Reducing mobile messaging scams

Evidence and options for addressing consumer harm

Call for Input

Published 29 July 2024
Closing date for responses: 7 October 2024

Contents

Section

Annex

1. Overview

1.1 Scammers use mobile messaging services, often alongside other communications channels such as telephone calls or email, to reach victims at a mass scale and trick them into sharing money or sensitive information. Mobile messaging scams lead to significant financial and emotional harm and can reduce confidence in telecoms services more broadly.

1.2 Through Ofcom's programme to tackle telecoms scams we have been closely monitoring mobile messaging scams. This Call for Input (CFI) seeks views and evidence from stakeholders to further support our assessment of the scale of the problem and whether and where further action should be taken by Ofcom, industry, or others.

1.3 This CFI covers Short Message Service (SMS) and Rich Communications Services (RCS). Both require a user's mobile telephone number in order to deliver a message over the mobile network and therefore are directly in scope of Ofcom's telecoms regulatory powers and duties:

- SMS is the traditional text messaging service on mobile networks. It is available to all mobile users, and UK operators have a range of measures in place to disrupt SMS misuse by scammers.
- RCS is a newer service that seeks to modernise SMS with additional functionality. In the UK, mobile operators currently partner with Google to deliver RCS. It is likely to become more widely available in future and we therefore expect that scammers will increasingly seek to exploit it. Disrupting the use of RCS by scammers raises some new challenges compared to SMS which we consider important to cover in this CFI.

1.4 We know that scammers also use other messaging services, such as WhatsApp, to carry out scams. While these services may require users to provide a telephone number to sign up, messages are not routed through the network using the number itself. Such online communication services (OCS) are out of scope of this document as they are covered by Ofcom's work to implement the Online Safety Act.[1]

This Call for Input

- **Sets out our understanding of the mobile messaging market and how scams are perpetrated within it.** SMS usage has declined in the past decade but it remains widely used, particularly by businesses to contact customers. Scammers are finding ways to contact people through SMS both by using SIM cards and by using the arrangements that businesses have in place for bulk SMS. The latter involves organisations - known as aggregators - which contract with businesses to arrange delivery of large volumes of messages. Scammers also appear to be using end-to-end encrypted RCS, delivered over Google's Jibe platform, and we wish to better understand how this occurs.
- **Summarises the existing evidence we have gathered on the scale of the problem.** Mobile network operators are blocking around 30 million suspicious SMS messages per month in the UK. However, scam SMS and RCS messages are still getting through. Over half (56%) of mobile phone users report having received a suspicious

[1] Ofcom, 2023. *Protecting people from illegal harms online*

text message in the past three months, though encouragingly this is down from 74% in 2022. **There are significant areas where the data we have reviewed is not conclusive, so we are seeking further input from stakeholders.**

- **Sets out measures used in the UK and internationally to tackle messaging scams.** These include measures: to stop scammers from accessing mobile networks in the first place, such as through due diligence checks; to identify and block suspicious messages while they are in transit, particularly through traffic monitoring tools; and to help consumers avoid and report messaging scams, such as through consumer education and handset-based tools. **We welcome input from stakeholders on the impact of existing measures and where further measures could have the greatest effect.**

This CFI closes for responses on 7 October 2024.

2. Introduction and background

Ofcom's telecoms scams programme

2.1 This publication forms part of a wider response to the prevalence and changing nature of telecoms scams. We published a policy statement in February 2022 explaining our approach.[2] In particular, we said:

- We aim to **disrupt scams** by making it harder for scammers to use communications services to reach consumers.
- We will **collaborate and share information** more widely, including with the Government, regulators, law enforcement and consumer groups.
- We are working to **help consumers avoid scams** by raising awareness so that consumers can more easily spot and report them.

2.2 To deliver our strategy, we have already implemented several measures to increase friction for scammers abusing phone calls. These include requirements on operators to block suspicious calls, including calls from abroad which are spoofing a UK network number, and know your customer (KYC) requirements on UK operators who sub-allocate numbers to other UK operators.[3]

2.3 In February, we launched an enforcement programme into phone and text scams[4] and published a roadmap setting out our future work plan.[5] Alongside this CFI, we have also published two further documents aimed at further disrupting scam calls being made to UK consumers from abroad.[6]

2.4 More broadly, we recognise that scammers' tactics are constantly evolving, including contacting people using online services. Following the passage of the Online Safety Act, Ofcom also has new responsibilities to oversee how online services fulfil their duties about tackling fraud. We are therefore working to tackle both telecoms and online scams under our respective regulatory regimes, and we are ensuring close coordination where appropriate.[7] For this CFI we treat online communication services such as WhatsApp and Facebook Messenger as out of scope.

[2] Ofcom, 2022. *Tackling scam calls and texts*
[3] Ofcom, 2024. *Tackling scam calls and texts webpage*
[4] Ofcom, 2024. *Enforcement programme into phone and text scams*
[5] Ofcom, 2024. *Calling Line Identification (CLI) authentication assessment and future roadmap*
[6] These are a statement setting out changes to further clamp down on spam calls spoofing UK landline numbers from abroad and a call for input on options to address scammers spoofing UK mobile numbers from abroad.
[7] This includes, for example, commissioning consumer research to understand experiences of scams across both areas, and joint engagement with stakeholders.

Ofcom's legal duties and powers

General duties

2.5 When formulating this call for input we have had regard to our general duties. 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.

2.6 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 disabled people, of the elderly and of those on low incomes; the desirability of preventing crime and disorder; and the opinions of consumers in relevant markets and of members of the public generally.[8] Additionally, Ofcom must have regard to the interests of those consumers in respect of, among other things, quality of service[9] and, in performing their duties, to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed.

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

Functions and powers relating to telephone numbers

2.8 Ofcom has a number of functions relating to telephone numbers,[10] including a general duty to ensure the best use is made of numbers, encouraging efficiency and innovation for that purpose.[11] To help us carry out these functions, Ofcom has the power to set rules around the allocation, adoption and use of telephone numbers.[12] Ofcom can impose numbering rules on communications providers (which are defined in our General Conditions[13] as persons who provide an Electronic Communications Network[14] or an Electronic Communications Service[15]).

---

[8] Section 3(4) of the Communications Act 2003 (the Act). We also have public sector equality duties, in particular we must have due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it. This involves considering the need to: remove or minimise disadvantages suffered by people due to their protected characteristics; and take steps to meet the needs of people with protected characteristics.

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

[10] Which are set out in sections 56 to 63 of the Act.

[11] Section 63 of the Act.

[12] Including under sections 45-47, 51, 56A, 58 and 61 of the Act.

[13] The General Conditions of Entitlement (General Conditions) are the regulatory conditions that all providers of electronic communications networks and services must comply with if they want to provide services in the UK. See Ofcom, *General Conditions of Entitlement*, May 2023.

[14] Electronic Communications Network (ECN) is defined in section 32(1) of the Act.

[15] Electronic Communications Service is defined in sections 32(2) and 32(2A) of the Act as any of the following types of service provided by means of an ECN, except so far as it is a content service: (a) an internet access service; (b) a number-based interpersonal communications service (NICS); and (c) any other service consisting in, or having as its principal feature, the conveyance of signals, such as a transmission service used for machine-to-machine services or for broadcasting. NICS is defined in s. 32A of the Act and in summary means a service made available to the public which (a) enables direct interpersonal and interactive exchange of

2.9 Ofcom has used its powers to impose conditions on communications providers around what they should be doing to protect the interests of consumers. For example:

a) B1.6 requires communications providers to ensure the effective and efficient use of numbers, which includes ensuring numbers are not misused.
b) B1.8 requires communications providers to take all reasonably practicable steps to ensure their customers comply with the General Conditions (including B1.6) in relation to their use of numbers.[16]
c) C6 requires providers[17] to provide Calling Line Identification (CLI) facilities by default and ensure that CLI data includes a valid, dialable number which uniquely identifies the calling party (where technically feasible).

2.10 We can also impose numbering rules on operators that are not communications providers but that have been allocated numbers.[18]

2.11 Importantly, our numbering rules do not only apply to providers that are based in the UK. Our rules apply to any provider that falls within the scope of the relevant definitions where there is also a territorial connection to the UK because, for example, a provider is providing services to customers in the UK. Our rules can therefore apply to providers outside of the UK to the extent they are providing a service with a territorial connection to the UK.

2.12 Ofcom also has a duty to publish and keep under review the National Telephone Numbering Plan (the Numbering Plan).[19] The Numbering Plan sets out telephone numbers that are available for allocation and any restrictions on how they may be adopted or used.

2.13 Where providers contravene our rules, such as where telephone numbers or services have been misused, Ofcom can take enforcement action including issuing a penalty;[20] requesting that providers block access to relevant numbers or public electronic communication services;[21] and withdrawing telephone number allocations.[22]

2.14 To further tackle messaging scams, if we consider it appropriate, we have the option to rely on the existing rules (supplemented by additional guidance, where considered necessary) or consider imposing further rules. Any new conditions or amendments to the existing conditions would need to: satisfy relevant legal tests[23] and consider the likely impacts of our

---

information by means of ECNs between a finite number of persons, where the persons initiating or participating in the communication determine its recipient; and (b) connects with or enables communication with numbers from a national/international numbering plan.

[16] Ofcom has also published a Good Practice Guide setting out the steps we expect communications providers to take to help prevent telephone numbers being misused when they are sub-allocating numbers (to other operators) or assigning numbers to business customers, including to ensure compliance with General Conditions B1.6 and B1.8. See Ofcom, 2022. *Good practice guide to help prevent misuse of sub-allocated and assigned numbers*. Paragraph 2.15 of that Good Practice Guide confirms that "misuse of numbers, for example to facilitate scams, is not an effective and efficient use of numbers".

[17] General Condition C6 applies to all providers of NICS and public ECNs over which NICS are provided.

[18] Section 59 of the Act. This includes operators that have applied for or have been allocated numbers by Ofcom (or its predecessors) as well as operators that have been suballocated numbers under our General Conditions.

[19] Section 56 of the Act.

[20] In accordance with sections 96A -97 of the Act. We have powers to impose significant financial penalties of up to 10% of annual turnover.

[21] General Condition B4.4.

[22] Section 61 of the Act and General Condition B1.18.

[23] Including the test set out in sections 47 of the Act.

proposals.[24] In addition, we would need to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed and any other principles appearing to us to represent the best regulatory practice. [25]

Specific powers relating to the misuse of networks or services

2.15 Ofcom also has powers under sections 128 to 130 of the Act to take enforcement action against a person who has persistently misused an electronic communications network or service, which can result in a penalty of up to £2m.[26] In brief, "misuse" of electronic communications networks and services in this context involves using a network or service in ways which cause or are likely to cause someone else to suffer annoyance, inconvenience or anxiety, including where the network or service is used to scam individuals.[27] Misuse is persistent where it is repeated enough for it to be clear that it represents a pattern of behaviour or practice, or recklessness about whether others suffer the relevant kinds of harm. Any enforcement action for persistent misuse would take into account Ofcom's Persistent Misuse statement.[28]

[24] Including in accordance with our duties under section 7 of the Act.
[25] Section 3(3) of the Act.
[26] See Ofcom, 2016. *Persistent misuse statement*
[27] Misuse is defined in section 128(5) of the Act.
[28] Ofcom, 2005. *Statement of policy on the persistent misuse of an electronic communications network or electronic communications service*

3. The mobile messaging market and how scams are perpetrated

3.1 In this chapter we summarise the features of key services which are in and out of our scope. We then explain our understanding of how scammers are accessing mobile messaging services.

Mobile messaging context

3.2 In this CFI we consider mobile messages which have number-based routing. Mobile messages were originally designed for mobile-to-mobile communications, routed across and between mobile networks to their destination. Although it is now possible for applications to create and send messages and for messages to be received on devices other than mobile phones, in general the conveyance of messages occurs through communications networks using number-based routing. This is in contrast to other messaging services where messages are exchanged between central servers and retrieved separately by applications on mobile devices.

Short Message Service messages

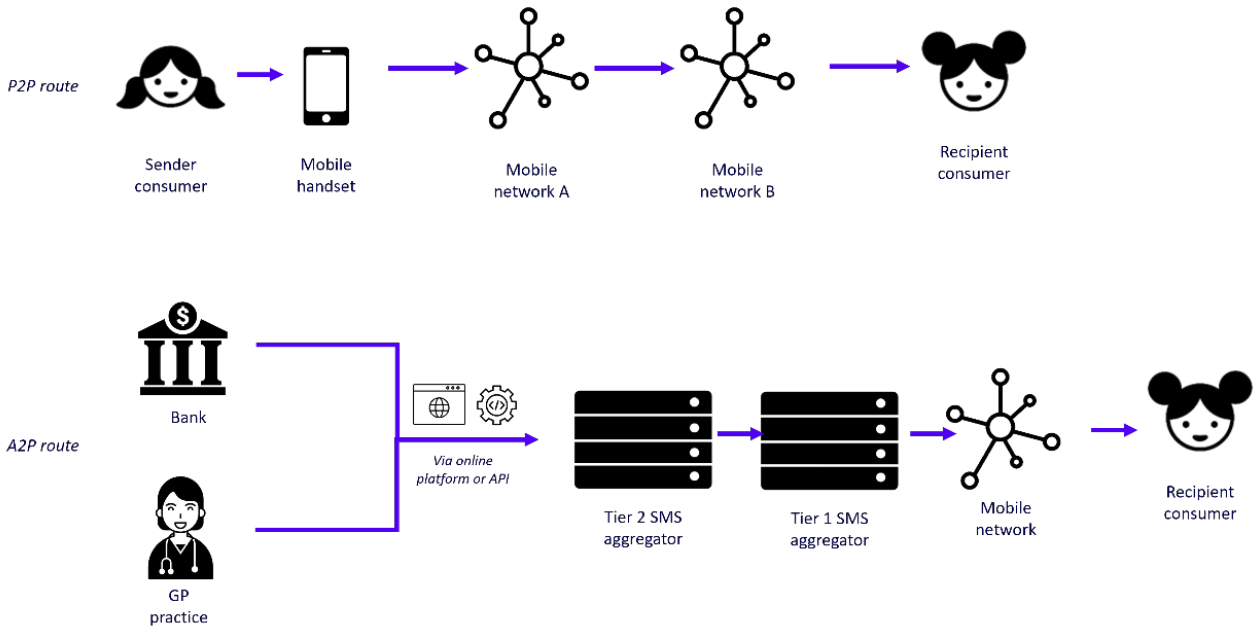
3.3 Short Message Service (SMS) enables text messaging between mobile devices using mobile numbers. SMS has been available since the 1990s and, although alternative messaging services are now widely used, SMS remains valuable to consumers and businesses in part because of its simplicity and its availability on all mobile phones.

3.4 For the purposes of our analysis, we have categorised SMS by those which can be sent from person-to-person (P2P) or application-to-person (A2P). These are summarised in Figure 1. We defined these services as:

- P2P messages are sent from one SIM card to another through and between mobile networks. Typical use cases include sending messages between family and friends.
- A2P messages are sent through an online platform or an API,[29] and then subsequently through a mobile network, to which the online platform links. A2P messaging allows for automation and scalability. Typical use cases include sending one-time passcodes to log into various online services, appointment reminders, promotional messages, as well as customer service and surveys. A2P SMS is attractive to businesses and public bodies due to its wide availability, reliability, and the familiarity of SMS as means of communication for consumers.

[29] API (Application Programming Interface): a piece of software that allows different systems to communicate with each other.

Figure 1: How SMS messages are sent over P2P and A2P channels



3.5 The A2P value chain includes SMS aggregators. These are companies that act as intermediaries between business message senders and mobile networks, and typically operate the service which injects messages into mobile networks. Depending on how closely they are connected to the operators, aggregators can be classed as Tier 1 where they have a direct contractual relationship with a mobile network operator (MNO), or lower tiers (such as Tier 2 or Tier 3) where the connection to the operator is not direct.

3.6 Information provided to Ofcom by MNOs shows that, as of May 2024, each UK MNO has direct relationships with around 10-20 aggregators. In total, 32 SMS aggregators have a direct connection with at least one UK MNO. Typically, a smaller group of the largest aggregators account for the majority of the traffic on each network.

SMS volumes overall are declining but P2P messaging has risen in recent years

3.7 Overall, SMS use has declined significantly in recent years. However, this masks underlying differences between P2P and A2P channels.

- **A2P SMS messaging levels have increased in recent years.** We understand anecdotally that A2P messaging volumes increased significantly during the Covid-19 pandemic and have since remained above their pre-pandemic level. Data shared with Ofcom by an MNO shows that the total volume of A2P SMS on its network increased between 2019 and 2022, and is projected to remain above 2019 levels until at least 2027.
- **P2P SMS messaging has historically been larger than A2P but has fallen sharply.** Total P2P SMS volumes have declined significantly in the past decade. The total number of outgoing SMS and MMS[30] messages in the UK fell from the peak of around 151 billion in 2012 to 32 billion in 2023.[31] P2P SMS has been largely displaced by Online

[30] Multimedia Messaging Service is a communication protocol that allows users to send multimedia content over a mobile network.

[31] Ofcom, 2024. *Telecommunications Market Data Update Q4 2023* – *csv datafile* (Mobile Table 2: 'Call, message and data volumes by type')

Communication Services (OCS), which rose more than tenfold between 2012 and 2022.[32]

3.8 Data provided to Ofcom by MNOs shows that their customers received more A2P SMS messages than P2P SMS messages in May 2024.

Rich Communication Services messages

3.9 Rich Communication Services (RCS), sometimes referred to as Chat, is a standardised communications protocol[33] which the GSMA states "enhances traditional SMS messaging" as "a modern messaging experience akin to popular OTT platforms."[34] RCS also supports business messaging, known as RCS Business Messaging or Rich Business Messaging (RBM).

3.10 Operators can implement their own RCS solution into their networks or access the services through a hosted solution. In the UK, we understand that all MNOs currently outsource management of RCS to Google. [35] In this document, therefore, we refer to Google's implementation of RCS.

3.11 Google describes its Jibe Cloud platform as helping "carriers quickly scale RCS services" through its GSMA-certified, hosted service.[36] Google states that RCS chats are "sent and received through Google's RCS backend over the Internet" and that to ensure delivery it uses information including user phone numbers, device identifiers and SIM card numbers.[37]

3.12 RCS shares some features with both SMS and Online Communication Services[38] (such as WhatsApp or Facebook Messenger). For example:

- RCS is similar to SMS in that it uses number-based routing, is interoperable and integrated with mobile networks. Default messaging apps can be configured to send RCS, rather than SMS, automatically where sender and recipient have enabled it.
- RCS is similar to many OCS in its enhanced features, such as group chats, read receipts, typing indicators and support for end-to-end encryption. It is based on the internet protocol (IP) and requires WiFi or a data connection for full functionality, but falls back to SMS when there is no internet access or when the sender and recipient are not both RCS users.

3.13 While RCS it not currently ubiquitous across all handsets like SMS is,[39] it appears likely that its availability will expand in future. Apple has announced that for the first time iPhone devices will support RCS in the upcoming iOS 18 release later this year offering interoperability between iMessage and RCS.[40] And handset manufacturers using Android are

---

[32] The number of online messages sent in the UK has increased from approximately 100 billion messages a year in 2012 to over 1,300 billion messages a year in 2022. See paragraph 2.31 in Ofcom, 2023. *Personal online communication services*

[33] The GSMA publishes RCS Interworking Guidelines. See Version 19.0 from November 2022.

[34] GSMA, RCS *Rich Communication Services* .

[35] For information on collaboration with Google, see for example information from EE, Three, Vodafone, VirginMediaO2.

[36] Jibe, *How Jibe can help*

[37] Google, *RCS by Google FAQ*

[38] Also known as over-the-top (OTT) messages.

[39] For example, Google reported 1 billion active users with RCS enabled in Google Messages as of November 2023. In 2018 the GSMA reported 100 million users.

[40] Apple, *iOS 18 preview*

increasingly likely to sell their devices with Google Messages pre-installed as the default messaging app.[41] Google Messages supports RCS messaging by default.

Online Communication Services are increasingly important to consumers but are out of scope of this Call for Input

3.14 OCS are applications that provide an over-the-top messaging service on a user's device. They can include websites or standalone applications, very commonly used on mobile devices, that provide communications in the form of text-based messaging and/or voice or video calls to a closed number of participants. They have a wide scope, including services which provide private messaging and calling services as their primary functions, such as WhatsApp, Facebook Messenger and iMessage.[42] OCS are typically free of charge for users and offer a range of enhanced functionality, from typing indicators[43] to easy sharing of photos and video.

3.15 We consider that OCS are not dependent on a telephone number, unlike most traditional telephony services. This means that although many OCS require the user to provide a mobile number on sign-up, the messages and calls are not routed using the number itself. Services are not provided or controlled by mobile operators and communications are made over the internet. As such, for the purposes of this CFI, we distinguish between mobile messaging services and OCS as illustrated in Table 1 below.

3.16 OCS are increasingly important to meeting people's communication needs. The use of OCS rose more than tenfold between 2012 and 2022[44] and is now significantly higher than SMS overall. It is used by people of all age groups, although the younger people are, the more likely they are to do so.[45]

3.17 Some scammers may be shifting their tactics including towards using OCS, partly due to a general shift towards online communications and partly because of the work undertaken by mobile operators to disrupt fraudulent SMS messages. Our market research shows that around a quarter (26%) of mobile users reported having experienced suspicious OCS messages in the three months prior to the end of January 2024, as shown in Figure 3. This remains less than half the proportion that received suspicious text messages. However, whereas the level of people experiencing suspicious OCS remains similar to that seen in August 2022, there has been a decline in the equivalent text message figures year on year.[46]

---

[41] 9to5Google, September 2023. *Google Messages has been installed 5 billion times*

[42] Our focus for OCS is mainly on services used for private and general-purpose communications, which are widely used, and are therefore more 'telecoms-like' in nature.

[43] Which show recipients when a sender is typing a message.

[44] The number of online messages sent in the UK has increased from approximately 100 billion messages a year in 2012 to over 1,300 billion messages a year in 2022. Paragraph 2.31 in 'Ofcom, 2023. *Personal online communication services*'

[45] Ranging from 64% of 16-24s to 42% of 75+ mobile users sending outgoing OCS messages and similar proportions receiving incoming messages to/from family and friends. Ofcom, 2024. *Experiences of suspicious calls, texts and app messages data tables* Q13, Table 26.

[46] We did not record incidence of receiving suspicious OCS messages in September 2021. Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 40. Question: (Q1/Q28/Q36) 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? N.B. whether a message is regarded as being suspicious is entirely subjective on the part of the receiver.

Table 1: Differences between mobile messaging services and OCS, for the purposes of our work

	Mobile messaging services *SMS, RCS, MMS*	**OCS** *e.g. WhatsApp, Facebook Messenger, iMessage*
Role of phone number	Phone number required to route the message through communications networks	Phone number not required to route the message, but might be used as part of user authentication on sign up.
Routing of messages	SMS/MMS exclusively sent over the mobile network using signalling protocols RCS sent over the internet, falling back to SMS where a connection is not available, or RCS is not enabled for all parties	Exclusively sent over the internet using IP-based protocols
Provider of service	Mobile operators enable the service for their subscribers	Service provided by online platforms
Encryption	SMS/MMS messages not end-to-end encrypted RCS supports end-to-end encrypted conversations	Popular OCS support end-to-end encrypted conversations

3.18 Last year Ofcom published a discussion document on OCS. This was designed to increase our knowledge and understanding of these services, and to provide evidence-based thinking through the lens of our existing competition and consumer protection duties in the telecoms market.[47]

3.19 Following the passage of the Online Safety Act, Ofcom has new responsibilities to help make online services safer for all users, including overseeing how these services fulfil their duties about tackling fraud. These online services include messaging services such as WhatsApp and Facebook Messenger. Ofcom will have a range of tools to ensure that messaging services that fall in scope satisfy their online safety duties, including setting out codes of practice and guidance for the providers of regulated services. Ofcom has consulted on some of these[48] and the new rules will come into force once the codes and guidance are approved by Parliament.

[47] Ofcom, 2023. *Personal online communication services*. While we do not have powers to put in place ex-ante (before the event) rules on OCS for consumer protection or competition reasons, we are a converged regulator with a number of powers that are relevant to digital communications markets. As a competition regulator, we can undertake market studies or launch an investigation under the Competition Act including for abuse of dominance or anticompetitive agreements. We also have concurrent consumer protection powers in the case of unfair contractual terms or commercial practices, or if consumer law was being broken. In these cases, we could take enforcement action to protect consumers and remedy the infringements.

[48] Ofcom, 2023. *Consultation: Protecting people from illegal harms online*

3.20 Through our programme to tackle telecoms scams we will continue to monitor intelligence on the nature of scams being perpetrated over OCS.[49] However, because these services are not dependent on telephone numbers for routing, OCS are out of scope of this CFI.

How scammers are using mobile messaging services to defraud consumers

Scam tactics and consumer behaviour

3.21 Mobile messaging scams are usually sent at a mass scale, on the expectation that a low proportion of recipients will respond. A common approach is to set up a situation (such as a lost parcel or a job recruitment campaign) which includes a call to action, urging the victim to click on a link or dial a call-back number.[50] Another method known as conversational scams does not initially include a call to action, seeking instead to establish trust with the victim by either pretending to be a close family member or by building a friendly or romantic relationship.

3.22 While scammers typically seek to send large volumes of non-personalised messages, in some cases they adopt more bespoke tactics. So-called spearphishing scams target specific individuals, drawing on social engineering techniques and using personal information about the victim. Spearphishing scams are difficult to identify as they often resemble genuine conversations.

3.23 We have conducted consumer research to understand consumer attitudes and behaviour around scams. Our 2024 research showed that the most common indicators that raise suspicions that a message may be fraudulent are: not expecting to receive a text from the originator (cited by 73% of mobile and/or landline users), poorly written content (70%), the message asking you to do something (such as click on a link) (68%) and the URL quoted in the message looking suspicious (54%).[51]

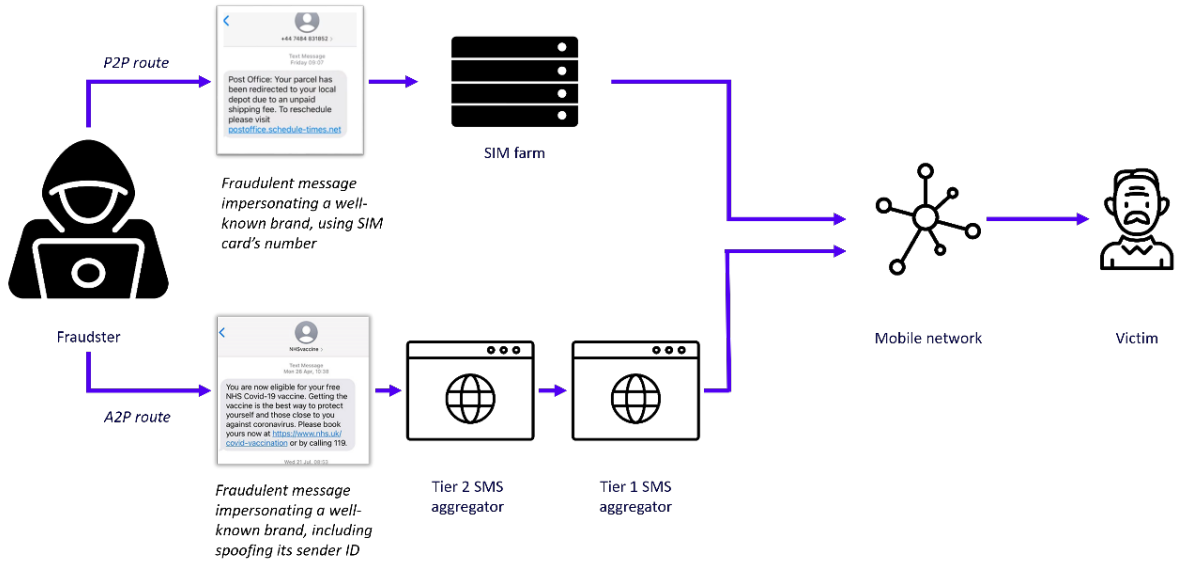
3.24 Consumers have different responses when they spot a suspicious text. The most common reactions are to block the sender (done by 63% of those who received them), delete the message (54%), check the number's veracity (30%) or to simply ignore it (28%). A quarter (25%) of those who had received a suspicious text message said they had reported it and a fifth (22%) had told friends or family about it.[52]

[49] For example, this will help us to understand how scammers' tactics are evolving and measures to counter them in OCS that may be relevant to mobile messaging services.
[50] The link typically leads to a fraudulent website, which requires the user to enter sensitive personal information or download malware onto their handset.
[51] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 34. Question: Which of the following factors do you consider when deciding whether a text or other type of message is genuine or not?
[52] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 48. Question: Which, if any, actions have you taken as a result of receiving these suspicious texts/calls?

Scammers use different techniques to contact victims over mobile networks

3.25 In this section, we set out how scammers may use P2P and A2P channels to contact potential victims over SMS and RCS services. Figure 2 illustrates different routes used by scammers for SMS.

Figure 2: How scammers use SMS to send messages over A2P and P2P channels



Person to Person (P2P) SMS

3.26 For consumer contracts, mobile terms and conditions typically state that SIM cards should be reserved for personal communications. However, many small businesses also make use of consumer SIM cards and their SMS plans to contact their customers.

3.27 A P2P SMS is generated on a consumer SIM card, originating on the sender's mobile network, and terminating on the recipient's mobile network. For messages originated in the UK, the chain of providers involved is straightforward, as messages are commonly routed directly from the originating operator to the terminating operator. They display a mobile long number (starting with 07) as the Sender ID.

3.28 Scammers who exploit P2P messaging often rely on SIM farms. These are devices which allow scammers to generate messages and transmit them as SMS through SIM cards over mobile networks. They typically house tens or hundreds of SIM cards and, while sometimes used by businesses (including for marketing purposes), can also be used by scammers to run large-scale scam campaigns.

3.29 The number of SMS messages that can be sent per SIM card affects the volume of messages that can be sent through SIM farms, and we discuss the role of volume limits in Chapter 5. In the UK, users of prepaid SIM cards are not required to register their personal details with the operator.

Application to Person (A2P) SMS

3.30 Businesses, financial institutions, and public bodies often use A2P messaging to efficiently distribute large volumes of SMS messages. This allows the sender to use an online platform or an API that connects to its systems, to send messages in bulk to consumers. A2P messaging is often provided through a Communications Platform as a Service (CPaaS), which offers services as an SMS aggregator or mass text aggregator. These companies aggregate large volumes of text messages from senders and distribute them to mobile networks.

3.31 SMS aggregators include companies such as Sinch and Infobip. They can operate at different positions in supply chains, depending on how far removed they are from the message recipient. A Tier 1 aggregator has a direct link into an MNO's network to enable termination of messages with customers of that MNO. Tier 1 aggregators commonly generate part of their business by routing traffic from lower tier aggregators. There may be multiple SMS aggregators in the delivery chain of a single SMS message, transferring that message from aggregator to aggregator, potentially to some aggregators located outside the UK, before it reaches the recipient. We understand that it is not uncommon for aggregator companies to operate at different points in this aggregator supply chain.[53]

3.32 An important feature of A2P SMS is the ability to display an alphanumeric Sender ID, so that the message is displayed as coming from a named organisation (such as 'HMRC') rather than an '07' mobile number. If an aggregator in a supply chain does not conduct sufficient know your customer (KYC) checks on clients to verify that they have a reasonable right to use an alphanumeric ID, scammers may be able to exploit this and pose as known organisations. Weak links in the chain may occur at lower tiers, where aggregators do not have a direct connection to the MNOs whose networks the messages are delivered to.

3.33 By spoofing an alphanumeric ID, it is possible that scammers may be able to make their messages appear more credible to some recipients. This could be, for example, because the alphanumeric ID looks more believable, or because a scam message may be added to an existing legitimate message thread where it spoofs an ID that has previously sent messages to the recipient. Our market research shows that, when considering whether a text is genuine or not, 43% of users consider whether it comes from a named company or a phone number.[54]

RCS messaging

3.34 RCS messaging includes a P2P messaging channel which is linked to a mobile number, as well as an A2P channel, known as RCS Business Messaging. RCS Business Messaging allows businesses to send messages in bulk to consumers. It relies on a business verification process and the content of the messages has to be approved. [55] Benefits for scammers of

[53] For example, one company may have a Tier 1 status with one mobile operator, and also have a Tier 2 status with another.

[54] This is based on users of mobile and/or landline. Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 34. Question: Which of the following factors do you consider when deciding whether a text or other type of message is genuine or not?

[55] The GSMA provides examples of organisations that could conduct verification checks: specialised entities who offer this service in other sectors, Mobile Network Operators (MNOs) themselves, or Chatbot Platform providers.

using RCS channels could include that it is free to use, can offer additional functionality, [56] and may support large scale campaigns.

3.35 Scammers may seek to exploit different routes into the RCS network. This could include SIM card-based routes (on mobile handsets or SIM-farm style products); exploiting any weaknesses in the RCS Business Messaging verification processes; or finding software-based routes to directly access the network.[57] We would welcome responses from stakeholders with evidence of how scammers are accessing RCS messaging.

Scammers also seek ways to circumvent mobile networks

3.36 To support mass scale campaigns, scammers may also seek other ways to distribute fraudulent messages. One example is through the use of SMS blasters. These are portable base stations, which connect to nearby handsets and are used to distribute messages bypassing the operators' network monitoring tools. Earlier this year, the City of London Police reported that two arrests had been made in connection to SMS blasters.[58] To support this, officers from the Dedicated Card and Payment Crime Unit, worked with mobile network operators, Ofcom and the National Cyber Security Centre.

Question 1: Do you agree that the routes described in this chapter cover all of the main methods that scammers use mobile messaging services to scam people? If not, please explain other methods.

Question 2: Which routes do you think are the most important today and will be over the next 3 years for the perpetration of mobile messaging scams? Please provide evidence for your views.

Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?

[56] Given that communication through this channel can include a verified badge and business logo, there is potential for it to be more persuasive to potential victims.
[57] Such methods could include, for example, software such as RCS emulators. These are legitimate tools for testing, for example, but have the potential to be misused by fraudsters to send large volumes of messages or to spoof sender IDs.
[58] City of London Police, June 2024. *Two people arrested in connection with investigation into homemade mobile antenna used to send thousands of smishing text messages to the public*

4. Evidence on mobile messaging scams

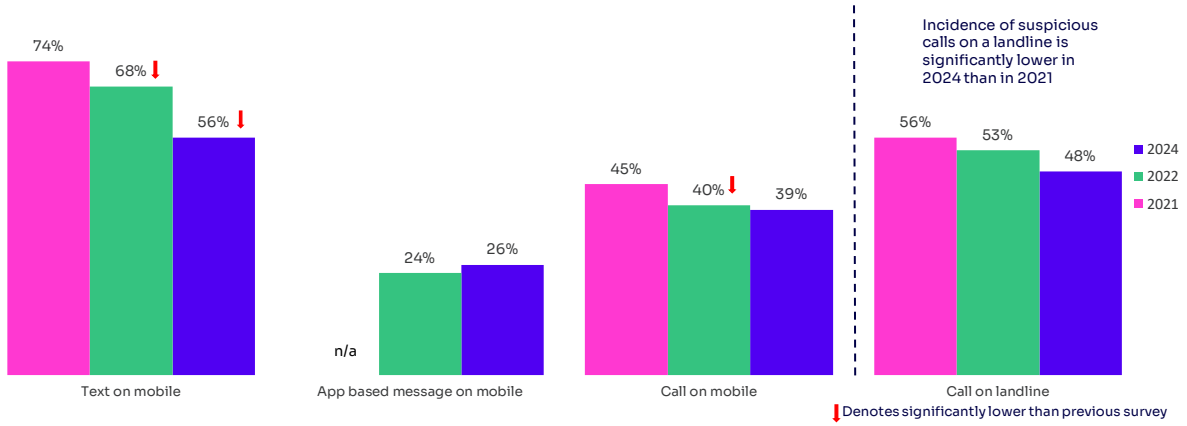
4.1 This chapter summarises the data we have reviewed on the scale and nature of mobile messaging scams in the UK. It includes consumer research, industry data on blocked scam messages, and data from consumer reporting.

Market research

4.2 The majority of UK adults aged 16+ use mobile phones, the vast majority of which are smartphones.[59] Our research suggests that suspicious texts[60] are more common than either suspicious mobile or landline calls amongst people who use each service.[61] In January 2024, more than half (56%) of mobile phone users claimed to have received at least one suspicious text in the last three months. In the same period, 39% claimed to have experienced at least one suspicious call.

4.3 The proportion of landline users experiencing suspicious calls was higher (48%). It is important to note that the proportion of the UK population using a landline is significantly lower than that using a mobile, so the experience of suspicious landline calls among the total population is lower overall.[62]

Figure 3: Experience of suspicious texts, app messages and calls over time



Source: Experiences of suspicious calls, texts and app messages Yonder 2021, 2022 and 2024
Question: (Q1/Q28/Q36) 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 mobile users 2021 (n=2036) 2022 (n=1901), 2024 (n= 2052), All landline users 2021 (n=1492) 2022 (n=996), 2024 (n= 953)

[59] Ofcom, 2024. *Technology Tracker data tables*, QM1, Tables 38, and QM2, Table 39: 97% of UK adults personally use a mobile phone, and 97% of these use a smartphone.
[60] For the purposes of this research, respondents were given examples of texts on mobile as including *SMS, RCS chat and iMessage.*
[61] In our January 2024 research, 48% of those with a landline service claimed to have received a suspicious call on their landline.
[62] Ofcom, 2024. *Technology Tracker data tables*, QL1, Table 33: 40% of UK adults live in a household that has a landline that can be used for incoming calls.

4.4 Since we began tracking the incidence of suspicious texts in 2021, we have observed a steady, and significant, decrease in the proportion of mobile users claiming to have experienced such messages. As shown in Figure 3, experience in the previous three months fell from 74% in September 2021, to 68% in August 2022, to 56% in January 2024. Factors contributing to this decline could include greater effectiveness of scam prevention measures and scammers moving to other technologies.

Consumer reporting through the 7726 service

4.5 The 7726 service allows consumers to report unwanted or suspicious texts or calls received on their mobile phones.[63] Operators use the reports to monitor scam activity and can update their network protections accordingly.[64]

4.6 We have collected 7726 data from MNOs using our formal information gathering powers. Our analysis shows that the four MNOs have historically received around 1 million reports per month collectively, up until the summer of 2023 when this number began to rise steadily. These aggregated industry figures also show spikes of scam activity, such as significant increases during periods in 2022, which are likely to have been linked to certain scam campaigns, such as Flubot.[65]

One click reporting functionality significantly increases 7726 reports

4.7 In recent months two MNOs have implemented iOS one clock reporting functions.[66] This has led to significant increases in 7726 reports from their customers. Our analysis shows that 7726 reporting for these MNOs increased by more than 800% in April 2024 compared to April 2023. This is more likely to be linked to greater ease and awareness in reporting than an increase in underlying scam activity.

4.8 Data from the two MNOs that have not yet implemented iOS one click reporting shows a 45% increase in 7726 reports in April 2024 compared to April 2023. Our market research does not show that awareness of the service overall is rising, so it is possible that this increase is driven at least in part by an increase in suspicious messages being received by consumers.

The data has some important limitations

4.9 The 7726 data has limitations and should be treated with caution, for reasons including:

- **The service relies on consumer reporting so the reports comprise of scam, spam and other nuisance texts.**[67] To understand what proportion of 7726 messages relate to SMS

[63] The number '7726' was chosen because it spells 'SPAM' on an alphanumeric phone keypad. This service primarily captures SMS messages, but MNOs also receive reports of voice calls, RCS, and iMessages reported using the manual (rather than one click) reporting route. Where iMessages are reported using one click reporting, this information is shared with Apple but not MNOs. As such, it is not included in our data gathering. In reviewing 7726 data, there are also challenges in isolating RCS and iMessage from the SMS messages.
[64] The reports can provide insights on the latest scam trends, malicious URLs used, phone numbers used and which brands are most susceptible to impersonation.
[65] FluBot is a type of malware spread through phishing SMS messages. Europol, 2022. *Takedown of SMS-based FluBot spyware infecting Android phones*
[66] Historically, consumers have needed to manually forward messages to the number '7726'. More recently, Android and Apple have added one-click reporting routes, allowing users to report the message with one click when they have a message open.
[67] As the service relies on user reporting, reports could also include other messages such as texts from a person known to the recipient.

scams, we have analysed samples of 1,000 messages submitted by each MNO. Our analysis is designed to provide *indicative* context to the overall 7726 figures across MNOs. We concluded that around a fifth of the 7726 messages that we reviewed are likely to be scams. The remainder are comprised of likely spam (around half) or genuine messages (about a quarter).[68]

- **Consumer awareness of the service remains low.** Our 2024 consumer research found that three quarters of mobile phone users had not heard of either 7726, or more generally the existence of a number that could be used to report suspicious texts or calls. Just 6% claimed to have used 7726 to report a suspicious text and 4% had used it to report a suspicious call.[69] Even where consumers are aware of the service, they will not all choose to report suspicious messages. As a result of these factors, the data is likely to under-report the number of scam messages received by the wider population.

7726 data provides limited insights on the use of A2P and P2P channels

4.10 Data from 7726 can provide some limited, indicative insights on the extent to which scammers are using A2P versus P2P SMS channels. In our analysis, where reported messages are linked to an alphanumeric Sender ID or a shortcode,[70] we assume that these have come from an A2P channel. When the reports include a long form numeric mobile number, messages could be from P2P or A2P channels.[71]

4.11 Our analysis of sample 7726 reports submitted by three MNOs suggests that around a quarter of scam messages sent to 7726 were from an alphanumeric ID, around half were from an 07 number, and about a fifth were from an 'other' or unknown origin.[72] This suggests that at least around a quarter of reported scam messages are coming from A2P providers (and this will be higher if scammers are applying 07 numbers to messages sent over A2P).

Messages blocked by mobile operators

4.12 Mobile operators have a variety of measures in their networks to prevent the delivery of scam texts to their customers, including traffic monitoring tools and filters. All four MNOs currently use SpamShield, a fraud control tool provided by Mavenir.[73] SpamShield scans incoming and outgoing SMS traffic and, depending on its implementation, either flags or blocks suspicious messages when scams are identified.

---

[68] When analysing these samples, we categorised messages as scams where they included common characteristics like suspicious calls to action and potential impersonation. We categorised spam as likely unsolicited marketing messages from businesses (such as seasonal sales), and genuine messages as those sent to the individual for specific reasons (such as one-time passcodes for logging into online accounts or voicemail notifications).

[69] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 53. Question: Have you heard of or used the special text number, 7726 that you can use to report a suspected suspicious text or call?

[70] These are specialised numbers used for sending SMS, typically 5 to 6 digits long.

[71] While P2P traffic originates from 07 numbers, A2P senders may choose an alphanumeric Sender ID, a shortcode or an 07 number. Some scams tactics, such as recruitment impersonation or conversational scams, may use A2P for scale and apply a numeric sender ID to appear more genuine.

[72] This is based on analysis from three of the four MNOs. 'Other' sender IDs include: UK numbers that are not 07, emails, and international numbers.

[73] Mavenir, *SpamShield*. Blocking of suspicious traffic can be more or less automated, depending on the operator's implementation. Decisions about this may be influenced by the operator's risk appetite for false positives, where legitimate messages are mistakenly blocked by automated systems.

4.13 SpamShield data can provide insights into the scale and nature of scam SMS. We have collected SpamShield data from MNOs using our formal information gathering powers. This shows that collectively the MNOs block around 1 million messages a day. There were spikes in activity in March and September 2022, similar to those for 7726. There was also a noticeable, but smaller, spike in summer 2023, which did not show up in the 7726 data. Apart from these spikes, industry-wide blocking has been relatively stable at around 30 million messages per month since November 2022.

4.14 SpamShield data has limitations meaning that it is difficult to draw firm conclusions about the scale of messaging scams using it in isolation. Some scam messages still get past Spamshield where it is in place, and SpamShield is not applied to all mobile messaging. For example, MVNOs with their own Short Message Service Centre (SMSC) do not use SpamShield and some MNOs do not put all A2P traffic through it, as discussed in the next chapter. It cannot scan the content of RCS messages due to encryption.

Data on financial harm from mobile messaging scams

4.15 Law enforcement bodies collect information on individual fraud cases as they are reported, but do not currently routinely capture the channels used by scammers to initiate contact.

4.16 The ONS publishes annual survey data on the incidence and nature of fraud. This shows that in the year ending March 2023, the victims of fraud overall were contacted in some way by fraudsters in 19% of incidents.[74] The victims confirmed that they were contacted first using a text message in 1% of all incidents of fraud. This appears to be a reduction from 2019.[75] Use of SMS as a first method of contact is higher for certain types of scams, such as for 'advance fee fraud and other fraud', for which SMS was the first method of contact in 6% of cases in the year to March 2023.[76]

4.17 UK Finance collects scams data from banks. This data shows that the total value of reported losses caused by authorised push payment (APP)[77] fraud in 2023 was £460 million, down from a peak of £583 million in 2021. UK Finance also splits the data to show the scale of losses linked to telecoms channels overall, but it is not currently split between message and call channels. APP fraud originated on telecoms channels accounted for 16% of reported cases and 43% of the total value of loss (equating to around £200 million).[78] This suggests that APP fraud enabled by telecoms services has a significantly higher financial loss per case than APP fraud overall. The data also shows a slight decrease in the share of APP fraud that was telecoms-originated, down from 18% in 2022 to 16% in 2023.[79]

4.18 The Payment Systems Regulator has introduced a transparency regime that mandates that certain financial institutions must provide them with data about their fraud performance.

---

[74] In other causes of fraud, victims may not be contacted by fraudsters. ONS, 2024. *Nature of crime: fraud and computer misuse - year ending March 2023*, Crime Survey for England and Wales, Table 5a.

[75] There was a decrease from the peak of 4% in in the year ending in March 2019, when victims also reported being contacted in some way in 37% of cases.

[76] ONS, 2024. *Nature of crime: fraud and computer misuse - year ending March 2023*, Crime Survey for England and Wales, Table 5d

[77] This type of fraud occurs when a victim is tricked into sending their money to an account controlled by the fraudster.

[78] UK Finance, 2024. *Annual Fraud Report*

[79] We still do not have a clear understanding from this data on the scale of financial harm linked specifically to mobile messaging, as data sources usually include both calls and messaging when referring to telecoms scams.

The PSR publishes this annually.[80] In the 2023 UK Government Fraud Strategy the PSR also committed to gather the data that their regulated firms hold on the systems and platforms outside the payments industry that are most commonly used by fraudsters to contact potential victims an persuade them to make payments.[81] The PSR has gathered this data and will shortly consult on publishing it in 2024 as well as expanding the scope of the data to include MNOs or landline providers at entity level in the future.

Evidence of mobile messaging scams: summary

4.19 All of the data we have described in this chapter has limitations. Reviewing it in the round shows that a significant level of scam activity is occurring, comprising both of messages that are being blocked off at source or in transit and messages that are successfully reaching mobile users.

4.20 Some data suggests that the number of messages reaching consumers may have reduced slightly in recent years. This includes our market research showing an 18 percentage point fall in the proportion of mobile users receiving suspicious messages since 2022. And for the telecoms services overall, UK Finance data shows a two percentage point fall in the share of APP fraud that was telecoms-originated from 2022 to 2023.

4.21 On the other hand, although 7726 data has significant limitations as described above, we observe a 45% increase in reported messages over the past year when isolating for the rollout of iOS one click reporting. Isolated spikes in activity from 7726 and SpamShield data over the past two years also show that consumers remain vulnerable to new messaging scam tactics.

4.22 Our provisional view based on this evidence is that there is a case for considering whether further measures, or improvements to the application of existing measures, can be put in place to disrupt further the use of SMS to perpetrate scams. The evidence on the extent of scams through A2P versus P2P channels is not definitive and it may not be possible to get reliable information on this. The 7726 data suggests that at least around a quarter of scam messages reported are coming from A2P channels, while half come from 07 numbers which could be A2P or P2P. We would be particularly interested in further insights on this.

4.23 Without further data, any consideration of further measures may need to focus on a qualitative understanding of the channels that are more vulnerable to scammers, and/or to focus on measures that block both A2P and P2P channels.

4.24 For RCS messaging, we are aware of evidence that scammers are using this channel[82] but our understanding remains limited. We recognise that RCS availability is growing and likely to accelerate in future so we consider this is an important area to gather more information on. We are seeking stakeholder views on how best to do this.

---

[80] This is part of the PSR's wider work which includes interventions in the payments industry to incentivise prevention and detection of fraud by their regulated firms. PSR, *APP fraud performance data*

[81] HM Government, 2023. *Fraud Strategy*

[82] As well as being included in our market research and 7726 data, this assessment is also based on anecdotal reports from stakeholders and media reports such as 'Dark Reading, March 2024. *'Darcula' Phishing-as-a-Service Operation Bleeds Victims Worldwide'*

Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?

Question 5: What is your understanding of which channels are supporting the greatest harm (such as A2P or P2P SMS, or RCS)? Please provide any supporting evidence.

Question 6: What do you think will happen to RCS availability and adoption in the next few years? Please provide supporting evidence and or reasons for you views.

5. Measures taken to disrupt mobile messaging scams

5.1 This chapter sets out the measures that are used in the UK and internationally to tackle mobile messaging scams. The measures are organised by those that: prevent scammers from accessing mobile messaging services; identify and block suspicious messages in transit; and support consumers to avoid and report suspicious messages that they receive. The measures covered for SMS are summarised in Table 2.

Table 2: Existing measures used in the UK and internationally to tackle scam SMS messages

	Stopping scam messages from entering mobile networks	Blocking suspicious messages in transit	Helping consumers identify and report scams
P2P	• Numbering regulations • Volume limits • Criminalising SIM farms • *SIM registration, IMEI suspension*	• Traffic monitoring tools	• Consumer education • Consumer reporting to 7726, police and operators • Handset solutions to block and filter messages on device
A2P	• Due diligence checks in the aggregator chain • Contracts between MNOs and Tier 1 aggregators	• Traffic monitoring tools • Voluntary Sender ID registry • MNO Sender ID lists and requirements • *Mandatory Sender ID registry*	
Measures in *purple italics* are used internationally.			

Stopping scam messages from entering mobile networks

Measures to address scam SMS messages being sent from SIM cards

Ofcom rules on numbers

5.2 Ofcom has set rules relating to the allocation, adoption, and use of telephone numbers in General Condition B1. This includes a requirement on communications providers to ensure they use numbers effectively and efficiently, which includes ensuring numbers are not misused (B1.6). It also requires communications providers to take all reasonably practicable steps to ensure their customers comply with the General Conditions (including B1.6) and the Numbering Plan in relation to their use of numbers (B1.8). Ofcom has also published a Good Practice Guide setting out the steps it expects providers to take to help prevent valid telephone numbers being misused, including to facilitate scams.[83] The guide provides clarity for providers on how Ofcom expects them to meet their existing obligations (including under General Conditions B1.6 and B1.8) and includes various practical steps they can take such as undertaking 'Know Your Customer' due diligence checks.

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

5.3 Mobile operators have the ability to suspend service for SIM cards, such as where their terms and conditions have been violated.

Criminalising SIM farms

5.4 SIM farms can be used by criminals to achieve significant scale for scam messaging campaigns. It is already illegal to supply or possess SIM farms in the UK if they are intended to be used for fraud, but it can be difficult for law enforcement to prove intent.[84]

5.5 To help law enforcement disrupt such tactics the previous UK Government brought forward legislation in the Criminal Justice Bill to create a new criminal offence to supply or possess a SIM farm, subject to certain exemptions for legitimate use and where adequate due diligence has been undertaken.[85] This Bill did not complete its passage through Parliament before the 2024 UK General Election.

Volume limits

5.6 Consumer SIM card packages used by scammers in SIM farms often offer unlimited SMS messaging allowances. To mitigate against abuse, mobile operators can apply volume limits on the number of SMS messages that a SIM card can send in a specified period.

5.7 In the UK, all MNOs have volume limits in place for some contracts, although there is significant variation in the application of limits between packages within a provider and between providers. Where thresholds are applied, they are typically set at an hourly, daily, or monthly rate. Limits most commonly equate to the equivalent of around 250 – 2,500 messages a day. Some approaches include both daily and monthly limits, and in some cases, limits are applied as a temporary measure when a contract starts.[86]

5.8 Where volume limits are used as a tool to prevent scams, a balance needs to be struck between facilitating legitimate use on one hand, and disrupting illegitimate use on the other. Volume limits have the potential to cause a negative impact on consumers if they restrict legitimate use.

5.9 **We believe consideration should be given to whether and how volume limits could be made more effective as a tool for disrupting scammers, without disrupting legitimate use. We would welcome views on how this could be done and the issues involved, including on:**

- **How limits should be set and what constitutes a reasonable need;**
- **Whether limits should be standardised;**
- **What action should be taken if limits are breached; and**
- **What monitoring of limits should take place.**

[84] Home Office, 2023, *Preventing the use of SIM farms for fraud*
[85] UK Parliament, 2024. *Criminal Justice Bill.* This followed a consultation process, see: Home Office, 2023. *Preventing the use of SIM farms for fraud: consultation*
[86] MNO responses to Ofcom information request.

SIM registration requirements

5.10 Knowledge of SIM ownership can help law enforcement and other bodies identify scammers. Internationally, many countries have SIM registration requirements.[87] These are typically designed to counter terrorism or fraud, acting to support law enforcement efforts by linking each SIM card to a named individual.[88]

5.11 In the UK, there are no requirements for network operators to collect registration information when issuing SIM cards. Nonetheless, for pay monthly SIMs all MNOs have policies to conduct credit checks and to gather some personal information for billing purposes. Credit checks typically include bank account details and historic address information. For pre-pay[89] contracts, credit checks are not typically applied.

5.12 Although SIM registration can help to disrupt scams, it can also have drawbacks. SIM registration may, for example, limit how widely SIM cards are available or taken up,[90] raise concerns over privacy, or incentivise the creation of black markets.[91] In a discussion of different models, the GSMA noted that where SIM registration has not been pursued, "*the absence of evidence— in terms of providing significant benefits for criminal investigations*" was a key reason.[92]

5.13 **We would welcome views on whether SIM registration requirements merit any further exploration in the UK.**

Suspension based on International Mobile Station Equipment Identity

5.14 Every mobile phone has a unique identifier, known as an International Mobile Station Equipment Identity (IMEI) number. Mobile operators can use this number to identify and track devices with SIM cards installed. Devices can be blocked at the network level by barring the IMEI number, which can prevent a device from accessing the network entirely or specifically block it from sending SMS messages.

5.15 In Australia, an industry code registered by the Australian Communications and Media Authority (ACMA) requires originating providers to investigate and undertake appropriate action to block fraudulent texts that originate from their own customers, including the option of blocking the IMEI of devices used for fraudulent communications.[93]

5.16 Limitations of this method include the fact that it is linked to a device rather than to a SIM card, which means scammers may be able to circumvent measures by using a new device or seeking to alter their device's IMEI.

5.17 **We would be interested in respondents' views on whether a similar approach to IMEI suspension could be effective in the UK.**

---

[87] Most countries have forms of mandatory registration, with exceptions including countries such as the UK, the USA, Canada, Portugal and New Zealand. See GSMA, 2018. *Access to Mobile Services and Proof-of-Identity,* Figure 5.1.

[88] The Australian Communications and Media Authority, 2023. *The ACMA's rules on ID checks for prepaid mobiles*

[89] Otherwise known as pay as you go (PAYG) contracts.

[90] Both in terms of the number of retail outlets or channels, and in terms of affecting some consumers who lack forms of ID.

[91] GSMA, 2013. *The Mandatory Registration: A White Paper*

[92] GSMA, 2013. *The Mandatory Registration: A White Paper*

[93] Communications Alliance, 2022. *INDUSTRY CODE C661:2022, REDUCING SCAM CALLS and SCAM SMS*

Measures to address scam SMS messages sent through aggregators

5.18 As discussed in Chapter 3, A2P channels can be used by scammers to send bulk messages. Complex supply chains, with multiple tiers of aggregators, can create opportunities for scammers to identify and exploit vulnerable entry points (such as an aggregator with weaker due diligence processes). Due diligence measures are important to prevent scammers from accessing A2P messaging. To ensure these are effective, upstream aggregators and mobile operators should have confidence that all aggregators in their supply chain have sufficient due diligence processes in place.

5.19 While there is currently no regulation in the UK that explicitly refers to SMS messages sent through aggregators, SMS aggregators may be required to comply with some of our existing rules, in particular in General Condition B1.[94] This will depend on: whether the nature of the service they are providing falls within the scope of the relevant General Conditions;[95] and whether there is a territorial connection with the UK, for example, because the SMS aggregator is providing services to customers in the UK.

5.20 We understand that some aggregators have voluntarily implemented measures to guard against scams.

5.21 We also know that MNOs have used contractual agreements with Tier 1 providers to put requirements in place related to scam messages. Two MNOs have told us that they have included requirements in specific enforceable 'code of practice'-style documents governing aggregators' use of bulk messaging services. Such approaches may help to place additional emphasis on anti-scam measures and, where they include additional measures beyond those set out in commercial agreements,[96] could help to further disrupt scams.

5.22 In the event of breaches to contractual obligations, mobile operators may pursue damages or fines, issue suspensions, or terminate an agreement with an aggregator. We understand that two of the four MNOs have issued sanctions like these in the last year.

Know Your Customer checks

5.23 To ensure that they only work with legitimate customers, aggregators may carry out due diligence checks on potential customers, sometimes described as 'Know Your Customer' (KYC) checks. Some MNOs use the threat of fines to incentivise Tier 1 aggregators to conduct these checks. Measures typically include examining proof of identity, company registrations and other details.

---

[94] This includes the requirement in General Condition B1.6 to ensure they use numbers effectively and efficiently, which includes ensuring numbers are not misused. It also includes the requirement in B1.8 to take all reasonably practicable steps to ensure their customers comply with the General Conditions (including B1.6) and the Numbering Plan in relation to their use of numbers. We note that our Good Practice Guide is currently focused on addressing the misuse of numbers that have been sub-allocated or assigned to businesses and individuals. While some of the measures it sets out could be relevant to addressing scam SMS messages sent through aggregators, it does not contain any explicit reference to SMS aggregators.

[95] For example, an SMS aggregator may in principle fall under the definition of an electronic communications provider in section 32(2A) of the Act. This may be because it is providing a number-based interpersonal communications service as defined in section 32A of the Act.

[96] We note that there may be overlap between the measures in these bespoke codes and those in the standard commercial contracts relied on by other MNOs.

5.24 A challenge for due diligence in the A2P market is that messages may pass through multiple aggregators before reaching the recipient's mobile network. It may therefore be difficult for an aggregator to verify the legitimacy of every actor in the chain, as they may not be aware of them all. Checking processes across the full supply chain can add costs or delays to sending bulk.

5.25 Where scam messages are identified by an aggregator as coming from a lower tier aggregator, this is an important warning sign that KYC checks are not being implemented effectively further down the supply chain. Issuing sanctions on this aggregator can help to block scam messages and create incentive structures for lower tier aggregators to improve their KYC processes.

5.26 To incentivise Tier 1 aggregators away from agreeing to deliver A2P messages for risky third parties, one UK mobile operator operates a system of yellow and red cards for Tier 2 aggregators. These cards warn an MNO's Tier 1 aggregator partners where Tier 2 aggregators have failed to prevent the delivery of scam messages. If a Tier 1 aggregator is found to have worked with a Tier 2 aggregator that had a current red card, they are then subject to pay damages to the MNO for each scam campaign identified.

Dedicated connections

5.27 Some brands, like banks and government bodies, may be at higher risk of Sender ID spoofing through A2P channels. Consumers may be more likely to take action on messages that seem to be from these brands, making them attractive to scammers. Equally, genuine messages from these brands may be of critical importance to the recipient, who may be harmed if the message is blocked.

5.28 To establish more control over traffic associated with these types of brands, two UK MNOs operate 'whitelisting' or 'trusted traffic' policies. MNOs specify to the aggregator a list of brands that are required to be treated differently to others. Traffic from these specified brands and organisations must be sent over specific connections in their network, to separate it from other traffic. The aggregator is required to verify the authenticity of the sender, and any traffic purporting to be from these brands that is not sent over the trusted specified connection is then blocked. Separating this traffic may also allow the MNO to take a potentially more robust approach to blocking on their connections for other traffic, as they can be more confident that any blocked false positives are unlikely to be of critical importance.

5.29 This measure is limited in that it may only protect the brands specified by the mobile operator from spoofing. Other measures have been implemented to protect alphanumeric Sender IDs, as discussed later in this chapter.

Intelligence sharing and reporting incentives

5.30 Industry can help disrupt scams more widely by sharing intelligence. This could include reporting intelligence at an aggregator level (aggregators that have facilitated suspicious traffic) or at an end user level (customers that have been identified as trying to send suspicious messages). For example, at an aggregator level, the yellow and red card system described above at 5.26 helps to alert Tier 1 aggregator partners where Tier 2 aggregators have failed to prevent the delivery of scam messages. MNOs also told us that they share intelligence with aggregator partners about incidents and threats. For example, one MNO told us that it shares information with aggregators relating to suspicious traffic that is has blocked from their channels to create a feedback loop.

5.31 Recognising the importance of intelligence sharing, mobile operators may use contractual obligations to require aggregators to report instances of A2P SMS scams to them in a timely manner. Efforts to share intelligence can be undermined if aggregators are reluctant to share information due to concerns about sanctions that may arise due to contractual agreements. To address this risk, one UK MNO operates a policy that exempts the aggregator from their damages regime if the incident is reported immediately. This attempts to incentivise aggregators to report incidents.

5.32 **We would welcome input from stakeholders on how else intelligence is shared amongst aggregators and operators and any ways in which this could be improved.**

Challenges surrounding A2P messages and questions for stakeholders

5.33 We believe that tackling scam messages sent through aggregators is likely to be a key area for further consideration, particularly given that the use of A2P for businesses use remains significant. We have also observed some differentiation in approaches by the industry to tackling scams which come through the A2P route.

5.34 **We would welcome views from respondents on what more can be done to make the A2P route more impervious to scams. In particular we are interested to understand views on:**

- **What could be done to further drive good practice amongst the aggregator sector;**
- **Whether more standardisation would help to close the loopholes that scammers have sought to exploit;**
- **How effective KYC checks are across the aggregator supply chain, especially where there are many parties involved in the delivery of messages; and**
- **How best to mitigate associated supply chain uncertainties, such as by building on the contractual obligations and dedicated connections described above, taking steps to reduce the number of parties in the supply chain, or other methods.**

Measures to address SMS messages being sent through illegal equipment

5.35 Scammers can circumvent mobile networks by using their own illegal equipment, such as SMS blasters, to send scam messages to potential victims.

5.36 To address such risks, industry, law enforcement, government and regulators can work together both to monitor emerging tactics, and to share intelligence where illegal activity is identified. The recent announcement of two arrests by the City of London Police demonstrates that this kind of collaboration can work in practice.[97]

Measures to address RCS scams

5.37 Some of the measures described above are also relevant for RCS. This includes the equivalent of KYC checks for business senders: we understand that business senders have to be registered with and verified by a verification authority. [98] Once a brand has been verified,

[97] City of London Police, June 2024. *Two people arrested in connection with investigation into homemade mobile antenna used to send thousands of smishing text messages to the public*

[98] GSMA, 2019. *RCS Verified Sender Product Feature Implementation Guideline*. This could be, but is not limited to, a commercial business, for example verification companies from the internet world, an operator or a government department.

it can add a logo, brand name and user interface indication to designate its verification status. We also understand that RCS has the technical capability to apply volume limits.

5.38 Measures can also be taken to disrupt scammers who are using software-based routes into the RCS network. We are aware, for example, of reports that Google has removed RCS functionality from mobile handsets which are 'rooted'.[99] These are phones which have undergone a process to gain additional permissions relating to features such as system files, applications and settings.

5.39 Our understanding of these measures, and other steps that may be being taken to stop scams accessing RCS networks, is limited. **Therefore, we are seeking input from stakeholders on the full range of measures that are used to protect consumers and their effectiveness.**

Blocking suspicious messages in transit

Measures to identify suspicious traffic

5.40 Not all scam messages can be prevented before they enter mobile networks, so measures to identify and block suspicious messages in transit are also important for consumer protection.

Traffic monitoring tools

5.41 Traffic monitoring can be conducted on a voluntary or mandatory basis, including to monitor and filter SMS traffic to identify suspicious messages before they are delivered to consumers. Advanced network monitoring tools can assign a risk profile to messages based on factors such as their contents (including phrases and URLs), sender and recipient telephone numbers, and volumes and patterns of traffic. Such tools can be applied by originating and terminating operators and can be applied to P2P as well as A2P messages. They can be used to block messages or to apply warning labels.

5.42 In the UK, MNOs[100] conduct traffic monitoring on a voluntary basis using SpamShield, a fraud control tool provided by Mavenir.[101] Each MNO has its own policies on how SpamShield is implemented in practice, such as whether it is applied to all SMS traffic or whether there are exemptions for some A2P traffic. We understand that some SMS aggregators conduct their own filtering on messages that originate on or transit through their systems and would welcome information from stakeholders on how this is applied across the sector.

5.43 We calculate that the MNOs have collectively blocked over 1 billion suspicious SMS messages since the start of 2022. On average, industry-wide blocking has been relatively stable at around 30 million messages per month since November 2022.[102] This is broadly consistent across industry, although we have sought further information from one MNO

[99] The Verge, March 2024. *Google is blocking RCS on rooted Android devices*
[100] MVNOs hosted on the MNOs' Short Message Service Centre (SMSC) are also covered by SpamShield.
[101] See: Mavenir, *SpamShield: Messaging Fraud.* Blocking of suspicious traffic can be more or less automated, depending on the operator's risk appetite.
[102] As described in Chapter 4, this included some spikes in activity around March and September 2022 and July 2023.

which had significantly lower levels of blocked SMS until partway through our reporting period.[103]

5.44 The telecoms sector fraud charter, set up by the previous UK Government and which MNOs have signed up to on a voluntary basis, includes a commitment to sharing information within the industry to detect and reduce fraud against customers and providers, including through the Messaging Scams Group.[104] Traffic monitoring tools require data, such as on suspicious information in the contents of messages (text or URLs) and patterns of messaging.

5.45 Internationally other approaches have been taken. For example:

- Poland introduced legislation in 2023 requiring operators to block SMS messages that match a pattern associated with smishing and empowers them to block any other SMS messages if indicated by an automated mechanism.[105]
- In Ireland, the regulator ComReg consulted on proposals in 2023 to require SMS scam filters. It subsequently noted widespread support for the policy but explained it could not proceed without legislative action from government. It said it will continue to engage with its parent department on this matter and will publish a separate consultation in summer 2024 to consider other options to address SMS scams.[106]
- In France, the National Assembly passed a bill this year to 'secure and regulate the digital space (SREN bill)', which includes a provision to implement an anti-scam cybersecurity filter, which will warn the public when they receive a fraudulent SMS message or email that includes a link to a malicious website.[107] The details of the filter will be determined by a subsequent Decree.

Limitations of traffic monitoring tools

5.46 Traffic monitoring tools like SpamShield are not completely effective at identifying and blocking scam messages for a variety of reasons. In particular:

- Blocking can be more or less automated depending on the operator's risk appetite. Allowing for more automated blocking may prevent more scams, but simultaneously create more false positives, blocking legitimate communications which could harm senders and recipients. More manual blocking requires human review, which takes time and resources.
- There is likely to be a lag in identifying and blocking messages when scammers use new tactics. SpamShield relies on identifying suspicious patterns, so where new scam campaigns emerge, messages will not be blocked until the campaigns are identified. The speed at which this happens will depend on factors such as the quality of supervision, of software, thresholds applied and collaboration between industry.

5.47 The deployment of traffic monitoring tools appears to have led to significant levels of messages being blocked before they reach consumers.

---

[103] For the remainder of the reporting period its blocked traffic was broadly consistent with wider industry levels.

[104] Home Office, 2021. *Fraud sector charter: telecommunications*

[105] In September 2023, Poland introduced legislation aimed at tackling the generation of artificial traffic, smishing and CLI spoofing. See '*https://orka.sejm.gov.pl/proc9.nsf/ustawy/3069_u.htm*'

[106] ComReg, 2024. *Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications*

[107] Vie publique, May 2024. *Law of 21 May 2024 on securing and regulating the digital space*

5.48 **We are interested in exploring whether and how the use of these tools can be made more effective across industry. We would particularly welcome views from stakeholders on:**

- **Should more parties, like MVNOs and aggregators, be making use of similar tools?**
- **How can existing tools and the human systems around them be better configured, or made more sophisticated?**
- **Would more consistent implementations across parties, and better-quality information sharing improve blocking efforts, and how might these be achieved?**

RCS and traffic monitoring tools

5.49 Solutions which rely on content analysis do not work for end-to-end encrypted messages, including RCS. Instead, other measures can be taken, such as metadata analysis of message frequency, traffic patterns, or handset location. Insights from metadata can be combined with information from other handset-based solutions described later in this chapter for richer insights on scam risks. Based on analysis, users can be assigned risk profiles, which can lead to account limitations being applied on suspected scammers.

5.50 **We would welcome further input from stakeholders on what can be done, and on what is being done, to identify suspicious RCS messages in transit.**

Measures to protect alphanumeric Sender IDs for SMS messages

5.51 To identify the sender of the message, all SMS messages display a Sender ID or 'header' to the recipient. Organisations often use alphanumeric Sender IDs[108] with their names (such as 'HMRC') to help consumers identify who an SMS message is from. As described in Chapter 3, scammers can abuse alphanumeric Sender IDs to send messages that impersonate legitimate brands and organisations, and trick consumers.

5.52 Where fraudsters are able to bypass KYC checks, scam messages spoofing alphanumeric Sender IDs can be detected and blocked before they reach consumers through other measures.

Sender ID registries

5.53 Alphanumeric Sender IDs can be protected using registries. Brands and organisations can register the alphanumeric Sender IDs that they use when sending SMS messages to customers, by proving they are the legitimate user of the Sender ID. Once an alphanumeric Sender ID is registered, other brands or organisations should not be able to use it when sending A2P SMS messages to consumers via aggregators and mobile operators.

5.54 The design of registries can vary significantly. Key differences include:

- Whether registries are voluntary or mandatory. Where the registering of alphanumeric Sender IDs is mandatory, there can then be a requirement to block all other alphanumeric IDs that are not registered. Where a registry is voluntary, brands are only protected if they have registered their Sender IDs.
- Whether checks on Sender ID traffic are done before messages are delivered or as a retrospective assessment that informs future blocking actions. Retrospective

[108] The most common Sender IDs are phone numbers (e.g. 07xx xxx xxx), but some organisations use short-codes (usually five to six digits e.g. 12345), or alphanumeric IDs (e.g. 'Barclays', or 'Vodafone')

assessments may be less burdensome for the parties involved, but also may allow some unauthorised uses of registered Sender IDs to occur before they are detected.

- How suspicious messages are treated when identified, in terms of whether messages are blocked in transit, have warning labels added, or information is shared after the event with industry to prevent ongoing exploitation.
- Whether the registry is run by industry bodies, regulators, government agencies or other private entities, and which party in the message supply chain is tasked with checking the registry.

5.55 There is also a risk that brands that have been registered can be impersonated with visually similar IDs (e.g. 'Ofcom' could be spoofed as '0fcom' using a zero). To address this, blocklists and protected lists can be compiled by registries, aggregators, or mobile operators themselves, with likely alternatives and those known to have been used by scammers.

5.56 A voluntary model is operated in the UK. The Mobile Ecosystem Forum (MEF), a trade body, operates a cross-sector Sender ID registry initiative called the 'Sender ID Protection Registry'. We understand that the MEF registry adopts a retrospective approach and charges brands a fee to sign up. MEF reports that it has registered over 700 trusted Sender IDs.[109] MEF also operates a blocklist and reports that it has registered over 3,750 unauthorised Sender ID variants.[110]

5.57 Sender ID registries also operate or are being actively considered in other countries. Examples include:

- In Singapore, registering with the Singapore Sender ID Registry (SSIR) was made mandatory for any organisation that wants to use alphanumeric Sender IDs in early 2023. Research with consumers suggests that this has been highly effective.[111]
- The Australian Government recently introduced new legislation to give the ACMA powers to establish and run an SMS Sender ID Register.[112] Earlier this year, it consulted on a voluntary and a mandatory registration approach.[113] As referred to in paragraph 5.15 above, the ACMA registered an industry code in July 2022 that sets out processes for reducing scam calls and scam SMS messages. This requires originating mobile operators to ensure customers have a valid use case for use of an alphanumeric Sender ID and to prevent carriage of messages where the sender does not hold rights to use the number.[114]
- In Ireland, the communications regulator, ComReg, recently announced that it will be proceeding with its mandatory Sender ID registry, with ComReg being responsible for overseeing the operation of the registry.[115]

---

[109] Mobile Ecosystem Forum, *SMS Sender ID Protection Registry*
[110] Mobile Ecosystem Forum, *SMS Sender ID Protection Registry*
[111] 87% of Singapore consumers reported that SSIR had made it easier to identify whether SMS messages are legitimate, and 63% noted a decline in the number of spam or scam messages they received since its introduction 2023. Toku, November 2023. *Singapore Consumers More Confident in Recognising Scams*,
[112] Minister for Communications, 2024. *New legislation to crack down on SMS scams*
[113] Australian Government, 2024. *Fighting SMS Scams – What type of SMS sender ID registry should be introduced in Australia?*
[114] Communications Alliance, 2022. *INDUSTRY CODE C661:2022, REDUCING SCAM CALLS and SCAM SMS*
[115] ComReg, 2024. *Combatting scam calls and texts: Response to Consultation on network-based interventions to reduce the harm from Nuisance Communications*

- Italy has operated an SMS Sender ID registry since 2014, which has been set up and continues to be operated by the Italian regulator, AGCOM.[116]
- In Lithuania, legislation was recently introduced that would require service providers to block SMS messages with alphanumeric or numeric numbering that has not been registered.[117]

5.58 Setting up and running a registry involves costs which are usually recovered through fees charged to brands registering Sender IDs. Costs can vary depending on design features and the number of brands that sign up. In exploring Sender ID models, the Australian Government cited illustrative costs from Singapore where SMS Sender ID Registration is mandatory, and costs include a one-off set-up fee of S$500 for each registered organisation, and an annual charge of S$200.[118]

5.59 Under a voluntary model, some brands may not register, which can leave them more vulnerable to having their Sender ID spoofed. In the UK, some major brands have not signed up to the MEF registry.

5.60 Under a mandatory model, businesses that find the cost prohibitive may be unable to use alphanumeric Sender IDs, which could disadvantage them. Measures can be taken to address this, such as using price structures which offer tiered tariffs, reflecting company size, the volume of messages sent, or charitable status.

5.61 For consumers, a mandatory registry has the potential to provide a clearer distinction between different messages and the risks associated with them. If no unregistered alphanumeric IDs can be used, and use of registered IDs is tightly controlled, recipients can have more confidence that messages with an alphanumeric header are genuine. They may then apply more scrutiny to messages purporting to be from brands but sent from an unknown number.

5.62 **For the UK, we are interested in stakeholders' views on the best way forward. Broadly, there appear to be two main approaches:**

- **Firstly, to continue with the registry run by the MEF and to seek to make it more effective (such as through wider adoption by brands that haven't yet signed up, or by moving closer to a real time approach); or**
- **Secondly, to switch to a mandatory approach as adopted by other countries described above, which would need to be run by an appropriate organisation.**

MNO Sender ID policies

5.63 Through contractual terms and codes of practice, UK MNOs provide additional guidance to aggregator partners on how to guard against abuse of alphanumeric Sender IDs. Some include lists of specific Sender IDs to block or ensure to protect and some include additional requirements on aggregators to ensure brands are not being used inauthentically or risk fines.

5.64 Some MNOs also implement Sender ID specific measures within SpamShield, their traffic monitoring tool. SpamShield can be configured to block or flag messages with suspicious

[116] AGCOM, *Guida alla registrazione al Registro degli Alias v.2*
[117] Communications Regulatory Authority, 2024. *Dėl Apsimestinių trumpųjų žinučių identifikavimo tvarkos aprašo patvirtinimo*
[118] Australian Government, 2024. *Fighting SMS Scams – What type of SMS sender ID registry should be introduced in Australia?*

Sender IDs for review. This can include rules targeting the use of 'special' alphanumeric characters often used mimic legitimate letters. One UK MNO blocks the use of any alphanumeric Sender ID that uses characters outside of a restricted standard set and another has told us that it plans to adopt a similar approach in the near future.

5.65 **We welcome views on the efficacy of these additional policies, and whether there would be benefits to ensuring similar measures are taken across MNOs in a standardised fashion.**

RCS verification

5.66 As described at paragraph 5.37 above, business senders have to be registered with and verified by a verification authority. We would welcome insights from stakeholders on how well this process works currently.

5.67 **We are not aware of other tools, such as sender ID registries, designed to specifically protect brand IDs for RCS, but would welcome input from stakeholders if other mechanisms are used.**

Supporting consumers to identify and report scam messages

5.68 Given the pace at which scammers change their tactics, it is unlikely to be possible to stop all scams reaching consumers. Measures can be taken to help consumers better identify scam messages and know what to do when they receive them. This can help people avoid falling victim to fraud themselves and increase intelligence sharing which in turn can help disrupt scams more widely.

5.69 This section includes measures taken to educate consumers, and other tools to help consumers identify and report scam messages. Handset-based approaches are particularly important for RCS, because encryption prevents the content of messages from being analysed in transit in the same way as SMS messages.

Education

5.70 A number of organisations have acted to educate consumers. For example, the UK Government launched a 'Stop! Think Fraud' campaign in February 2024, backed by a coalition of law enforcement, industry and consumer groups.[119] The campaign included advice on how to spot scam text messages and what to do when this happens.

5.71 MNOs provide advice on their websites and have also proactively contacted customers to share advice on how to avoid scams. Our market research shows that advice from a mobile provider was a significant source of awareness for consumers of how to report a suspicious text (mentioned by 28% of those who reported a suspicious text).[120]

5.72 As set out in paragraph 2.1, one of the three key elements of our strategic approach is to help consumers avoid scams by raising awareness so they can more easily spot and report them. We have published advice on our website,[121] including how to report suspicious

[119] Gov.uk, *How to spot a fake text message,*
[120] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 50 Question: How did you know where to report the suspicious message/call?
[121] Ofcom, 2024. *Top tips to stay safe from the scammers*

messages to 7726. We have also published advice widely on our social media channels, including to support campaigns such as 'Stop! Think Fraud' and International Fraud Awareness Week. Our video explaining how to report scam texts is the most viewed video on our YouTube channel, with over 40,000 views.[122]

5.73 Education can also be used to support wider interventions that can be made at the network level. For example, French businesses are not permitted to send messages using regular mobile phone numbers.[123] Consumer awareness campaigns can then explain to consumers that all legitimate business messaging should come from alphanumeric or shortcode Sender IDs, and that business messages sent from regular mobile numbers should be treated with suspicion. This allows a clear message to consumers and can help to prevent impersonation scams. On the other hand, it also restricts communications options available to legitimate businesses, particularly smaller organisations who may not be able to contract with A2P providers.

5.74 **We would welcome suggestions of any of other approaches which could be used to effectively support consumer education on mobile messaging scams.**

Consumer-facing tools and services

5.75 Tools on mobile handsets can help consumers identify and report suspicious messages. Key features include additional screening, the ability to block specific numbers, and support to report suspicious activity.

Identifying or filtering suspicious messages on the handset

5.76 Additional screening, through pre-installed or commercially available apps, can be used to detect scam messages that reach consumers' devices. Our market research shows that a quarter (25%) of mobile users report using a text screening app or function on their phone.[124] Providers of such services include Hiya, Truecaller and Textkiller.[125] These apps can offer the ability to block, filter or apply warning messages for suspicious messages. Native operating system services can also offer similar functionality.

5.77 The contents of RCS messages cannot, unlike SMS messages, be filtered on the network due to end-to-end encryption. Content from RCS messages can, however, be analysed on the recipient's device to help identify scams. Handset-level monitoring can be used to identify suspicious messages, such as through identification of harmful URLs.

5.78 Where suspicious messages are identified on the device, these can be flagged to users, filtered into a spam inbox or blocked. This can help people to treat messages with caution, although will not stop all people from engaging. Our consumer research shows that a

[122] Ofcom, 2021. *How to report a scam text to 7726 on an iPhone*

[123] Rather, they must instead use A2P channels and specific Sender IDs.

[124] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 26. Question: There are ways to screen/block calls on mobile phones . These may be built into the phone itself (e.g. the phone blocks callers who aren't on your contact list) or as an app that needs to be downloaded (e.g. TrueCaller, Hiya, Should I answer, Calls Blacklist, Call Control, Callapp, Norton Mobile Security, RoboKiller etc). Do you have an app or function on your mobile phone to screen/block calls?

[125] See Hiya, Truecaller, Textkiller

minority (14%) of respondents said that they would sometimes, usually or always engage with a message marked as suspicious.[126]

5.79 **We welcome input from stakeholders on any ways in which handset-based solutions could be improved or used further to help consumers.**

Blocking specific numbers

5.80 The ability to manually block a number from delivering further messages can also help users avoid fraudulent messages. Most screening apps allow users to do this. Blocking individual numbers does not prevent further scams arriving from different numbers.

Reporting suspicious messages

5.81 Consumers can report suspicious messages to different organisations, such as to 7726 or Action Fraud. To report messages to 7726, consumers can forward messages manually or use one-click reporting buttons which are now present on many iOS and Android devices. Our market research shows that two fifths (41%) of mobile users who had reported a suspicious text had done so via a function on their mobile phone, and a third (33%) said they had reported it using a special reporting number.[127]

5.82 Awareness of the 7726 service among mobile users remains low, at 15%. Nonetheless, our research suggests that the service is attractive when it is described to people. We found that, after having it described to them, the majority of those who had previously been unaware of 7726 said they would be likely to use it the next time they received a suspicious call or text.[128]

5.83 In the context of low awareness, one-click functionality included in messaging inboxes can help increase reporting. Where reporting buttons are labelled as 'spam' or 'junk' or 'submit a report' alongside deleting the message received, this can lead to nuisance messages being reported alongside scam messages. Some screening apps offer extensions to one-click reporting functionality, which allow the user to specify why they are reporting a message (e.g. 'spam', 'fraud' or 'survey'). This approach might produce more actionable data for a reporting service.

5.84 For end-to-end encrypted services such as RCS, user reporting is an important tool to inform sender reputation, which can in turn be used to disrupt scammers through measures such as account limitation or suspension.

5.85 **We welcome input from stakeholders on how consumers could be better supported to report suspicious messages. For example, are there ways to make reporting tools more widely accessible to consumers, and could more be done to distinguish between suspected scam and spam messages (either through consumer facing services or through design of back end systems used for analysis)?**

---

[126] Ofcom, 2024. Experiences of suspicious calls, texts and app messages, slide 32. Question: Even if you don't have a function on your mobile to screen for unwanted text messages, some messages may display a warning on your screen. If you received a text that was marked 'potential fraud' or 'potential spam', how often do you think you would engage with the text anyway (e.g. reply/click the link/call back the number)?

[127] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 49. Question: How did you report the suspicious message/call?

[128] Ofcom, 2024. *Experiences of suspicious calls, texts and app messages*, slide 54. Question: Now that you know about the reporting number, how likely do you think you will be to use it the next time you receive a suspicious text or call?

Measures taken to disrupt mobile messaging scams: summary

5.86 In the UK, industry has been active in taking measures to disrupt SMS message scams. Across the stages set out in this chapter, industry has driven innovation including Sender ID registries, codes of practice between MNOs and aggregators, SMS filtering and education campaigns. Scammers constantly adapt their tactics and the problem of scam SMS messages remains significant, but does not appear to be rising. We are using this CFI to understand how existing measures can be improved, or whether new ones should be considered, to further disrupt scammers.

5.87 In terms of stopping scam SMS messages from entering mobile networks through P2P channels, we are particularly interested in stakeholder views on whether volume limits could be made more effective as a tool for disrupting scammers. For A2P, we are interested in what could be done to further ensure that due diligence is effective across the whole supply chain.

5.88 To identify suspicious SMS messages in transit, we are interested in what can be done to build on the existing success of MNO blocking processes, which could include through wider adoption (by more MVNOs or aggregators) or better application of existing tools. On A2P channels, we have set out a number of different design features of Sender ID registries and would welcome views on the best way forward in the UK context to build on existing measures.

5.89 Support for consumers to identify and report suspicious messages, such as through education and device-level services, is also important. We are seeking stakeholder views on how well existing measures in this area are supporting consumers and what more could be done.

5.90 Protecting consumers from RCS scams requires different approaches in some areas, not least due to end-to-end encryption. Our understanding in this area is currently limited but we recognise that it may be a significant area of potential growth for future scam messaging activity. Therefore, we are seeking more information on what is done at each stage of measures set out in this chapter as well as any data on how effective these measures are.

Question 7: Do you have views on the effectiveness of the measures discussed in this chapter? For measures where we have identified specific issues, please comment on these in your answer, providing reasoning and evidence if possible.

Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?

Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?

6.Next Steps

6.1 In publishing this document, we aim to gather input from stakeholders on the scale of the problem of mobile messaging scams, and on any necessary actions from Ofcom, industry or others to tackle messaging scams.

6.2 We welcome anyone with views on this area to submit comments and evidence to: mobilemessagingscamsresponses@ofcom.org.uk. We encourage respondents to submit responses within a 10-week window until 7 October 2024.

6.3 We will consider all responses submitted to this CFI. We will also continue monitoring available data as well as any industry and international developments. We will continue to facilitate information sharing across industry, including to support solutions already in use or being considered by other UK stakeholders.

6.4 If we believe further Ofcom-led action is necessary, this could include taking enforcement action where our existing rules are being broken, or introducing new regulations or guidance. Ofcom will always prioritise the action it takes according to where we identify the greatest harm and where we can have greatest impact. We will also always weigh the benefits of intervention against the costs and any potential unintended consequences.

A1. Call for input questions

Questions in this Call for Input

Question 1: Do you agree that the routes described in this chapter cover all of the main methods that scammers use mobile messaging services to scam people? If not, please explain other methods.

Question 2: Which routes do you think are the most important today and will be over the next 3 years for the perpetration of mobile messaging scams? Please provide evidence for your views.

Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?

Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?

Question 5: What is your understanding of which channels are supporting the greatest harm (such as A2P or P2P SMS, or RCS)? Please provide any supporting evidence.

Question 6: What do you think will happen to RCS availability and adoption in the next few years? Please provide supporting evidence and or reasons for you views.

Question 7: Do you have views on the effectiveness of the measures discussed in this chapter? For measures where we have identified specific issues, please comment on these in your answer, providing reasoning and evidence if possible.

Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?

Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?

A2. Responding to this call for input

How to respond

A2.1 Ofcom would like to receive views and comments on the issues raised in this document, by 5pm on 7 October 2024.

A2.2 You can download a response form from https://www.ofcom.org.uk/phones-and-broadband/scam-calls-and-messages/call-for-input-reducing-mobile-messaging-scams/. 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 mobilemessagingscamsresponses@ofcom.org.uk, as an attachment in Microsoft Word format, together with the cover sheet.

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

Mobile Messaging Scams Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

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

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

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

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

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

A2.9 It would be helpful if your response could include direct answers to the questions asked in the call for input. The questions are listed at Annex 1. It would also help if you could explain why you hold your views, and what you think the effect of any measures discussed would be.

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

Confidentiality

A2.11 Calls for input are more effective if we publish the responses before the response period closes. This can help people and organisations with limited resources or familiarity with the issues to respond in a more informed way. So, in the interests of transparency and good regulatory practice, and because we believe it is important that everyone who is interested in an issue can see other respondents' views, we usually publish responses on the Ofcom website at regular intervals during and after the consultation period.

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

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

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

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

A3. Call for input coversheet

Basic details

Call for input title:

To (Ofcom contact):

Name of respondent:

Representing (self or organisation/s):

Address (if not received by email):

Confidentiality

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

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

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

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

Yes ☐ No ☐

Declaration

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

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

Name: Signed (if hard copy):