the elderly and of those on low incomes; the desirability of preventing crime and disorder; and the opinions of consumers in relevant markets and of members of the public generally. This is set out in section 3 of the Communications Act 2003 (the Act).

Persistent misuse

A1.2 Ofcom has powers under sections 128-130 of the Act to take enforcement action against a person who has persistently misused an electronic communications network or service. A person misuses a network or service if:

a) the effect or likely effect of the use is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety, e.g. where a person makes silent or abandoned calls; or

b) the person uses the network or service to engage in conduct the effect or likely effect of which is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety e.g. using the phone in a way that misleads others into calling premium rate or revenue sharing numbers.

A1.3 The misuse is persistent if repeated on a sufficient number of occasions for it to be clear that it represents a pattern of behaviour or practice, or recklessness as to whether persons suffer annoyance, inconvenience or anxiety. Ofcom may impose a penalty of up to £2m on the misuser.

A1.4 We must publish a statement of our policy on the exercise of our powers under sections 128-130. In our 2016 statement we said our top priority was to tackle silent calls, that we were also concerned to tackle abandoned calls and might take action in relation to other forms of persistent misuse where there is significant harm. We gave examples of activities that may fall within section 128, including misuse of a CLI facility, use of numbers in a way that is inconsistent with the Numbering Plan and improper behaviour by call centre agents.

Calling Line Identification (CLI) rules

A1.5 General Condition (GC) C6 applies to providers of number-based interpersonal communications services and public electronic communications networks over which those services are provided:

a) Under GC C6.2, regulated providers must provide CLI facilities and enable them by default, unless they can demonstrate it is not technically feasible or economically viable to do so. GC C6.5 requires that subscribers must not be charged any additional or separate fee for standard CLI facilities.

b) GC C6.4 requires providers to ensure, so far as technically feasible, that the CLI data associated with a call includes a valid, dialable number which uniquely identifies the caller. They must respect end-users' privacy choices about the display of CLI data, subject to the requirements of relevant data protection legislation.

c) Under GC C6.6, where technically feasible, providers must take all reasonable steps to identify and block calls, other than calls to Emergency Organisations, in relation to which invalid or non-dialable CLI data is provided.

A1.6 We have published the Calling Line Identification guidelines, setting out what is expected of providers to meet these requirements. We may also take the guidance into account when exercising our powers to take enforcement action in relation to persistent misuse.

Blocking access to numbers and services

A1.7 Under GC B4.2, all communications providers (CPs) must ensure, where technically and economically feasible and subject to GC C6.6, that end-users in any part of the UK or EU are able to (a) access and use those non-geographic numbers the CP adopts; and (b) access all telephone numbers provided in the UK or EU, regardless of the technological devices used by the operator.

A1.8 GC B4.4 provides that Ofcom can request that CPs block access to telephone numbers or public electronic communications services on the basis of fraud or misuse, and in such cases withhold revenue associated with those numbers or services.

A1.9 Section 8 of our Enforcement Guidelines explains the process we will usually follow when issuing a direction under GC B4.4 requiring CPs to block access. It sets out that we consider fraud or misuse in this context may include: call-back scams, other artificial inflation of traffic (AIT) schemes or scams, misuse of a CLI facility, calls made following the use of services obtained by providing false information, use of numbers in breach of requirements in the Numbering Plan or GC 17 (now B1), use of a number to make calls or send messages in breach of PECR,[72] and spoofing.

A1.10 Some forms of fraud or misuse may also constitute persistent misuse and Ofcom may additionally or alternatively take action under sections 128-130 of the Act. Some may also

[72] The Privacy and Electronic Communications (EC Directive) Regulations 2003.

represent contraventions of other consumer protection legislation and we would liaise with the relevant authorities as to which set of requirements is more appropriate and may be more effectively deployed.

Allocation, adoption and use of telephone numbers

A1.11 Condition B1 sets out the terms under which CPs may apply for, be allocated and adopt telephone numbers so as to ensure their effective and efficient use. Among other requirements:

a) GC B1.6 provides that where telephone numbers have been allocated to a CP, that provider must secure that the numbers are adopted or otherwise used effectively and efficiently.

b) GC B1.8 requires the CP to take all reasonably practicable steps to secure that its customers, in using numbers, comply (where applicable) with the provisions of GC B1, the Numbering Plan and the non-provider numbering condition.

c) GC B1.9 provides that the CP shall not transfer use of telephone numbers from the Numbering Plan unless:

i) the numbers have been allocated to the CP; or the CP has been authorised (either directly or indirectly) to adopt the numbers by the person allocated those numbers;

ii) the numbers are used in accordance with the Numbering Plan; and

iii) the numbers are adopted or otherwise used effectively and efficiently.

Withdrawing number allocations

A1.12 In 2018 we introduced GC B1.18 (d) and (e), enabling us to withdraw an allocation of numbers from a CP where:

a) the CP has used a significant proportion of the numbers, or used the allocation to a significant extent, inconsistently with GC B1, or to engage in fraud or misuse; or

b) Ofcom has advised the CP that a significant proportion of the numbers has been used, or the allocation has been used to a significant extent, to cause harm or a nuisance, and the CP has failed to take adequate steps to prevent such harm or nuisance.

A1.13 We explained in our 2018 statement how we would exercise the power.

Privacy and Electronic Communications Regulations

A1.14 The ICO has primary responsibility for enforcing the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR). These cover marketing calls, texts, emails and faxes; use of cookies; security of public electronic communications services; and privacy of customers using communications networks or services (including presentation of CLI data). The ICO can pursue criminal prosecution, non-criminal enforcement and audit, and impose fines of up to £500,000 for breaches of PECR.

A1.15 An activity may amount to misuse under section 128 of the Act and breach the PECR. We may take action on the basis the conduct amounts to persistent misuse. In our 2016 policy statement we said that when considering such cases, we would consult with the ICO to determine who is best placed to take action.

A2. Glossary and abbreviations

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

Calling Line Identification (CLI): means data that enables identification of the number from which a call could be made or to which a return call could be made.

CLI authentication: implementation of standards that make it possible for the network originating a call to confirm the caller's authenticity before passing it to the network of the person receiving the call.

CLI data: means the contents of all signalling messages which can be used between Communications Providers and/or between Communications Providers and End-Users to signal the origin of the call and/or the identity of the calling party, including any associated privacy markings.

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.

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.

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.

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.

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

SMS: stands for 'Short Message Service' and means a text message delivered to a handset.

Spoofing: where callers hide 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.

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

Unwanted calls: calls that consumers do not want to receive. These can range from nuisance calls, through to scams.