Combatting mobile messaging scams

New rules and guidance

Statement

Published 15 July 2026

For more information on this publication, please visit ofcom.org.uk

Contents

Section

Annex

1. Overview

1.1 Organised criminals around the world target people and businesses in the UK with scams over social media, online messaging apps, online ads, phone calls and mobile messages. Scammers may use multiple channels simultaneously, but contacting people with number-based mobile messages is an important tactic for them. People expect friends, family and trusted organisations to contact them in this way, which in turn enables scammers to build trust and to pressure or to manipulate potential victims into making payments or revealing sensitive information.

1.2 Fraud accounts for an estimated 45% of all reported crime incidents in England and Wales[1] and victims of fraud lost £1.28 billion to criminals in 2025.[2] Victims may not only lose money but suffer emotional distress and lasting effects on their lives, while fraud also distorts markets and hits small businesses disproportionately hard. Where fraud starts with a mobile message or phone call, victims may cease to trust the calls and messages that they receive entirely.

1.3 Protecting people from scammers is a priority for Ofcom. We use the range of our powers to stop scammers from accessing and using telecoms and online services, adding friction to their activities across all the channels we regulate. Our work supports the UK Government's Fraud Strategy 2026 to 2029, which sets out how robust regulation will help ensure the industry is accountable for further tackling fraud.[3]

1.4 This statement sets out how we will require mobile operators and business messaging aggregators to protect people from scam mobile messages.[4] Our new rules and guidance are part of how we are strengthening protections for people and businesses against receiving scam communications over telecoms services and ensuring that they can continue to make, send and receive calls and messages with confidence.[5]

1.5 Many mobile operators have been proactive in disrupting scam mobile messages in recent years. For example, we estimate that mobile operators are identifying and blocking at least 600 million suspected scam messages a year with network-level and, in some cases, AI-enabled tools.[6] Mobile operators set volume limits on SIMs that can prevent scammers from sending large volumes of person-to-person (P2P) messages from a single SIM. Some operators and business messaging aggregators also have measures in place that make it harder for criminals to gain access to business messaging services (application-to-person messaging, or A2P).

---

[1] National Crime Agency, 2026. National Strategic Assessment 2026 of Serious and Organised Crime.
[2] UK Finance, 2026. Annual Fraud Report 2026. Page 12.
[3] Home Office, 2026. Fraud Strategy 2026-2029.
[4] We refer to mobile messages to mean messaging services that are regulated under the Communications Act 2003. Scammers also use online mobile services to send scam messages, such as WhatsApp and Facebook Messenger, alongside other communications technologies and services. We set out in section 2 how we are using our powers to tackle fraud and scams across all the services we regulate.
[5] In July 2026, we have also published our decision to amend guidance for communications providers on tackling scams calls from abroad that 'spoof' UK mobile numbers. See Ofcom, 2026. Tackling scam calls from abroad: Updating our Calling Line Identification Guidance to prevent scammers abroad from spoofing UK mobile numbers.
[6] Estimate based on formal information request responses, which indicated that mobile operators' scam detection tools blocked an average of c.50 million messages each month between January and March 2025.

1.6 However, despite these measures, scam mobile messages continue to cause significant harm and industry must do more to protect people. Forty per cent of UK mobile users report having received at least one suspicious message on their mobile phone in the past three months[7] and UK mobile users reported an estimated 100 million suspicious messages to mobile operators through the 7726 service in the year to April 2025.[8] [9]

1.7 Not all mobile operators and aggregators apply strong counter-scam measures. Criminals exploit the gaps that providers have left in these protections: for example, to send P2P messages at scale from SIM farm devices and to imitate legitimate businesses to be able to send A2P messages. The value chain that supports A2P messaging can also be complex, making it more vulnerable to scammers.

1.8 The new rules and guidance we are introducing will help protect mobile users by addressing these gaps in protections. They will take effect alongside the Government's ban on the use of SIM farms[10] and mobile operators' commitments under the Fraud Sector Charter to secure trust in mobile messaging and prevent fraud.[11] We are working with the Home Office, law enforcement, industry and other stakeholders to contribute to delivery of the Government's Fraud Strategy, including by improving scam call tracing processes and further enhancing the integrity of our numbering system.

1.9 Ofcom is also helping to protect the public by contributing to a cross-agency response to criminals' use of SMS blasters. Messages from these false base stations can bypass network-level protections and tackling them requires a coordinated response from regulators and law enforcement.

What we have decided - in brief

We are implementing new rules and guidance to significantly reduce the risk that people and businesses receive P2P and A2P scam messages.

This package of measures is intended to stop scammers from accessing mobile messaging services in the first place and also to stop their activities where they have gained access.

For **P2P messaging,** we are introducing **new General Conditions (GCs)** to require mobile operators to prevent scam messages from being sent or received on their networks, by:

- **Setting volume limits** for pay-as-you-go (PAYG) SIMs, to make it harder for scammers to message large numbers of potential victims.
- **Blocking numbers used by scammers**: preventing scammers from sending messages from numbers that have been identified as responsible for scams. This includes having

[7] Ofcom, 2026. Experiences of suspicious calls, texts and app messages, Q26 (rebased for all mobile users). "Suspicious messages" refers to messages received via a mobile phone's default messaging service (i.e. via SMS/RCS and/or iMessage). This survey was conducted in February 2026 using an online panel with a representative sample of the UK population aged 16+.

[8] 7726 is a number that people can send messages to on a mobile device to report unwanted mobile messages or calls.

[9] This figure is an extrapolation of data reported to us by UK mobile network operators. They reported that customers had made a total of 90 million 7726 reports between May 2024 and March 2025 (inclusive), with an average of over 10 million per month between December 2024 and March 2025, driven by further implementation of one-click 7726 reporting by mobile network operators on Apple iOS devices.

[10] Following the passage of the Crime and Policing Act into law (it received Royal Assent in April 2026), the possession or supply of SIM farms without a legitimate reason is illegal. See Home Office, 2026. Crime and Policing Act 2026.

[11] Home Office, 2025. Fraud Sector Charter: telecommunications.

processes in place to receive scam reports from customers and third parties such as anti-fraud organisations about telephone numbers and web links (URLs[12]) that are being used for scams.
- **Blocking scam messages in transit**: identifying and blocking scam messages in transit on their networks by detecting scam URLs and telephone numbers, based on scam reports from customers and third parties.

For **A2P messaging**, we are introducing **new GCs** to require mobile operators and aggregators to prevent scam messages from being sent or received on their networks, by:

- **Conducting due diligence**: preventing criminals from using A2P services to contact potential victims by ensuring that effective Know Your Customer (KYC) checks are made at the onboarding stage.
- **Preventing the use of fake alphanumeric sender IDs**, including by corroborating Sender IDs against information gathered through KYC checks and maintaining a policy on restricting the use of protected sender IDs and generic sender IDs.
- **Conducting ongoing Know Your Traffic checks**, including reviewing account activity and promptly investigating reports of fraud.
- **Applying incident management processes** where scam activity is identified, to block message senders and address any compliance failures by other providers.
- **Blocking scam messages in transit**: identifying and blocking scam messages in transit on their networks by detecting scam URLs and telephone numbers, based on scam reports from customers and third parties (as we are requiring for P2P messaging).

We are also introducing **new GCs for mobile operators and aggregators** to ensure the requirements are effective and to minimise the risk that providers block legitimate messages. These include: a right for mobile users to challenge a decision to block a number or message; and requirements relating to reviewing policies, training staff, record keeping and compliance with data protection legislation.

We have published **guidance** on how providers can meet these requirements.

We have amended the proposal in our 2025 consultation[13] to require mobile operators and aggregators to ensure the transmission of legitimate messages. Instead, we will require providers to identify, monitor and address instances where messages are blocked in error.

We also consulted on a requirement for providers to notify message senders when certain messages are blocked. In the light of new evidence, we have decided not to implement this proposal. We have made further amendments to the rules and guidance we proposed in our 2025 consultation, taking into account respondents' feedback.

The new rules and new guidance that apply to **P2P messaging** will come into effect on **18 January 2027.** Those that apply to **A2P messaging** will come into effect on **15 July 2027**.

1.10 Our decisions are set out in section 8, the new GCs are in Annex 1 and our guidance for industry is in Annex 10.

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

[12] Uniform Resource Locator, a reference that specifies the location of a resource accessible by means of the internet. Includes short URLs.
[13] Ofcom, 2025. Combatting mobile messaging scams: Proposals for new rules and guidance.

2. Background

2.1 This section sets out:

- The actions we have already taken to make it harder for scammers to use communications services to contact potential victims.
- How scammers send mobile messages to people and businesses.
- The scope of our review of scam mobile messages and our policy objective.
- A brief description of the legal framework for our measures to combat scams.

We are tackling fraud and scams across all the services we regulate

2.2 Scammers use a range of communications technologies and services to contact potential victims and to try to manipulate them into making payments or sharing sensitive information. For example, scammers may make initial contact with a potential victim by sending them a Short Message Service (SMS) message or may encourage the victim to make contact by posting a fraudulent advert on a search engine or on social media. The scammer may then ask the victim to communicate with them using an online messaging app, such as WhatsApp or Facebook Messenger.

2.3 Ofcom has powers under the Communications Act 2003 (the Act) to ensure that telecoms services, such as mobile messaging services, are used efficiently and effectively and are not misused, for example to facilitate fraud or scams. Ofcom also has powers under the Online Safety Act 2023 to oversee how online services fulfil their duties to tackle fraud.

2.4 We work to protect users of all the services that we regulate from harm from fraud and scams. To do this, we require industry to take measures to stop scammers from accessing and using communications services, disrupting scammers' activities.

We have introduced rules to disrupt scams online and have proposed more measures to tackle fraudulent advertising

2.5 The Online Safety Act requires regulated user-to-user services[14] and search services[15] to conduct a risk assessment for illegal harms, including relevant fraud and financial services offences. Ofcom recommends that service providers adopt proportionate measures to address these illegal harms. Relevant services in scope of these duties include social media platforms, online marketplaces, dating services, general search services and online messaging apps on a user's device.[16]

[14] We define 'user-to-user services' as internet services that enable users of the service to generate, share or upload content (such as messages, images, videos, comments, audio) on the service that may be encountered by other users of the service. This includes services that enable user interactions. See Ofcom, Overview of regulated services.

[15] We define 'search services' as those that are, or include, a search engine, which allows users to search more than one website or database.

[16] Online messaging apps are not considered number-based telecoms services (under section 32A of the Act) for which Ofcom has responsibilities under the Act (although some of these services may use a mobile number to verify users when they sign up).

2.6 Our Illegal Harms Statement contains cross-cutting measures (e.g. governance, moderation, reporting and terms of service) that tackle all illegal harm, including fraud.[17] It also recommends fraud-specific measures, including dedicated reporting channels for expert trusted flaggers (e.g. the Financial Conduct Authority (FCA) and Metropolitan Police),[18] so they can report suspicious activity and content easily to in-scope services.

2.7 In June 2025, we published a consultation on additional safety measures to strengthen our Codes of Practice for providers of online services.[19] Our proposals include measures regarding the use of proactive technology to detect, or support the detection of, relevant illegal content, including fraud.[20] The proposals also include measures for the preparation and application of user sanctions policies against offending UK users. We will continue to work to ensure that effective and proportionate protections are in place to detect and address fraud and other harms online. We expect to publish our decisions in the autumn.

2.8 In July 2026, we published a consultation on the Fraudulent Advertising Code.[21] These proposals set out the steps that, in our assessment, platforms should take to combat fraudulent advertising. Our proposals focus on providers having effective governance and risk assessment processes that make it harder for criminals to access advertising accounts, the robust testing of AI tools and strengthening reporting functions via an effective advertising library and fraudulent advertising direct reporting channel. The proposals apply to paid-for advertising content on Category 1 and Category 2A services (and not to user-generated content or non-sponsored search content). We expect to publish our decisions by mid-2027 at the latest.

We have rules in place to prevent criminals from accessing numbers and making scam calls

2.9 In 2022, we published a statement on our role and approach to tackling scam calls and mobile messages.[22] Since then, we have issued guidance setting out the measures we expect operators to take to comply with our rules on the use of numbers and the provision of Calling Line Identification (CLI) facilities. These measures make it harder for scammers to use UK telecoms services, including:

- Guidance to help operators identify and block numbers that are associated with trusted organisations, such as banks and public bodies, which are never intended to make outbound calls.[23] We record these in the Do Not Originate list, which we share with providers.[24]
- Clarifying the due diligence that UK providers should carry out when suballocating numbers to other providers.[25]

---

[17] Ofcom, updated 25 June 2026. Quick guide to illegal content codes of practice.
[18] We are working with trusted flaggers to assess early compliance with the dedicated reporting channels measure, supported by supervision.
[19] Ofcom, 2025. Additional Safety Measures: Online Safety.
[20] Ofcom, 2025. Consultation on additional safety measures. This includes proposals on the use of proactive tech, covering user-to-user services (the proposals do not cover private messaging). The consultation also includes a proposal on user sanctions policies, covering all services in scope of the Online Safety Act.
[21] Ofcom, 2026 Consultation: Fraudulent Advertising Codes of Practice.
[22] Ofcom, 2022. Tackling scam calls and texts: Ofcom's role and approach.
[23] Ofcom, 2022. Submitting numbers to the 'Do Not Originate' list: Guide for organisations.
[24] Ofcom, 2023. Do Not Originate List.
[25] Ofcom, 2022. Good practice to help prevent misuse of sub-allocated and assigned numbers.

- Guidance on the provision of CLI facilities and other related services.[26]
- Setting out the steps that operators are expected to take to identify calls from abroad that spoof UK landline Network Numbers and block them.[27]

2.10 In 2024, we launched an enforcement programme focused on scam calls, to help ensure that providers and their customers are following our rules.[28] Alongside this statement, we have published our final decision to introduce new measures to protect people from scam calls from abroad that appear to come from UK mobile numbers.[29]

2.11 Our consumer research shows that the proportion of telecoms service users that report having received suspicious calls in the previous three months prior to fieldwork has fallen over the last four years, although it remains high:[30]

- The proportion of landline users that had received at least one suspicious call on their landline phone in the three months prior to fieldwork fell from 53% in 2022 to 39% in 2026.
- The proportion of mobile phone users that had received at least one suspicious call on their mobile in the three months prior to fieldwork fell from 40% in 2022 to 32% in 2026.

2.12 We have a significant role to play to support delivery of the Government's Fraud Strategy 2026 to 2029, which sets out how robust regulation will help ensure the industry is accountable for further tackling fraud. We are working with the Home Office, law enforcement, industry and other stakeholders to contribute to delivery of the Strategy, including improving scam call tracing processes, further enhancing the integrity of our numbering system and continuing to enforce our rules.

2.13 The measures we have taken to address telecoms and online fraud work in tandem, because scammers will use whatever communication tools are most effective and most vulnerable. Better prevention across the board will reduce consumer harm from scams and support confidence in all of the services we regulate.

2.14 In the following section, we explain why additional measures to address mobile messaging scams are needed.

Scammers are sending mobile messages to contact potential victims

2.15 Although we have rules in place to prevent scammers from exploiting telecoms services, people and businesses continue to receive scam mobile messages. This is because scammers are gaining access to the different channels available to people and businesses to enable them to send and receive mobile messages. Scammers deceive providers into conveying scam messages or gain access via bad actors that enable their activities.

---

[26] See Ofcom, 2022. Guidance on the provision of Calling Line Identification facilities and other related services. In July 2026, we published our decision to amend this guidance to set out how we expect communications providers to tackle scams calls from abroad that spoof UK mobile numbers. See Ofcom, 2026.
[27] Ofcom, 2024. Tackling scam calls - expecting providers to block more calls with spoofed numbers.
[28] Ofcom, 2024. Enforcement programme into phone and text scams.
[29] Ofcom, 2026. Tackling scam calls from abroad.
[30] Ofcom has conducted research annually (excluding 2023) among a representative sample of the UK population aged 16+ to understand consumers' experiences of receiving suspicious communications via their landline and mobile phones (including calls, texts and app messages) in the previous three months. Fieldwork dates: August (2022), Feb (2026).

2.16 The volume of mobile messages that are sent and received over UK telecoms networks has fallen in recent years, but use remains substantial. In 2025, over 21 billion SMS and Multimedia Messaging Service (MMS)[31] messages were sent in the UK.[32]

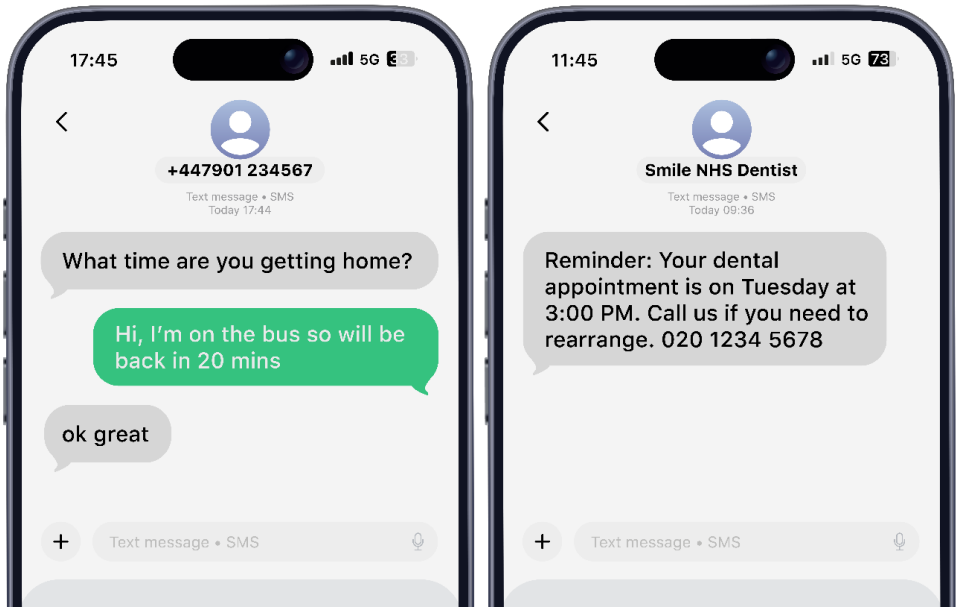
2.17 There are benefits, to end-users and to the wider economy, of having a choice of trusted means to send and receive mobile messages. However, we set out below how scammers infiltrate the different channels for mobile messages.

People and businesses can send and receive messages over person-to-person and application-to-person channels

2.18 There are two main channels for sending and receiving mobile messages, illustrated in Figure 2.1:

- Person-to-person (P2P) messages are sent (in almost all cases) from one SIM to another, through and between mobile networks. Mobile operators[33] are typically the only companies involved in the delivery of P2P messages. Consumer end-users send most P2P messages, between family and friends.
- Application-to-person (A2P) messages come from business senders (such as doctors' surgeries or hairdressers), which contract with A2P providers to send mobile messages on their behalf. Businesses and other organisations use them to, for example, send appointment reminders, service updates (such as an overdraft notification from a bank) or promotional messages.

Figure 2.1: Illustration of a P2P message (left) and A2P message (right)



Note: This image has been stylised for illustration purposes. Where the sender of a P2P messages is a saved contact in the recipient's phone, the ID that the recipient would see would be the saved contact name.

[31] MMS is a communication protocol that allows users to send multimedia content over a mobile network.
[32] Ofcom, 2026. Telecommunications Market Data Update. Page 14.
[33] Mobile operators comprise of mobile network operators (MNOs), 'thick' mobile virtual network operators (MVNOs) and 'thin' MVNOs. Thick and thin MVNOs both rely on host MNOs to operate. A thick MVNO runs more of its service in-house, such as elements of its own mobile core network.

2.19 A2P messaging channels often operate over a complex supply chain. Different kinds of companies convey A2P messages from business senders:

- **Terminating mobile operators**, which receive A2P messages for termination on their networks (i.e. to telephone numbers).[34]
- **Messaging Service Providers (MSPs)** or **Communications Platform as a Service (CPaaS) providers** that specialise in interfacing directly with business senders (in this statement we refer to these companies as MSPs). MSPs often provide an Application Programming Interface[35] that enables business senders to access different messaging services online and may generate messages on the business sender's behalf. MSPs may pass messages to aggregators and terminating mobile operators or enable senders to initiate messages with these providers through their platform. Where a company is acting as an MSP but not providing an Electronic Communication Service (ECS) or Electronic Communication Network (ECN) [36] they are not a regulated communications provider for the purposes of any of our General Conditions (GCs).
- **Aggregators**, which contract with business senders, MSPs and other aggregators to arrange for the delivery of large volumes of A2P messages. 'Tier 1' aggregators have a direct contractual relationship with a mobile operator to purchase message termination (either directly, or indirectly through an interconnect arrangement). 'Tier 2' aggregators contract with a tier 1 aggregator, and so on. We consider that all aggregators provide a public ECS in the form of the provision of mobile messaging services that consist of, or have as their principal feature, the conveyance of signals and/or a public ECN in the form of a transmission system for the conveyance of mobile messages.

2.20 In practice, many companies offer both MSP and aggregator services and can also operate as aggregators at different tiers in different transactions. In May 2024, more than thirty aggregators operated at tier 1, with direct connections to at least one UK mobile operator.[37] The nature and scale of the downstream aggregator market (i.e. tier 2 and above) is complex, but the market appears to be fragmented: in February 2025, there were at least 500 aggregators or MSPs transmitting messages to tier 1 aggregator services.[38]

---

[34] There may also be mobile operators in the chain that are not terminating mobile operators, where a tier 1 aggregator sends messages to a mobile operator, which sends them on to another mobile operator ('off-net').
[35] Software that allows different systems to communicate.
[36] Electronic Communications Network (ECN) is defined in section 32(1) of the Act. 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 (NBICS); 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. An NBICS is defined in section 32A of the Act and in summary means a service made available to the public that: (a) enables direct interpersonal and interactive exchange of 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.
[37] Information provided to Ofcom by mobile operators. Typically, a smaller group of the largest aggregators account for most of the traffic on each mobile network.
[38] Information provided to Ofcom from a sample of nine aggregators. We expect there to be significantly more aggregators and MSPs that contract with other tier 1 aggregators and in positions further downstream.

Scammers are finding ways to access both P2P and A2P channels and evade detection when sending scam messages

2.21 Although the volume of legitimate mobile messages being sent and received in the UK has declined in recent years, mobile messaging remains attractive to scammers as a means to communicate with potential victims. This is because:

- Scammers deceive people by impersonating trusted organisations, such as public authorities or banks, and by contacting potential victims over channels that people expect these organisations to use. Trusted organisations often use mobile messaging to contact people, because mobile messaging can reach nearly everyone. Almost all users of mobile devices can send and receive mobile messages.
- When scammers can gain access to telecoms services they can send large volumes of mobile messages. These can be cheaper for scammers than, for example, making high volumes of scam calls, and recipients may be more likely to read them than e.g. scam emails.

2.22 We expect the usefulness of these channels to scammers to endure for the foreseeable future, even if overall volumes of mobile messages continue to decline.

2.23 To send P2P messages, scammers typically use illegal SIM farm devices.[39] These devices allow scammers to generate messages and transmit them over mobile networks using SIMs. Scammers insert SIMs into SIM farms, which typically house tens or hundreds of SIMs.

2.24 Scammers use SIMs for both pay-as-you-go (PAYG) and pay-monthly services to send P2P messages. However, mobile operators typically do not require the same level of credit or other identity checks for PAYG SIMs as they do for pay-monthly contracts.[40] Scammers acquire SIMs by buying them in-store or buying stolen cards.

2.25 To send A2P messages, scammers may approach MSPs and impersonate a legitimate business, attempting to pass any Know Your Customer (KYC) checks. They may also take over legitimate accounts.

2.26 With access to A2P messaging services, scammers may be able to send messages with an alphanumeric sender ID, so that their messages appear to the recipients to come from a named organisation (such as 'HMRC'). This can make messages appear more credible to recipients.[41] Our research shows that, when assessing the authenticity of a message, 44% of mobile and/or landline users look at whether a company is named and 31% consider the trustworthiness of the company mentioned.[42]

2.27 Although many MSPs and aggregators have introduced measures to block scammers from accessing networks and to identify suspicious activity, these will not be sufficiently comprehensive as long as scammers can find companies downstream that do not have these measures in place and that accept their messages.

2.28 Figure 2.2 illustrates how scammers are gaining access to both A2P and P2P channels.

---

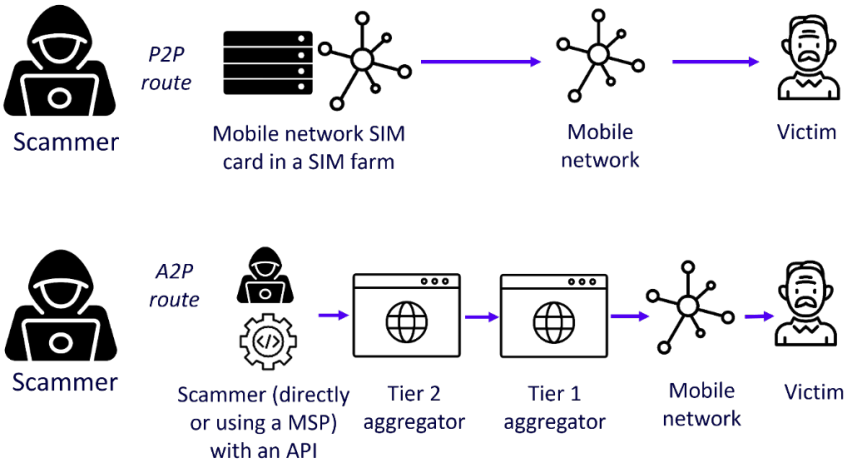
[39] Following the passage of the Crime and Policing Act into law (it received Royal Assent in April 2026), the possession or supply of SIM farms without a legitimate reason is illegal. See Home Office, 2026. Crime and Policing Act 2026.

[40] Evidence from some mobile operators indicates that a disproportionately high number of PAYG customers are suspended for SMS fraud by comparison with pay-monthly customers.

[41] The alphanumeric ID may look convincing, or scammers may spoof an ID and send new messages to an existing message thread so that the messages appear to come from a legitimate sender.

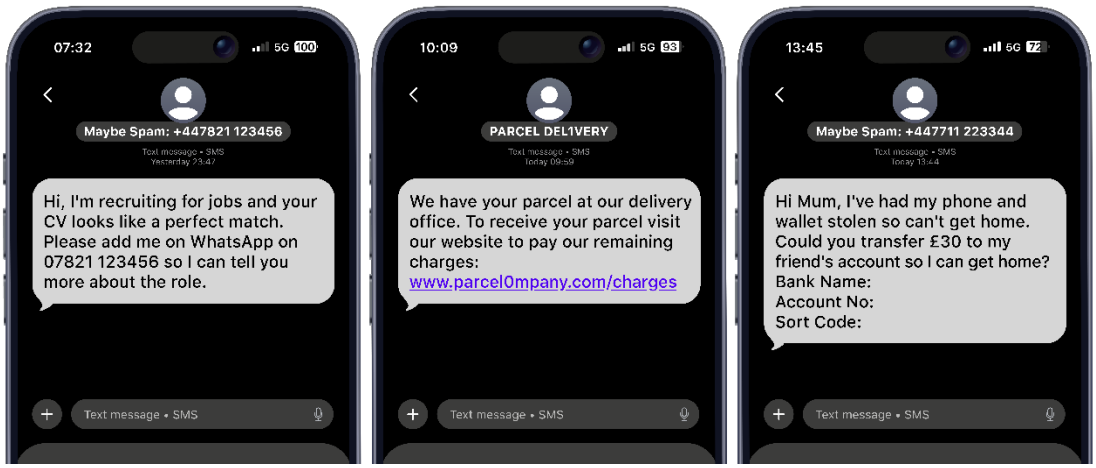
[42] Ofcom, 2026. Experiences of suspicious calls, texts and app messages, Q25.

Figure 2.2: How scammers send messages over A2P and P2P channels



2.29 Figure 2.3 illustrates how scammers use different channels to initiate further engagement with potential victims, including through phone calls, online messaging apps and websites or bank payments (section 3 sets out more examples).

Figure 2.3: Scammers use mobile messages in conjunction with other communications to conduct recruitment (left), parcel delivery (centre) and 'Hi Mum' scams (right)



Our new measures to tackle scam mobile messages draw on our Communications Act powers

2.30 Below we summarise the distinctions between messaging services that fall within the scope of the Communications Act, which are the focus of this review, and services in scope of the Online Safety Act.

Our Communications Act powers apply to public electronic communications services, including number-based services

2.31 The measures in this statement apply to mobile messaging services that are regulated under the Communications Act. We define these further below. The measures do not apply to services that Ofcom regulates under the Online Safety Act, such as online messaging apps.

2.32 For many users, online messaging apps may appear similar to mobile messaging services. A mobile device typically has a pre-installed native messaging app,[43] which may send and receive messages over multiple different technologies and standards, such as SMS, MMS, Rich Communications Services (RCS)[44] and proprietary online messaging standards such as iMessages (it may not be clear to the user what technology or standard a native messaging app uses to send or receive an individual message). Users may also have one or more online messaging apps installed on their mobile device. In legal and regulatory terms, however, there is a distinction between messaging services, as follows:

- Public electronic communications services, including "number-based" communications services, are regulated under the Communications Act. This includes traditional voice telephony, SMS and MMS.
- Online messaging apps are regulated under the Online Safety Act. In the Communications Act, these services are referred to as "number-independent" interpersonal communications services.

Our definition of mobile messaging services

2.33 When we refer to mobile messages or mobile messaging services in this statement, we refer to services that are regulated under the Communications Act. That includes public electronic communications services[45] and, in particular, number-based interpersonal communications services (NBICS).[46] NBICS are services that meet both of the following criteria:

- They enable direct interpersonal and interactive exchange of information by means of electronic communications networks between a finite number of persons, where the persons initiating or participating in the communication determine its recipient.
- They connect with or enable communication with numbers from a national/international numbering plan.

2.34 SMS and MMS are regulated under the Communications Act, but the messaging services landscape is changing continually. Whether a particular operator is currently, or could be in the future, providing a messaging service that is regulated under the Communications Act will depend on whether a service meets the relevant definitions in that Act, taking into account both the underlying European legislation on which those definitions are based and relevant case-law.[47] This requires a technical, commercial/contractual and practical assessment of how a service is implemented, including but not limited to consideration of:

- The presence and role of a telephone number in the delivery of a message.
- Whether the service enables users to send and receive messages to/from any number in the in the National Telephone Numbering Plan (the Numbering Plan) without restriction,[48] or

[43] Applications that mobile platforms (e.g. those operated by Apple and Google) provide and typically pre-install on smartphones to enable users to send and receive messages.
[44] RCS is a standardised communications protocol that enables mobile users to send and receive messages over an internet connection. It offers features such as group chats, read receipts, typing indicators and support for end-to-end encryption. It supports both P2P and A2P messaging.
[45] See section 32(2) and (2A) of the Act.
[46] See sections 32(2A)(b) and 32A of the Act.
[47] See, for example: the Judgment of the European Court, 13 June 2019 in Google LLC v Bundesrepublik Deutschland, Case C-193/18; and the Judgment of the European Court, 5 June 2019 in Skype Communications Sàrl v Institut belge des services postaux et des télécommunications (IBPT), Case C-142/18.
[48] i.e. the end-to-end connectivity associated with public numbering resources.

whether a user can only send and receive messages to other users that have enabled specific messaging functionality on their device and/or where other conditions have first been met.

- Which operator is in control of the service and responsible to the sender for the conveyance of signals required to ensure their message is delivered[49] and whether that operator is acting in the capacity of an internet service provider or a provider of a messaging service.

2.35 Widely adopted online messaging apps such as WhatsApp and proprietary online messaging standards such as iMessage use functionality that is not dependent on telephone numbers and they are not regulated under the Communications Act.

2.36 Services such as RCS share characteristics of the traditional messaging services like SMS and MMS but also share characteristics of online messaging apps. Whether such a service is now, or could in the future be, regulated under the Communications Act will depend on how it is implemented in the UK. It is for operators to determine in the first instance whether their current implementation of RCS constitutes a service that is regulated under the Communications Act or the Online Services Act.[50]

Our objective is to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages

2.37 Taking into account our general duties, and our functions and powers relating to telephone numbers (see below), we have a longstanding objective of countering telecoms scams. Our 2022 statement set out how we are working to make it harder for scammers to operate at every stage of the supply chain for calls and mobile messages.[51] To meet our longstanding objective, we have strengthened our rules and guidance in a number of areas, as described above.

2.38 In the course of this review, we have monitored the evidence of harm from scam mobile messages (see section 3) and the implementation of industry-led initiatives to combat them (see section 4). Despite significant industry-led counter-scam activity, scam messages remained a persistent problem for people and businesses. We therefore published a call for input in 2024, which outlined our understanding of the issues.[52] We invited stakeholders to comment on the effectiveness of the measures that industry had deployed to stop scam mobile messages, and on potential further measures, to help us understand whether to take additional action to protect people and businesses in the UK.

[49] An operator can be considered to be in control of a service even if they do not have the infrastructure required to carry out the transmission themselves, for example, because they have outsourced the provision of the service. See, for example, section 32(4) of the Act and the Judgment of the European Court, 30 April 2014 in UPC DTH Sàrl v Nemzeti Média- és Hírközlési Hatóság Elnökhelyettese, Case C-475/12 (paragraph 43).
[50] In the July 2024 call for input, we stated that RCS uses a telephone number to route a message through communications networks (see Table 1, Ofcom, Call for input: Reducing mobile messaging scams). However, the way in which RCS is currently implemented and provisioned in the UK has an impact on whether it should be considered a NBICS or a user-to-user service under the Online Safety Act. Given that the technical, commercial/contractual and practical configuration of RCS continues to change, we consider that operators are best placed to assess, in the first instance, whether the way in which they have currently implemented RCS in the UK is a service that is regulated under the Communications Act or the Online Services Act.
[51] Ofcom, 2022. Tackling scam calls and texts.
[52] Ofcom, 2024. Call for input: Reducing mobile messaging scams.

2.39 Having considered responses to the 2024 call for input and information we gathered using our formal powers, we published a consultation in 2025[53] on proposals to achieve the policy objective of **significantly reducing the likelihood that consumer and business end-users receive scam mobile messages.**

2.40 We consider that the measures we set out in this statement are necessary to achieve our objective, noting the evidence of harm (set out in section 3) and in the light of our view that existing interventions are unlikely to achieve our objective (section 4).

The legal framework for our measures to combat scam mobile messages

2.41 We set out below a summary of our powers and duties that are relevant to the measures in this statement. Full details of the relevant legal framework are set out in Annex 5 to this statement.

Our general duties

2.42 When formulating the measures in this statement, we have had regard to our general duties including our principal duty under the Act 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.[54]

2.43 When carrying out our duties, we have also had regard to:

- The principles under which our regulatory activities should be transparent, accountable, proportionate, consistent, and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice.[55]
- The interests of consumers in respect of, among other things, choice, price, quality of service and value for money.[56]
- A number of matters, as they appear to us to be relevant in the circumstances, including the:
    - Desirability of promoting competition in relevant markets.
    - Desirability of promoting and facilitating the development and use of effective forms of self-regulation (except in relation to our Online Safety functions).
    - Desirability of encouraging investment and innovation in relevant markets.
    - Desirability of ensuring the security and availability of public electronic communications networks and services.
    - Desirability of ensuring that relevant markets facilitate end-to-end connectivity in the interests of consumers in those markets.
    - Vulnerability of children and of others whose circumstances appear to us to put them in need of special protection.
    - Needs of disabled people, of the elderly and of those on low incomes.
    - Desirability of preventing crime and disorder.
    - Opinions of consumers in relevant markets and of members of the public generally.

[53] Ofcom, 2025. Combatting mobile messaging scams: Proposals for new rules and guidance.
[54] Section 3(1) of the Act.
[55] Section 3(3) of the Act.
[56] Section 3(5) of the Act.

2.44 When carrying out our functions, we have acted in accordance with six requirements for regulation, which include promoting the interests of all members of the public in the United Kingdom.[57] We have also had regard to the UK Government's Statement of Strategic Priorities for telecommunications, management of radio spectrum and postal services[58] and the desirability of promoting economic growth.[59] We set out how we have taken account of our growth duty in section 8.

Functions and powers relating to telephone numbers

2.45 Ofcom has a number of functions relating to telephone numbers,[60] including a general duty to ensure the best use is made of numbers, encouraging efficiency and innovation for that purpose.[61]

2.46 Ofcom has powers under section 45 of the Act to impose rules relating to mobile messaging services. In particular, we can impose conditions:

- Which we consider appropriate for protecting the interests of end-users of public electronic communications services, including conditions:
    - Relating to the supply, provision or making available of goods, services or facilities in association with the provision of public electronic communications services (section 51(2)(a) of the Act).
    - Requiring the provision, free of charge, of specified information, or information of a specified kind, to end-users (section 51(2)(d) of the Act).
    - Requiring a communications provider, in specified circumstances, to block access to telephone numbers or services in order to prevent fraud or misuse, and enable them to withhold fees payable to another communications provider in those circumstances (section 51(2)(f) of the Act).
- Relating to the allocation, adoption and use of telephone numbers, including:
    - Rules relating to the use by a communications provider, for the purpose of providing an electronic communications network or electronic communications service, of telephone numbers not allocated to that provider (section 58(1)(b) of the Act).
    - Restrictions on the adoption of telephone numbers by a communications provider, and on other practices by communications providers in relation to telephone numbers allocated to them (section 58(1)(c) of the Act).
    - Requirements on a communications provider in connection with the adoption by them of telephone numbers (section 58(1)(d) of the Act).
    - Requiring communications providers to secure compliance with such rules relating to the use of telephone numbers by their customers as Ofcom may set out in General Conditions or determine in accordance with provisions made by the General Conditions (section 58(1)(i) of the Act).

[57] Section 4 of the Act.
[58] In accordance with section 2B of the Act. See Department for Science, Innovation and Technology, 2026. Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services.
[59] In accordance with section 108 of the Deregulation Act 2015.
[60] These are set out in sections 56 to 63 of the Act.
[61] Section 63 of the Act.

2.47 We can impose these conditions on persons that are communications providers (i.e. providers of electronic communications networks[62] or electronic communications services[63]). The conditions relating to the allocation, adoption and use of telephone numbers can also be imposed on persons that are not communications providers but have applied for or been allocated numbers.[64]

2.48 Our rules can also apply to providers outside the UK to the extent they fall within the scope of the relevant definitions and there is a territorial connection to the UK. This could be because, for example, a +44 call is being routed into the UK where the intended recipient is based.

2.49 Ofcom also has a duty to publish the Numbering Plan and keep it under review.[65] The Numbering Plan sets out telephone numbers that are available for allocation and any restrictions on how they may be adopted or used.

2.50 Where providers contravene our rules, such as where telephone numbers or services have been misused, Ofcom can take enforcement action including: issuing a penalty;[66] suspending a provider's entitlement to provide an electronic communications network or service, or to make associated facilities available;[67] requesting that providers block access to relevant numbers or public electronic communication services;[68] and withdrawing telephone number allocations.[69] Ofcom also has powers under the Act to take enforcement action against persons who persistently misuse an electronic communications network or services.[70]

Respondents to our 2025 consultation

2.51 Below we provide information on stakeholders that provided non-confidential responses to our 2025 consultation on measures to combat mobile messaging scams, to which we refer throughout this document.

Mobile operators and resellers of mobile services

2.52 We received responses from a range of mobile operators. These include:

[62] Electronic Communications Network (ECN) is defined in section 32(1) of the Act.
[63] 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 (NBICS); 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. An NBICS is defined in section 32A of the Act and in summary means a service made available to the public that: (a) enables direct interpersonal and interactive exchange of 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.
[64] Section 59(1)-(2) of the Act. The current conditions binding persons other than Communications Providers are set out in Numbering Conditions Binding Non-Providers.
[65] Section 56 of the Act.
[66] In accordance with sections 96A -97 of the Act. We have powers to impose significant financial penalties of up to 10% of annual turnover.
[67] Section 100 of the Act.
[68] General Condition B4.4.
[69] Section 61 of the Act and General Condition B1.18.
[70] Sections 128-130 of the Act.

- The UK mobile network operators (MNOs): BT Group (EE), Virgin Media O2 (O2) and VodafoneThree (Vodafone and Three).
- Mobile virtual network operators (MVNOs): Gamma, Sky and Utility Warehouse.
- We also received a response from Verastar Limited (trading as Clear Business), which operates as a 'thin' MVNO and a reseller of mobile services.

Business messaging service providers

2.53 Several companies that provide A2P business messaging services responded to the consultation, including Simwood, Stour Marine Limited and Twilio.

Consumer and rights groups

2.54 Several bodies that work on consumer issues responded, including:

- Citizens Advice Scotland.
- The Communications Consumer Panel and Advisory Committee on Older and Disabled People (CCP-ACOD). These expert groups advocate for consumers and microbusinesses in the UK and older and disabled people, respectively.
- Consumer Scotland.
- Which?

2.55 We also sought responses from some groups focussed on human rights issues regarding the rights assessment we set out in our consultation. We received a response from Amnesty International UK.

Trade and industry groups

2.56 We received several responses from trade associations and groups representing different parts of the telecoms sector and other sectors:

- The Association of British Insurers (ABI).
- Comms Council UK (CCUK), an organisation that represents UK telecommunications companies that provide services to business and residential customers.
- The Federation of Communications Services (FCS), an organisation that represents companies that provide communications services to business users.
- The Mobile Ecosystem Forum (MEF), a global trade body representing companies involved in the provision of mobile services.
- Mobile UK, a trade association representing the UK's three MNOs.
- techUK.
- The UK Competitive Telecommunications Association (UKCTA), a trade association representing fixed line telecommunications and broadband companies.

Anti-fraud technology and service vendors

2.57 We also received responses from some companies that offer relevant technology solutions, either to market participants or to consumers:

- Ask Silver, a service that allows users to check suspicious communications they receive.
- The Campaign Registry, a company that provides a registration hub for business messaging senders.

- iconectiv UK, a company providing anti-fraud telecoms infrastructure solutions.
- Pinnacle Teleservices, a global CPaaS provider, which offers a platform to detect business messaging fraud.
- XConnect, a company that provides services to mobile operators, business messaging services and others related to fraud prevention in voice and messaging.

Structure of this statement

2.58 The rest of this document is structured as follows:

- Section 3 describes the evidence of harm that results from messaging scams.
- Section 4 sets out our assessment of whether we could address these harms and achieve our policy objective by relying on existing measures that industry, Government, law enforcement and Ofcom have implemented, or whether further regulatory intervention is required.
- Section 5 assesses a set of measures to address scam P2P messages.
- Section 6 assesses a set of measures to address scam A2P messages.
- Section 7 assesses a set of cross-cutting measures that apply to both P2P and A2P channels and enhance the efficacy of the measures outlined in sections 5 and 6 and safeguard human rights.
- Section 8 contains our overarching assessment of the benefits of the overall package of measures, our assessment of their proportionality and impact on individual rights, followed by our final decisions.
- Section 9 sets out our approach to implementation of the new rules and guidance.

2.59 The annexes to this statement are as follows:

- Annex 1 sets out the new GCs and Legal Notification.
- Annex 2 sets out the Non-Provider Conditions and Legal Notification.
- Annex 3 summarises the impact assessments we have conducted.
- Annex 4 provides more detail on our rights assessment.
- Annex 5 sets out the relevant legal framework.
- Annex 6 includes a link to our guidance for providers on how they can implement our rules.

3. Harm from scam mobile messages

Introduction

3.1 In this section, we provide an assessment of the harm from scam mobile messages, taking into account responses to our 2025 consultation and drawing on more recent data where available. We consider:

- How scammers use mobile messages to reach potential victims, with examples of some typical messaging scams and general features of such scams.
- An illustrative assessment of the impact of mobile messaging scams[71] on their victims and, more widely, on UK consumers and on businesses that use mobile services.
- The available evidence of the scale of mobile messaging scams.
- The available evidence of the scale of financial and other harms that arise from mobile messaging scams.

3.2 In response to our 2025 consultation, the large majority of stakeholders agreed with our findings on the types and scale of harm that scam messages cause. However, some noted that data limitations make it difficult to determine the true extent of harm.

3.3 In the following paragraphs, we begin by setting out our assessment of harm from scam messages. Next, we summarise stakeholder responses on this topic. Finally, we conclude that the scale of harm from scam mobile messages is significant.

Scammers abuse mobile messaging services using a variety of tactics

3.4 In our consultation, we set out that mobile messaging scams enable two broad categories of scams: authorised push payment (APP) and unauthorised payment scams.

3.5 In APP scams, the scammer seeks to impersonate a person, company or other institution and, ultimately, to persuade the victim to send them money. Some current examples are:

- 'Hi Mum' scams, in which the scammer pretends to be the message recipient's son or daughter, claiming to have a new number or to be using a friend's phone because their own has been lost or damaged. Once trust is gained, the scammer typically asks the victim to transfer money to a bank account they control.
- Scammers claiming the victim has won a prize in a lottery and that the prize will be released when a processing fee is paid.

[71] We are specifically assessing the harm from messaging scams on "Number based interpersonal communications services" (NBICSs). As discussed in section 2, NBICSs are services that: (i) enable direct interpersonal and interactive exchange of information by means of electronic communications networks between a finite number of persons, where the persons initiating or participating in the communication determine its recipient; and (ii) connect with or enable communication with numbers from a national/international numbering plan (section 32A of the Act).

- Scammers impersonating tax authorities, claiming the recipient has an outstanding tax penalty and that legal action will be taken if payment is not made immediately.
- Fake Penalty Charge Notices (PCN): Spoofed messages claiming you have an unpaid £20 parking fine, threatening legal action if a linked fake government or council website isn't visited immediately to pay.

3.6 Unauthorised payment scams involve stealing victims' credentials and/or gaining control over their bank account and then making transactions without the victim's permission. This may involve manipulating the victim into clicking on a malicious URL or accessing a mobile account to request a replacement SIM, which will then be misused in the course of the scam. Recent examples include:

- Apple scam text: a message claims that the recipient's Apple account has been paused due to a problem processing their billing details. The message includes a link to a website which will request personal and financial data.
- Mis-sold car finance scams: a scam text sent from a supposed claims management firm tells you that you could be owed a stated sum in mis-sold car finance and provides a link to see how much you're owed. The linked website then asks for personal and financial details.
- FCA scams: a message supposedly from the FCA suggesting that the recipient's personal data is at risk and providing a number to call. If the victim calls the number a scammer will try to get them to reveal personal and banking details.
- Bank impersonation scams, such as a text message supposedly from a bank saying a direct debit has been set up or a credit card application has been approved and again providing a number to call.[72]

3.7 Scammers generally adopt the strategy of sending messages to many telephone numbers, in the expectation that a small percentage will respond by making a payment or sharing sensitive information. Which? has noted the potential use of AI in various scams, including using large language models to generate well-crafted written communications including text messages.[73]

3.8 As shown in Figure 2.3, some scams such as 'Hi Mum' and recruitment scams use the P2P channel, while others, such as delivery scams, use the A2P channel. A variety of both P2P and A2P messaging scams have been reported by consumer bodies and in the press.[74]

Scam mobile messages negatively impact UK consumers, businesses and the wider economy

3.9 In our 2025 consultation, we set out our view that mobile messaging scams have wide-ranging negative effects, extending beyond those who fall victim directly. These harms include both financial and non-financial harms to UK consumers, businesses and public sector organisations.

3.10 Firstly, individuals who are deceived by messaging scams often suffer serious financial consequences. Many face direct financial losses from scammers making unauthorised

[72] These examples are from Which? June 2026. The latest scam alerts from Which?.
[73] Which?, December 2024. Five scam trends for 2025.
[74] See for example Which?, December 2024. Five scam trends for 2025 and This Is Money, September 2025. Five sneakiest scam texts fraudsters are plaguing your phone with today.

payments. Such financial losses can also have significant knock-on impacts: victims may lose some or all of their savings, go into debt or lack money for essentials as a result of scams.[75] While in some cases such losses are reimbursed by a financial services provider, they then become a cost to that provider, as we discuss below.

3.11 Beyond the monetary losses, victims must endure the nuisance and administrative burden of resolving the fraud. This can include time-consuming efforts to regain access to compromised accounts, to secure personal information or to seek redress through customer service channels or formal processes.

3.12 Scams can also cause significant emotional harm to victims. For example, a 2025 Home Office report found that victims of fraud may experience a wide range of emotional harms, such as anger, stress and anxiety.[76] While rarer, some victims may also experience serious health harms, including suicidal thoughts and self-harm. [77] A report by Visa on the impact of APP scams highlighted the harm to personal health and wellbeing: one in three victims reported that their mental health has suffered as a result of an APP scam and many also reported that they have reduced confidence in their own money management and financial institutions.[78] Female and ethnic minority victims are also significantly more likely to experience some types of emotional and health harms by comparison with males and non-ethnic minority people, respectively.[79]

3.13 Secondly, attempted scams impact all mobile users, not just those who have been successfully defrauded. Even when scam attempts are unsuccessful, they impose a drain on attention and time. Users must remain vigilant, scrutinise unexpected messages and spend time deleting or reporting suspicious mobile messages, adding friction to everyday digital interactions.

3.14 Thirdly, mobile network operators and messaging aggregators also bear costs relating to scam traffic, due to the need for additional customer support. These messages also consume bandwidth and resources, as large volumes of scams are being carried on mobile networks.

3.15 Finally, scam messages have broader implications for the economy and society. Financial institutions incur substantial costs when reimbursing victims and investigating fraudulent activity. Public services, including law enforcement, need to support affected individuals and to tackle criminal networks. On a systemic level, widespread exposure to scams may erode trust in digital communications, making people more hesitant to engage with legitimate mobile messaging-based services or online platforms and transactions. This reluctance can affect the reputations and operations of trusted organisations that are impersonated in scam messages. In addition, firms may incur costs of investigating and resolving complaints relating to scams.

---

[75] Communications Consumer Panel, 2020. Scammed! Exploited and afraid What more can be done to protect communications consumers from the harm caused by scams?, Pages 11-13.
[76] Home Office, 2025. Experiences of victims of fraud and cyber crime, section 3.1.1 2025.
[77] Home Office, 2025. Experiences of victims of fraud and cyber crime, section 3.1.2 2025.
[78] Visa, 2023. The Impact of APP Scams.
[79] Home Office, 2025. Experiences of victims of fraud and cyber crime, section 3.1.2 [accessed 30 June 2026]. We have taken this into consideration in our Equality Impact Assessments in Annex 3.

3.16 As we discuss below, stakeholder responses to our 2025 consultation generally agreed with our assessment of the negative impact of messaging scams, with some noting impacts on specific vulnerable groups, and evidence of recent increases in the rate of such harms.

Large volumes of scam messages are blocked by operators, but many continue to reach mobile users

3.17 As set out above, scammers generally adopt the strategy of sending messages to many telephone numbers, in the expectation that a small percentage will respond.

3.18 In our 2025 consultation, we assessed the scale of mobile messaging scam activity in the UK, drawing on the following sources of evidence:[80]

- Records of suspicious mobile messages blocked by mobile operators.
- Consumer research indicating the proportion of mobile users who reported having received suspicious messages in the three months prior to fieldwork (December 2024 to February 2025).
- Reporting of suspicious messages by mobile users using the 7726 service.

3.19 Operators use firewalls to block scam mobile messages and data from firewalls can therefore provide some useful insights into the possible scale and nature of mobile messaging scams. The data showed that, on average, mobile operators blocked just over 30 million messages per month between May 2024 and March 2025. This blocking increased over the reporting period, reaching over 50 million messages per month in February and March 2025.[81] Mobile UK has reported that mobile operators blocked over 166 million scam messages in the first quarter of 2026.[82] **These results suggest that mobile operators are blocking at least 600 million messages per annum.**

3.20 Evidence from our most recent consumer research, published in March 2026, shows that 40% of UK mobile users reported receiving at least one suspicious text message[83] via their default messaging service in the three months prior to fieldwork,[84] down from 75% in 2021[85] and from 50% in 2025.[86] This fall may reflect improvements in the scam blocking measures deployed by mobile operators, or the declining popularity of mobile messaging, as set out in section 2. However, indicatively, this suggests that in the order of **100 million suspicious messages per annum are getting through to mobile users** - and potentially substantially more.[87]

---

[80] We had asked stakeholders about evidence to inform the types and scale of harms resulting from mobile messaging scams as part of our 2024 call for input, and our 2025 consultation reported on this evidence.
[81] Formal information request responses.
[82] Mobile UK, 2026. Protecting UK Customers From Mobile Fraud – Q1 Update
[83] "Text message" refers to messages received via SMS/RCS and/or iMessage.
[84] Ofcom, 2026. Experiences of suspicious calls, texts and app messages, Q26. Rebased for all mobile users. Fieldwork was conducted in February 2026.
[85] Ofcom, 2021. Scams survey, Q1. Rebased for all mobile users. Respondents were only asked about suspicious "text on [their] mobile" in the previous three months in 2021. Fieldwork was conducted in September 2021.
[86] Ofcom, 2025. Experiences of suspicious calls, texts and app messages, Q26. Rebased for all mobile users. Fieldwork was conducted in February 2025.
[87] If around 22 million people (40% of the UK adult population of 55 million) received at least one suspicious message every three months, this would suggest around 100 million such messages being received per year in the UK. This should be seen as broadly indicative of the magnitude of scam messages getting through to

3.21 The 7726 service allows consumers to report unwanted or suspicious messages or calls received on their mobile devices, which operators can use to monitor scam activity and update their network protections accordingly.[88] **The number of messages reported to mobile operators as suspicious via this service exceeded 100 million** in the year to March 2025.[89] This figure does not include 7726 reporting to thick MVNOs, which accounted for approximately 7% of the UK mobile market in 2025.[90]

Scam mobile messages cause significant levels of harm to UK consumers

3.22 The scale of financial and other harms to UK people and businesses resulting from scam mobile messages is significant. Based on the available evidence on financial harms, we estimate that tens of millions of pounds are lost to messaging scams each year.[91]

3.23 As discussed in paragraphs 3.4 to 3.6, scams can take the form of both APP and unauthorised push payment fraud:

- UK Finance, which represents over 300 banking and finance firms and collects data on fraud from its members, reported an estimated **£1.28 billion in total losses** from fraud in 2025 from authorised and unauthorised scams combined, with broadly similar figures in previous years.[92] Of this, £575 million was authorised and £700 million unauthorised.[93]
- The Payment Systems Regulator (PSR) reported losses from APP scams amounting to **£340 million** in the UK in 2023. Of these, **around £107 million** of losses from scams originated with a voice call or text message (over 27,000 scams, i.e. losses of £4,000 per scam).[94]

customers: on the one hand, not all suspicious messages are scams; on the other hand, survey respondents who recalled receiving suspicious messages may have received more than one such message over the past three months.

[88] The reports can provide insights on the latest scam trends, malicious URLs and telephone numbers, as well as brands being impersonated.

[89] Formal information request responses.

[90] Ofcom 2025 Technology Tracker, Table 49. Market shares of [✂] were summed to ascertain this figure. Note, the figure is likely to be minimally higher than this, as the data in the table does not capture [✂], a thick MVNO. 2025 Technology Tracker - Core Data Tables.

[91] We note that as with the scale of scam activity, the harm from messaging scams is also difficult to estimate with accuracy. Law enforcement bodies collect information on reports of individual fraud cases, but do not currently routinely capture the channels used by scammers to initiate contact. However, the available evidence indicates that messaging scams are a persistent source of significant financial harm to UK consumers.

[92] UK Finance, 2026. Annual Fraud report 2026. Page 11.

[93] Authorised fraud increased from the previous year while unauthorised fraud decreased, but there is not a clear trend up or down for either.

[94] Based on data from the 14 largest banks and other UK payment service providers, all of which are also UK Finance members. Payment Systems Regulator, 2024. Unmasking how fraudsters target UK consumers in the digital age. Pages 4 and 11.

- Based on the UK Finance and PSR figures, combined with Crime Survey of England and Wales (CSEW) data on initial contact methods for scams, we estimate that approximately **£50 million** is lost to messaging scams per annum.[95,96]

3.24 Some survey evidence suggests that the UK may be subject to more harm from fraud than other European countries.[97]

3.25 As we discuss below, some stakeholders who responded to our 2025 consultation agreed with our assessment of the scale of harms from mobile messaging scams, while others suggested that the scale of such harms may be even higher than our estimates.

3.26 Table 3.1 below summarises evidence on harms from scam mobile messages, that we set out at consultation, with updated figures.

Table 3.1: Summary of harms from scam mobile messages

	Estimated scale per annum:
Suspicious messages blocked	At least 600 million
Survey evidence of suspicious messages received	In the order of 100 million (potentially substantially more)
Messages reported to 7726	At least 100 million
Financial harm from APP and unauthorised payment scams	c.£50m
Emotional harm to consumers	Significant - but unquantified
Time and resources to resolve scams for businesses/consumers	
Reputational harm to banks and communications services	
Costs to businesses from reimbursing consumers	

3.27 In our 2025 consultation, we set out our view that, despite industry's work to tackle scam mobile messages, the financial cost to victims remains significant, as indicated by the evidence set out above.

---

[95] UK Finance reports that APP scams account for around 45% of total losses from fraud. If we assume this is true of voice and text scams in particular, we can scale up PSR's reported losses of £107m from voice and text APP scams, to reach an illustrative estimate of total losses from APP and unauthorised scams of around £240m. To isolate total losses from scam messages, we use the ratio of scams originating from calls to texts from the CSEW (we have used this ratio relating to England and Wales as a proxy for the UK, as we do not have data for Scotland and Northern Ireland). In the past three surveys, call scams were larger than text messages by a factor ranging from three to ten. Applying the average ratio from these three years to the £240m figure gives us an estimate of around £50m lost to messaging scams and £200m lost to call scams per year.

[96] The CSEW does not distinguish between SMS and other types of text messaging. Office of National Statistics, 2026. Nature of crime: fraud and computer misuse, Crime Survey for England and Wales, Table 6a.

[97] See for example The Fintech Times, August 2022, The UK Is the Only European Country to Have a Four Figure Average Monthly 'Fraud' Search Volume; and Credit-Connect, June 2021, UK hardest hit European country for online fraud.

3.28 In terms of the non-financial impacts discussed in paragraphs 3.11-3.15, we also set out that we considered the emotional impact on victims to be significant, in line with the impact of fraud more generally.

Stakeholder responses

3.29 Respondents to our consultation broadly agreed with our provisional conclusions on the types and scale of harm that scam messages cause.

a) VodafoneThree said it agreed with our view that mobile messaging scams have wide-ranging effects on UK consumers and businesses, including emotional harm to victims and reputational damage to businesses as well as financial losses.[98]
b) Virgin Media O2 agreed with the types of harm identified in our consultation based on the available evidence.[99]
c) Sky said it agreed with our assessment of the harms caused by telecoms scams and their negative impacts on consumers, businesses and the wider economy, and that the high volume of 7726 reports demonstrate that scam messages are still reaching customers.[100]
d) [✂] agreed with our assessment of the types and scale of harms caused by scam messages.[101]

Types of harm and messaging scams

3.30 Some cited additional types of harm beyond those we had discussed, and others provided examples of specific messaging scams (summarised below).

3.31 Which? stated that being a victim of fraud can lead to physical harm, e.g. nausea and sleep issues.[102] Research cited by Pinnacle Teleservices reported 63% of scam victims feeling stressed by their experience.[103]

3.32 Citizens Advice Scotland noted that some scams appear to target more vulnerable groups specifically, such as older people and those with a disability or health condition.[104] It also reported that many scam messages impersonate organisations that the recipient already deals with, or that are trusted institutions.[105]

3.33 The MEF noted more generally that scam messages are on the rise, and scammers are becoming more sophisticated in adapting tactics to evade the protections in place.[106]

3.34 The Association of British Insurers cited examples of insurance fraud that can occur through mobile messaging (e.g. selling fraudulent insurance policies, resulting in victims driving without a genuine insurance policy). It cited a seven-fold increase in cases of identity theft linked to insurance fraud facilitated by identities stolen over SMS since 2021.[107] Which? also

[98] VodafoneThree response to 2025 Consultation. Page 3.
[99] Virgin Media O2 response to 2025 Consultation. Page 4.
[100] Sky response to 2025 Consultation. Page 2.
[101] Name withheld 1 response to 2025 Consultation. Page 2.
[102] Which? response to 2025 Consultation. Page 2.
[103] Pinnacle Teleservices response to 2025 Consultation. Pages 8-9.
[104] Citizens Advice Scotland response to 2025 Consultation. Page 2.
[105] Citizens Advice Scotland response to 2025 Consultation. Pages 2-3.
[106] MEF response to 2025 Consultation. Page 4.
[107] The Association of British Insurers response to October 2025 Consultation. Pages 1-2.

reported that messaging scams were among the most common scams identified by its Scams Sharer tool, accounting for 20% of all reports.[108]

Scale of harm

3.35 Stakeholders broadly agreed with our conclusions on the scale of harm, but some submitted that the magnitude of harm was greater than in our assessment and that data limitations prevent establishing the true scale.

3.36 Some stakeholders cited estimates of greater financial losses than UK Finance's estimate of the total cost of fraud in 2024 (£1.17 billion), which we noted in the consultation. For example, the survey-based research highlighted by Pinnacle Teleservices found that victims reported £9.4 billion lost to scams in the UK in a 12-month period.[109] [✂] cited a Home Office estimate of the total cost of fraud to individuals of £6.8bn in 2019/20. It also noted that funds obtained through scams may help finance other criminal activity, further amplifying the societal harm these messages cause.[110]

3.37 Which? stated that we had underestimated the emotional impact of scams, which it considers to be greater than the financial impact. It considered that the impacts of scams have long been underestimated, citing its 2023 research that found scam victims to have lower levels of life satisfaction and happiness and higher levels of anxiety, leading to an estimated total loss in wellbeing equivalent to £9.3bn per year.[111]

3.38 Some stakeholders highlighted that data limitations make it difficult to confirm the scale of messaging scams. [✂].[112] Stour Marine said that more evidence would be needed in order to agree with our conclusion that significant numbers of scam messages continue to reach end-users.[113,114] techUK also noted that evidence from consumer reporting and surveys is incomplete, stating that only 14% of victims report fraud.[115]

3.39 Consumer Scotland requested that we capture any available data on the money lost to messaging scams and number of reported incidents in Scotland, as it said we only cite data for England and Wales.[116]

3.40 Stour Marine encouraged us to strengthen the evidence base on downstream harm attribution, particularly where messaging is one step in a multi-channel scam, to help ensure regulatory measures remain targeted at the most effective intervention points.

3.41 Finally, some stakeholders considered that we should assess harm caused by scam messaging in the round, including for example iMessage, WhatsApp and RCS, instead of focusing solely on SMS and MMS channels.[117]

---

[108] As set out by Which? in their response to our 2025 Consultation (page 3) this refers to reports which were defined as 'text scams' by the person submitting the report.
[109] Pinnacle Teleservices response to 2025 Consultation. Pages 8-9.
[110] [✂] response to 2025 Consultation.
[111] Which? response to 2025 Consultation. Page 2.
[112] [✂] response to 2025 Consultation.
[113] It stated the 7726 data we used to support our conclusion hasn't been made available (and is known to contain reports that are not of scam messages); and the small sample of 4000 messages that we assessed may not be representative.
[114] Stour Marine response to October 2025 Consultation. Pages 2-3.
[115] techUK response to 2025 Consultation. Page 1.
[116] Consumer Scotland response to 2025 Consultation. Page 2.
[117] Utility Warehouse response to 2025 Consultation. Page 2; VodafoneThree response to 2025 Consultation. Page 3.

Our assessment

Types of harm and messaging scams

3.42 We welcome the additional insights offered by stakeholders, including consumer groups with expertise in this area. We agree that the harms caused by scam messaging can be wide-ranging in nature and are not limited to direct financial costs.

3.43 We also acknowledge stakeholders' observations about scammers' evolving tactics. We consider these responses support our analysis above that scammers are adopting a wide variety of approaches to scam messages.

Scale of harm

3.44 We note there are a range of estimates of the financial harm caused by scams, which vary depending on the scope and methodology applied. Available estimates indicate that total fraud losses are very high. UK Finance estimated the direct impact to be £1.28bn in 2025, based on data reported to it by financial institutions. The Home Office report cited by [✂], which is based on survey data for England and Wales, estimated total economic and social losses of £6.8bn, of which c.£3.1bn is estimated to be the direct cost from financial losses.[118,119] Based on these estimates, we consider financial losses from fraud to be in the order of billions of pounds per annum.

3.45 We welcome the submissions by Which? identifying the wider impacts of scam messages. We agree that there are significant indirect and social impacts; even though we cannot quantify the scale of these harms with confidence, we have taken these impacts into account in our assessment above.

3.46 We also note the concerns raised by stakeholders regarding data limitations, including the inherent challenges that affect data relying on consumer reporting. We agree that there are significant data limitations in measuring the scale of messaging scams and their harm, which is why we consider a range of evidence sources in our analysis.

3.47 In response to Consumer Scotland's concern that our data relates to England and Wales only, we note that our estimated scale of harm from scam messages is for the whole of the UK. We have used data from the Crime Survey for England and Wales as a proxy for the ratio of scams originating from calls to texts in the UK (which is an input into our calculations), and we expect this ratio to be similar across Scotland, Northern Ireland, England and Wales. We are not aware of robust estimates of the total harm caused by messaging scams in Scotland. However, while not specific to mobile messaging scams, we note that the Scottish Crime and Justice Survey reported an increase in the incidence of fraud between 2023/24 and 2024/25.[120]

3.48 We note stakeholders' arguments that we should assess harm caused by scam messaging in the round. However, the measures we are imposing apply to services that are regulated under the Communications Act only. Therefore, we have only estimated the harm caused by scams on these channels in this document.

---

[118] We note that the estimate cited by [✂] is based on data from 2019/20, and relates to England and Wales only.

[119] Fraud Strategy: stopping scams and protecting the public (accessible) - GOV.UK, Annex 3: Cost of fraud methodology.

[120] It reported an increase in the proportion of adults in Scotland experiencing fraud from 8.3% in 2023/24 to 9.9% in 2024/25.

Our Conclusion

3.49 Overall, we remain of the view that messaging scams give rise to significant harm. We consider that the evidence summarised in Table 3.1 provides an indicative picture of the scale of harm in the UK. While there is uncertainty around the precise scale, the available evidence consistently indicates that both financial and non-financial harms are substantial.

4. The case for further intervention to combat scam mobile messages

Introduction

4.1 In section 3, we set out the significant harm that arises from scam mobile messages. In this section, we evaluate the impact of:

- Ofcom's existing rules, guidance and enforcement powers that help to combat scam mobile messages.
- Industry measures to prevent scams on P2P channels.
- Industry measures to prevent scams on A2P channels.
- Government's interventions to combat scams.
- The work of law enforcement and other agencies.

4.2 In response to our 2025 consultation, most stakeholders agreed with both our assessment of the impact of existing measures and our provisional conclusion that further intervention is necessary to meet our policy objective. These stakeholder responses, and our assessment, are set out at the end of this section.

4.3 We therefore conclude that existing measures to combat scam mobile messages are insufficient to address harm from scam mobile messages and that further intervention is required.

Our existing rules, guidance and enforcement powers

4.4 We have already put in place rules and guidance relating to the use of telephone numbers, which we can use to act against scammers or providers that are responsible for letting scam messages reach people and businesses. For example:

- GC B1.6 explains that providers must ensure numbers they have been allocated by Ofcom are used effectively and efficiently. The misuse of numbers, for example to facilitate scams, is not an effective and efficient use of numbers.
- GC B1.8 explains that providers must take reasonably practicable steps to ensure their customers comply with GC B1 (including B1.6) when using numbers.[121]

4.5 These rules enable Ofcom to take enforcement action against a communications provider (as defined in the GCs)[122] that we do not consider has taken reasonable steps to prevent

[121] Similarly, GC B1.9 explains that providers must not transfer numbers unless certain conditions are met, including ensuring telephone numbers are used effectively and efficiently.
[122] 'Communications Provider' is defined in our GCs as "a person who (within the meaning of section 32(4) of the Act) provides an Electronic Communications Network or an Electronic Communications Service".

scams originating on numbers they have been allocated (including where a customer is using the provider's numbers for scams).[123]

4.6 In 2022, Ofcom published a good practice guide (the Guide) to clarify the steps we expect providers to take to comply with GCs B1.6 and B1.8 and B1.9 and help prevent misuse of sub-allocated and assigned numbers (including for scams).[124] These steps include:

- Undertaking due diligence checks before sub-allocating or assigning numbers to business customers, including: KYC checks; making enquiries about the intended use of the numbers; and assessing the risk of misuse.
- Monitoring for potential misuse of numbers and regularly reassessing the risk of misuse once numbers are transferred.
- Investigating incidents of suspected misuse (such as reports of scams) and taking action to prevent further misuse, including, where appropriate: applying temporary blocks to numbers or customer accounts; suspending services; and requiring urgent action from the customer through contractual controls.
- Ensuring that the measures applied reflect the risk of misuse associated with the intended use of the numbers.

4.7 We have various enforcement powers we may use in the event we find a breach of our GCs, including: imposing a financial penalty; suspending a provider's entitlement to provide an electronic communications network or service; or withdrawing numbers.[125]

4.8 We also have enforcement powers under section 128 of the Act to take action against any person who persistently misuses an electronic communications network or services (even if they are not considered a communications provider).[126]

Messaging scams persist despite existing rules and enforcement powers

4.9 Our existing GCs were established with the broad objective of ensuring the effective and efficient use of numbers (which includes ensuring that numbers are not misused for scams). They apply to numbers used for both calls and mobile messages and afford providers with flexibility on how to ensure compliance.

4.10 We consider that our existing GCs have created friction in the supply chain for scammers: for example, by requiring providers to take reasonable steps to prevent scammers using their numbers.

---

[123] We could also potentially take action against providers under GCs B1.2 or B1.3. GC B1.2 explains that providers can only use numbers they have been directly allocated by Ofcom or authorised to use by another provider. We could therefore potentially take action against a provider that has spoofed the number of a legitimate business (i.e. a number they are not authorised to use). GC B1.3 explains that providers can only use numbers that have been allocated by Ofcom. We could therefore potentially take action against a provider that has spoofed or used an unallocated number.

[124] Ofcom, 2022. Good practice guide to help prevent misuse of sub-allocated and assigned numbers. The Guide clarified how providers are expected to comply with GCs B1.6, B1.8 and B1.9.

[125] Ofcom has powers to withdraw numbers under 61(1) of the Act, including when withdrawal is in accordance with GC B1.18(d) or (e).

[126] In this context, persistent misuse means using that network or service to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety, or using it to engage in conduct the effect or likely effect of which is to cause another person unnecessarily to suffer annoyance, inconvenience or anxiety. Further detail is set out in Annex 5. Paragraphs 1.19-1.20 of our Persistent Misuse Statement also discuss the persons against whom we may enforce.

4.11 However, as set out in sections 2 and 3, scammers will take advantage of any weaknesses in the value chain, while messaging scams continue to drive significant harm. We explain in paragraphs 4.18-4.58, below, how providers' existing measures to tackle P2P and A2P scam messages vary significantly.

4.12 This variability could result in part from the flexibility the GCs afford to providers. For example, our analysis of responses to formal information requests sent to providers in 2024 and 2025 showed that most providers did not report that blocking numbers was an important part of their counter-scam measures (while evidence shows that this is a highly effective way to stop scam messages).[127] In this context, scammers exploit gaps left by providers that have less effective policies, systems and processes in place.

4.13 Our existing GCs do not include specific requirements relating to mobile messaging, nor do they include requirements aimed specifically at preventing mobile messaging scams.[128] In particular, there are no specific requirements for how providers should seek to identify and prevent scam messages from being sent and/or received, nor any rules targeted at addressing harms from P2P or A2P messages (or which refer to the role of aggregators).

4.14 Many of our existing GCs (and the Guide) are also focused on requiring providers to take steps in relation to numbers they have been allocated or in relation to their own customers. They do not require providers to take a more comprehensive approach by preventing scam messages from reaching the customers of other providers.

4.15 While we could potentially use our powers under section 128 of the Act to enforce against individual scammers for the persistent misuse of services or networks, scammers often use PAYG SIMs and can be difficult to identify and enforce against. It may also not be appropriate to use our powers to act against a provider over whose network or service the persistent misuse takes place.[129]

4.16 In this context, we therefore consider that more targeted obligations are needed to drive industry to consistently adopt measures necessary to effectively tackle scam messages. We assess that it is likely that rules adapted to combatting scam messages that clearly identify the steps different types of providers should take to tackle the problem, will be effective in addressing mobile messaging scams in ways that existing measures cannot (we discuss these benefits further in sections 5-8). Following our 2025 consultation, our view is that the specific rules we are implementing will ensure providers take a more comprehensive approach to preventing scam messages.

4.17 Overall, having used the evidence gathered from our consultation to reach our conclusion, we consider that relying on our powers to enforce existing rules in the GCs (or section 128 of the Act) is not sufficient to address the harms identified and will not enable us to meet our objective to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages. On this basis, it is our view that further action is necessary to address scammers' ability to access and use both P2P and A2P channels.

---

[127] Formal information request responses.

[128] We note that, while the Guide explains what is expected of providers in terms of KYC checks, ongoing due diligence and responding to incidents, this applies to sub-allocating and assigning numbers, rather than the provision of mobile messaging.

[129] Ofcom, 2016. Persistent Misuse Statement, paragraph 1.20.

Industry measures to prevent scams on P2P channels

4.18 Mobile operators are already implementing measures to combat scam P2P messages: primarily volume limits and blocking tools. We explore these below.

4.19 However, for the reasons we set out below, we consider that these are unlikely to adequately reduce the flow of scam messages to consumers and thus meet our objective in relation to the P2P channel.

Setting volume limits

4.20 Many mobile operators set volume limits on the number of messages that SIMs can send (or the number of unique recipients that it can reach) over a specified period. Volume limits can disrupt scammers' ability to use SIMs (typically in SIM farms) to send large volumes of P2P messages. They do this by forcing scammers to acquire more SIMs, and potentially more SIM farm capacity, to send the same number of messages as they would be able to send without limits in place. By limiting the number of messages that can be sent from a SIM, volume limits reduce the number of potential victims that might receive or respond to scam mobile messages.[130]

4.21 Most mobile operators in the UK set volume limits on some or all of their voice, messages and/or data services to prevent their misuse. However, some providers do not appear to have implemented any volume limits on products they offer and have not indicated any plans to do so.

4.22 Where providers set volume limits, their application varies in a number of ways, including:

- Their levels: message limits are generally applied on an hourly, daily or monthly basis, ranging from approximately 100 messages per hour to tens of thousands over a month. Some providers use a combination of daily and monthly limits and, in certain cases, providers impose limits temporarily at the start of a contract.[131]
- How they are enforced: when limits are reached, some providers have systems in place to ensure that their users cannot send any further messages. Others may not have systems in place to ensure that limits are applied in real time and are instead subject to a manual investigation to determine if scam activity is taking place. In the meantime, users may be able to continue to send messages.

4.23 Providers' application of volume limits is inconsistent.[132] For instance, some mobile operators:

- Do not set limits at all.[133]
- Do have limits but set them at a very high level.[134]
- Reset them at short intervals.[135]

[130] They can also function to prevent misuse of the network (including to prevent fraud against mobile operator) and safeguard legitimate P2P messaging.
[131] Formal information request responses.
[132] Ofcom analysis, including from formal information request responses.
[133] [✂]
[134] [✂]
[135] [✂]

- Do not enforce their limits in an effective way.[136]

4.24 The issues we identified included: technological shortcomings that impact mobile operators' ability to enforce limits within the timeframe set by a policy; and time lags in enforcing limits. These inconsistencies mean that some policies are not effective on their own terms and create opportunities that scammers can exploit.

Blocking numbers used by scammers and blocking scam messages in transit

4.25 Mobile operators can deploy measures to identify and block suspicious messages in transit (i.e. messages being conveyed between source and destination) before they are delivered to consumers. These measures can vary in sophistication, but some of the more advanced tools have the capability to search messages automatically, on the basis of:

- Content that indicates a scam message (including phrases and embedded telephone numbers or URLs).
- The sender's telephone number (e.g. to identify messages from numbers reported to be sending scam messages).
- Volumes and patterns of traffic (e.g. to identify very high volumes of messages sent from newly activated SIMs, which could indicate scam activity).

4.26 Both originating and terminating providers can apply these blocking tools to messages that their networks are carrying and providers can apply them to both P2P and A2P channels. They can be used to block messages or to apply warning labels to them.

4.27 In the UK, MNOs that use blocking tools do so on a voluntary basis.[137] Each MNO has its own policies on how they implement blocking tools, such as whether they are applied to all SMS traffic or just a subset. MNOs also apply blocking tools to the messaging traffic that transits across their partner thin MVNOs.

4.28 Blocking tools have had a significant impact. As set out in paragraph 3.19, on average, mobile networks blocked just over 30 million messages per month between May 2024 and March 2025. Blocking increased over this period, reaching over 50 million messages per month in February and March 2025.[138]

4.29 However, the deployment of blocking tools is inconsistent. First, not all mobile operators use them: we are aware of at least one MVNO that does not use any form of blocking tool, potentially allowing scam messages to enter and originate from its network.[139]

4.30 Second, some MVNOs may only have blocking tools with limited functionality that are not as effective or automated as they could be in blocking scam messages.[140] We consider providers' inconsistent use of these tools in relation to A2P traffic, below.

4.31 Despite significant efforts by many mobile operators to develop and implement these blocking tools, consumers are still receiving a high volume of scam messages (see paragraph 3.20 for our indicative estimate that around 100 million suspicious messages reach mobile users annually). This is in part because blocking tools, like all scam prevention measures, will never be 100% effective.

---

[136] [✂]
[137] [✂]
[138] Formal information request responses.
[139] [✂]
[140] We are aware of one such MVNO which appears to have a lower blocking rate than is typical of the MNOs.

4.32 However, through responses to our consultation and informal engagement with industry, we are not aware of concrete plans to address gaps and inconsistencies in the use of blocking tools voluntarily. We expect the current limitations in deployment and functionality to persist, meaning a voluntary approach is insufficient to significantly reduce the flow of scam messages to consumers.

Industry measures to prevent scams on A2P channels

4.33 Mobile operators and aggregators have also implemented measures to combat scam messages sent over A2P channels. These include up-front KYC, ongoing Know Your Traffic (KYT) checks, measures around the use of sender IDs, contractual terms and sanctions, as well as the use of blocking tools. However, for the reasons we set out below, we consider that these are also unlikely to sufficiently reduce the flow of scam messages to consumers and thus meet our objective in relation to the A2P channel.

Conducting initial KYC checks on business senders

4.34 Companies may perform KYC checks to verify a customer's identity, their business and financial activities and any risk they may pose. In the A2P sector, aggregators conduct KYC checks to confirm the legitimacy of a business sender at the point that they sign up to use their services. Measures vary across the sector but typically include examining proof of identity and company registrations, ensuring that these match with other details provided.

4.35 Many tier 1 aggregators conduct some forms of KYC checks.[141] Some of these include email or telephone number validation checks and checks to determine whether the IP address the customer used to sign up matches the location in which they want to send messages.[142]

4.36 However, not all aggregators are applying strong KYC checks:

- Tier 1 aggregators have widely different KYC processes, with some performing significantly more upfront checks than others.
- Aggregators are not consistently applying best practices, in part because there is no common baseline.
- Typically, mobile operators and aggregators do not specifically require downstream aggregators to perform KYC checks on business senders. They are also not informed about the policies those aggregators use when accepting new senders.

4.37 We believe many aggregators (in particular lower-tier aggregators) are not conducting effective KYC checks consistently. In response to our 2024 call for input, several respondents said that harmonising the level of KYC and due diligence that the industry undertakes for the purposes of combatting A2P scam messages should be a priority.[143]

---

[141] As explained in section 2, we define aggregators as tier 1 when they operate with a direct contractual relationship with a mobile operator to purchase message termination, tier 2 if they contract with a tier 1 aggregator, and so on. Mobile operators do not generally accept A2P traffic directly and therefore do not routinely engage directly with business senders or conduct KYC checks.

[142] Some aggregators use third-party systems whereas others use their own processes, and these can include automated and manual processes.

[143] BT Group response to 2024 Call for Input. Page 4; Vodafone response to 2024 Call for Input. Page 7; MEF response to 2024 Call for Input. Page 13; The Campaign Registry response to 2024 Call for Input. Page 12; iconectiv UK response to 2024 Call for Input; Page 4; Twilio response to 2024 Call for Input. Page 8; Individual responses to 2024 call for input.

4.38 We consider that the absence of effective and consistent baseline checks has enabled many scammers to access A2P messaging services. Because of the inconsistency identified above, we do not consider that relying on individual firms' current KYC policies is sufficient to achieve our objective. This is particularly important because the complex and opaque nature of A2P supply chains, as described in section 2, may allow scammers to shop around and use companies with limited or no KYC checks to gain an entry point to A2P messaging networks.

Preventing the use of fake alphanumeric sender IDs

4.39 Many mobile operators and aggregators maintain lists of protected alphanumeric sender IDs to prevent scammers from spoofing them. Some lists serve primarily to protect mobile operators and aggregators' own brands and include the alphanumeric sender IDs that they use to contact their customers. Other mobile operators and aggregators maintain broader lists that include sender IDs associated with other companies at high risk of impersonation, such as banks and delivery companies.

4.40 Mobile operators and aggregators may use other controls, including blocklists, to prevent the use of generic sender IDs (such as 'Customer service') and restrict the use of special characters to prevent close imitation of genuine brands (for example, 'Ofcom' could be imitated as '0fcom').

4.41 The MEF operates a cross-sector sender ID registry, which brands can pay to join. It reports that it has registered over 700 trusted sender IDs and a blocklist of over 3,750 unauthorised sender ID variants.[144] Our analysis suggests that these measures are having an impact in protecting listed brand names.[145]

4.42 However, from reviewing evidence provided by stakeholders through our consultation and information requests, existing industry efforts relating to sender IDs are not consistent and this leaves them open to abuse by scammers. We note that scammers are sending messages bearing fabricated or obscure business names as alphanumeric sender IDs (these IDs appeared next to most of the A2P scam messages in a sample of end-user scam reports we analysed in 2025[146]). This suggests that existing KYC and dedicated sender ID measures are often not picking up scammers' activities.

Conducting ongoing KYT checks on A2P traffic and business senders

4.43 Many mobile operators and aggregators conduct ongoing KYT checks on A2P traffic and user profiles. Companies use a range of checks to identify potentially suspicious traffic: both traffic that originates from message senders that they contract with and traffic that flows through their networks from other aggregators. Some of the most common scam indicators[147] that industry uses are:

---

[144] MEF, SMS Sender ID Protection Registry.

[145] Based on analysis of a of sample SMS messages with alphanumeric sender IDs reported to 7726. A minority (30%) of those appeared to be a fraudulent attempt to impersonate a real brand.

[146] Our analysis of a sample of 4,000 7726 reports found that of these 137 SMS were both scam messages and using an alphanumeric sender ID. Of these, we determined that around 65% were using fabricated or obscure business names, which did not appear to be associated with a real company, suggesting that criminals are exploiting loose controls on the provision of alphanumeric ID.

[147] Other indicators that some aggregators monitor include: regular reviews of the most-used sender IDs; monitoring for international senders; monitoring consumer complaints; and conducting spot checks. These factors are in some cases blended to create a risk profile. As set out at paragraphs 4.53-56, some mobile

- Significant changes in volume patterns.
- Use of new alphanumeric sender IDs.
- The purchase of virtual long numbers from which to send messages.[148]
- Other changes to account details or status (such as a change in billing address or upgrading an account).
- Reports from other parties in their supply chain about scam traffic.

4.44 KYT checks are an important safeguard, because even if providers implement KYC checks effectively across the A2P supply chain, some scammers may still find ways to access A2P channels.[149] However, although some providers are conducting a range of the KYT checks, industry's current application of these checks is inconsistent.

4.45 Further, the characteristics of the supply chain mean that companies can check only a limited number of useful scam indicators where messages originate more than one step downstream of them in the supply chain. For example, where traffic originates from an aggregator, the aggregation process means that a mobile operator may not be able to access information important to performing KTY checks for a given sender's account, unless they have requisite contractual agreements in place.

4.46 These factors mean that scammers who gain access to A2P messaging services can find channels where they can evade detection. The length and opacity of the A2P supply chain means that it is particularly important that firms perform effective KYT consistently and across the whole supply chain, especially by the firm that originates the traffic.

Contractual requirements and codes of practice

4.47 Most mobile operators and many tier 1 aggregators have contractual terms in place with downstream aggregators that aim to prohibit downstream aggregators from passing on harmful or illegal messages.[150] These terms vary in function but generally give mobile operators and aggregators the option to suspend services where fraudulent messages are later identified.

4.48 In addition, some mobile operators set out dedicated anti-fraud codes of practice for downstream aggregators.[151] These contractual codes go further than most other commercial agreements: including, for example, by setting specific due diligence requirements and obligations to pass requirements on to downstream aggregators. As such, they can address the opacity of the supply chains that support A2P channels and corresponding challenges in enforcing good practice.

4.49 The MEF also maintains a self-regulatory Business SMS Code of Conduct.[152] This provides guidance to mobile operators and aggregators on monitoring their networks for suspicious

---

operators and aggregators are conducting further checks, or blocking or otherwise sanctioning users, as a result of KYT monitoring. This is based on formal information responses.

[148] Virtual long numbers are telephone numbers, provided by aggregators, from which A2P customers can send and sometimes receive messages.

[149] This could include, for example, using fake IDs to bypass KYC or hijacking legitimate existing business accounts.

[150] Formal information request responses.

[151] Formal information request responses. As of March 2025, at least one other mobile operator had been planning to introduce a new A2P Code.

[152] MEF, Trust in Enterprise Messaging Code of Conduct.

activity, investigating incidents and securing user accounts. It also prohibits the misuse of unlicensed short codes[153] or alphanumeric sender IDs for termination and the manipulation of Global Titles.[154]

4.50 Contractual requirements and codes can be an important means to incentivise good practice. A small number of mobile operators have sophisticated agreements in place to tackle mobile messaging scams. Overall, however, most existing contractual provisions are limited to setting a generic prohibition on harmful or illegal messages.[155] Typically, they do not set out detailed expectations for downstream aggregators on what they should be doing to prevent scams, nor do they provide a clear framework for engagement between firms when incidents occur.

4.51 As discussed in section 2, the complexity of supply chains in the A2P market means that, even though many organisations have introduced measures to block scammers from accessing networks and to identify suspicious activity, they cannot be fully effective while scammers are able to find companies that will accept their messages.

4.52 Further, where companies do not have direct relationships with business senders, they do not have direct sight of KYC checks or KYT information in relation to patterns from individual business senders. Where they do not pass down and monitor compliance, lower-tier aggregators may not implement KYC and KYT checks, which provides an access point to A2P messaging for scammers. Additionally, while voluntary industry codes can help promote good practice, only a proportion of providers operating in the A2P supply chain overall have signed up to codes like the MEF's.[156]

Imposing sanctions to ensure compliance throughout the supply chain

4.53 When fraudulent traffic is identified, some mobile operators and aggregators have formal processes in place to block criminals from using A2P messaging and to escalate compliance issues with any downstream aggregators that have been responsible for passing on the traffic.

4.54 We observe that many tier 1 aggregators routinely issue suspensions against suspected criminal business message senders that they contract with directly.[157] This usually involves suspending an online account or access to APIs.

4.55 A small number of mobile operators have issued sanctions against tier 1 aggregators for delivering fraudulent traffic between February 2024 and February 2025, primarily those mobile operators that have dedicated codes for their aggregator partners.[158] Further, a

[153] Some organisations use short codes to send A2P messages. These are usually five to six digits (e.g. 12345).
[154] Global Titles are numbers created from ranges of mobile numbers we allocate to mobile operators. Operators use Global Titles as a routing address for the exchange of signalling messages with other mobile networks and to support their provision of mobile services.
[155] Formal information request responses.
[156] Some but not all aggregators have signed up. Sanctions set out in the code are the withdrawal of the Trust in Enterprise Messaging Badge and/or sharing a written report with regulators and law enforcement bodies. The code includes requirements, for example, that message providers detect, report and block traffic, if needed, based on suspicious traffic patterns, such as unusual volumes or suspicious traffic origin or content.
[157] Formal information request responses.
[158] Three out of nine mobile operators that we gathered information from have issued sanctions to aggregators in the year period, including fines, suspensions and termination of service against tier 1 aggregators. Others told us that they manage fraud cases collaboratively or have not identified issues.

number of tier 1 aggregators have issued sanctions against aggregators by passing on fines they received from mobile operators where contractual provisions have been in place.

4.56 Overall, despite some evidence that codes of practice can help to improve tier 1 aggregators' KYC and KYT activity, our 2025 formal information requests revealed that most mobile operators and aggregators had not issued sanctions against downstream aggregators in the past year.[159] Given the large number of scam A2P messages that consumers are receiving, we do not consider that industry sanctions create sufficient incentives for aggregators to conduct effective due diligence.[160]

Blocking scam messages in transit

4.57 As described in the P2P section above, providers can apply blocking tools to mobile messaging traffic. Currently many mobile operators and aggregators apply blocking tools to A2P traffic. However, some mobile operators do not currently apply their blocking tools to A2P traffic and some aggregators do not use blocking tools. Where companies do use blocking tools, they vary in their capabilities and sophistication.

4.58 For some mobile operators, the decision not to apply these tools to A2P traffic means millions of messages reach customers without any checks.[161] Not only does this leave the MNOs' own customers vulnerable to scams but it exposes the customers of associated thin MVNOs that rely on the MNO's network infrastructure to perform any blocking functions.

Government's interventions

4.59 In developing our proposals, we engaged with Government on its ongoing work to prevent fraud and scams. As set out in section 2, its Fraud Strategy 2026 to 2029 sets out how robust regulation will help ensure the industry is accountable for further tackling fraud.

Voluntary industry measures

4.60 Government have also published a new Fraud Sector Charter containing commitments by the telecoms sector. The Charter includes commitments to "Secure Network Originated SMS as a Trusted Channel".

4.61 We welcome the progress made through the Government's Fraud Strategy and Telecommunications Fraud Sector Charter. However, we note that not all relevant parties have signed up to the Charter's commitments. On this basis and that evidence set out in section 3 shows that mobile messaging scams continue to cause significant harm, we therefore consider that further intervention is necessary to meet our objective.

The work of law enforcement and other agencies

4.62 Sending messages with the intention to defraud mobile users is already a criminal offence in the UK under the Fraud Act 2006. Law enforcement and intelligence agencies - such as the police, the National Crime Agency and the National Cyber Security Centre - are working

[159] Formal information request responses.
[160] We note for example that some aggregators have been sanctioned multiple times by certain mobile operators but never by others that they contract with.
[161] Formal information request responses.

to tackle criminals exploiting mobile messaging services and other channels.[162] Prosecutions and enforcement work are essential to deter and stop individual scammers.

4.63 Following the passage of the Crime and Policing Act into law (it received Royal Assent in April 2026),[163] the possession or supply of SIM farms without a legitimate reason is illegal. Law enforcement can issue unlimited fines in England and Wales and £5,000 fines in Scotland and Northern Ireland.[164] Law enforcement's additional powers to tackle scammers using SIM farms, such as the introduction of fines, should act as a stronger deterrent to scammers sending scam P2P messages at scale.

4.64 However, we consider it is unlikely that this measure alone can negate the impact of scammers' use of SIM farms on consumers entirely: for example, because the Act's provisions will apply in the UK only.

4.65 Therefore, despite the significant and widespread work conducted by law enforcement, the evidence set out in section 3 shows that mobile messaging scams continue to cause significant harm. We consider that using our regulatory powers to impose requirements that prevent scams before they occur, and enforcing these rules, is an important complement to law enforcement's work and necessary to meet our objective.

Stakeholder responses

Stakeholder responses to our assessment of existing measures

4.66 In our consultation, we asked stakeholders if they agreed with our assessment of the extent and effectiveness of existing measures to combat scam mobile messages. There was general agreement with our assessment.

4.67 A number of respondents broadly agreed with our conclusion that current measures are often applied inconsistently across the industry, limiting their overall effectiveness.[165]

4.68 However, a number of respondents highlighted the effectiveness of measures already taken by industry in tackling scam messages.[166] VodafoneThree recognised the extensive efforts MNOs take to monitor and filter mobile messaging scams.[167] It stated that effective firewall deployment resulted in messaging scams from their SIMs falling from 1.4m to 20k per day. Mobile UK welcomed Ofcom's recognition of the steps mobile operators have taken to reduce messaging scams, reporting that more than 1.4 billion scam messages were blocked by mobile operators in 2025.[168]

---

[162] In addition, industry bodies such as the Cyber Defence Alliance are working closely with law enforcement and other agencies to tackle messaging scams.
[163] Home Office, 2026. Crime and Policing Act 2026.
[164] Home Office, 2025. Major step for fraud prevention with landmark ban on SIM farms.
[165] Twilio response to October 2025 Consultation. Page 5; Name withheld 1 response to October 2025 Consultation. Page 1; XConnect response to October 2025 Consultation. Page 1; Which? response to October 2025 Consultation. Page 3; Stour Marine response to October 2025 Consultation. Page 2; [✂] response to October 2025 Consultation; VodafoneThree response to October 2025 Consultation. Page 3; iconectiv UK response to October 2025 Consultation. Page 2; MEF response to October 2025 Consultation. Page 4; Pinnacle Teleservices response to October 2025 Consultation. Pages 4-5.
[166] Utility Warehouse response to October 2025 Consultation. Page 2; Virgin Media O2 response to October 2025 Consultation. Page 4; Citizens Advice Scotland response to October 2025 Consultation. Page 3; [✂] response to October 2025 Consultation; Stour Marine response to October 2025 Consultation. Pages 1-2.
[167] VodafoneThree response to October 2025 Consultation. Page 3.
[168] Mobile UK response to October 2025 Consultation. Page 1.

4.69 [✂] considered that our consultation did not fully account for the effectiveness of the current anti-fraud ecosystem. It stated that industry measures, such as KYC checks and using filtering and monitoring to block fraudulent messages, are already effective.[169]

4.70 On the other hand, respondents also agreed that existing measures do not cover the full supply chain or lifecycle of scam activity, meaning that bad actors can exploit gaps or target the weakest point in the chain.[170] Stour and Pinnacle Teleservices noted that existing measures have not kept pace with the scale and adaptability of scam campaigns.[171] Others considered that more consistent and proactive approaches are needed for A2P messages, specifically.[172]

4.71 Respondents highlighted the importance of taking a joined-up approach to tackling fraud, including improved collaboration across industry and internationally.[173]

Stakeholder responses on whether further intervention is needed

4.72 In our consultation, we also asked stakeholders if they agreed with our provisional conclusion on the case for further intervention to combat scam messages. Respondents broadly agreed with our position that further intervention was needed to achieve our policy objective.

4.73 A number of stakeholders agreed that consistent adoption of scam prevention measures across industry is needed to fill gaps that can be exploited by scammers.[174]

4.74 Twilio noted that establishing baseline standards prevents creating a disadvantage for responsible providers and improves trust and stability for A2P messaging.[175] However, the MEF and VodafoneThree stated that our proposals should apply more broadly to all messaging platforms to be effective, which they considered would prevent an uneven playing field (which could emerge if messaging channels like app-based business messaging are out of scope of the rules).[176]

---

[169] [✂] response to October 2025 Consultation.

[170] iconectiv UK response to October 2025 Consultation. Page 2; Twilio response to October 2025 Consultation. Page 5.

[171] Stour Marine response to October 2025 Consultation. Page 1; Pinnacle Teleservices response to October 2025 Consultation. Page 4.

[172] The Campaign Registry response to October 2025 Consultation. Page 4; UKCTA response to October 2025 Consultation. Page 2; VodafoneThree response to October 2025 Consultation. Page 3; Sky response to October 2025 Consultation. Page 2.

[173] The Association of British Insurers response to October 2025 Consultation. Page 3; techUK response to October 2025 Consultation. Page 1; BT Group response to October 2025 Consultation. Page 2; Pinnacle Teleservices response to October 2025 Consultation. Page 5; techUK response to October 2025 Consultation. Page 2; iconectiv UK response to October 2025 Consultation. Page 2.

[174] Twilio response to October 2025 Consultation. Page 5; Stour Marine response to October 2025 Consultation. Page 2; Consumer Scotland response to October 2025 Consultation. Page 1; Which? response to October 2025 Consultation. Pages 3-4; [✂] response to October 2025 Consultation; [✂] response to October 2025 Consultation; iconectiv UK response to October 2025 Consultation. Page 3; The Campaign Registry response to October 2025 Consultation. Page 5; Utility Warehouse response to October 2025 Consultation. Pages 2-3; CCUK response to October 2025 Consultation. Page 3; techUK response to October 2025 Consultation. Page 2; Virgin Media O2 response to October 2025 Consultation. Page 4.

[175] Twilio response to October 2025 Consultation. Page 5.

[176] MEF response to October 2025 Consultation. Page 4; VodafoneThree response to October 2025 Consultation. Page 4.

4.75 One stakeholder disagreed with our conclusion that further intervention is required and considered our proposals to be duplicative of measures already in place by industry and overly prescriptive.[177]

4.76 Other respondents noted that further intervention needs to be proportionate to avoid unintended consequences and undue burden on businesses.[178]

Our final assessment

4.77 Having considered stakeholder responses, we have decided that it is unlikely that existing measures will be sufficiently effective and further action is necessary to tackle scam messages.

4.78 We recognise the current role of industry, Government and law enforcement in driving forward existing measures and interventions to prevent scam messages. However, despite the friction that this causes, as set out in section 3, we consider that messaging scams continue to cause significant harm as scammers can exploit weaknesses caused by inconsistent application across industry. This is supported by some of the evidence from stakeholders set out above, which indicates that although measures implemented by industry exist and can be effective, without addressing the industry wide inconsistencies identified, mobile users will continue to receive high volumes of scam messages.

4.79 We consider that existing GCs (or section 128 of the Act) are not sufficient and further action is necessary to address scammers' ability to access and use both P2P and A2P channels. We recognise the need to tackle scams across all communications channels and note that the challenges differ between these channels. We have set out our approach to combatting fraud on online services in section 2.

4.80 We conclude that it is necessary to introduce rules to combat mobile messaging scams and establish a consistent standard across all providers. While we recognise effective measures that are already in place in parts of the industry create friction for scammers, inconsistent application creates gaps which can be exploited. Therefore, introducing requirements will help close these gaps across the supply chain and ensure providers take a more comprehensive and consistent approach, enabling us to meet our policy objective of significantly reducing the likelihood that consumer and business end-users receive scam messages.

4.81 In the next section we outline our decisions for new rules and guidance to address scam messages.

[177] [✂] response to October 2025 Consultation.
[178] Simwood response to October 2025 Consultation. Page 1; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 4; MEF response to October 2025 Consultation. Page 4; VodafoneThree response to October 2025 Consultation. Page 4.

5. Measures to address P2P scam mobile messages

Introduction

5.1 In section 4, we set out our conclusion that additional measures are necessary to meet our policy objective of significantly reducing the likelihood that consumer and business end-users receive scam messages.

5.2 In this section, we explain our assessment and decisions on a set of measures to address P2P scam mobile messages. As part of the assessment, we consider stakeholders' responses to these measures from our 2025 consultation.

5.3 In summary, the measures we assess are requirements for providers to:

- Set volume limits for PAYG SIMs (GC C9.4 and C9.5).
- Have processes in place to receive scam reports[179] from customers and appropriate third parties on telephone numbers and URLs that are being used for scams (GC C9.2).
- Block numbers used by scammers, by using information from scam reports to identify telephone numbers that providers believe have sent scam messages (GC C9.3(a)).
- Identify and block scam messages that:
    - Originate from telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.3(b)); or
    - Contain URLs and telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.3(c)).

5.4 The measures we assess are applicable as follows:

- GC C9.2(b)-(c), C9.3(b)-(c), C9.4 and C9.5 are applicable to any Communications Provider that transfers and/or terminates P2P Messages.
- GC C9.2(a) and C9.3(a) are applicable to any Communications Provider that has Assigned Mobile Numbers.

5.5 Taking into account stakeholders' responses to our 2025 consultation, for each measure we assess:

- What it will require providers to do to combat scam mobile messages and why we consider it necessary to achieve our overall policy objective.
- The expected benefits to people and businesses.
- The financial costs of our requirements.
- Any potential adverse impacts on people and businesses in the UK, including on providers that would be subject to the new rules, and steps we propose to take to mitigate these.

[179] We define scam reports in our GCs as a report made by any person about a scam message (or other forms of scam), including complaints from customers and reports from law enforcement, regulatory or consumer bodies or other third parties.

- Whether we consider the expected benefits of each measure to outweigh any costs or adverse impacts.

Table 5.1: Summary of our final P2P measures

Summary of our final P2P measures		
Measure	**To which providers does it apply?**	**Our decision**
Setting volume limits for PAYG SIMs, to make it harder for scammers to message large numbers of potential victims.	Mobile operators that transfer and/or terminate P2P messages.	Largely retained from consultation proposal as **GC C9.4 and GC C9.5.** Additions made to our supporting guidance.
Having processes in place **to regularly and proactively receive scam reports** from customers and appropriate third parties, relating to the customers they have assigned mobile numbers to.	Mobile operators that have assigned mobile numbers.	Minor updates to **GC C9.2, under GC C9.2(a)**. Additions made to our supporting guidance.
Having processes in place to **regularly and proactively receive scam reports** from customers and appropriate third parties about telephone numbers and URLs that have been used for scams.	Mobile operators that transfer and/or terminate P2P messages.	Largely retained from consultation proposal but renumbered as **GC C9.2(b) and GC C9.2(c)**. Additions made to our supporting guidance.
Blocking numbers used by scammers: preventing scammers from sending messages from numbers that providers believe have sent scam messages, based on scam reports.	Mobile operators that transfer and/or terminate P2P messages and/or that have assigned mobile numbers.	Retained from consultation proposal as **GC C9.3(a).** Additions made to our supporting guidance.
Identifying and blocking scam messages in transit that: originate from telephone numbers that providers believe have been used for scams; or that contain URLs and telephone numbers that providers believe have been used for scams, based on scam reports.	Mobile operators that transfer and/or terminate P2P messages.	Retained from consultation proposal as **GC C9.3(b) and GC C9.3(c).** Additions made to our supporting guidance.

Setting volume limits for PAYG SIMs

What we proposed

5.6 In our 2025 consultation, we proposed a new GC C9.4, which would require mobile operators to implement and maintain appropriate and effective processes restricting the

volume of messages that PAYG customers can send from a specific mobile number, in a specified period, to more than one mobile number. We set out that this would require providers to set limits following an evidence-based assessment on the level of volume limit that is likely to disrupt scammers' activity, without preventing legitimate use.

5.7 We also proposed a new GC C9.5, which would require mobile operators to block messages being sent by a number, via automated means and without delay, when the user of a PAYG SIM (including eSIMs), reaches the provider's volume limit.

5.8 We expected this proposal to increase the cost and complexity of sending scam P2P messages in bulk and would have the effect of reducing the volume of scam messages reaching consumers.

5.9 In addition, we set out that:

- We expected the incremental cost of our volume limit proposals for mobile operators to be low.
- We recognised a potential risk that volume limits would constrain legitimate users but considered that mobile operators would have sufficient discretion to manage and mitigate this risk.

Stakeholder responses

5.10 Stakeholders were broadly supportive of our volume limits proposal. They noted that having volume limits in place is already a common practice and necessary to address the harm caused by scammers sending large volumes of fraudulent messages to consumers, specifically through the use of SIM farms.[180] More specific comments related to our proposed approach of giving operators flexibility to set their own volume limits, technical deployment, cost and any potential impact on legitimate messages are set out below.

Flexibility in setting volume limits

5.11 Most stakeholders agreed with our proposal that operators should retain flexibility over how to implement appropriate and effective volume limits.[181] BT and VodafoneThree warned that, if Ofcom were to take the approach of defining and publishing the level of appropriate volume limits, scammers could more easily 'game' them.[182] The CCP-ACOD and the Campaign Registry said that providers should review volume limits regularly to ensure

---

[180] BT Group response to October 2025 Consultation. Pages 6-7; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; CCUK response to October 2025 Consultation. Page 3; iconectiv UK response to October 2025 Consultation. Page 4; MEF response to October 2025 Consultation. Pages 6-7; Name withheld 2 response to October 2025 Consultation. Page 1; Simwood response to October 2025 Consultation. Page 5; Stour Marine response to October 2025 Consultation. Pages 2-3; techUK response to October 2025 Consultation. Page 2; The Campaign Registry response to October 2025 Consultation. Pages 5-6; Utility Warehouse response to October 2025 Consultation. Page 10; VodafoneThree response to October 2025 Consultation. Page 4-5; XConnect response to October 2025 Consultation. Page 1; Virgin Media O2 response to October 2025 Consultation. Pages 2-3.

[181] BT Group response to October 2025 Consultation. Pages 6-7; VodafoneThree response to October 2025 Consultation. Page 4; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; iconectiv UK response to October 2025 Consultation. Pages 4-5; Utility Warehouse response to October 2025 Consultation. Page 3; Stour Marine response to October 2025 Consultation. Page 2; techUK response to October 2025 Consultation. Page 2; The Campaign Registry response to October 2025 Consultation. Pages 5-6.

[182] BT Group response to October 2025 Consultation. Page 7; VodafoneThree response to October 2025 Consultation. Page 4.

they remain appropriate and effective.[183] iconectiv UK and Utility Warehouse said that volume limits should reflect legitimate use of SIMs.[184]

5.12 However, a small number of stakeholders raised concerns about this flexibility. In particular, Virgin Media O2 said that scammers may target providers with higher volume limits if Ofcom does not provide guidance about their level.[185] Similarly, Which? considered that, in the absence of further guidance, providers might set volume limits too high or reset them at short intervals.[186] [✂] considered that Ofcom should maintain appropriate oversight of the limits operators set.[187]

Technical deployment

5.13 [✂] raised concerns that our proposed volume limit would relate to the number of messages a PAYG customer sends to "more than one mobile number" in a specified period. It highlighted that its systems do not currently permit this and that it would be difficult for it to automate this rule.[188]

5.14 VodafoneThree highlighted that MVNOs have their own systems and customer configurations, which differ to those of their host MNO. It considered the MVNO to be best placed to monitor its customers' messages and engage with them directly when needed.[189] However, Verastar said that MVNOs cannot carry out network-wide monitoring or apply network-wide restrictions. It suggested GCs C9.4 and C9.5 should not apply to MVNOs.[190] More generally, Utility Warehouse sought clarity on which of our measures would apply to MVNOs, if thin MVNOs may not be technically able to implement many of our measures. It considered the MNO may be best placed to ensure compliance.[191]

Costs

5.15 Many respondents did not raise any concerns about our assessment that the overall cost of our P2P measures is likely to be limited, including the cost of volume limits. iconectiv UK considered that the anticipated benefits of the P2P proposals clearly outweigh the associated costs.[192] The Campaign Registry said that the P2P proposals would not require entirely new capabilities and would build on the existing practices of many operators.[193] Stour Marine said that it would not expect the P2P proposals to cause a materially negative impact on its ability to compete or innovate.[194] However, Pinnacle Teleservices said that the P2P measures could increase compliance and support costs, which our impact assessment did not take into account.[195]

---

[183] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; The Campaign Registry response to October 2025 Consultation. Pages 5-6.
[184] iconectiv UK response to October 2025 Consultation. Page 4; Utility Warehouse response to October 2025 Consultation. Page 3.
[185] Virgin Media O2 response to October 2025 Consultation. Pages 2-3.
[186] Which? response to October 2025 Consultation, pages 4-5.
[187] [✂] response to October 2025 Consultation.
[188] Name withheld 1 response to October 2025 Consultation. Page 2.
[189] VodafoneThree response to October 2025 Consultation. Page 5.
[190] Verastar response to October 2025 Consultation. Page 1.
[191] Utility Warehouse response to October 2025 Consultation. Page 1.
[192] iconectiv UK response to October 2025 Consultation. Pages 5-6.
[193] The Campaign Registry response to October 2025 Consultation. Page 6.
[194] Stour Marine response to October 2025 Consultation. Page 3.
[195] Pinnacle Teleservices response to October 2025 Consultation. Page 9.

5.16 Some stakeholders raised specific concerns about the cost of our volume limits proposal. [✂] submitted that we had underestimated the cost and complexity of implementing the volume limit requirements for some operators.[196] [✂] said that it would be costly to analyse the effectiveness of the level of the volume limit.[197]

Impact on legitimate messages

5.17 Some stakeholders argued that our volume limits proposal could risk providers blocking or delaying legitimate messages. [✂] was concerned about the effects of any service disruption on customer safety.[198] Pinnacle Teleservices said that static volume limits could disrupt legitimate traffic from small enterprises and service organisations, which may easily exceed P2P volume limits.[199] The CCP-ACOD called for operators to provide clear escalation routes for legitimate high-volume PIN based or alert messaging by small charities, medical practices, community groups and microbusinesses.[200]

5.18 Some stakeholders suggested however that P2P channels are not an effective route for legitimate high-volume messages. The MEF said that legitimate business messaging should flow through A2P channels.[201] Similarly, the Campaign Registry recommended that these messages should be sent over A2P channels, with appropriate KYC and KYT measures in place.[202]

Other issues

5.19 Other respondents suggested that these proposals should go further. Utility Warehouse argued that we should apply limits to pay monthly as well as PAYG SIMs, to prevent scammers shifting to pay monthly SIMs.[203] [✂] suggested developing rules to improve the tracking of SIM distribution, to prevent scammers from getting around volume limits by accessing large numbers of SIMs or using SIM farms.[204]

Our assessment

5.20 As described in sections 2 and 3, scammers' tactics are often to send large volumes of mobile messages to reach as many potential victims as possible. We set out in section 4 (paragraphs 4.20-4.21) that many mobile operators already set volume limits. These can reduce the number of scam mobile messages that reach mobile users by stopping scammers from sending high volumes of messages from PAYG SIMs within a specified period, increasing the cost and complexity of sending P2P messages at scale (in particular from SIM farms).

5.21 However, as set out in paragraphs 4.22-4.24, we consider that there are gaps and inconsistencies in current volume limits across the mobile sector. Currently, some providers have no limits in place, while others have limits that are either very high or that are reset at

[196] [✂] response to October 2025 Consultation.
[197] Name withheld 1 response to October 2025 Consultation.
[198] Name withheld 1 response to October 2025 Consultation. Page 3.
[199] Pinnacle Teleservices response to October 2025 Consultation. Pages 6-7.
[200] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3.
[201] MEF response to October 2025 Consultation. Page 6.
[202] The Campaign Registry response to October 2025 Consultation. Pages 5-6.
[203] Utility Warehouse response to October 2025 Consultation. Page 3.
[204] [✂] response to October 2025 Consultation.

short intervals, so only restrict the user from sending messages for a short period of time. These factors create vulnerabilities that scammers can exploit.

5.22 Requiring mobile operators to apply appropriate and effective volume limits will address these vulnerabilities and ensure more consistent and effective implementation of PAYG volume limits across the mobile sector.

5.23 Having considered stakeholders' responses, and for the reasons we set out below, we consider that our proposed requirement for operators to implement and maintain appropriate and effective processes relating to the volume of messages that their PAYG customers can send from a SIM in a specified period is a necessary and proportionate remedy to achieve our policy objective.

5.24 To further ensure the proportionality of this remedy, we have decided to amend our 2025 consultation proposal to apply volume limits to messages sent to any mobile number (not messages sent to "more than one mobile number").

5.25 Below, we describe how we will make this measure effective, and the rationale for it, in more detail. We also assess the likely costs of implementing volume limits, as well as other potential adverse impacts on stakeholders, and explain why we consider the benefits of the measures to outweigh these. In doing so, we respond to stakeholders' comments.

Setting appropriate volume limits

5.26 As set out in our 2025 consultation, we will require providers to implement appropriate volume limits for PAYG SIMs following an evidence-based assessment of the level of volume limit that is likely to disrupt scammers' activity, without preventing legitimate use. In response to Which? and Virgin Media O2's concerns about volume limits that may be set too high and potential inconsistencies in the limits, we consider that giving providers (with their knowledge of customer traffic patterns) flexibility to set evidence-based limits is more likely to ensure that their limits are effective than an approach where Ofcom would, in effect, set a limit for all relevant providers.

5.27 Enabling operators to make their own evidence-based assessments of volume limits will also mitigate against the concern that volume limits could result in blocking of legitimate messages. We consider this further in paragraphs 5.43-5.45.

5.28 Our guidance identifies the factors we expect providers to take into account when deciding what volume limit may be appropriate (paragraph 2.53).

Effective implementation of volume limits

5.29 We consulted on the proposal that volume limits should apply to messages that PAYG customers send "to more than one number". However, we have removed this provision in light of [✂] comments. This will help ensure our requirement is proportionate by taking into account the technical limitations of certain operators' systems for detecting to how many numbers a customer has sent messages.

5.30 However, we recommend that providers monitor whether end-users are sending high volumes of messages to unique numbers, where technically feasible. This will help providers improve detection of scams and avoid penalising legitimate users (we set this out in our accompanying guidance at paragraph 2.55).

5.31 GC C9.5 will require mobile operators to block numbers from sending messages, via automated means and without delay, as soon as that number reaches the provider's

volume limit, for the duration of the time specified in the policy. We understand from engagement with some providers that there is currently a time lag before blocking messages, but we consider it important for the limit to be applied without delay to ensure the limit is effective. This should prevent scammers from continuing to send messages after they reach the volume limit (see paragraphs 4.22-4.23, above) and will address other gaps in existing protections (as described in section 4).

5.32 There is a risk that scammers may respond to the deployment of more volume limits by acquiring more SIMs and SIM farm capacity. Nonetheless, volume limits should constrain the number of messages that can be sent from each PAYG SIM, increasing the cost and complexity of sending scam P2P messages in bulk and making these tactics less feasible.

5.33 We recognise, as VodafoneThree commented, that MVNOs have different systems to their host MNO and we agree that MVNOs may often be better placed to monitor their own customers' messaging patterns, particularly where they use their own Short Message Service Centres (SMSCs)[205] to transfer and terminate P2P messages. Thick MVNOs[206] use their own SMSC and we have therefore decided that thick MVNOs will be responsible for ensuring compliance with GCs C9.4 and C9.5.

5.34 GCs C9.4 and C9.5 will not however apply to all MVNOs, specifically to thin MVNOs (or branded resellers) as they do not have their own SMSC and they rely on their host MNOs to transfer and terminate messages. Only the MNO is therefore likely to be able to monitor and control the messages sent from its thin MVNOs' customers and know when a volume limit has been reached. We recognise that some thin MVNOs may be capable of applying their own volume limit, through billing systems for example. However, there may be a significant delay in a thin MVNO applying a limit if the thin MVNO needs to obtain information from its host MNO to understand when a volume limit has been reached and what SIM to block, and this delay may undermine the effectiveness of the limit. We therefore consider it appropriate for the obligation to be on MNOs to ensure compliance with GCs C9.4 and C9.5 in relation to SIMs distributed by their thin MVNOs (or branded resellers) and MNOs will be responsible for ensuring that their thin MVNO (and branded reseller partners) comply with our volume limits measure. Individual MNOs and thin MVNO partners should work to agree specific arrangements to implement and maintain appropriate and effective volume limits that are applied via automated means and without delay. We set this out in our accompanying guidance.[207]

5.35 To reflect the fact MNOs are responsible for setting volume limits in relation to their thin MVNOs' PAYG customers and may block their thin MVNOs' PAYG customers from sending further messages when they reach the relevant volume limit, we have amended the definition of Pay As You Go Customer in the GCs. We have also amended the definition to ensure it captures all types of pre-paid SIMs including where a customer is required to have a pre-pay credit balance to continue to use the service or service outside of any inclusive allowance, so it now reads as follows:

"'Pay As You Go Customer' in the context of Condition C9 means a Customer who accesses a Mobile Communications Service (either directly from a Regulated Provider or indirectly via

[205] An SMSC is the core network infrastructure responsible for storing and routing SMS messages between end-users' mobile devices, or between businesses and end-users.
[206] We recognise there are different forms of MVNOs, but for the purposes of this statement, we have simplified to refer to thick MVNOs and thin MVNOs.
[207] Paragraphs 1.35-1.38.

another Communications Provider using that Regulated Provider's Public Electronic Communications Network) and who pays only for services that they use, without signing up to a contract of a fixed duration."

5.36 Stakeholders may consider it appropriate to reset a SIM's volume limit after a period of time (meaning SIMs can continue to send messages again after that period has elapsed), if they consider this to strike an effective balance between constraining scam activity and allowing legitimate use. We expect mobile operators to keep the duration of the period after which a volume limit may be reset under close review and to revise it if it is making the volume limit less effective in constraining the ability of scammers to use PAYG SIMs to send large volumes of messages. Providers should also consider whether it is necessary to reset limits given senders will know when a volume limit has been applied and their SIM has been blocked and can therefore raise this with their provider.

5.37 We expect that consumers and businesses will benefit from a significant reduction in harm associated with scam messages following the implementation of the volume limit requirements, in conjunction with our other measures. We set out the nature of these benefits in more detail in paragraphs 8.4-8.8.

5.38 Further information on how we expect providers to comply with GCs C9.4 and C9.5 is set out in paragraphs 2.47-2.62 of our guidance.

Applying cross-cutting measures

5.39 Under GCs C9.17-C9.27, mobile operators will also be required to: regularly review their policies and keep appropriate records of the impact of their volume limit to ensure it remains appropriate and effective; appropriately train relevant staff; and comply with relevant data protection legislation. We discuss the cross-cutting measures we are imposing further in section 7.

Financial costs of our requirements

5.40 Below, we identify the likely costs of our volume limit requirements to be: (i) implementation costs of systems; (ii) ongoing costs of systems and their operation and (iii) costs of setting of effective limits.

5.41 In our 2025 consultation, we noted that there may be some additional costs for providers that do not currently apply volume limits or that need to ensure their current practices meet our requirements. However, we did not expect these incremental costs to be significant, for industry or for individual providers:

- **Implementation costs of systems:** we understand that providers can use systems of varying sophistication and cost to implement volume limits: for example, billing or general traffic management systems (which we expect providers to already have in place) can be readily adapted to implement appropriate and effective volume limits.[208] We also understand that most mobile operators in the UK already set some form of volume limit. [✂] said that we had underestimated the cost and complexity for some operators of implementing the volume limit requirements. [✂][209] We recognise there could be

[208] This is based on our understanding of how mobile operators manage customer accounts. One provider [✂] noted that the costs of introducing its volume limit were negligible as it was a configurable feature of its existing system. [✂] response to formal information request dated 27 March 2025, question 14.
[209] [✂] response to October 2025 Consultation.

additional costs (in the order of hundreds of thousands of pounds) for operators that require a new system to block numbers when they reach their volume limit. However, as other stakeholders did not raise concerns about our cost assessment, we remain of the view that incremental implementation costs will be low for industry overall.

- **Ongoing costs of systems and their operation:** the potential ongoing costs for providers we have identified relate primarily to the day-to-day operation and maintenance of the relevant systems (including staff costs).[210] Prior to our 2025 consultation, one provider noted that the cost of maintaining its volume limit is negligible, as it is a configurable feature of its existing system, indicating that the incremental ongoing costs to industry and individual providers would be low.[211] Additionally, the responses to our 2025 consultation did not raise any concerns over ongoing costs. We note that MNOs and thin MVNOs may incur some additional costs as MNOs must ensure that their thin MVNO partners comply with our volume limits measure. However, given the relatively low cost of implementing the volume limits requirements, and the existing commercial relationships between MNOs and their thin MVNOs, we do not consider these costs are likely to impose a significant burden. Therefore, we remain of the view that these ongoing costs will be low.
- **Costs of setting effective limits:** we consider that some operators may incur additional costs of assessing what an appropriate and effective volume limit should be and setting its overall policy. For instance, we note [✂] comment that it would require considerable time, effort and cost to analysis the effectiveness of a volume limit. However, in practice we do not expect the cost of this analysis to be material. We also note that, if providers do not assess the effectiveness of their volume limit, it may be set too high and allow scammers to send a significant number of messages without blocking their number (which is likely to significantly undermine our objective).

5.42 As we note above, some of our cross-cutting GCs will also apply to our volume limits measures (we discuss this further in section 7). However, we do not consider that these GCs will materially add to the cost of implementing and maintaining volume limits.

Potential risks of other adverse impacts

Constraining legitimate users

5.43 We recognise the potential risk that our volume limits measure could constrain messaging by legitimate users and we note stakeholders' concerns about this. For example, depending on the design of a volume limit, it could hypothetically block an individual from sending further messages after they have sent an unusually high number of messages to friends and family.

5.44 However, mobile operators will have discretion to manage this risk appropriately. We expect providers to set their limits at a level that would strike an appropriate balance between ensuring limits are effective in combatting scam messages without restricting legitimate users, based on their knowledge of customer traffic patterns.

5.45 We note CCP-ACOD's suggestion for clear escalation routes for legitimate high-volume PIN based or alert messaging, but we expect this type of messaging to occur on A2P channels where these escalation routes already exist.

---

[210] The relevant system (billing/traffic management/firewall) will differ for different operators, as this depends on how an operator implements their volume limit.
[211] [✂] response to formal information request dated 27 March 2025, question 14.

Impact on competition and innovation

5.46 We consider the potential impact on competition and innovation for all of our measures in the round. This is set out in section 8 as part of our proportionality assessment. We do not expect this measure to have a material negative impact on competition and innovation.

Other issues

5.47 Our volume limits requirement will not constrain legitimate users from sending messages on pay monthly SIMs, as it will only apply to PAYG SIMs (including eSIMs).[212] In response to Utility Warehouse's concern that excluding pay monthly SIMs from our rules could displace scam messages to this channel, we consider that there are significant barriers to acquiring large numbers of pay monthly SIMs, which mitigate this risk: these SIMs are not as readily available for purchase over the counter; contractual agreements and payment systems add further hurdles for criminals; and scammers are less able to use these SIMs anonymously, as credit checks and personal information for billing purposes are usually required.

5.48 We remain of the view that pay monthly SIMs are at lower risk of use for sending high volumes of scam P2P messages. Therefore, we do not consider it would be proportionate to require mobile operators to apply volume limits to messages sent from pay monthly SIMs at this time.

We expect the benefits of our volume limits requirement to outweigh any costs and adverse impacts

5.49 As set out in paragraphs 8.4-8.8, we consider that this volume limits requirement (alongside our other measures) will lead to a significant reduction in the harms associated with scam mobile messages, including a lower risk of financial loss and wider harms. Consultation responses generally supported this view. We received varied evidence from stakeholders on the cost of implementing this measure. Operators will also incur some ongoing cost, as they will need to ensure that their volume limit is set at an effective limit.

5.50 Taking into account all relevant factors (including our assessments above and in relation to our overall package of measures in section 8), we consider that the benefits of this requirement, as part of the package of anti-scams measures we are implementing, will make it materially more difficult for scammers to reach potential victims using mobile messages. On this basis, we consider our volume limits measure to be proportionate. We have therefore decided to implement our proposed volume limit.

5.51 As explained above, we have made an amendment to GC C9.4 to require providers to apply volume limits to messages sent to any mobile number (not messages sent to "more than one mobile number"). We have also updated the definition of 'Pay As You Go Customer' to reflect the fact MNOs are responsible for complying with our volume limits measure in relation to their thin MVNOs' PAYG customers and to reflect the different types of PAYG SIMs.

[212] PAYG customers, also known as pre-pay customers, include any customer that has accessed a mobile service without being on a fixed post-pay contract. This includes no-contract monthly rolling options, where the customer pays a recurring fee in advance for a service, traditional top-up-based SIMs and any hybrid of the two. We have amended the definition of PAYG customer in our GCs to make this clearer, by acknowledging the requirement for a pre-pay credit balance in order to continue to use the mobile service, or services outside of any inclusive allowance.

Blocking numbers used by scammers and blocking scam messages in transit

What we proposed

5.52 In our 2025 consultation, we proposed rules that mobile operators must:

- Have processes in place to receive scam reports[213] from customers and third parties on telephone numbers and URLs that are being used for scams (GC C9.2).
- Identify and block scam messages that:
  - Originate from telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.3(b)); or
  - Contain URLs and telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.3(c)).

5.53 In addition, we set out that:

- We expected our proposals may impose additional costs on some providers, but that the incremental costs to industry would not be significant.
- We recognised that there was some uncertainty about the incremental impacts on smaller providers, on which we invited further evidence.
- We had identified risks related to potential interference with the right to privacy and the right to freedom of expression, which a set of proposed cross-cutting measures would mitigate.

Stakeholder responses

5.54 Responses to our 2025 consultation broadly supported requiring providers to have processes in place to receive scam reports. Some respondents commented on what they considered should be the sources and processes for receiving scam reports.

5.55 Several respondents said that providers do not apply existing blocking measures consistently across the industry and that introducing consistent rules on blocking scam numbers and messages could help address consumer harm. However, some respondents were concerned about the costs of our proposed blocking measures and said it would not be feasible for smaller operators to meet these requirements. Others were concerned about the risk that our proposals could lead to more blocking of legitimate messages (false positives): for example, because they may contain a number or URL that has been incorrectly flagged as associated with scams.

5.56 In the following paragraphs, we begin by setting out stakeholders' comments on the proposal to have processes to receive scam reports. We then outline comments on the proposals to block numbers associated with scam and scam messages in transit, cost concerns and broader concerns regarding blocking of P2P messages.

[213] We define scam reports in our GCs as a report made by any person about a scam message (or other forms of scam), including complaints from customers and reports from law enforcement, regulatory or consumer bodies or other third parties.

Sources of scam reports and processes for receiving them

5.57 There was broad support from respondents for our proposals to strengthen policies, systems and processes for providers to receive scam reports.[214] Some stakeholders commented that third-party reporting of suspected scams provides useful intelligence sources to block P2P scam messages.[215]

5.58 Some respondents requested more clarity in our guidance on the sources of scam reports that operators could use to comply with GC C9.2.[216] Which? suggested that we should update our guidance to broaden the range of sources we had suggested to include financial services and law enforcement. It also said that providers should be required to proactively obtain scam intelligence from third parties on a monthly basis.[217] BT recommended that we require providers to receive scam reports only from third parties named in the guidance, rather than requiring them to have the capacity to receive scam reports from any third party (BT noted that providers could receive reports from other third parties if they chose to).[218]

5.59 Utility Warehouse said that Ofcom should have a central role in overseeing intelligence sharing, providing guidance on what information should be shared and ensuring best practice across industry.[219]

5.60 Mobile UK raised concerns about the quality of 7726 reports, noting that genuine messages and unwanted spam are often reported as scam messages.[220] Comms Council UK and [✂] said that inaccuracies in 7726 reports can lead to false positives.[221] Comms Council UK called for us to require providers to apply checks before acting on scam reports.[222]

5.61 Verastar raised concerns over the application of the proposal to thin MVNOs and said that MNOs are responsible for implementing processes to receive scam reports under GC C9.2.[223]

5.62 Finally, [✂] suggested that we maintain a verified list of inactive or decommissioned numbers to support identification of fraudulent messages.[224]

---

[214] iconectiv UK response to October 2025 Consultation. Pages 4-5; The Campaign Registry response to October 2025 Consultation. Page 6; CCUK response to October 2025 Consultation. Pages 3-4; BT Group response to October 2025 Consultation. Page 6; VodafoneThree response to October 2025 Consultation. Page 5; Which? response to October 2025 Consultation. Page 5.
[215] iconectiv UK response to October 2025 Consultation. Pages 4-5; The Campaign Registry response to October 2025 Consultation. Page 6; BT Group response to October 2025 Consultation. Page 6.
[216] Stour Marine response to October 2025 Consultation. Page 3; BT Group response to October 2025 Consultation. Page 6.
[217] Which? response to October 2025 Consultation. Page 6.
[218] BT Group response to October 2025 Consultation. Pages 6-7.
[219] Utility Warehouse response to October 2025 Consultation. Pages 4-5.
[220] Mobile UK response to October 2025 Consultation. Page 1.
[221] CCUK response to October 2025 Consultation. Page 3; [✂] response to October 2025 Consultation.
[222] CCUK response to October 2025 Consultation. Page 3.
[223] Verastar response to October 2025 Consultation. Page 1.
[224] [✂] response to October 2025 Consultation.

Feasibility and costs of message blocking for smaller operators

5.63 Many respondents agreed with the requirement for mobile operators to block scam messages and numbers associated with scams on P2P channels.[225] techUK agreed that blocking scam numbers can be part of an effective solution to reduce scam messages.[226]

5.64 Several stakeholders set out that our proposals must be proportionate and feasible for smaller operators and some stated that it would not be feasible for smaller providers (including thin MVNOs) to apply blocking measures on P2P channels.[227] In particular, Verastar said thin MVNOs cannot apply network-wide monitoring or restrictions where scam activity is identified. [228]

5.65 Utility Warehouse said the proposals should clearly outline that MNOs are responsible for blocking scam messages transferred or terminating on their network, including those sent by customers of MVNOs they host.[229]

Other issues

5.66 [✂] and Pinnacle Teleservices raised concerns that our blocking measures for P2P channels could result in false positives and that, despite blocking, scam campaigns often re-appear on other networks.[230] techUK also said that implementation of blocking must be proportionate to avoid the risk of false positives.[231]

5.67 Amnesty International UK agreed with restricting mandatory scanning of messages to known scam URLs and numbers, but raised concerns about false positives, specifically in relation to how providers could scan messages in ways that our measures do not require directly.[232]

5.68 [✂] requested more clarity on responsibility for blocking messages between the originating and terminating provider and whether providers are expected to apply blocking to both outgoing and incoming messages.[233]

5.69 Virgin Media O2 said that tracking URLs would be complex for providers and that there does not appear to be a suitable or consistent way of doing this accurately.[234]

5.70 BT requested we clarify the definition of 'P2P Messages' in the proposed GCs. It said that the proposed definition appeared to describe messages generally, rather than messages

---

[225] iconectiv UK response to October 2025 Consultation. Page 4; Pinnacle Teleservices response to October 2025 Consultation. Page 9; Utility Warehouse response to October 2025 Consultation. Page 4; FCS response to October 2025 Consultation; techUK response to October 2025 Consultation. Page 2. [✂] response to October 2025 Consultation; BT Group response to October 2025 Consultation. Page 6; Mobile UK response to October 2025 Consultation. Page 2; VodafoneThree response to October 2025 Consultation. Page 5.

[226] techUK response to October 2025 Consultation. Page 2.

[227] techUK response to October 2025 Consultation. Page 3; Utility Warehouse response to October 2025 Consultation. Page 4; FCS response to October 2025 Consultation. Page 1; Verastar response to October 2025 Consultation. Page 1.

[228] Verastar response to October 2025 Consultation. Page 1.

[229] Utility Warehouse response to October 2025 Consultation. Page 4.

[230] Name withheld 1 response to October 2025 Consultation. Pages 1-2; Pinnacle Teleservices response to October 2025 Consultation. Page 9.

[231] techUK response to October 2025 Consultation. Page 3.

[232] Amnesty International UK response to October 2025 Consultation. Page 2.

[233] [✂] response to October 2025 Consultation.

[234] Virgin Media O2 response to October 2025 Consultation. Page 3.

which are ECS and specifically, SMS and MMS. It suggested we amend the definition to refer to SMS and MMS messages.[235]

Our assessment

5.71 Having considered the above stakeholder comments, we remain of the view that requiring blocking measures for mobile operators, including receiving scam reports and blocking numbers, remains a necessary and proportionate remedy to achieve our policy objective (in combination with our other measures). These measures are contained in GCs C9.2 and C9.3. We are mandating similar measures for A2P messages (we discuss these from paragraph 6.133).

5.72 In this subsection, we describe these measures and their rationale in more detail. We then assess the likely costs of implementing these measures, as well as other potential adverse impacts on stakeholders, and explain why we consider the benefits outweigh these impacts. In doing so, we respond to stakeholders' comments.

5.73 As described in sections 2 and 3, scammers exploit P2P channels to impersonate legitimate mobile users and manipulate potential victims into sending them money or sharing personal and financial information (for example, using 'Hi Mum' scams). As discussed in section 4 (paragraphs 4.25-4.32), many mobile operators already implement blocking measures to combat scam P2P messages. However, the deployment of these tools remains inconsistent across mobile operators. For instance, we are aware that at least one MVNO does not use any form of blocking tool and some MVNOs may only have limited blocking tools available. Absent intervention, we expect the current limitations in the deployment and functionality of blocking tools to persist, which creates vulnerabilities that scammers can exploit.

Receiving scam reports

5.74 We are requiring mobile operators to collect scam reports to support how they block numbers used by scammers and scam messages in transit. Many mobile operators currently use tools to identify and block scammers' numbers and messages in transit, before they can reach potential victims, the effectiveness of which relies heavily on the intelligence that they feed into them. This can include details of the latest scam campaigns, such as telephone numbers that scammers use and scam URLs.

5.75 However, our information gathering suggests that not all mobile operators have processes in place to collect the most useful data. For example, some appear not to have access to, or to use, reports to 7726, which we consider a key source of intelligence on scam practices.

5.76 We expect any communications provider that has assigned mobile numbers to implement and maintain processes to receive scam reports. We disagree with Verastar's comment that GC C9.2 should not apply to thin MVNOs because we consider that thin MVNOs need to receive scam reports to inform any suspected scam activity associated with their customers' numbers in order to comply with GC C9.3(a). We have therefore amended GC C9.2 to ensure that any provider that has assigned mobile numbers must implement processes for receiving scam reports. For thin MVNOs, this is limited to reports about their own customers which we understand they can likely access from their host MNO (we set this out in our accompanying guidance at paragraph 2.10).

[235] BT Group response to October 2025 Consultation. Page 10.

Sources and mechanisms for receiving scam reports

5.77 We do not consider it likely that, to achieve our objective, it would be sufficient for mobile operators that transfer and/or terminate P2P messages to draw on scam reports from their own customers alone. Instead, we consider that mobile operators that transfer and/or terminate P2P messages should also obtain reports from third parties with expertise in identifying scams. We note that several stakeholders agreed that providers should access third-party scam reports.[236]

5.78 We note Which?'s comments about extending the range of suggested sources of intelligence reports in our guidance and we agree there are broader sources that may provide relevant scams intelligence. We have therefore updated our guidance to broaden the range of examples of appropriate sources from which operators may receive scam reports, noting financial services and law enforcement. Paragraphs 2.14-2.16 of the guidance provides further details on different sources and mechanisms for receiving scam reports. The guidance does not limit operators from using sources of scam reports beyond those listed.

Requirements for receiving scams reports

5.79 Which? proposed that we should require operators to proactively obtain intelligence on scams. We agree that this change to our proposals would help strengthen the intelligence that providers would have available, by making clearer that they should seek out relevant information. We have therefore made a minor amendment to GC C9.2,[237] to set out that mobile operators are required to implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive scam reports from end-users and appropriate third parties relating to:[238]

- A customer they have assigned Mobile Numbers to (GC C9.2(a));
- Telephone numbers that the customer, or third party, believes sent messages intended to scam the recipients (GC C9.2(b)).
- URLs and telephone numbers that the customer, or third party, believes were used as part of a scam (GC C9.2(c)).

---

[236] iconectiv UK response to October 2025 Consultation. Pages 4-5; The Campaign Registry response to October 2025 Consultation. Page 6; CCUK response to October 2025 Consultation. Page 3; BT Group response to October 2025 Consultation. Page 6; VodafoneThree response to October 2025 Consultation. Page 5; Which? response to October 2025 Consultation. Page 5.

[237] At consultation, GC C9.2 proposed that Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to receive (and where appropriate, validate) Scam Reports from End-Users and third parties, relating to: (a) Telephone Numbers that the End-User and/or third party believes sent P2P Messages intended to Scam the recipients; and (b) URLs and Telephone Numbers that the End-User and/or third party believes were used as part of a Scam, including URLs and Telephone Numbers included in P2P Messages. We have decided to amend GC C9.2 to require that Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and where appropriate, validate) Scam Reports from End-Users and appropriate third parties, relating to: (a) Customers they have assigned Mobile Numbers to; (b) Telephone Numbers that the End-User and/or third party believes sent P2P Messages intended to Scam the recipients; and (c) URLs and Telephone Numbers that the End-User and/or third party believes were used as part of a Scam, including URLs and Telephone Numbers included in P2P Messages.

[238] Third parties in this context are those organisations that monitor and/or collect intelligence on actual scam messages that could be used to detect and block similar scams from entering mobile networks. These could be financial institutions, law enforcement bodies, intelligence agencies or telecoms sector partners. We have included a non-exhaustive list in the guidance.

5.80 We note BT's recommendation to limit the scope to require providers only receive scam reports from third parties named in the guidance. We do not consider this appropriate, given the range of potential sources of scam reports and how this may evolve other time. We therefore continue to believe it is appropriate for our guidance to provide examples of source of scam reports.

5.81 However, we have decided to make a minor amendment to GC C9.2 to refer to obtaining scam reports from "appropriate" third parties. In deciding from what third parties it may be appropriate to obtain scam reports, we expect mobile operators to take into account the extent to which third parties have expertise in, and a legitimate basis for, identifying or aggregating scams and whether they provide a rich source of timely information and can provide detailed information on current and emerging threats (we set this out in paragraph 2.14 of our accompanying guidance).

Validation of scam reports

5.82 We note that Comms Council UK and [✂] raised concerns that inaccuracies in end-user reporting to 7726 can lead to false positives. We agree that operators should interrogate and validate scam reports, where appropriate: for example, reports based on 7726 may contain incorrectly reported messages that are not scams, including commercial messages, spam or other content that the user simply did not want to receive. We expect mobile operators to interrogate such reports to filter out messages that they do not reasonably believe were intended to scam the recipients, to reduce the risk of false positives.

5.83 Other sources of intelligence, such as lists of known scam URLs provided by a credible third party, may not require such interrogation by the provider if the third party has already undertaken this step. Therefore, depending on the type of scam report a provider is using, it may be reasonable to presume it is valid without further interrogation. We provide further details in our guidance, from paragraph 2.18-2.25, on how mobile operators can ensure they validate scam report information and reduce the risk of false positives.

Sharing scam reports with other providers and third parties

5.84 We have considered Virgin Media O2's request for more information on the tracking of URLs and the interaction between providers, customers and third parties in sharing intelligence. We have also considered [✂] suggestion that we maintain a verified list of inactive or decommissioned numbers to be used as a signal for identifying a fraudulent message. Ofcom publishes information on allocated number ranges which providers can use to inform blocking.[239] Our guidance encourages mobile operators to establish intelligence-sharing mechanisms to strengthen the quality and timeliness of the intelligence available to them and better combat scam messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law. We have added details in our guidance at paragraphs 2.26-2.29 on how mobile operators can share intelligence with each other and with third parties.

5.85 The purpose of GC C9.2 is to ensure mobile operators regularly and proactively obtain targeted and intelligence scam reports to enhance their ability to detect and block scam messages, as set out in GC C9.3 (we discuss GC C9.3 further in the sub-section below). We expect that GC C9.2 will help to ensure mobile operators take effective steps to receive up

[239] Ofcom, Download numbering data.

to date intelligence on current scams, which will strengthen their ability to act quickly to effectively identify and then block scam messages before they reach customers.

Blocking numbers used by scammers

5.86 We are intervening to require that, where mobile operators reasonably believe that a mobile number they have assigned to a customer has sent P2P messages intended to scam the recipients, the operator must prevent that number from sending further P2P messages, as set out at GC C9.3(a). We are requiring that mobile operators do this without undue delay.

5.87 Many stakeholders supported our proposed blocking requirements on P2P channels[240] and said that blocking tools could reduce consumer harm from scam messages.[241] iconectiv UK added that blocking measures are implemented unevenly across industry and that this inconsistency undermines the effectiveness of blocking tools materially.[242]

5.88 Verastar and Utility Warehouse considered that it would not be feasible for thin MVNOs to apply blocking measures on P2P channels. While we agree that it would not be feasible for these providers to apply blocking measures to messages in transit, we consider that they can take action to revoke a customer's use of a number. Where a number is suspected to be sending scam P2P messages, the provider that has assigned the number is the best placed and the most appropriate party to implement a permanent block of this kind. We discussed in our 2025 consultation (paragraph 5.48) that MNOs do not tend to block numbers on behalf of any thin MVNOs with which they contract, as they do with messages, which leaves a gap scammers can exploit on P2P channels. We have clarified the scope of GC C9.1(b) to explain that GC C9.3(a) applies to any provider that has assigned mobile numbers which includes thin MVNOs.

5.89 We expect that requiring mobile operators to block numbers that send suspicious P2P messages will significantly reduce the number of scam messages entering networks. If all mobile operators block scam numbers effectively, it will be much harder for scammers to send customers scam messages.

Identifying and blocking scam messages in transit

5.90 In section 4 at paragraphs 4.25-4.32, we explained that while mobile operators use tools that identify and block scam messages in transit (typically provided by third parties), such measures are not applied consistently across all operators. Some thick MVNOs do not use these tools at all, while others have tools that are insufficient[243] or that they do not update quickly enough to target new scam threats. Scammers can exploit this inconsistency by bypassing the more sophisticated blocking protections of larger networks and reaching mobile customers through less-protected channels. This may account in part for the high volume of scam messages that still reach customers.

5.91 Therefore, as set out in GC C9.3(b) and C9.3(c), we will require that:

---

[240] VodafoneThree response to October 2025 Consultation. Page 5; BT Group response to October 2025 Consultation. Page 6.
[241] Pinnacle Teleservices response to October 2025 Consultation. Page 8; techUK response to October 2025 Consultation. Page 2; Utility Warehouse response to October 2025 Consultation. Page 4.
[242] iconectiv UK response to October 2025 Consultation. Page 4.
[243] For example, they may rely on the manual addition of keywords to blocklists rather than automatic detections.

- Mobile operators block P2P messages sent from telephone numbers where they reasonably believe that those telephone numbers have sent P2P messages intended to scam the recipients. This blocking can be carried out using automated tools or as a result of human review but must be done without undue delay.
- Mobile operators block P2P messages that contain URLs or telephone numbers that they reasonably believe were used as part of a scam. We will require that they carry out this blocking using automated tools, without undue delay. We recognise that some degree of human review of messages is likely to be necessary to ensure the automated tools are working as intended.

5.92 We note at paragraph 2.42 of our guidance that some mobile operators may carry out other monitoring of messages on their network that does not draw on scam reports. For example, providers may review messages on their network based on probabilistic search methods[244] that indicate suspicious behaviour. Our rules do not require or prevent this form of monitoring. We note that it may be considered an intrusive measure and mobile operators should therefore ensure they comply with other relevant legislation (see paragraph 2.41-2.42 of our guidance).

5.93 We have considered Verastar and Utility Warehouse's comments on the challenge for MVNOs of applying network-wide restrictions and their view that MNOs should be responsible for blocking scam messages on their networks, including messages from MVNOs' customers. We consider that the requirement to identify and block messages in transit should apply to either an MNO or an MVNO it hosts, depending on whether the MVNO is technically able to comply. As MNOs transfer and terminate P2P messages on behalf of thin MVNOs they host, the requirement to identify and block messages does not apply to thin MVNOs. However, as thick MVNOs transfer and terminate messages using their own SMSCs, they are responsible for identifying and blocking scam messages in transit on their network. Individual MNOs and thin MVNO partners should work to agree specific arrangements for the MNO to block scam messages on the thin MVNO's behalf.

5.94 We note [✂] request for more clarity on responsibility for blocking messages between the originating and terminating provider. The requirement applies to all mobile messaging traffic on in-scope providers' networks.

5.95 We note BT's request for clarity regarding the definition of P2P messages in the proposed GCs. It said that the proposed definition appeared to describe messages generally, rather than messages which are an ECS and specifically, SMS and MMS. We have considered this request and have explained our definition of mobile messaging services within the scope of GC C9 in section 2. We also note that our proposed definition for P2P messages already referred to messages being sent using a Mobile Communications Service (as defined in the GCs), which is an ECS. We have however amended the definition to further clarify that the rules apply only to messaging services that fall within the scope of public electronic communications services.[245] We have defined 'P2P Message' as a "message sent from one

[244] Probabilistic search methods involve making decisions based on the likelihood of something happening. This includes reviewing messages for a broad set of scam indicators, including phrases such as "Hi Mum …". In contrast, our measures require the review of messages for known scam numbers or URLs. We consider that, in effect, our measures require providers to implement a database matching tool.

[245] This will ensure that any messages delivered from one SIM to another will be in scope of the definition (regardless of whether or not they may fall under the definition of a Mobile Communications Service).

SIM to another, using a Mobile Communications Service or otherwise using a Public Electronic Communications Service."[246]

5.96 Mandating that operators use appropriate blocking tools will address the limitations of existing industry measures. In response to Amnesty International UK, we have made various updates to our guidance, and our blocking requirements are designed with various safeguards in mind, which we discuss in more detail in our rights assessment in section 8 and Annex 4.

Reviewing blocking policies regularly

5.97 Given the constant evolution of scammers' tactics, there will be an ongoing risk that scammers bypass or evade blocking measures. Mobile operators will need to continually refresh their understanding of scam campaigns. As set out in GC C9.19, we will require mobile operators to regularly review their policies, systems and processes to:

- Confirm that they remain appropriate and effective and are operating as intended.
- Ensure the mobile operator is complying with its policies, systems and processes.
- Ensure that any issues identified are promptly and effectively addressed and that they update policies, systems and processes as appropriate.

5.98 By complying with GC C9.19, we expect that mobile operators will maintain better protections against mobile messaging scams. The requirement for regular reviews of policies, systems and processes will apply in relation to all rules implemented under Condition C9 and we discuss this, alongside other cross cutting requirements, and associated costs, in section 7. We also provide further information on how we expect providers to conduct reviews of anti-scam measures, including reviews in response to false positive incidents, in our guidance.

5.99 We will require that mobile operators provide a right of challenge for anyone that has been impacted by any blocking of numbers or messages under GC C9.3. We are also requiring mobile operators to: keep appropriate records (including on the effectiveness of their blocking measures); appropriately train relevant staff; implement appropriate systems and processes to identify, monitor and address false positive rates arising from blocking under GCs C9.3(b) and (c); and comply with relevant data protection legislation. These cross-cutting measures are set out in GCs C9.17-C9.18 and C9.20-C9.27 and discussed in section 7.

Financial costs of our requirements

5.100 As set out in our 2025 consultation, we expect our rules may impose additional costs on some providers, but we do not expect the incremental costs to industry to be significant. We recognised that there was some uncertainty about the incremental impacts on smaller providers. We invited further evidence from stakeholders on this point, but in our view they did not identify any specific examples of material risks to smaller suppliers.

5.101 We set out the main costs we identified for MNOs and thick MVNOs below:[247]

---

[246] We define public electronic communications services in paragraph A5.18 in Annex 5. We have also amended the definition to remove the reference to P2P messages being sent "between individuals", taking into account the fact some P2P messages may be sent from SIM farms.

[247] We note the comments raised by some thin MVNOs that they should not be responsible for implementing blocking measures that are outside of their control. In line with paragraph 5.93, the costs explained here do

- **Implementation costs of systems**: we understand that most, but not all, mobile operators already have suitable systems in place that can fulfil our requirements for blocking messages and numbers.[248] As such, we do not expect the resulting additional incremental implementation costs to industry to be significant. We estimate these to be around £600k (excluding VAT), borne across all mobile operators without suitable firewall systems already in place.[249] We note that several mobile operators would incur implementation costs (some of whom are significant players in the market) and that the costs individual providers incur would vary depending on their size. On this basis, we do not expect the costs of our intervention to be significant, either for individual mobile operators or for industry as a whole.
- **Ongoing system costs:** we expect there to be systems upkeep costs associated with the blocking measures, such as maintenance costs. Given that most mobile operators appear to already have the necessary systems in place, they incur such costs as part of their ordinary course of business. Beyond this, we estimate the resulting additional costs faced by industry to be less than £100k (excluding VAT) per annum, borne across all mobile operators without suitable firewall systems already in place.[250] As set out above, the same mobile operators would bear ongoing system costs, which would scale according to providers' size. While the figures mentioned above are not precise estimates, we consider that the total costs are unlikely to be disproportionate given the scale of financial and other harms from telecoms-enabled scams, as set out in section 3, and we do not consider the costs for any given operator to be unduly high.[251]
- **Ongoing staff costs:** these can include operational costs relating to maintaining blocking systems[252] and staff costs relating to processing challenges from people affected by blocking. On the former, we understand that most mobile operators already have members of staff working on fraud management.[253] For these mobile operators, we do not expect incremental staff costs to be substantial, given that these activities should largely align with existing staff expertise. On the latter, we expect providers could incorporate complaints of over-blocking into existing complaints processes, limiting costs. Our safeguards related to the risk of false positives (explored in more detail in our rights assessment in section 8 and Annex 4) should also limit the number of complaints that mobile operators receive and must process. We therefore do not expect these staff costs

---

not apply to thin MVNOs given that they do not transfer or terminate P2P messages, and our requirements to block messages in transit will be fulfilled by their host MNOs. However, see paragraph 5.102 for costs that do apply to thin MVNOs.

[248] We also note that thin MVNOs can rely on their MNOs' systems to extend to them.

[249] We derived this estimate by requesting information from firewall providers on the cost of their services to operators of different sizes and then applied these costs to the existing providers whom we understand may not currently have suitable firewall protections in place (based on information gathered via formal information requests). The estimate is the sum of the likely firewall costs across these operators.

[250] Formal information request responses.

[251] We also note that number blocking is the only element of our P2P proposals that would impose costs on thin MVNOs, given that MNOs do not tend to block numbers on behalf of any thin MVNOs they contract with, as they do with messages. However, we also do not expect these additional costs to be significant for thin MVNOs, given that they are likely to already have the capability to block numbers, and we expect they can still rely on intelligence from their host MNO to inform this.

[252] For example, the creation of new blocking rules to respond to new scam types, the addition of detected URLs to firewall and DNS blocklists, identification/termination of SMS services of MSISDNs originating scam messages from the provider's network, and monitoring of SMS patterns.

[253] Formal information request responses.

to impose significant additional incremental costs on industry or individual mobile operators.

- **Scam intelligence costs:** we understand from stakeholder engagement that most (but likely not all) mobile operators already receive appropriate scam reports. We also understand that thin MVNOs can likely access some scam intelligence reports relating to their customers from their host MNO.[254] Further, we have observed costs of securing 7726 reports as low as £[✂] per annum[255] and understand that intelligence is available for free from other sources.[256]
- We note that there are other cross-cutting measures (that enhance our measures and safeguard individual rights) that apply to our blocking requirements for P2P messages, as discussed in section 7. We do not consider that these GCs would materially add to the cost of this measure.

5.102 Thin MVNOs, as explained in paragraphs 5.76 and 5.88 above, will be required to implement two elements of our P2P identifying and blocking measures. These are: implementing and maintaining processes to receive scam reports associated with their own customers; and preventing mobile numbers they have assigned to a customer from sending P2P messages where they reasonably believe they have been used to send scam messages. We expect the costs associated with these requirements for thin MVNOs to be limited to the scam intelligence costs described above (or even less, if MNOs share these reports with them) and minor costs of implementing blocks on mobile numbers if and when the thin MVNO's customers have been identified as scammers.

Potential risks of other adverse impacts

Potential interference with the right to privacy under Article 8 of the European Convention on Human Rights (ECHR) and data protection considerations

5.103 While the measures set out above are, to a great extent, already industry practice, we recognise that our rules to require mobile operators to identify scam URLs and telephone numbers in messages may interfere with the right to privacy under Article 8 ECHR. This is because we expect mobile operators will need to use technology to review the content of private messages.

5.104 All our blocking requirements are also likely to involve the processing of personal data, which can lead to a number of possible data protection harms, such as loss of control of personal data, invisible processing or unwarranted surveillance.[257]

5.105 We are including various safeguards in our rules to limit any interference with the right to privacy under Article 8 ECHR and potential adverse data protection impacts. We also consider the risk of those adverse impacts arising (and any associated harm) to be low (see our rights assessment in section 8 and Annex 4).

---

[254] Mobile operators can also share intelligence to help them build a more robust and up to date understanding of scam activity. Our guidance explains that we encourage mobile operators to establish intelligence sharing mechanisms for the purpose of significantly reducing the likelihood that consumers receive scam messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law.

[255] [✂] response to formal information request dated 27 March 2025, question 14.

[256] The Cyber Defence Alliance is an example of an organisation that provides free intelligence.

[257] See also ICO, 2022: Overview of Data Protection Harms and the ICO's Taxonomy.

Over-blocking and potential interference with the right to freedom of expression under Article 10 ECHR

5.106 While the rules we are introducing are already, to a large extent, industry practice, we recognise that our rules to require mobile operators to block scam numbers and messages could result in providers blocking legitimate numbers and messages.

5.107 In response to comments raised about the risk of false positives due to blocking requirements on P2P channels, we consider that this risk of over-blocking is low (see our rights assessment in section 8 and Annex 4) and can be effectively mitigated through the various safeguards we are including in our rules (see GCs C9.17-27).

Impact on competition and innovation

5.108 We consider the impact on competition and innovation of our rules in the round, as part of proportionality assessment in section 8. For the reasons set out there, we do not consider our intervention to have a material negative impact on competition and innovation.

We consider the benefits of our P2P blocking requirements to outweigh any costs and adverse impacts

5.109 Having considered stakeholder responses, our view is that our blocking requirements will address issues that have been created by certain mobile operators not having any, or sufficient, processes in place. We consider that the cost to industry of filling these gaps and any associated adverse impacts on stakeholders will be low, relative to the scale of benefits from preventing scammers from exploiting gaps in protections on UK mobile networks.

5.110 Taking into account all relevant factors (including our assessments above and in relation to our overall package of measures in Section 8), we consider our P2P blocking requirements to be proportionate. We have therefore decided to implement our proposed requirements, which includes having processes in place to receive scam reports, blocking numbers used by scammers and blocking scam messages in transit.

5.111 As explained above, we have made an amendment to GC C9.2 to require providers to "regularly" and "proactively" ensure they receive scam reports and to refer to obtaining these scam reports from end-users and "appropriate" third parties. As explained above, we have also updated the definitions of 'P2P Messages'. We have further made various updates to our guidance to reflect stakeholders' comments.

6. Measures to address A2P scam mobile messages

Introduction

6.1 In section 4, we set out our view that additional measures are necessary to meet our policy objective of significantly reducing the likelihood that consumer and business end-users receive scam messages.

6.2 In this section, we explain our assessment and decisions on a package of measures to address scam mobile messages that originate from A2P business messaging channels. As part of the assessment, we consider stakeholders' responses to our 2025 consultation on these measures.

6.3 Below, we assess two complementary sets of measures. The first set of measures should ensure mobile operators and aggregators can identify scammers posing as legitimate business senders. In summary, these measures are requirements on providers to:

- Conduct up-front due diligence during the onboarding of a new business sender, via effective Know Your Customer (KYC) checks (GCs C9.8, C9.9, C9.10 and C9.14).
- Prevent the use of fake alphanumeric sender IDs, including by corroborating Sender IDs against information gathered through KYC checks, and maintaining a policy on restricting use of protected sender IDs and generic sender IDs (GCs C9.8, C9.9, C9.11 and C9.13).
- Conduct ongoing Know Your Traffic (KYT) checks, including reviewing account activity and promptly investigating reports of fraud (GCs C9.8, C9.9 and C9.12).
- Pass requirements through the supply chain, through clear and unambiguous contractual terms, to ensure downstream parties supplying A2P messages are held contractually responsible for undertaking KYC, KYT and alphanumeric Sender ID checks (GC C9.9).
- Apply incident management processes where scam activity is identified, to block business senders and address any compliance failures by other providers (GCs C9.15 and C9.16).

6.4 The second set of measures should ensure providers identify and block messages from scammers that evaded detection. They are requirements for mobile operators and tier 1 aggregators to:

- Have processes to receive scam reports from customers and appropriate third parties on telephone numbers and URLs that are being used for scams (GC C9.6).
- Block messages that contain URLs and telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.7).

6.5 The measures we assess are applicable as follows:

- GCs C9.8 to C9.12 and C9.14 to C9.16 are applicable to any Communications Provider that transfers and/or terminates A2P messages, including all Aggregators.[258]

[258] We define Aggregators in our GCs as an intermediary that transfers (either directly or indirectly) A2P Messages between Business Senders and Mobile Service Providers that could terminate those messages to recipients (excluding intermediaries that contract directly with Business Senders but are acting in a capacity where that Business Sender is required to have separate contractual relationship with a third party to transfer A2P Messages).

- GC C9.13 is applicable to any Communications Provider that terminates A2P messages.
- GCs C9.6 and GC C9.7 are applicable to any Communications Provider that transfers and/or terminates A2P messages, except Lower-Tier Aggregators.[259]

6.6 Taking into account stakeholders' responses to our 2025 consultation, this section sets out our assessment of our measures, including:

- What they will require providers to do to combat scam mobile messages and why we consider it necessary to achieve our overall policy objective.
- The expected benefits to people and businesses.
- The financial costs of our requirements.
- Any potential adverse impacts on people and businesses in the UK, including on providers that would be subject to the new rules, and steps we are taking to mitigate these.
- Whether we consider the expected benefits of each measure to outweigh any costs or adverse impacts.

Table 6.1: Summary of our final A2P measures

Summary of our final A2P measures		
Measure	**To which providers does it apply?**	**Our decision**
Conducting due diligence: preventing criminals from using A2P services to contact potential victims by ensuring that effective KYC checks are made at the onboarding stage.	Mobile operators and aggregators that transfer and/or terminate A2P messages.[260]	Retained from consultation proposal as **GCs C9.8, C9.9, C9.10 and C9.14.** Additions made to our supporting guidance.
Preventing the use of fake alphanumeric sender IDs, including by corroborating sender IDs against information gathered through KYC checks and maintaining a policy on restricting use of protected sender IDs and generic sender IDs.	Mobile operators and aggregators that transfer and/or terminate A2P messages.[261] Mobile operators that terminate A2P messages must maintain a policy.	Retained from consultation proposal as **GCs C9.8, C9.9, C9.11 and C9.13.** Additions made to our supporting guidance.

[259] We define Lower-Tier Aggregators in our GCs as an aggregator that is acting in a capacity in which it does not contract directly with a Mobile Service Provider that directly terminates A2P Messages to recipients.
[260] While the provider that onboards the business customer will be directly responsible for conducting due diligence checks, all other providers that transfer/terminate A2P messages are required to do so by taking the steps in Condition C9.9 regarding contractual terms.
[261] While the provider that onboards the business customer will be directly responsible for conducting alphanumeric sender ID checks, all other providers that transfer/terminate A2P messages are required to do so by taking the steps in Condition C9.9 regarding contractual terms.

Summary of our final A2P measures		
Conducting ongoing KYT checks, including reviewing account activity and promptly investigating reports of fraud.	Mobile operators and aggregators that transfer and/or terminate A2P messages.[262]	Retained from consultation proposal as **GCs C9.8, C9.9 and C9.12.**
Applying incident management processes where scam activity is identified, to block business senders and address any compliance failures by other providers.	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Retained from consultation proposal as **GCs C9.15 and C9.16**. We have extended the deadline for taking action in some limited circumstances. Additions made to our supporting guidance.
Passing requirements through the supply chain, through clear and unambiguous contractual terms, to ensure downstream parties supplying A2P messages are held contractually responsible for undertaking KYC, KYT and alphanumeric Sender ID checks.	Mobile operators and aggregators that transfer and/or terminate A2P messages.	Retained from consultation proposal as **GC C9.9.** Additions made to our supporting guidance.
Have processes to **regularly and proactively ensure they receive scam reports**, from customers and from appropriate third parties, relating to telephone numbers and URLs that have been used for scams	Mobile operators and tier 1 aggregators that transfer and/or terminate A2P messages	Largely retained from consultation proposal as **GC C9.6.** Additions made to our supporting guidance.
Blocking scam messages in transit: identifying and blocking scam messages in transit by detecting malicious URLs and telephone numbers, based on scam reports.	Mobile operators and tier 1 aggregators that transfer and/or terminate A2P messages	Retained from consultation proposal as **GC C9.7.** Additions made to our supporting guidance.

[262] While the provider that onboards the business customer will be directly responsible for conducting KYT checks, all other providers that transfer/terminate A2P messages are required to do so by taking the steps in Condition C9.9 regarding contractual terms.

Identifying scammers posing as business senders: conducting up-front due diligence, ongoing checks and incident management requirements

What we proposed

6.7 In our 2025 consultation, we proposed new rules that would set out that mobile operators and aggregators must:

- Conduct due diligence up-front to prevent scammers from using A2P services to contact potential victims. To do this, they must ensure that effective KYC checks are conducted at the point where a new business sender is acquired or signs up (the onboarding stage) (GCs C9.8 and C9.10).
- Prevent the use of fake alphanumeric sender IDs, including by corroborating sender IDs against the business information provided in KYC checks. Mobile operators must maintain a policy on protected brand IDs, generic IDs and special alphanumeric characters (GC C9.11).
- Conduct ongoing KYT checks, including reviewing data on: volume patterns; new or different use of alphanumeric sender IDs or telephone numbers; and any notifications of changes in business senders' profiles (GC C9.12).
- Take appropriate steps to ensure that business senders notify them of changes to their business or use of alphanumeric sender IDs (GC C9.14).
- Apply incident management processes where scam activity is identified to both block senders of scam messages from being able to send further messages and to ensure any compliance failures by other parties are addressed (GCs C9.15 and C9.16).
- Ensure that requirements related to up-front due diligence, ongoing checks, incident management and other measures are passed through the supply chain where needed, including to MSPs, by using clear and unambiguous contractual terms (GC C9.9).

6.8 In addition, we set out that:

- For mobile operators, we did not expect the costs of implementing our proposals to be significant in the round.
- We expected that aggregators and MSPs would incur costs beyond those that mobile operators would face, but we did not expect our proposals to impose significant or undue costs.
- As with our P2P blocking proposals, we identified risks related to potential interference with the right to privacy and the right to freedom of expression. We considered that our proposed safeguards would mitigate these.

6.9 Below, we take each aspect of our measures in turn, summarise comments we received and set out our assessment of each.

Stakeholder responses about these measures overall

6.10 Many respondents supported this set of proposals overall. Some respondents thought we should go further, while others raised concerns about the cost and impact of the proposed measures on the A2P market.

6.11 We did not receive formal responses from lower-tier or smaller aggregators. To ensure we could consider the perspective of these providers, we sought engagement from them following the consultation. Those we spoke to did not express significant concerns about

the proposed obligations.[263] [✂] said that the proposed obligations did not appear difficult to implement.[264]

Definitions including MSPs and aggregators

6.12 As set out above, these measures generally apply to communications providers that either act as aggregators or to providers that onboard business customers (which may include mobile operators).[265] However, the MEF said that the distinction we had drawn in our 2025 consultation between (i) providers that act as aggregators and/or onboard business customers and (ii) wider MSPs was not clear or workable. The MEF argued that modern messaging platforms routinely perform the functions of both.[266]

6.13 We had set out in the consultation that aggregators are providers that contract with business senders, MSPs, and other aggregators to arrange for the delivery of large volumes of A2P messages.[267] We had stated that MSPs are firms that specialise in interfacing directly with business senders and that, where a firm is acting purely as an MSP, it is not a regulated provider.[268]

6.14 For the purposes of clarifying firms' obligations under the GCs, we define business messaging providers as 'aggregators', subject to certain of our rules to combat scam messages, where they provide an ECS or ECN (such that the company is a regulated provider)[269] and act as an intermediary that transfers (either directly or indirectly) A2P messages between business senders and mobile operators.

6.15 We expect that this definition of an aggregator will include many companies that onboard business senders, which are the providers that must conduct due diligence and prevent the use of fake alphanumeric sender IDs.

6.16 Some MSPs require their business sender customers to sign up with a third-party aggregator, which will subsequently bill the business sender for messages they send. We intend for relevant rules to apply to aggregators that hold this billing relationship with business senders and not to these MSPs. Therefore, we have excluded from our definition of an aggregator any provider acting as such an intermediary that, while it may contract directly with business senders, it is acting in a capacity where its business sender customers must have a separate contractual relationship with a third party to transfer A2P messages.

---

[263] Meetings between Ofcom and [✂] in April 2026.
[264] Email sent by [✂] to Ofcom on 17 April 2026.
[265] Other than the requirement to set a policy restricting the use of protected alphanumeric sender IDs, which only applies to terminating mobile operators (GC C9.13).
[266] MEF response to October 2025 Consultation. Page 3.
[267] We stated that we consider all aggregators to be providing a public ECN in the form of a transmission system for the conveyance of mobile messages and/or a public ECS in the form of the provision of mobile messaging services that consist of, or have as their principal feature, the conveyance of signals. Ofcom, 2025. Combatting scam mobile messages. Page 9.
[268] We stated that, where a company is acting solely as an MSP (i.e. where they are not also providing an Electronic Communication Service (ECS) or Electronic Communication Network (ECN) such that they are also an 'aggregator'), we do not consider that it would be a communications provider for the purposes of the General Conditions (GCs). Ofcom, 2025. Combatting scam mobile messages. Page 9.
[269] These companies may be communications providers, as defined in the GCs, to the extent they are providing a public ECN in the form of a transmission system for the conveyance of mobile messages and/or a public ECS in the form of the provision of mobile messaging services that consist of, or have as their principal feature, the conveyance of signals.

6.17 To reflect this, we have amended the definition of aggregator in the GCs to exclude "intermediaries that contract directly with **Business Senders** but are acting in a capacity where that **Business Sender** is required to have a separate contractual relationship with a third party to transfer **A2P Messages"**. Therefore, where we refer to MSPs in this statement, we are referring to business messaging providers that are either not a communications provider as defined in the GCs or are acting in a capacity where their business sender customers must also sign up with a third-party aggregator, which will subsequently bill the business sender for messages they send. Our GC requirements do not apply to such MSPs directly (although aggregators may require them to be contractually responsible for undertaking checks).

6.18 We have also amended the definition of 'Business Sender' to ensure this captures any person (whether an individual, sole trader, partnership, company or other organisation).[270] We have further updated our definition of 'A2P Messages' to clarify that our rules relate to any messaging services that are sent using a public electronic communications service and/or network.[271]

Overall approach to A2P messaging

6.19 BT commented on the cost of our proposals in the light of our 2025 Business Messaging Review. In our January 2025 Business Messaging consultation, we proposed to cap the price that providers can charge for A2P messages. Following that consultation, MNOs made voluntary commitments relating to their pricing of A2P SMS termination and we did not impose a price cap.[272] BT commented that our proposals to address scams would increase operators' costs while the efforts of the Business Messaging Review would limit the profits it can make from A2P messaging.[273]

6.20 We consider that the voluntary commitments in relation to A2P termination are necessary to address our competition concerns in the A2P market. However, we also consider that the measures we are introducing in this Statement are needed to ensure consistent and effective protections from scams for customers.

Other issues

6.21 The Association of British Insurers (ABI) said that there should be a trusted flagger regime for fraudulent mobile messages and brand abuse, equivalent to that established by the Online Safety Act.[274] Our measures will ensure that providers access and make use of relevant intelligence on scam messages (both A2P and P2P), from end-users and appropriate third parties, and that they use it to protect consumers (see paragraphs 5.74-5.89, below).

---

[270] We have defined this as "any person, other than a Regulated Provider, that communicates with members of the public via A2P Messages. This includes, but is not limited to banks, schools, public bodies and retailers".
[271] We have defined 'A2P Messages' as "a message from a Business Sender, sent (either directly or indirectly) to Mobile Numbers using a software application and using a Public Electronic Communications Service and/or Public Electronic Communications Network".
[272] Ofcom, 2025. Business messaging statement. Pages 3-4.
[273] BT Group response to October 2025 Consultation. Page 4.
[274] The Association of British Insurers response to October 2025 Consultation. Page 3.

Know Your Customer checks

What we proposed

6.22 In our 2025 consultation, we proposed to require that all providers (mobile operators and aggregators) ensure effective KYC checks are carried out up-front. We proposed:

- An obligation for providers to implement and maintain appropriate and effective policies, systems and processes to ensure that, for any A2P messages that they transfer and/or terminate, KYC checks are conducted, in accordance with proposed GC C9.10. The provider could conduct the checks itself or could ensure that it has contractual terms in place to comply with proposed GC C9.9(a).
- That providers do not transfer and/or terminate A2P messages unless they are reasonably satisfied with the outcome of these checks or with the checks carried out by parties in their supply chain (proposed GC C9.8(b)).
- Minimum requirements for KYC checks, to require providers to carry out appropriate risk assessments to identify whether enhanced checks are necessary in a particular case and, if so, to carry out these checks. Our proposed guidance provided more information on the KYC checks we expect providers to make, indicators of a risk of scams that they should look out for and enhanced checks that may be appropriate to further inform their risk assessments.

Stakeholder responses

6.23 Some respondents suggested ways in which the KYC measures might be strengthened. Which? suggested that we should require enhanced due diligence checks for business senders based in high-risk countries and suggested expanding the list of indicators of a risk of scams in our guidance.[275] [✂] said that our KYC guidance should include directing providers to assess further red flags: for example, the presence of multiple companies linked to the same director.[276] [✂] said that industry should designate a neutral third-party verification authority as part of the due diligence process.[277]

6.24 We received some comments on the impact of our proposals on business senders. VodafoneThree said that any increased complexity or delay in onboarding could lead to loss of legitimate traffic.[278] The CCP-ACOD stressed that microbusinesses should not face disproportionate onboarding burdens as a result of our proposals.[279] [✂] said that the processes we proposed should not be allowed to impact critical communications, like NHS and HM Revenue & Customers messages.[280]

6.25 [✂] opposed the proposals, arguing that the existing trajectory of measures being taken by industry represented a more agile and effective approach to addressing our concerns. It characterised our proposals as a rigid checklist, which risked a compliance-driven culture at the expense of agile, intelligence-led fraud-prevention.[281]

Our assessment

6.26 Having considered the above stakeholder comments, we remain of the view that, despite some good practice in the A2P sector, current industry KYC measures as a whole are not

[275] Which? response to October 2025 Consultation. Pages 6-7.
[276] [✂] response to October 2025 Consultation.
[277] [✂] response to October 2025 Consultation.
[278] VodafoneThree response to October 2025 Consultation. Page 6.
[279] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 4.
[280] [✂] response to October 2025 Consultation.
[281] [✂] response to October 2025 Consultation.

sufficient to address the risk of scammers posing as legitimate businesses, as processes vary and providers apply them inconsistently. Accordingly, we have decided to require all providers (mobile operators and aggregators) to ensure effective KYC checks are carried out up-front by any provider that onboards business senders, as we proposed at consultation.[282]

6.27 We disagree with [✂] characterisation of these requirements, which we consider set out a necessary common industry standard for due diligence. This will not be at the expense of agile, intelligence-led fraud prevention, because we expect that providers will continue to carry out such activities, whilst meeting the standards set by our rules.

6.28 GC C9.8 requires providers to implement and maintain appropriate and effective policies, systems and processes to ensure that, for any A2P messages that they transfer and/or terminate, KYC checks are conducted in accordance with GC C9.10, either by the provider itself or by the provider ensuring that it has contractual terms in place to comply with GC C9.9(a).

6.29 The measures further require that providers do not transfer and/or terminate A2P messages unless they are reasonably satisfied with the outcome of these checks, or with the checks carried out by parties in their supply chain (GC C9.8(b)).

6.30 We have set out in the GCs what the KYC checks include, as a minimum. GC C9.10 sets outs the minimum baseline KYC checks we consider to be necessary, which include checks against:

- Information relating to the trading or registered name and registered office or trading address.
- The nature of the services being provided (and the purposes for which a business sender is seeking access to A2P messaging).
- Payment / bank account information, existing telephone numbers, websites, directors and persons of significant control.[283]

6.31 GC C9.10 also requires providers to carry out appropriate risk assessments to identify whether enhanced checks are necessary in individual cases and, if so, to carry out these checks.

6.32 In response to Which?'s suggestion that we require enhanced checks where a sender is operating in a high-risk country, we have updated our guidance to specify geographic location as a potential risk factor relevant to a provider's risk assessment, which might warrant undertaking enhanced checks. We have also updated our guidance to note that using an IP address that does not correspond to the purported business location would be an indicator of a risk of scams.

---

[282] As set out in section 2, we recognise that where regulated providers do not contract directly with business senders, they cannot conduct KYC checks directly. As explained above, MSPs are also not required to conduct KYC checks where they are either not a communications provider as defined in the GCs or are acting in a capacity where their business sender customers must also sign up with a third-party aggregator, which will subsequently bill the business sender for messages they send. Instead, we will require all parties to include clear and unambiguous contractual terms to ensure KYC checks are conducted by their downstream partners (see paragraph 6.73 and below).

[283] Companies House. Guidance: People with significant control (PSCs): How to identify and record the people who own or control your company.

6.33 In response to [✂] suggestion that our KYC guidance should include directing providers to assess further red flags (for example, the presence of multiple companies linked to the same director), we consider that our guidance already sets out relevant enhanced checks. In particular, the guidance sets out providers should undertake enhanced checks where risk factors are identified, including from details about individuals with influence over the businesses, such as owners and directors.

6.34 In paragraphs 2.87 to 2.95 of the guidance, we explain further:

- What KYC checks we expect providers to carry out (including that providers should assess whether information available publicly about the business sender matches information provided by that business sender).
- What indicators of a risk of scams providers should look out for.
- Where there are indicators of a risk of scams, the enhanced checks that may be appropriate to further inform the risk assessment (such as checking against the Cifas National Fraud and Insider Threat databases).[284]

6.35 It is important that the information providers hold from KYC checks remains up to date, to enable the KYT checks, reviews and updates of risk assessments we discuss below. As such, we will require that providers take appropriate steps to ensure that the business senders from whom they receive A2P messages are required to notify them promptly of any changes to their business profiles and changes in their use of the alphanumeric sender IDs (GC C9.14).

6.36 We expect that the application of baseline KYC checks across the whole of the A2P market will make it significantly harder for scammers to access A2P networks. Our accompanying guidance provides further details on how providers can comply with the obligations relating to KYC and alphanumeric sender IDs checks.

6.37 We note the view of some stakeholders that there may be a trade-off between a quick and easy onboarding experience for new business senders and one that includes the robust due diligence checks we will require. However, we consider that it will be possible for providers to perform onboarding processes that comply with our rules and do not discourage legitimate business senders from using A2P services.

6.38 We note comments from [✂] in favour of Ofcom designating a neutral third-party verification authority. However, we do not consider that this would be necessary to achieve our objective, while it could unduly constrain how providers conduct due diligence and how they prevent the use of fake alphanumeric sender IDs.

6.39 We want to ensure providers take a consistent approach across the A2P market. Our intervention will establish a common industry standard for robust up-front due diligence checks, while providers may determine the appropriate approach to meeting this standard. A common standard will ensure that those providers with more robust checks are not disadvantaged simply because they are operating responsibly to combat scams. We also consider that any additional burden these measures may place on new business senders when providing information necessary for KYC is necessary and proportionate to our policy objective.

[284] Cifas, National Fraud Database.

Preventing the use of fake alphanumeric sender IDs

What we proposed

6.40 In our 2025 consultation, we proposed to require that all providers (mobile operators and aggregators) ensure effective checks on new uses of alphanumeric sender IDs are carried out. We proposed:

- An obligation for providers to implement and maintain appropriate and effective policies, systems and processes to ensure that for any A2P messages that they transfer and/or terminate, alphanumeric sender ID checks are conducted in accordance with proposed GC C9.11. This could be either by the provider conducting the checks itself, or by the provider ensuring that it has contractual terms in place to comply with proposed GC C9.9(a).
- That providers do not transfer and/or terminate A2P messages unless they are reasonably satisfied with the outcome of these checks or with the checks carried out by parties in their supply chain (proposed GC C9.8(b)).
- To require providers to ensure that the proposed use of alphanumeric IDs is consistent with the nature of the business applying to use them, as set out in response to KYC checks. In our proposed guidance, we explained further how providers can carry out these checks, including that providers will have collected information from the business sender on the purpose for which they are seeking to send A2P messages as part of KYC checks, and that new uses of alphanumeric sender IDs must be compared against this stated purpose to make sure they align. We also explained that we do not expect a provider to allow a sender to use a brand name that it is not authorised to use to represent itself.
- That terminating mobile operators implement and maintain appropriate and effective policies, systems and processes on the use of certain protected alphanumeric sender IDs and communicate this policy to their downstream supply chain (proposed GC C9.13).

Stakeholder responses

6.41 [✂] suggested that our proposals related to alphanumeric sender IDs were duplicative of existing practices, were therefore unnecessary and introduced undue restrictions on brands.[285]

6.42 VodafoneThree expressed concern that our proposals to prevent the use of fake sender IDs would not be workable, due to the large number of UK business senders.[286] It suggested that the proposals would require business senders to undertake audits of the sender IDs they already have in use. VodafoneThree suggested that Ofcom should instead focus protections on the sender IDs used by larger businesses most at risk of impersonation and encourage further adoption of the sender ID registry run by the MEF.

6.43 The Campaign Registry and Twilio suggested that our proposals would reinforce inconsistencies in the approaches different providers take to address scams.[287] Twilio said that the new rules we proposed for onboarding and terminating providers risked entrenching fragmentation in how providers manage the use of sender IDs. Where different providers protect different IDs, it argued this would result in an inconsistent experience for legitimate business senders, while scammers could continue to exploit inconsistencies in

[285] [✂] response to October 2025 Consultation.
[286] VodafoneThree response to October 2025 Consultation. Page 6.
[287] The Campaign Registry response to October 2025 Consultation. Page 7; Twilio response to October 2025 Consultation. Page 8.

the types of sender IDs they can use on different networks. It argued for a central, regulator-led sender ID registration solution. [288]

6.44 We received other stakeholder comments in relation to a mandatory and centralised system of sender ID registration. We discuss this in section 8.

Our assessment

Requirements for checks on the use of new alphanumeric sender IDs

6.45 Having considered stakeholders comments, we remain of the view that our proposed measures regarding alphanumeric Sender IDs are necessary and proportionate. As such, GC C9.11 sets out obligations to prevent the use of fake alphanumeric sender IDs whenever customers are seeking to use a new alphanumeric ID. We will require providers to ensure that the proposed use of alphanumeric IDs is consistent with the nature of the business applying to use them. Providers will have gathered information on the nature of the business as part of KYC checks.

6.46 GC C9.8 requires providers to implement and maintain appropriate and effective policies, systems and processes to ensure that, for any A2P messages that they transfer and/or terminate, checks relating to the use of any alphanumeric sender IDs are conducted in accordance with GC C9.11, either by the provider itself or by the provider ensuring that it has contractual terms in place to comply with GC C9.9(a).

6.47 The measures further require that providers do not enable the use of the relevant alphanumeric sender IDs unless they are reasonably satisfied with the outcome of these checks, or with the checks carried out by parties in their supply chain (GC C9.8(b)).

6.48 In paragraphs 2.98-2.103 of the guidance, we explain further how providers can carry out these checks, including that providers will have collected information from the business sender on the purpose for which they are seeking to send A2P messages as part of KYC checks. They must compare new uses of alphanumeric sender IDs against this stated purpose to make sure they align. We also set out that we do not expect a provider to allow a sender to use a brand name that they are not authorised to use to represent themselves.

6.49 The obligations will help prevent a scammer from posing as a legitimate low-risk business (such as a restaurant seeking to send booking reminders) and subsequently abusing access to alphanumeric IDs to send scam messages that are clearly unrelated to their stated purpose (such as a delivery fee scam, using an alphanumeric ID that appears to be a delivery company).

6.50 Noting VodafoneThree's comments that the proposed requirements would be unfeasible due to the number of currently active senders, we do not consider that new measures would require providers to undertake audits of sender IDs already in use. Rather, the requirement will apply to the registration of new business senders and to existing business senders seeking to use new alphanumeric sender IDs. We recognise there is some risk in not extending our requirements to sender IDs already approved for use. However, we agree that to do so would be a significant burden on providers. In addition, our requirement for ongoing KYT checks and incident management will address fake sender IDs already in use, as many of these will be caught as part of these ongoing checks and measures.

[288] Twilio response to October 2025 Consultation. Page 8.

Requirements to set a policy on protected alphanumeric sender IDs

6.51 To further protect against the abuse of alphanumeric sender IDs, GC C9.13 requires terminating mobile operators to implement and maintain appropriate and effective policies, systems and processes on the use of specific protected IDs,[289] generic IDs[290] and special alphanumeric characters[291] within alphanumeric IDs. We have imposed this requirement on terminating mobile operators only, as these providers should have the ability to communicate sender ID restrictions to their downstream supply chain and enforce them with respect to all traffic that downstream providers transfer to them.[292] This should ensure that the measure is effective.

6.52 All other providers will, where applicable, need to review any proposed use of new alphanumeric sender IDs against these policies (GC C9.11(b)). We set out in our guidance ways in which providers can design these policies to minimise the risk of brand impersonation by scammers (paragraphs 2.129-2.138).

6.53 We disagree with those stakeholders that suggested these policies would introduce inconsistencies between providers' approaches. We consider that, by requiring terminating mobile operators to implement and maintain these policies, we will ensure a more consistent approach to sender IDs than is in place at present. We have amended our guidance to encourage providers to proactively share their policy and lists with other terminating providers to help enable this.

Conducting ongoing KYT checks

What we proposed

6.54 In our 2025 consultation, we proposed to require that all providers (mobile operators and aggregators) ensure effective KYT checks are carried out on A2P message traffic. We proposed:

- Obligations for providers to implement and maintain appropriate and effective policies, systems and processes to ensure that, for any A2P messages that they transfer and/or terminate, KYT checks are conducted in accordance with proposed GC C9.12 (proposed GC C9.8(a)).
- That providers do not transfer and/or terminate A2P messages unless they are reasonably satisfied with the outcome of these KYT checks or with the checks carried out by parties in their supply chain (proposed GC C9.8(b)).
- That providers: monitor and review data on volume patterns; identify new or different use of alphanumeric sender IDs or telephone numbers; and check any information on or notifications of changes in business profiles, for any indicators of scam activity, as part of these KYT checks (proposed GC C9.12(a)).

[289] Alphanumeric sender IDs that should only be used by high-profile organisations and brands they relate to, or close imitations of these that should not be used by any sender.
[290] Alphanumeric sender IDs that do not help to identify the sender but could be used by scammers to add credibility to their messages, e.g. 'Delivery', 'Alert' or 'Urgent'.
[291] Special alphanumeric characters include those outside of the standard Aa-Zz alphabet and 1-9 number set. They can include obscure punctuation, or non-Latin alphabet characters, which can be used to closely mimic legitimate business names.
[292] GC C9.13 has also been amended to make clear that the objective of the policies, systems and processes relating to Protected Alphanumeric Sender IDs is to prevent their use for scams.

- That insights from this work should be used to review and update customer risk assessments (proposed GC C9.12(b)).
- That, where there are indicators of scam activity, appropriate evidence that the messages are legitimate must be sought. Providers must block A2P messages that they reasonably believe were intended to scam the recipients (proposed GC C9.12(c)).

Stakeholder responses

6.55 Twilio supported approach in principle but sought clarity on how to perform KYT checks in accordance with guidance we set out elsewhere in the consultation on the rights of users and data protection considerations.[293]

Our assessment

6.56 Taking into account respondents' comments, we remain of the view that mobile operators and aggregators applying more consistent and effective KYT processes would help protect consumers where scammers successfully evade KYC processes and compromise legitimate, operative sender accounts.

6.57 Some scammers are likely to find ways around baseline up-front due diligence checks. As set out in section 4, providers' inconsistent approaches to managing this risk by applying effective KYT checks are likely to allow scammers to further evade detection.

6.58 GC C9.8(a) imposes obligations on providers to implement and maintain appropriate and effective policies, systems and processes to ensure that, for any A2P messages that they transfer and/or terminate, KYT checks are conducted in accordance with GC C9.12. These checks must be performed either by the provider themselves, or the provider must ensure that it has contractual terms in place, compliant with GC C9.9, to ensure they are carried out by others in their supply chain.

6.59 We will require that providers do not transfer and/or terminate A2P messages or enable business senders to use requested alphanumeric sender IDs unless they are reasonably satisfied with the outcome of these KYT checks or with the checks carried out by parties in their supply chain (GC C9.8(b)).

6.60 The obligations ensure that providers conduct specific ongoing KYT checks for scam indicators. Our rules require providers to: monitor and review data on volume patterns; identify new or different use of alphanumeric sender IDs or telephone numbers; and check any information on or notifications of changes in business profiles, for any indicators of scam activity (GC C9.12(a)).

6.61 Some of these checks may not, in isolation, identify that scam activity is occurring with a high level of reliability. Therefore, it is important that providers consider a range of factors and gather further evidence where they identify scam indicators. Under GC C9.12(b), providers should use insights from this work to review and update customer risk assessments. Our accompanying guidance for industry sets out some indicators of a risk of scams and what enhanced checks providers can carry out when these arise.

6.62 GC C9.12(c) further requires that, where there are scam indicators, providers must seek appropriate evidence that the messages are legitimate and block messages where the provider reasonably believes that the relevant A2P messages were intended to scam the intended recipients.

---

[293] Twilio response to October 2025 Consultation. Page 7.

6.63 We recognise that some upstream mobile operators and aggregators will not have sight of all of the information necessary to conduct these checks effectively. Therefore, as we set out below, where providers do not contract directly with the business senders, they will be required to apply clear and unambiguous contractual terms to ensure partners in their supply chain conduct KYT checks. This requirement will help to address issues of opacity in the supply chain and ensure that there is a second layer of defence for consumers from scam A2P messages.

6.64 Our guidance (paragraphs 2.106-2.115) provides further details on how providers could comply with the obligations relating to KYT, including how providers could monitor volume patterns, use of sender IDs and changes in business profiles. As explained at paragraph 2.115 of the guidance, we encourage mobile operators and aggregators to establish intelligence sharing mechanisms and encourage them to share information with other companies in their supply chain on tactics of detecting and assessing potential scam activities.

6.65 In response to Twilio's query about conducting KYT checks in line with users' rights and data protection, we consider that the guidance we have set out provides the necessary clarity on these points, including associated scam indicators that providers must monitor.

6.66 While our KYT rules do not require providers to access the content of messages, providers may consider this appropriate on a case-by-case basis if, in doing so, they are satisfied they are complying with any other relevant legal obligations (including relevant data protection legislation as set out in paragraphs 2.248-2.258 of our guidance).

Ensuring that requirements are passed through the supply chain

What we proposed

6.67 In our 2025 consultation, we proposed to require all providers to have clear and unambiguous contractual terms that ensure downstream parties from whom they receive A2P messages are held contractually responsible for performing or ensuring that KYC, KYT and alphanumeric sender ID checks are undertaken (proposed GC C9.9(a)). We also proposed to require providers to have contractual terms governing other aspects of downstream parties' activities in relation to preventing scams and our rules.

6.68 We proposed to require providers to ensure ongoing compliance with the obligations imposed and to take appropriate, effective and prompt action to address non-compliance (proposed GC C9.9(b)).

Stakeholder responses

6.69 Several providers expressed concerns about proposed GC C9.9, which would require certain contractual terms to flow down through supply chains, and about how these terms could be enforced. This measure is intended to ensure that downstream aggregators and MSPs are made contractually responsible for undertaking KYC, KYT and alphanumeric Sender ID checks.

6.70 BT, Mobile UK, [✂], VodafoneThree and Virgin Media O2 all commented on the importance of Ofcom's role as the enforcer of firms' compliance with the proposed

requirements.[294] BT said that a robust Ofcom enforcement programme should underpin the required contractual obligations.[295] VodafoneThree said that, where an aggregator fails to implement KYC checks properly, Ofcom should enforce its obligations, rather than other operators.[296] [✂] argued that the proposals would position it as a regulator for a global supply chain and create significant legal and operational burdens.[297] Virgin Media O2 argued that the contractual requirements were well intentioned but overly burdensome.[298] Mobile UK said that relevant businesses were often competitors in some form and that there was potential for operators to face unfair action.[299]

6.71 Twilio and BT raised reservations about the complexity of changing contractual agreements already in operation to comply with the proposed requirements.[300] Twilio said that this could be time-consuming and that commercial renewal cycles and negotiations would constrain this.[301]

6.72 Twilio also said that, while it agreed with Ofcom's objective of ensuring KYC checks take place, it would welcome additional guidance on how Ofcom expects providers to demonstrate compliance with the requirement to be 'reasonably satisfied' that checks are being performed by other parties. It also raised this question in relation to existing contracts.[302]

Our assessment

6.73 Having considered stakeholders' comments, we remain of the view that contractual requirements are necessary and proportionate to achieve our policy objective. As set out in section 4, mobile operators and aggregators often rely on generic contractual provisions for downstream aggregators to prevent scams. Some mobile operators have sought to address this through dedicated commercial codes.[303] These codes typically aim to prohibit downstream aggregators and MSPs from passing on harmful or illegal messages, but do not generally specify the preventative actions that these parties should take or the consequences of non-compliance.

6.74 We consider that applying KYC, KYT and fake alphanumeric sender ID requirements to all providers is necessary to ensure providers undertake checks in all circumstances. We also recognise that some upstream mobile operators and aggregators will not hold the relationship with the business sender necessary to conduct these checks. Therefore, to ensure that providers pass requirements to combat scam messages through the supply chain, GC C9.9(a) will require all providers to have clear and unambiguous contractual

---

[294] BT Group response to October 2025 Consultation. Page 9; VodafoneThree response to October 2025 Consultation. Page 6; Virgin Media O2 response to October 2025 Consultation. Page 3; Mobile UK response to October 2025 Consultation. Page 3; [✂] response to October 2025 Consultation.
[295] BT Group response to October 2025 Consultation. Page 9.
[296] VodafoneThree response to October 2025 Consultation. Page 6.
[297] [✂] response to October 2025 Consultation.
[298] Virgin Media O2 response to October 2025 Consultation. Page 3.
[299] MEF response to October 2025 Consultation. Pages 2-3.
[300] Twilio response to October 2025 Consultation. Page 6; BT Group response to October 2025 Consultation. Page 8.
[301] Twilio response to October 2025 Consultation. Page 6.
[302] Twilio response to October 2025 Consultation. Pages 6-7.
[303] As described in paragraph 4.48, contractual codes currently used by a small number of mobile operators include, for example, specific due diligence requirements and obligations to pass requirements on to downstream aggregators.

terms that ensure downstream parties from whom they receive A2P messages are held contractually responsible for:

- Undertaking KYC checks, KYT checks and checks relating to the use of sender IDs.
- Not transferring A2P messages or enabling the use of sender IDs unless they are reasonably satisfied with outcomes of the checks set out above.
- Taking appropriate, effective and prompt action in response to any reports of A2P message coming from their service that are suspected of being sent with the intention to scam the recipients.
- Retaining records in line with GCs C9.22-C9.25.
- Taking appropriate steps to ensure that business senders notify the party with the direct relationship to the business sender of changes to a business sender's business profile or otherwise ensure that party will be notified of such changes.

6.75 GC C9.9(b) will also require providers to implement and maintain appropriate and effective policies, systems and processes to ensure ongoing compliance with the contractual terms, monitor and assess compliance with the obligations imposed and take appropriate, effective and prompt action to address non-compliance.

6.76 We note some stakeholders' concerns that ensuring other firms' ongoing compliance with contractual terms places a burden on providers to enforce regulatory requirements. We consider it appropriate to require industry to conduct due diligence that covers whether potential partners comply with rules to combat A2P scam messages. This is particularly important given the number of stakeholders involved in complex supply chains, which will often mean industry, rather than Ofcom, is best placed to quickly identify and address potential non-compliance. We also note that, as set out in section 4, some operators already have processes in place to enforce compliance with existing contractual codes of practice and take action to address non-compliance.

6.77 Ofcom has powers take enforcement action against potential non-compliance and we will consider how it may be appropriate to monitor over time whether providers are complying with our rules. Industry may also report potential non-compliance to Ofcom. We will decide whether, and against which provider(s), to take enforcement action, taking into account evidence of potential non-compliance and our administrative priorities framework in our Regulatory Enforcement Guidelines.

6.78 Twilio queried how providers can demonstrate that they are reasonably satisfied that other parties have performed relevant checks on business senders. Under GC C9.9(a)(i-iv), it is for providers to set clear and unambiguous contractual terms for downstream parties to hold them contractually responsible for performing checks. However, under these terms, downstream parties must not transfer A2P messages or enable to use of relevant alphanumeric Sender IDs unless *they* (the downstream party) are reasonably satisfied with the checks they have undertaken, or with the checks that the party that onboarded the business sender conducted. In practice, parties in the supply chain may need to communicate to ensure that the party that onboarded the business sender is subject to the relevant terms and conducts relevant checks.

6.79 We are more likely to take action against the provider we consider primarily responsible for any non-compliance but may also take action against providers that we consider have failed to take appropriate steps to prevent that non-compliance. We have updated our guidance to reflect this.

6.80 We consider that these measures will reinforce our direct regulatory requirements, drive compliance within industry and provide for engagement between firms for incident management purposes.

6.81 As stakeholders have noted, we recognise that implementing new contractual and/or technical arrangements will take some time. We consider that we have reflected this in the implementation period for the A2P package of measures, set out in section 9.

6.82 Our accompanying guidance for industry (paragraphs 2.118-2.126) provides further details on how providers could comply with the obligations relating to contractual requirements, including how providers may ensure compliance with any contractual terms they impose on downstream parties.

Incident management requirements

What we proposed

6.83 In our 2025 consultation, we proposed to require providers to take certain actions, within a specified period, when they become aware of scam messages.

6.84 Proposed GC C9.15 set out actions to be completed within one working day, where the provider holds a direct relationship with the business sender that sends, or attempts to send, an A2P message that the provider reasonably believes was intended to scam the recipient.

6.85 Proposed GC C9.16 set out actions to be completed within two or three working days, where the provider does not hold a direct relationship with the business sender, when there is a 'Significant Scams Incident' as defined in our proposed GCs.

6.86 In both cases, these proposed measures would ultimately require a provider to prevent a business sender from sending further messages, absent satisfactory explanation and evidence.

Stakeholder responses

6.87 [✂] said that the incident management requirements would help to mitigate the impact of and losses from mobile messaging scams.[304]

6.88 Sky and [✂] disagreed with the proposed timelines for certain actions associated with the proposed incident management requirements.[305]

Our assessment

6.89 Taking into account stakeholders' comments, we have retained the incident management requirements, which we continue to consider necessary and proportionate, with one amendment. At present, we understand that in many cases where providers identify scams, aggregators do not follow up with downstream aggregators or MSPs to identify the original business sender or establish how incidents occurred, including whether downstream firms made the right checks.[306] We consider that this approach to incident management is not sufficient to meet our policy objective, because it does not do enough to expel scammers from A2P channels.

---

[304] [✂] response to October 2025 Consultation.
[305] Sky response to October 2025 Consultation. Pages 3-4; [✂] response to October 2025 Consultation.
[306] Formal information request responses.

6.90 To address this, we will require providers to take certain actions, within a specified period, when they become aware of an incident of scam messages. As set out in our 2025 consultation, these measures ultimately require a provider to prevent a business sender from sending further messages, absent satisfactory explanation and evidence.

6.91 Two stakeholders commented on the specified periods within which we proposed providers must take action:

- Sky said that deadlines of two or three working days would offer insufficient time to confirm the business sender and prevent them from sending further messages (under proposed GC C9.16, these deadlines would apply where an incident takes place involving a business sender that the provider did not onboard and where one or more aggregators are involved, respectively). Sky argued that, in some cases, lengthy international supply chains would make two or three working days insufficient to be able to gather evidence from other parties. It proposed that Ofcom extend the deadlines to ten working days.[307]
- [✂] made similar points and said that the requirement to pause a direct customer within one working day was operationally untenable. It argued that the incident management timelines we proposed were disproportionate and an unreasonable burden to place on providers.[308]

6.92 We expect providers to hold appropriate contact details for their customers and that parties down the supply chain should also hold appropriate contact details for parties from which they received messages:

- In cases involving a business sender that the provider itself has onboarded (i.e. its direct customer), it is reasonable to expect providers to take appropriate action to prevent the sender from sending further messages within one working day. We note that this requirement applies where providers are reasonably satisfied that the messages were intended to scam the recipient.
- In cases where there is only one aggregator involved, we consider two working days is a reasonable and proportionate period to carry out the actions we require, as only one point of contact is required.
- In cases involving more than one aggregator, we expect parties may require more time to communicate across the supply chain. We have therefore decided to extend the relevant deadline from three up to five working days, which we consider is a reasonable and proportionate period to undertake the actions we require. We consider that, if this period were extended beyond five working days, for example to ten working days as Sky has suggested, there would be a significant risk that customers would receive a large number of further messages from unchallenged scammers.

6.93 We have amended the incident management requirements accordingly.

6.94 Under GC C9.15, providers that hold a direct relationship with a business sender that sends, or attempts to send, whether directly or indirectly through MSPs, an A2P message that the provider reasonably believes was intended to scam the recipient, must within one working day:

[307] Sky response to October 2025 Consultation. Pages 3-4.
[308] [✂] response to October 2025 Consultation.

- Confirm the identity of the business sender responsible for those messages (GC C9.15(a)). This should enable providers to rule out the possibility that messages originated from a different source or confirm the business sender's account has not been compromised.
- Implement appropriate measures to prevent the sender from sending further A2P messages using the provider's services, unless they have satisfactory evidence that either the sender was not responsible for sending the scam messages or the relevant message was not intended to scam the recipients (GC C9.15(b)).

6.95 GC C9.16 requires providers that do not hold a direct relationship with a business sender responsible for scam messages to take certain actions where there is a significant scams incident.[309] These are:

- To take appropriate steps to confirm the relevant sender and prevent that sender from sending further messages, unless they have satisfactory evidence that either the sender was not responsible for sending the scam messages or the relevant message was not intended to scam the recipients (GC C9.16(a)). We require providers to carry out these actions within two working days in cases involving no more than one aggregator or five working days in all other cases.
- To establish whether downstream aggregators or MSPs that delivered the relevant A2P messages to the provider complied with contractual requirements the provider placed on them to conduct the required checks (GC C9.16(b)(i)):
    - The provider will need to check that sufficient KYC checks, checks on the use of sender IDs and KYT checks had been conducted on the business sender.
    - Where they have not, the provider will need to take appropriate and effective action to address non-compliance and, if applicable, satisfy itself the downstream aggregator or MSP will comply in future (GC C9.16(b)(ii)).
    - The provider should follow a clear and robust escalation process to address non-compliance, leading ultimately to ceasing to accept downstream aggregators' messages where they are failing to comply.
    - Providers must carry out these actions promptly, within 15 working days.

6.96 We consider that these requirements will set clear expectations of providers where they detect A2P scam incidents. This will in turn mean that providers manage more incidents effectively and therefore shut down A2P scam campaigns more quickly.

6.97 Our guidance (paragraphs 2.148-2.162) provides further details on how providers could comply with their obligations relating to incident management, including how providers: may confirm and/or identify a business sender responsible for sending scam messages and prevent them from sending further messages; may establish whether their downstream parties complied with relevant contractual obligations, including conducting appropriate checks; and what actions they might take in the event of downstream parties not complying with the relevant contractual obligations.

[309] By significant scams incident we mean "a situation where it appears to the Regulated Provider that a particular Business Sender has cumulatively sent or attempted to send, directly or indirectly, at least fifty A2P Messages that the Regulated Provider reasonably believes were intended to Scam the recipient/s" (see the GC 'Definitions').

Measures to identify scammers posing as business senders: summary of assessment

6.98 Based on our assessment of each A2P measure above, we consider that our requirements for providers to conduct KYC and KYT checks, prevent the use of fake alphanumeric sender IDs, ensure that requirements are passed through the supply chain, and apply incident management processes, will work together as a set of measures to make it more difficult for scammers to pose as legitimate business senders.

6.99 Below, we consider the costs and impacts of this set of measures before concluding on its proportionality.

Costs and impacts of measures to identify scammers posing as business senders

Stakeholder responses

Cost of our proposals

6.100 The MEF, which represents companies involved in the provision of mobile services, said that we have underestimated the cumulative operational and financial impacts of our proposed A2P measures, including the time, resources and coordination required.[310]

6.101 The FCS, which represents companies that provide communications services to business users, highlighted additional costs for smaller providers and resellers and requested that we set out clearly the obligations of smaller providers at each level of the supply chain.[311]

6.102 [✂] submitted that our impact assessment did not account for high customer churn in the industry, which means there is no guarantee it will be able to recoup costs associated with KYC, KYT and sender ID checks.[312]

Impact on competition and innovation

6.103 Several stakeholders raised points relating to the impacts of our proposals on competition in the A2P market.

6.104 techUK argued that mandating KYC and KYT checks across all tiers of aggregators would introduce risks to competition, if this would require firms to share customer data with competitors.[313]

6.105 Twilio and techUK raised concerns that our proposed alphanumeric ID requirements would increase the regulatory burden on aggregators and raise barriers to entry in the A2P market.[314]

6.106 VodafoneThree and Utility Warehouse highlighted that regulatory frictions could push businesses towards online alternatives to A2P SMS.[315] Utility Warehouse highlighted the risk that increased regulation in the A2P market will displace fraud to other platforms.

---

[310] MEF response to October 2025 Consultation. Page 9.
[311] FCS response to October 2025 Consultation. Page 1.
[312] [✂] response to October 2025 Consultation.
[313] techUK response to October 2025 Consultation. Page 4.
[314] Twilio response to October 2025 Consultation. Page 8; techUK response to October 2025 Consultation. Page 4.
[315] VodafoneThree response to October 2025 Consultation. Page 6; Utility Warehouse response to October 2025 Consultation. Page 5.

6.107 [✂] said that requiring both MNOs and aggregators to implement our proposals could mean that [✂] faces cost recovery from both parties.[316]

Our assessment

Financial costs of our requirements

Costs to mobile operators

6.108 In our 2025 consultation, we noted the potential contractual and compliance-based costs to mobile operators from our requirements to identify scammers posing as business senders. However, we set out that we do not expect the incremental costs to be significant in the round:

- **One-off contractual costs:** we expect these costs of establishing contractual amendments and communicating these to aggregator partners to take the form mainly of amendments to existing contracts. We do not consider such costs to be significant, given that we expect mobile operators to have existing staff to engage with, and manage, downstream customers. Some additional staff time may be required but we do not expect this to require additional headcount or new systems.
- **Ongoing costs of incident management**: we understand from evidence gathered via formal information requests that many providers already have some processes in place for incident management and therefore we do not expect this to result in material additional costs to providers.[317]

6.109 We invited further evidence from stakeholders on our assessment of these costs and we did not receive evidence that suggests mobile operators will face significant direct costs, specifically. We remain of the view that mobile operators will not incur significant direct costs from conducting A2P KYC, sender ID and KYT checks, as we understand that aggregators and MSPs would bear most such costs. We discuss this below.

Costs to aggregators and MSPs

6.110 As set out in our 2025 consultation, we expect that aggregators and MSPs would incur costs beyond those faced by mobile operators. We note that there are likely to be hundreds of aggregators and MSPs across the market that our rules will impact, the vast majority of which operate at tier 2 level or below (there are around 30 tier 1 aggregators).[318] While many tier 1 aggregators already carry out KYC and KYT checks (which they or a third party conduct), we believe that lower-tier aggregators and MSPs are likely to undertake these checks inconsistently at present.

6.111 Regarding the specific costs we expect aggregators and MSPs to incur, these include:

- **One-off contractual costs:** we do not expect these costs to impose a significant additional burden on aggregators, given that (as for mobile operators) we expect aggregators to have existing staff who can engage with, and manage, upstream and downstream stakeholders. The MEF said that we have underestimated the cumulative operational and financial impacts of our proposed A2P measures, including the difficulty of making large-scale contractual changes across complex A2P supply chains, particularly for providers without direct relationships with business senders.[319] We recognise the MEF's view of the challenges,

[316] [✂] response to October 2025 consultation.
[317] Formal information request responses.
[318] Ofcom, 2024. Call for input: Reducing mobile messaging scams, paragraph 3.6.
[319] MEF response to October 2025 Consultation. Page 9.

which we consider we have accounted for in the implementation period for the A2P package of measures.

- **Ongoing administrative costs of KYC and sender ID checks:** we understand that some KYC checks might cost an aggregator or MSP around £30 per customer,[320] which we do not consider to be significant. [✂] said that we did not account for standard onboarding procedures or the high customer churn in the industry. It considered that this churn means there is no guarantee that aggregators will be able to recoup costs associated with KYC, KYT and sender ID checks. As explained below in paragraph 6.112, we recognise that these measures will create some additional burden for industry, but we consider this is proportionate to our policy objective. We also remain of the view that sender ID checks should be a standard administrative operation and not unduly costly.
- **Ongoing administrative costs of KYT checks:** we do not have specific information on the likely scale of the ongoing administrative costs of KYT checks. However, we understand that aggregators have the functionality to inspect traffic on their networks (e.g. through sender ID and/or volumetric searching/filtering) and therefore should already have at least a basic understanding of their traffic.[321]
- **Ongoing costs of incident management:** we understand that most aggregators do not currently have formal processes in place for incident management.[322] However, we do not consider that this will impose significant additional costs on aggregators or MSPs, as we expect these processes will not require new expertise and therefore should not require additional staff.

6.112 We note FCS and the MEF's broader comments that our A2P measures will have a significant cumulative financial impact, in particular for smaller providers and resellers. However, we recognise that these measures will create some additional burden for industry, but we consider this to be proportionate to their benefits.

6.113 We note that there are other cross-cutting measures (that enhance our measures and safeguard individual rights) that apply to our A2P measures, as discussed in section 7. We do not consider that these GCs would materially add to the costs that mobile operators, aggregators or MSPs incur.

Potential risks of other adverse impacts

Potential interference with the right to privacy under Article 8 ECHR and data protection considerations

6.114 Our requirements for up-front due diligence, ongoing checks and incident management requirements reflect in part some existing industry practice. However, we recognise that some of these measures may interfere with the right to privacy under Article 8 ECHR. In particular, our KYT requirements to monitor and review data on volume patterns for any scam indicators would involve reviewing traffic data and associated metadata.

6.115 Where providers identify scam indicators, there may be further impacts on the right to privacy under Article 8 if a provider reviews the content of messages to determine whether the messages are legitimate or not, and those messages are in fact legitimate.

---

[320] Mobile Ecosystem Forum, The Brand's Guide to 10DLC Business Texting, p. 34. Monetary units were originally in USD ($40) and converted to GBP.
[321] Formal information request responses.
[322] Based on our 2025 RFIs.

6.116 Our requirements are also likely to involve the processing of some personal data (i.e. data where an individual is identifiable).

6.117 We have included various safeguards in our rules to limit any interference with the right to privacy under Article 8 ECHR and potential adverse data protection impacts. We also consider the risk of those adverse impacts arising (and any associated harm) to be low (see our rights assessment in section 8 and Annex 4).

Over-blocking and potential interference with the right to freedom of expression under Article 10 ECHR

6.118 Any blocking that occurs under these requirements would result from the provider reasonably satisfying itself that the relevant numbers have sent scam messages or the relevant messages contain scam URLs or telephone numbers. If any legitimate messages are blocked, this is therefore likely to be the result of incorrect human review in the course of KYT checks, which we consider to be low risk.

6.119 We have included various safeguards in our rules to mitigate this risk of over-blocking and consider the risk of over-blocking (and any associated harm) to be low (see our rights assessment in section 8 and Annex 4).

Impact on competition and innovation

6.120 We consider the impact on competition and innovation for our package of measures in the round, as part of proportionality assessment in section 8. For the reasons set out there, we do not expect these measures to have a material negative impact on competition or innovation.

6.121 As noted in paragraphs 6.103-6.107 we received a number of concerns from stakeholders about the impact of our A2P measures on competition, which we address below.

6.122 techUK expressed concern about requiring KYC and KYT checks across all tiers of the aggregator supply chain, if this requires firms to share customer data with retail competitors. We note that the requirements to ensure KYC and KYT have been conducted, set out in GC C9.9, do not necessitate information sharing and providers can meet them by ensuring that downstream parties have undertaken checks. Our incident management requirements (GC C9.16) may require some customer data to be shared but should involve sharing data on a legitimate customer only in cases of false positives or account hacking.[323]

6.123 We have amended our guidance to set out the principles we expect providers to take into account when assessing what information may be necessary to share to comply with our incident management requirements.

6.124 Given the factors we have set out above, we do not expect that our measures pose a risk to competition from sharing of customer data to a degree that would outweigh the benefits of our incident management requirements in helping to achieve our objective.

6.125 Twilio and techUK raised concerns about our proposed alphanumeric sender ID requirements. Twilio said that fragmented sender ID checks would increase burdens on aggregators, as they would need to comply with different expectations from each operator. It considered that this would increase barriers to entry and harm competition and

[323] In cases where a scam business sender has been identified, any information shared will not belong to a legitimate customer that providers might otherwise compete for.

innovation in the A2P market.[324] techUK stated that mandatory sender ID registries have proven cumbersome and risk disrupting A2P traffic flows.[325]

6.126 We recognise that differences in how aggregators need to comply with operators' sender ID checks may increase their costs and that this could have a greater impact on smaller players or new entrants. However, our measures build on the processes already in place in the market, with which many aggregators will be familiar. In addition, our guidance (which outlines what we would expect from these sender ID checks) should enable greater consistency in operators' approaches and a level playing field. In this light, we do not expect the incremental costs arising from our measure to have a material impact on market entry costs, competition or innovation.

6.127 We note VodafoneThree and Utility Warehouse's concerns that additional regulation of A2P mobile messaging could drive businesses to use alternative online channels.[326] We note that the challenges of combatting scam messages differ between these channels and we set out our approach to tackling fraud on relevant online services in paragraphs 2.2-2.8.

6.128 With respect to A2P messaging, we require providers to implement best practice that some players already apply. We also consider a minimum and consistent standard across A2P SMS is necessary to reduce scam messages and protect consumers.

6.129 Finally, [✂] said that requiring both MNOs and aggregators to implement our proposals could mean that [✂] faces cost recovery from both parties. It considered this could increase the A2P termination rate and make it harder for [✂] or its partners to compete in the business messaging market.[327] We understand that many providers already have appropriate scam prevention measures in place and will not incur additional costs as a result of our measures. To the extent there is a cost associated with compliance with these measures, we would expect this to be reflected in wholesale and retail prices. We have not seen evidence of a price impact on providers such as [✂] that would materially affect market competition, and other respondents did not raise this as a concern.

We expect the benefits of these A2P measures to identify scammers posing as business senders outweigh any costs or adverse impacts

6.130 Taking into account stakeholder comments, we consider that these measures should not impose significant costs on mobile operators, aggregators or MSPs, although we expect aggregators and MSPs to bear most of the incremental costs. In addition to this limited financial impact, we expect that there will not be a material impact on competition and innovation.

6.131 The costs of these A2P requirements are likely to be low relative to the expected benefits of preventing scammers from accessing A2P channels, which we expect to be significant, as discussed in paragraphs 8.4-8.8.

6.132 Taking into account all relevant factors (including our assessments above and in relation to our overall package of measures in Section 8), we consider this collection of A2P measures

[324] Twilio response to October 2025 Consultation. Page 8.
[325] techUK response to October 2025 Consultation. Page 4.
[326] As noted in our business messaging statement, online messaging services have been growing faster than A2P SMS volumes, but the latter is still growing and remains much larger. Ofcom, 2025. Business messaging statement. Paragraph 3.18.
[327] [✂] response to October 2025 consultation. [✂]

to be proportionate. We have therefore decided to implement our proposed requirements, with one amendment to GC C9.16(a) relating to incident management involving more than one aggregator which has been amended to increase the time providers have to identify the business senders responsible for certain scam messages and take appropriate action to prevent further messages being sent from 3 to 5 working days. We have also updated the definition of 'Business Sender' (to refer to any person rather than an organisation) and 'A2P Messages' (to clarify that our rules relate to any messaging services that are sent using a public electronic communications service and/or network). We have made further corresponding updates to our guidance to reflect stakeholders' comments.

Receiving scam reports and blocking scam messages in transit

What we proposed

6.133 In our 2025 consultation, we proposed new GC requirements that set out that mobile operators and tier 1 aggregators must:

- Have processes in place to receive scam reports from customers and third parties on telephone numbers and URLs that are being used for scams (GC C9.6).
- Block messages that contain URLs and telephone numbers that providers believe have been used for scams by using information from scam reports (GC C9.7).

6.134 As regards the costs and risks of these proposals, we said that:

- For mobile operators, we did not anticipate that our proposed A2P blocking requirements for messages would result in any significant additional incremental costs to industry as a whole, or to individual providers, over and above the cost of the equivalent requirements for P2P messages, because they would use the same systems and processes.
- For tier 1 aggregators, we considered that the incremental costs to industry as a whole are unlikely to be significant, although we recognised that there was some uncertainty in relation to the impact on smaller tier 1 aggregators. We invited further evidence from stakeholders on this point.
- As with our P2P blocking proposal, we also identified risks related to potential interference with the right to privacy and the right to freedom of expression. We considered that our proposed safeguards would mitigate these (see section 7, below).

Stakeholder responses

6.135 The consultation responses indicated strong support for requiring providers to receive scam reports and use them for blocking on A2P channels. However, several stakeholders were concerned that blocking requirements would impose disproportionate regulatory burdens and costs on certain providers. There were some comments on the risks of incorrectly blocking legitimate enterprise traffic, as well as concerns that automated scanning could pose risks without sufficient contextual analysis.

Sources of scam reports and processes for receiving them

6.136 Several respondents expressed support for putting processes in place to receive scam reports from customers and other third parties.[328]

6.137 Twilio said that effective scam disruption depends on timely intelligence, rapid operational response and mechanisms to correct false positives.[329]

6.138 iconectiv UK agreed that blocking is a necessary and effective tool, and that the efficacy of blocking relies on the quality and timeliness of the underlying intelligence.[330]

6.139 Twilio asked for more clarity on the practical implications of the proposed requirement to validate scam reports and the "consent-based review" principle that our guidance advises.[331]

Identifying and blocking scam messages in transit

6.140 Several respondents, including the ABI, BT, Citizens Advice Scotland, iconectiv UK, Mobile UK, [✂], Twilio and Virgin Media O2 agreed with our proposals to require mobile operators and tier 1 aggregators to implement measures to block scam messages in transit on A2P channels.[332] [✂] and Twilio noted that our proposed measures would create more consistency in measures to address scam messages and reduce consumer harm.[333]

6.141 However, [✂] considered that the proposed guidance was unnecessary because it is duplicative of existing practices within the A2P mobile messaging industry.[334]

Application and scope of the proposals

6.142 Several respondents raised concerns about which providers would be covered by the proposed requirements for blocking A2P messages.[335]

6.143 Utility Warehouse said that the proposed rules should apply to providers that transfer and/or terminate messages and therefore 'thin' MVNOs should fall outside of the scope of GC C9.1, as they do not transfer or terminate their own traffic. It considered that, if scam messages originate from an MVNO's customers, the MVNO would need to work with its host MNO to take action.[336]

---

[328] BT Group response to October 2025 Consultation. Pages 8-9; [✂] response to October 2025 Consultation; Twilio response to October 2025 Consultation. Page 6; The Association of British Insurers response to October 2025 Consultation. Pages 2-3; Citizens Advice Scotland response to October 2025 Consultation; Page 3; iconectiv UK response to October 2025 Consultation. Pages 4-5.
[329] Twilio response to October 2025 Consultation. Page 9.
[330] iconectiv UK response to October 2025 Consultation. Page 7.
[331] Twilio response to October 2025 Consultation. Page 9. In relation to paragraph 2.13 of our 2025 Proposed guidance for providers on protections from scam mobile messages.
[332] The Association of British Insurers response to October 2025 Consultation. Page 2; BT Group response to October 2025 Consultation. Page 8; [✂] response to October 2025 Consultation. Twilio response to October 2025 Consultation. Page 9; Virgin Media O2 response to October 2025 Consultation. Page 5; Citizens Advice Scotland response to October 2025 Consultation. Page 3; iconectiv UK response to October 2025 Consultation. Page 7; Mobile UK response to October 2025 Consultation. Page 1.
[333] [✂] response to October 2025 Consultation; Twilio response to October 2025 Consultation. Page 6.
[334] [✂] response to October 2025 Consultation.
[335] CCUK response to October 2025 Consultation. Page 5; FCS response to October 2025 Consultation. Page 1; MEF response to October 2025 Consultation. Page 8; [✂] response to October 2025 Consultation. Utility Warehouse response to October 2025 Consultation. Page 5.
[336] Utility Warehouse response to October 2025 Consultation. Page 4.

6.144 VodafoneThree said that thick MVNOs and aggregators should implement their own blocking tools, have dedicated staff to monitor A2P SMS traffic and block malicious traffic on their own platforms before messages are sent to MNOs.[337]

6.145 Comms Council UK supported the proposed A2P blocking requirements but recommended that we should extend these to the whole supply chain.[338]

Financial costs of our requirements

6.146 [✂] said that certain operators should not be required to implement the same measures as a tier 1 aggregator.[339]

Over-blocking

6.147 Comms Council UK raised concerns about the risk of incorrectly blocking legitimate enterprise traffic, noting this could cause financial and reputational damage for businesses. It suggested a pre-registration system and an initial monitoring period, where false positives data is checked against the registration system, but under which any non-compliant messages would not be blocked until the legitimacy of the message is verified, to minimise disruption.[340]

6.148 The MEF said that automated scanning without sufficient contextual analysis is unsuitable for certain A2P use cases, because message semantics can vary significantly between customers and legitimate traffic may be blocked. To mitigate these risks, the MEF suggested introducing robust governance controls (e.g. account suspension for misuse).[341]

Impact on competition and innovation

6.149 Simwood said that our A2P blocking proposals could disrupt competition and innovation in the A2P market. It considered that the risk of fines for failing to block scam messages incentivises operators at the top of the supply chain to sign business customers directly (by "guaranteeing" delivery of their messages), thereby pushing out smaller aggregators and shortening the supply chain.[342] Comms Council UK also said that we should impose a duty on providers to not discriminate with respect to these measures, to prevent operators favouring direct business traffic over aggregators' traffic.[343]

Other issues

6.150 BT requested we clarify the definition of 'A2P messages' in the proposed GCs. It said that the proposed definition appeared to describe messages generally, rather than messages which are ECS and specifically, 'SMS and MMS. It suggested we amend the definition to refer to SMS and MMS messages.[344]

---

[337] VodafoneThree response to October 2025 Consultation. Page 3.
[338] CCUK response to October 2025 Consultation. Page 5.
[339] Name withheld 1 response to October 2025 Consultation. Pages 4-5.
[340] CCUK response to October 2025 Consultation. Page 5.
[341] MEF response to October 2025 Consultation. Pages 8-9.
[342] Simwood response to October 2025 Consultation. Page 4.
[343] CCUK response to October 2025 Consultation. Page 6.
[344] BT Group response to October 2025 Consultation. Page 10.

Our assessment

6.151 As described in section 2 and 3, scammers exploit A2P channels to deceive people by impersonating trusted organisations, such as public authorities or banks, and by contacting potential victims over channels that people expect these organisations to use. We set out in section 4 that many mobile operators and aggregators have implemented measures to block scam A2P messages. However, some mobile operators do not currently apply their blocking tools to A2P traffic, and some aggregators do not use blocking tools. Absent intervention, we expect the current limitations in the deployment and functionality of blocking tools to persist, which creates vulnerabilities that scammers can exploit.

6.152 Having taken into account stakeholders' responses, we consider that our proposed requirements for mobile operators and tier 1 aggregators to have processes in place to receive scam reports and block scam A2P messages remain a necessary and proportionate remedy to achieve our policy objective.

6.153 Below, we set out why we consider the measures necessary and proportionate. We also address the stakeholder responses set out above.

Receiving scam reports

6.154 Taking into account our assessment set out in paragraph 5.79-5.81 related to P2P messaging, we believe it is appropriate to make the same amendment to GC C9.6 as we did in GC C9.2. We have therefore decided to amend GC C9.6 to ensure mobile operators and tier 1 aggregators "regularly" and "proactively" ensure they receive (and, where appropriate, validate) scam reports from end-users and appropriate third parties linked to any URLs and telephone numbers that are suspected of being part of a scam. We have also set out in paragraph 2.22 of our guidance (which applies to P2P and A2P channels) how we expect providers to interrogate reports that may contain incorrectly reported messages. We set out at paragraph 2.72 that we expect mobile operators and tier 1 aggregators to take into account these principles.

6.155 In response to Twilio's concern about the feasibility of validating scam reports and implementing consent-based review, we expect that providers will use messages as a source of intelligence where a user has reported it and consented (explicitly or implicitly) to review of their message on the basis that it is a potential scam. Providers would base any subsequent blocking of messages on that validated intelligence.

6.156 We also expect providers to make clear to their customers that they may block messages on this basis, taking into account data protection principles including fairness and transparency (we set this out in paragraph 2.12 of our guidance).

6.157 Our guidance (paragraphs 2.67-2.82) provides further details on how mobile operators and tier 1 aggregators can comply with our blocking measures relevant to A2P messages, including in relation to:

- Different sources and mechanisms for receiving scam reports.
- How mobile operators and tier 1 aggregators can validate scam reports and reduce the risk of over-blocking.
- Information sharing: as noted above in relation GC C9.2, mobile operators and tier 1 aggregators can share intelligence with each other and with third parties to strengthen the quality and timeliness of the intelligence available to them. Our guidance therefore encourages mobile operators and tier 1 aggregators to establish intelligence sharing

mechanisms for the purpose of significantly reducing the likelihood that consumers receive scam messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law.

- The specific circumstances and conditions under which we consider it permissible for providers to exempt a limited number of verified business senders from their blocking tools.

Identifying and blocking scam messages in transit

6.158 Some mobile operators do not apply their blocking tools to A2P messages. This can allow scammers to evade detection when sending mobile message scams on A2P channels, weakening the benefits of the blocking tools and leaving customers vulnerable to harms. We consider that these measures will ensure that A2P messages are subject to the same counter-scam techniques as P2P messages, ensuring that scammers would not be able to exploit either channel.

6.159 For the reasons we set out below, we consider that these blocking requirements will reduce the volume of scam messages reaching consumers and thus consumers and businesses will benefit from a significant reduction in the harms associated with these scams. We set out the nature of these benefits in more detail in paragraphs 8.4-8.8.

6.160 We note [✂] and Twilio's comments that our measures would create more consistency in the market to address scam messages. We also note the strong support for requiring mobile operators and tier 1 aggregators to implement measures to block scam messages in transit on A2P channels.

6.161 Taking into account stakeholders' responses below, we are requiring mobile operators and tier 1 aggregators involved in the delivery of A2P messages to identify and block A2P messages in transit, where they believe their content contains scam URLs and telephone numbers.

Blocking messages using automated tools

6.162 GC C9.7 requires mobile operators and tier 1 aggregators to block messages that contain URLs or telephone numbers that they reasonably believe were part of a scam.[345] We are mandating that they carry out this blocking using automated tools and without undue delay. We are not, however, preventing human review and recognise that some degree of human review of messages is likely to be necessary to ensure the automated tools are working as intended.

6.163 We note the MEF's concern that automated scanning without sufficient contextual analysis would be unsuitable for checking some A2P messages. The requirement we are introducing is to use automated tools to search for embedded URLs and telephone numbers in

[345] GCs C9.6 and C9.7 relating to A2P messages are equivalent to GCs C9.2(c) and C9.3(c) relating to P2P messages and some of the discussion from paragraph 5.29 above is therefore relevant to our proposed identifying and blocking proposals relating to A2P messages. We are not imposing an equivalent of GC C9.2(a) or C9.2(b) or C9.3(a) or (b) in relation to A2P messages. We do not consider these appropriate for the A2P channel because it is possible for more than one business sender to send A2P messages that appear to be from the same sender ID. As such, automated blocking of A2P messages which appear to be from numbers or sender IDs associated with scams, may risk catching legitimate traffic. We have provided equivalent requirements to block A2P senders in GC C9.15(b)) and C9.16(a)(ii).

messages that are associated with scams.[346] In the context of our rules, we consider that any review of the context of messages should be intelligence-led and targeted. The risk that message semantics could lead to legitimate messages being blocked under our measures should therefore be negligible.

Application of blocking requirements

6.164 We have considered Utility Warehouse's comment that MNOs should be responsible for blocking scam messages on their networks, including messages from MVNO customers. We have also considered VodafoneThree's point that thick MVNOs and aggregators should implement their own blocking tools to monitor A2P SMS traffic before messages are sent to MNOs. As set out above for our P2P requirements, we consider that given MNOs transfer and terminate A2P messages on behalf of thin MVNOs they host, the requirement to identify and block messages does not apply to thin MVNOs. However, as thick MVNOs transfer and terminate messages using their own SMSCs, they are responsible for identifying and blocking scam messages in transit on their network (unless the thick MVNO relies on its host MNO to transfer or terminate A2P messages on behalf of its customers). In response to Comms Council UK's suggestion that the A2P blocking requirements should be extended to the whole supply chain and not only applied to mobile operators and tier 1 aggregators, we consider that there may be limited additional benefit to requiring other entities to identify and block messages before they reach providers subject to the requirements. We are therefore not introducing these requirements to aggregators beyond tier 1.

Regularly reviewing these blocking policies

6.165 Also as set out above for our P2P requirements, we are mandating various cross-cutting measures (that enhance our measures and safeguard individual rights): in particular, as set out in GC C9.19, we require that mobile operators and tier 1 aggregators must regularly review and update their identifying and blocking policies, systems and processes (as appropriate).

6.166 We will require that mobile operators and tier 1 aggregators provide a right of challenge for anyone that has been impacted by any blocking of messages under GC C9.7. We will also require mobile operators and tier 1 aggregators to: keep appropriate records (including on the effectiveness of their blocking measures); train relevant staff as appropriate; implement appropriate system and processes to identify, monitor and address false positive rates arising from blocking under C9.7; and comply with relevant data protection legislation. These other measures are set out in GCs C9.17-C9.18 and C9.20-C9.27 and discussed in section 7.

[346] Our measures do not, for example, require providers to carry out indiscriminate or a more general assessment of the contents of all messages based on broader probabilistic search methods. In other words, our measures should require providers to implement an exact data base matching tool (where a human sets a rule that is applied automatically), rather than a system making decisions based on the likelihood of something happening.

Financial costs of our requirements

Costs to mobile operators

6.167 We consider that the nature of the potential costs to mobile operators associated with these new requirements is similar to that of our identifying and blocking proposals for P2P messages, set out in paragraphs 5.100-5.102.[347] Broadly, we do not consider that our A2P message blocking requirements will result in significant additional costs to industry or individual providers beyond those discussed above for P2P messages, because it would use the same systems and processes.[348]

6.168 [✂] raised concerns that certain operators should not be required to implement the same measures as a tier 1 aggregator, given the potential implementation costs. [✂].[349] However, we consider it is necessary that all mobile operators implement effective protections, so that scammers are unable to exploit gaps. We also consider that the additional burden that providers without existing A2P blocking in place will incur is proportionate to the benefits of achieving our policy objective.

Costs to tier 1 aggregators

6.169 We expect aggregators to incur the same types of costs of blocking A2P messages as those that mobile operators will incur in relation to A2P and P2P blocking.

6.170 We consider that the incremental costs to industry as a whole are unlikely to be significant. However, in our consultation, we recognised that there is some uncertainty in relation to the incremental impacts on smaller tier 1 aggregators. We invited further evidence from stakeholders on this point:

- **System implementation and running costs:** in advance of our consultation, we sent formal information requests to nine tier 1 aggregators (which we believe are typical of the wider set of c.30 tier 1 aggregators in operation), in which we asked about their systems for identifying and blocking scam messages. All nine have systems in place, but it is possible that some aggregators may need to upgrade or obtain new systems to meet our requirements.[350] We expect solutions to be available at a reasonable cost for tier 1 aggregators without suitable existing systems in place, even for small firms. For example, one small tier 1 aggregator has been able to find an affordable solution and implement such a system despite its smaller scale.[351] On this basis, our view is that system implementation and running costs for tier 1 aggregators are unlikely to be significant.
- **Ongoing staff costs:** as set out in paragraph 5.101 for our P2P blocking requirements, we consider the likely incremental costs to industry and to individual aggregators are unlikely to be significant, given that these activities should largely align with existing staff expertise, rather than requiring entirely new skills.

---

[347] i.e. set-up and ongoing costs of the systems required as well as costs of intelligence.
[348] We note that, where providers do not currently apply its blocking measures to all of its traffic, they would incur some additional costs associated with doing so. For example, we understand that [✂] has identifying and blocking measures in place, that as of April 2025, were not applied to some of its A2P traffic. This is based on [✂] response to formal information requests dated 27 March 2025.
[349] Name withheld 1 response to October 2025 Consultation. Pages 4-5.
[350] Formal information request responses.
[351] This smaller tier 1 aggregator [✂] cited system implementation costs of around £[✂] in response to a formal information request dated 27 March 2025, question 14. We do not expect this would be a prohibitive cost for other small tier 1 aggregators. However, we note that factors beyond scale may influence system implementation costs.

- **Costs of intelligence:** based on the information we formally requested from nine tier 1 aggregators, we understand that many aggregators already rely on third party intelligence sources.[352] Where aggregators do not currently use such sources, we consider the incremental cost to be low, given the cost of existing sources.[353]

6.171 We note that there are other cross-cutting measures (that enhance our measures and safeguard individual rights) that apply to our A2P blocking measure, as discussed in section 7. We do not consider that these GCs materially add to the costs incurred by mobile operators and tier 1 aggregators.

6.172 Considering all of these costs in the round, we do not expect them to impose a significant additional burden on the aggregator industry as a whole but recognise that there is some uncertainty around existing system implementation and use of intelligence sources. We also do not expect these costs in the round to impose significant incremental costs on individual aggregators, even those of smaller scale.

Potential risks of other adverse impacts

Over-blocking and potential interference with the rights to privacy and freedom of expression

6.173 We expect the risk of adverse impacts for mobile users and providers to be the same as we have identified in relation to our blocking measures for P2P messages, set out in paragraphs 5.103-5.107.

6.174 These include potential interference with the right to privacy under Article 8 ECHR and potential data protection harms, as well as risks of over-blocking and interference with the right to freedom of expression under Article 10 ECHR.

6.175 As discussed in relation to P2P blocking requirements, and in light of stakeholder comments about the risk of false positives, we consider the risk of over-blocking is low and providers can mitigate it effectively through the various safeguards in our rules (see GCs C9.17-C9.27).

Impact on competition and innovation

6.176 In addition, as mentioned above for other measures, we consider the impact on competition and innovation for our package of measures in the round, as part of the proportionality assessment in section 8. For the reasons set out there, we do not expect this measure to have a material negative impact on competition and innovation.

6.177 Simwood raised a concern that our A2P blocking proposals could disrupt competition in the A2P market. It considered that larger integrated operators would be incentivised to reduce the number of steps in the A2P supply chain to address customers' potential concerns about the risks to their messages from blocking systems.[354]

6.178 As outlined in our business messaging statement, using an aggregator and/or MSP eliminates the need for business senders to establish direct connections with multiple

---

[352] Formal information request responses.

[353] As per paragraph 5.101, we understand 7726 reports to cost c.£[✂] per annum. We also note there are free sources of intelligence available from organisations such as the Cyber Defence Alliance. Tier 1 aggregators can also share intelligence to help them build a more robust and up to date understanding of scam activity. Our guidance explains that we encourage tier 1 aggregators to establish intelligence sharing mechanisms for the purpose of significantly reducing the likelihood that consumers receive scam messages, provided appropriate safeguards are put in place to ensure compliance with relevant data protection legislation and competition law.

[354] Simwood response to October 2025 Consultation. Page 4.

terminating mobile operators in order to reach the intended recipients of their messages.[355] We also note that a large number of providers compete in the A2P market, offering choice to business senders. In this context, we consider that consumers and A2P market players are best served by a competitive market where all providers apply a consistent high standard of protection against scammers.

We consider the benefits of our A2P blocking requirements outweigh any costs and adverse impacts

6.179 As with our P2P blocking measures, we consider that the A2P requirements will address gaps in protections for customers that some providers have left open by not having sufficient (or any) processes in place to combat scam A2P messages. We consider that the cost to industry, and the risk of adverse impacts on stakeholders, is low relative to the scale of benefits associated with the reduction in harms brought about by making it more difficult for scammers to use the A2P channel to reach consumers.

6.180 Taking into account all relevant factors (including our assessments above and in relation to our overall package of measures in Section 8), we consider our A2P blocking requirements to be proportionate. We have therefore decided to implement our proposed requirements, with an amendment to GC C9.6 to require providers to "regularly" and "proactively" ensure they receive scam reports and to refer to obtaining these scam reports from end-users and "appropriate" third parties. We have also made various updates to our guidance to reflect stakeholders' comments.

[355] Ofcom, 2025. Business messaging statement. Paragraph 2.10. Our 2025 statement on business messaging has informed our broader analysis of A2P competitive conditions and provides helpful context to some responses to our consultation. This statement explains our decision not to impose formal regulation on operators A2P termination rates, following voluntary pricing commitments from the largest MNOs, and in the light of increased uncertainty around the potential for competitive constraints to develop over the three-year market review period.

7. Enhancing our measures and safeguarding human rights

7.1 In sections 5 and 6 we set out our assessment and decisions on measures to combat scam P2P and A2P messages, respectively.

7.2 In this section, we explain our assessment and decisions on a set of cross-cutting requirements to support how providers implement the P2P and A2P remedies. The purpose of these measures is to ensure effective implementation of our rules, safeguard against any risk that our requirements will interfere with the right to privacy and data protection or the right to freedom of expression and ensure users have an effective and meaningful route to challenge any potential infringement of their rights. We expect them to make our P2P and A2P remedies more effective in achieving our policy objective and to mitigate any risk of unintended harm.

7.3 In summary, the measures we assess are requirements to:

- Implement and maintain appropriate and effective policies, systems and processes that enable any affected person to challenge any blocking of a message or number under GCs C9.3 or C9.7 (GCs C9.17 and C9.18).
- Regularly review their policies, systems and processes implemented under GC C9 (GC C9.19).
- Ensure all relevant staff are aware of, and appropriately trained on, the policies, systems and processes in place under GC C9 (GC C9.20).
- Implement and maintain appropriate record keeping policies, systems and processes (GCs C9.21 to C9.25).
- Implement and maintain appropriate and effective policies, systems and processes to identify and monitor false positives, and take appropriate, effective and prompt action when false positives are identified (GC C9.26).
- Ensure providers comply with relevant data protection legislation when they are seeking to comply with GC C9 (GC C9.27).

7.4 These measures we assess are applicable as follows:

- GCs C9.17 and C9.18 are applicable to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (except Lower-Tier Aggregators), and/or in the context of P2P Messages, has assigned Mobile Numbers.
- C9.19-C9.25 and C9.27 are applicable to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages (including all Aggregators), and/or in the context of P2P Messages, has Assigned Mobile Numbers.
- GC C9.26 is applicable to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, except Lower-Tier Aggregators.

7.5 Taking into account stakeholders' responses to our 2025 consultation, for each measure we assess:

- What it will require providers to do and why we consider it necessary to achieve our overall policy objective.
- The expected benefits to people and businesses.

- The financial costs of our requirements.
- Any potential adverse impacts on people and businesses in the UK, including on providers that would be subject to the new rules, and steps we propose to take to mitigate these.
- Whether we consider the expected benefits of each measure to outweigh any costs or adverse impacts.

7.6 We consider and respond to stakeholders' responses to the proposed measures from our 2025 consultation. We also consider evidence obtained via formal information requests (our 'May 2026 requests'), following concerns raised in consultation responses about certain proposed cross-cutting measures.

7.7 As part of our assessment, we also explain our decision not to implement the requirement we had proposed that providers must notify senders when they block their messages under GCs C9.3(b), C9.3(c) or C9.7 using automated tools or otherwise enable the sender to become aware their message has been blocked (proposed GC C9.17).

7.8 This section also considers stakeholders' general comments on the draft guidance we published alongside our 2025 consultation.

Table 7.1: Summary of our final cross-cutting measures

Summary of our final cross-cutting measures		
Measure	**To which providers does it apply?**	**Our decision**
Implement and maintain appropriate and effective policies, systems and processes that enable any affected person to **challenge any blocking of a message or number** under GCs C9.3 or C9.7. Requires an **accessible and reasonably prominent policy explaining the right to challenge**, including on providers' websites.	Mobile operators and tier 1 aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers, as applicable	Largely retained from consultation proposal but renumbered as **GC C9.17 and C9.18.** Additions made to our supporting guidance.
Regularly review their policies, systems and processes implemented under GC C9 to confirm that they remain appropriate and effective, and are operating as intended.	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers.	Retained from consultation proposal but renumbered as **GC C9.19.** Additions made to our supporting guidance.
Ensure that **all relevant staff are trained** on the policies, systems and processes in place under Condition C9, including on the right to challenge.	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers	Largely retained from consultation proposal but renumbered as **GC C9.20.** Additions made to our supporting guidance.

Summary of our final cross-cutting measures		
Implement and maintain **appropriate record keeping** policies, systems and processes.	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages and/or that have assigned mobile numbers, as applicable. Providers will only need to comply with a subset of the requirements as relevant to their business.	Largely retained from consultation proposal but renumbered as **GCs C9.21 to C9.25**. We have amended the requirements for certain categories of records. Additions made to our supporting guidance.
Implement and maintain appropriate and effective policies, systems and processes to **identify and monitor false positives** (under GCs C9.3(b) and (c) and C9.7) **and take appropriate action** when these are identified**.**	Mobile operators and tier 1 aggregators that transfer and/or terminate P2P or A2P messages, as applicable. Providers that carry out blocking under GC C9.3(b) and (c) and C9.7 will need to comply.	Amended consultation proposal but renumbered as **GC C9.26.** We have amended the proposed requirement to ensure the transmission of legitimate messages to focus it on identifying, monitoring and addressing false positives under GCs C9.3(b) and (c) and C9.7.
Ensure they **comply with relevant data protection legislation** when complying with GC C9.	Mobile operators and aggregators that transfer and/or terminate P2P or A2P messages, and/or that have assigned mobile numbers.	Retained from consultation proposal but renumbered as **GC C9.27.** Additions made to our supporting guidance.
Providers must **notify senders when they block their messages** under GCs C9.3(b), C9.3(c) or C9.7 using automated tools.	-	**We have decided not to implement this requirement**

Notifying mobile users about message blocking

What we proposed

7.9 As described in sections 5 and 6 of this statement, GC C9.3(b) will require providers to use human review and/or automated tools to block scam P2P messages from telephone numbers associated with scams and GCs C9.3(c) and C9.7 require providers to use automated tools to block P2P and A2P messages that contain scam URLs or telephone

numbers. We proposed in our 2025 consultation that providers using automated tools to block messages must notify the person whose message has been blocked or otherwise enable that person to become aware their message has been blocked, without delay. This proposed requirement was set out in proposed GC C9.17.

7.10 We set out that the proposed requirement to notify would help ensure that end-users are aware of blocking and can exercise the right to challenge blocking where necessary.

7.11 We did not propose that this requirement to notify should apply when providers block numbers or messages under GC C9.3(a), C9.3(b) or (c) (following a human review), C9.5, C9.8/C9.12(c), C9.15 or C9.16. This is because, in these circumstances, users should become aware their number or messages have been blocked and/or messages blocked following a human review are most likely to be scams.

7.12 We recognised there would be a cost to notifying senders that their message(s) have not been delivered but we did not have direct evidence on the scale of this cost. We welcomed evidence from operators on how they currently manage the potential negative outcomes of blocking legitimate messages.

Stakeholder responses

7.13 Stakeholders generally disagreed with our proposal to notify mobile users about message blocking. They raised concerns that these notifications would inform scammers when their campaigns had been detected (particularly on P2P channels); and that the cost and technical burden to implement this measure would not be proportionate.

Concerns that the notification requirement would be counter-productive and disproportionate as a means to achieve our policy objectives

7.14 Many respondents disagreed with the proposed requirement, commenting that sending notifications of a blocked message would tip off scammers when their messages are identified, allowing them to adapt by, for example, changing the contents or using new URLs or telephone numbers.[356] BT, Sky, Virgin Media O2 and VodafoneThree indicated that, given the majority of blocked messages would be scams, it would be disproportionate to introduce the notification requirement.[357]

7.15 Some responses queried whether any form of notification requirement could be justified on P2P channels, on the basis that their current blocking practices generate a low number of false positives. For example, BT said it had no record of complaints related to users that had had legitimate messages blocked because they contained a suspicious URL or scam telephone number.[358] [✂] said that, out of [✂] million messages blocked in a week, only [✂] containing a URL or number were incorrectly blocked.[359] We collected more

[356] BT Group response to October 2025 Consultation. Page 13; VodafoneThree response to October 2025 Consultation. Page 7; Sky response to October 2025 Consultation. Page 2; Virgin Media O2 response to October 2025 Consultation. Page 3; MEF response to October 2025 Consultation. Page 10; UKCTA response to October 2025 Consultation. Page 3; [✂] response to October 2025 Consultation; techUK response to October 2025 Consultation. Page 5; Stour Marine response to October 2025 Consultation. Page 4.

[357] Sky response to October 2025 Consultation; Page 2; BT Group response to October 2025 Consultation. Page 14. VodafoneThree response to October 2025 Consultation. Pages 7-8; Virgin Media O2 response to October 2025 Consultation. Page 3.

[358] BT Group response to October 2025 Consultation. Page 13.

[359] Email sent from [✂] to Ofcom on 10 February 2026.

comprehensive data on false positive rates from stakeholders in our May 2026 requests (see paragraph 7.29).

Collective impact of other GCs is more proportionate in protecting individual rights

7.16 VodafoneThree said that other safeguards on which we had consulted would be more proportionate in mitigating interference with human rights and ensuring the risk of false positives is low. This included ensuring there are appropriate channels of communication with the sender, either directly or through an aggregator, and maintaining our proposal for affected persons to have the right to challenge the blocking of messages.[360]

7.17 VodafoneThree said that the proposal for providers to take appropriate steps to ensure they do not block legitimate messages and to keep false positives and challenges to blocking under review would minimise the risks of our proposals.[361]

Cost and technical concerns

7.18 Respondents raised concerns regarding the financial and technical challenges of implementing our proposed notification requirement. This included concerns about the high cost associated with administering a system to send blocking notifications.

7.19 BT argued that building in the notification system for the P2P channel would cost approximately £[✂].[362] [✂] said the notification requirement would be challenging and costly.[363] [✂] said the notification requirement would constitute a significant additional administrative burden on mobile network operators, which in turn is likely to result in price increases across both P2P and A2P messaging.[364]

7.20 BT estimated that an obligation to notify senders when a message is blocked automatically would result in an additional £[✂] per month of termination costs for P2P messages alone.[365] It added that some of these costs may "net out", but that there will likely be an overall net outflow of payments to smaller operators. BT added that providers might exacerbate the issue by driving higher volumes of notifications, generating inbound traffic and benefiting from the net revenue gain.[366]

7.21 Some respondents raised concerns about the technical burden of implementing a notification system on P2P channels: for example, Stour stated that it would not be feasible to proactively notify subscribers, or send error messages, on P2P channels (but that these processes are already in place on A2P channels, using error codes).[367]

7.22 Other respondents raised concerns specific to implementing the measure on A2P channels: for example, Twilio said that the A2P market includes complex commercial arrangements involving intermediaries, such as software vendors that have direct relationships with business senders. Twilio said that, here, the intermediary should be responsible for notifying the business sender of message blocking, to avoid introducing operational

---

[360] VodafoneThree response to October 2025 Consultation. Page 7.
[361] VodafoneThree response to October 2025 Consultation. Page 7.
[362] BT Group response to October 2025 Consultation. Pages 13-14.
[363] Name withheld 1 response to October 2025 Consultation. Page 4.
[364] [✂] response to October 2025 Consultation.
[365] BT calculates this using [✂].
[366] BT Group response to October 2025 Consultation. Pages 13-14.
[367] Stour Marine response to October 2025 Consultation. Page 4.

complexity and confusion for business senders (that may otherwise receive notifications from entities with which they have no direct relationship).[368]

Comments in support of notification requirement

7.23 Some respondents were more supportive of our proposal to notify persons whose messages have been blocked. iconectiv UK and Pinnacle stated that this requirement would strengthen the proportionality of our measures.[369] Stour, techUK and the CCP-ACOD supported the notification requirement, subject to caveats.[370] For instance, techUK agreed that when a provider suspends a customer's account for sending a suspected scam message, they should be notified.[371]

7.24 Others recognised the benefit of a notification requirement, but in a different form. Sky recommended a non-delivery notification (or otherwise no notification at all).[372] Utility Warehouse said that we should consider a notification requirement that aims to prevent over-blocking but does not give useful information to scammers.[373]

7.25 The Campaign Registry expressed some support for the notification requirement on A2P channels, noting that their services can help notify other relevant parties.[374] Similarly, BT said that it was more straightforward to contact senders (such as aggregators) on A2P channels and that sending blocking notifications to aggregators was generally helpful in informing the approaches aggregators take to preventing scams.[375]

Our assessment

Rationale and benefits

7.26 We consulted on the proposed notification requirement primarily as a safeguard against the risk of false positive blocking when providers use automated tools to block messages under GC C9.3(b) and (c) and C9.7. Blocking of legitimate messages has the potential to interfere with individual rights of senders and intended recipients, specifically the right to freedom of expression. The proposed notification requirement would have mitigated any interference with individual rights by ensuring that mobile users would be aware when providers block a legitimate message they have sent, enabling them to challenge this.

Analysis of necessity and proportionality concerns

7.27 A number of respondents disagreed with the proposed notification requirement, in many cases because sending blocking notifications would risk providing scammers with information about how their tactics are performing against providers' defences. Stakeholders also said there were significant costs and technical challenges associated with implementing a notification requirement.

---

[368] Twilio response to October 2025 Consultation. Page 11.
[369] iconectiv UK response to October 2025 Consultation. Page 8; Pinnacle Teleservices response to October 2025 Consultation. Pages 14-15.
[370] techUK response to October 2025 Consultation. Page 5; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; Stour Marine response to October 2025 Consultation. Page 4.
[371] techUK response to October 2025 Consultation. Page 5.
[372] Sky response to October 2025 Consultation. Page 2.
[373] Utility Warehouse response to October 2025 Consultation. Pages 5-6.
[374] The Campaign Registry response to October 2025 Consultation. Page 11.
[375] BT Group response to October 2025 Consultation. Page 14.

7.28 We agree with stakeholders that we would expect only a very limited number of notifications to be sent in response to legitimate messages.[376] Instead, almost all notifications would be sent in response to scam messages (mainly to scammers that had sent scam P2P messages). This could significantly undermine our objective if, in practice, notifications provide scammers with information that helps them.

7.29 In relation to the risk of potential interference with individual rights, our 2025 consultation noted that current false positive rates are low.[377] Given the feedback from respondents to our consultation and the risks identified above, we obtained further evidence from providers in response to our May 2026 requests (see paragraph 7.6). This evidence indicates that false positive rates as a result of implementing GCs C9.3(b) or (c) or C9.7 are likely to be significantly lower than the already low rates from current blocking practices.[378]

7.30 Taking into account the limited circumstances in which providers are likely to generate false positives from an intelligence-led, focused and targeted review of messages, which involves identifying specific numbers and URLs associated with scam reports (which are subject to validation checks), we consider that false positive rates from blocking under our rules are likely to be very low.

7.31 We recognise that a notification requirement may still benefit end-users where a provider blocks a legitimate message and the sender is not otherwise notified. However, in these circumstances, the sender can still mitigate any adverse impact: for example, by using other means of communication to contact the intended recipient. Some providers or devices may also make senders aware that a message has not been sent (including where users turn on delivery reports).

7.32 Any interference with individual rights can be managed effectively through the other measures we are introducing, including the requirement to validate scam reports where appropriate (GCs C9.2 and C9.6), the right to challenge (GC C9.17) and the requirement for providers to have appropriate systems and processes in place to identify, monitor and address false positives under GCs C9.3(b) and (c) and C9.7 (GC C9.26, discussed below).

---

[376] Our 2025 consultation recognised this tip off risk in the context of sending notifications of a blocked message following a human review (which we considered was most likely to result in notifying a scammer).

[377] Footnote 184 of our 2025 consultation. The false positive rates we had considered at the time were based on providers' existing blocking practices, some of which are based on more probabilistic reviews of message content that go beyond the scope of what we had proposed. Probabilistic search methods involve making decisions based on the likelihood of something happening. This includes reviewing messages for a broad set of scam indicators including phrases such as "Hi Mum …" which are by their nature less precise meaning semantics and word patterns are likely to result in a higher rate of false positives. In contrast, our measures require the review of messages for known scam number or URL, which we consider effectively require providers to implement an exact data base matching tool.

[378] Responses to our May 2026 requests from [✂] indicate false positive rates may range from zero to just over 1 per month for both P2P and A2P (but reported rates are often wider than false positives rates directly related to a scam URL or number in a message, so these figures may be even lower). While [✂] reported P2P false positive rates are higher [✂] its rates are based on messages that are blocked as a result of the same/similarly worded campaigns based on an assessment of various attributes (including word patterns) rather as a direct result of the presence of a URL or number in a message. We note that reported false positive rates were largely based on complaints as well as some proactive monitoring and recognise that no provider currently captures the precise number of false positives arising from incorrectly identifying a scam URL or number in a message. There may therefore be some under-reporting of false positive rates based on existing processes if, for example, users may not have been aware a message was blocked or decided not to complain, or if providers did not otherwise identify all false positives.

7.33 In relation to A2P channels, we consider there are already commercial incentives for providers to inform downstream parties about non-delivery of A2P messages. As a result, we expect that, in many cases, providers are already likely to have processes set up to send blocking notifications to senders via A2P channels. We also note that our incident management requirements under GCs C9.15 and C9.16 will require providers to obtain evidence from business senders about messages they reasonably believe were intended to scam the recipient. We therefore expect that the benefits of a further notification requirement for A2P channels would be limited.

We do not consider the benefits of the notification requirement to outweigh the costs and adverse impacts

7.34 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we no longer consider it proportionate to require providers to send blocking notifications and have decided not to implement this aspect of our proposals.

7.35 In making this decision, we have weighed the very low risk of interference with individuals' rights (which, given the evidence of very limited false positives, is lower than we had understood at consultation) against the high risk that the vast majority of notifications would be sent in response to scam mobile messages, as well as financial and technical challenges associated with a notification requirement. Overall, we consider that the adverse impacts of a notification requirement outweigh the limited benefits.

7.36 It is important for providers to be transparent with users about the processing of personal data they carry out in order to comply with GC C9.3 and C9.7 (including the possibility that their messages may be blocked). We expect this information to be clearly and prominently displayed in an appropriate place on their website and in any terms and conditions or other relevant information they provide to customers. We understand providers should already do this to comply with data protection principles of fairness and transparency which will also give senders advance notice that their messages could potentially be blocked by measures intended to combat scam messages.

7.37 We further expect providers to be transparent with users about how they can turn on delivery reports on their device (where available). We have updated our guidance to reflect this.

Right to challenge

What we proposed

7.38 In our 2025 consultation, under proposed GC C9.18, we set out that we would require providers to implement and maintain appropriate and effective policies, systems and processes that would enable any person to challenge any blocking of their mobile number or messages under proposed Condition C9, or other action the provider could take under proposed Condition C9, that affects them.

7.39 We proposed these policies must set out:

- The circumstances under which any blocking or other action may occur.
- How challenges can be made.
- How these would be assessed.
- The range of possible outcomes following a challenge.

- The timeframe for making a decision.
- Routes for appeal.

7.40 We also set out under proposed GC C9.19 that providers must publicise the policies, systems and processes in place under Condition C9.18 and make them readily accessible, including on providers' websites, referencing them in relevant terms and conditions and providing them free of charge upon reasonable request.

7.41 In addition, we set out that:

- We expected providers to incur some additional costs associated with putting in place a process for people to challenge any blocking of numbers or messages.
- The extent of the costs would depend on what existing processes providers already have in place,[379] but we did not consider it likely that the cost of implementing and running a complaints process to enable the right to challenge would be significant across the sector as a whole.

Stakeholder responses

7.42 Responses from stakeholders on our proposed right to challenge obligation were mixed. Some supported the proposal while others raised concerns about the cost and practicalities of implementation.

Support for the right to challenge blocking

7.43 Several respondents agreed with proposed GC C9.18 on the basis that it would mitigate the risk of interference with individual rights. Amnesty International UK, Sky, The Campaign Registry, Utility Warehouse, and VodafoneThree supported the proposal to provide a right to challenge for any person whose message or mobile number is incorrectly blocked.[380]

7.44 Sky added that, in implementing measures such as message blocking, the risk of interference with the right to freedom of expression, including the inadvertent blocking of a very small proportion of legitimate traffic, must be recognised. It considered that the proposals had achieved this.[381]

7.45 Respondents also commented on the importance of implementing effective systems and processes to enable a person's right to challenge, under proposed GC C9.19. The Campaign Registry said that its platform already provides a public appeals process that could support the right to challenge.[382] The CCP-ACOD and Simwood stated that it is important that providers resolve challenges efficiently, requiring operators to maintain a fast and low-burden review process.[383]

7.46 Sky said that successful implementation of a disputes process would enable dialogue between a consumer and legitimate business sender. This would also help to enable the

[379] For example, having general complaints processes in place pursuant to GC C4.
[380] Amnesty International UK response to October 2025 Consultation. Page 2; Sky response to October 2025 Consultation. Page 2; The Campaign Registry response to October 2025 Consultation. Page 11; Utility Warehouse response to October 2025 Consultation. Page 6; VodafoneThree response to October 2025 Consultation. Pages 7-8.
[381] Sky response to October 2025 Consultation. Page 4.
[382] The Campaign Registry response to October 2025 Consultation. Page 11.
[383] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; Simwood response to October 2025 Consultation. Page 4.

provider to reinstate a business sender's service after a successful challenge, as appropriate.[384]

7.47 Which? went further and suggested that our guidance should oblige providers to make their customers aware of their rights to alternative dispute resolution if they believe that they have been harmed by a blocking decision.[385]

Implementation challenges

7.48 Some respondents raised concerns about the practicalities of addressing challenges from users that are not their direct customer. Mobile UK said that they were unclear how the challenge regime would work for P2P messages where the challenge comes from a mobile user that is not their customer. It queried whether the customer should challenge a third party that might have blocked their message.[386] BT said that proposed GC C9.18 would likely require providers to transfer sensitive personal data.[387]

7.49 Sky suggested that we could advise providers to manage a dispute resolution process in our guidance, rather than require it in the GCs.[388]

7.50 Other respondents made suggestions about how operators should be expected to implement the right to challenge and raised some technical, privacy and financial considerations that related to managing challenges from customers of other providers. Utility Warehouse said that providers should have discretion to maintain a decision to block where the affected party cannot demonstrate that their message was genuine.[389] The MEF agreed with the proposal in principle, but argued that we had not considered complexities for aggregators that do not have a direct relationship with the sender.[390] Twilio also agreed with our proposal but said that only a business sender should be allowed the right to challenge blocking of A2P messages, as only the sender would have the relevant information to meaningfully challenge a blocking decision.[391]

Costs

7.51 Some respondents disagreed with the right to challenge, citing the administrative burden it would impose.[392] BT disagreed with applying a right to challenge to blocked P2P messages. It said it would require [✂]FTE at a cost of £[✂] to retrieve consumer contacts and would mean all personnel currently working in BT's security team in this area need to be redeployed to review challenges rather than identifying and stopping scams.[393] [✂] said it would need new processes to retrieve blocking data, which would be costly, and that unblocking messages would be challenging.[394]

7.52 BT also said that proposed GC C9.19, which requires providers to ensure that the policies, systems and processes under proposed GC C9.18 are well publicised and readily available, is

---

[384] Sky response to October 2025 Consultation. Page 2.
[385] Which? response to October 2025 Consultation. Page 11.
[386] Mobile UK response to October 2025 Consultation. Page 2.
[387] BT Group response to October 2025 Consultation. Page 14.
[388] Sky response to October 2025 Consultation. Page 3. Sky noted the dispute resolution process set out in our guidance on the provision of Calling Line Identification facilities and other related services (paragraph A2.6).
[389] Utility Warehouse response to October 2025 Consultation.
[390] MEF response to October 2025 Consultation. Page 6.
[391] Twilio response to October 2025 Consultation. Page 11.
[392] [✂] response to October 2025 Consultation.
[393] BT Group response to October 2025 Consultation. Pages 13-14.
[394] Name withheld 1 response to October 2025 Consultation. Page 4.

disproportionate and highly burdensome. It said that specifying that the right to challenge process must be made available free of charge in hard copy, under proposed GC C9.19(c), is overly prescriptive.

Our assessment

Rationale and benefits

7.53 We proposed the right to challenge primarily as a safeguard against the risks that false positive blocking could pose. While we consider that the risk that our measures will generate significant numbers of false positives is very low (and we are implementing various safeguards to mitigate the risk of false positives arising), we recognise that some false positives will still arise. Where they do arise, we consider the right to challenge will be an important protection.

7.54 The right to challenge reflects the fundamental right to a fair trial and we consider it will be particularly important where false positives arise from automated monitoring of the content of messages under GCs C9.3(c) and C9.7.

7.55 We also consider it important for:

- Any person (senders, intended recipients and potentially other parties) to be able to challenge any blocking of a mobile number or message the provider takes under GC C9.3 or C9.7.
- Any person to be able to raise a challenge with any provider subject to our rules, which could be the challenger's provider or the provider that has applied a block.

7.56 In some instances, a challenger may not know which provider has applied a block on a message when it fails to reach the intended recipient. Their only option may be to challenge their own provider. In other circumstances, they may become aware of which provider has applied the block and challenge that provider.[395]

7.57 Ensuring anyone potentially affected by a blocking decision can challenge their own provider, or another provider, is important to ensure users have an effective and meaningful route to challenge decisions relating to messages that have been incorrectly blocked and have their service reinstated if confirmed as legitimate. It should also provide users with a prompt resolution and ensure that challengers are not passed around between providers, with no operator taking responsibility for resolving the challenge.[396]

7.58 While a customer's provider may also voluntarily seek to resolve issues relating to blocking by another provider, we consider it important for a customer's provider to be required to take reasonable steps to resolve a challenge (we set out our expectations in our guidance, paragraphs 2.168-2.181).

7.59 Absent a right to challenge, where an individual has a legitimate message blocked they would have no opportunity to challenge that decision short of legal action, which is

[395] For example, on P2P channels, a sender can obtain confirmation from their own provider whether they applied the block. If they have not, the sender will know the block was applied by the intended recipient's provider. On A2P channels, a sender may become aware that messages are being blocked by a particular provider because delivery failures are limited to that provider's network.

[396] In practice, it will mean that where Individual A knows that its message has not been delivered to Individual B, either Individual A can complain to their provider or Individual B can complain to their provider (which may be particularly important if one of those individuals is more vulnerable or otherwise less capable of raising a challenge with their own provider).

invariably time-consuming and expensive. While Ofcom could potentially take action for non-compliance with GC C9.3 and C9.7, it is unlikely to be feasible or appropriate to do so to resolve individual customers' challenges.

7.60 To help ensure the right to challenge is an effective safeguard, it is also important for providers to be transparent about their policy, which should be clear and accessible on their website. We consider this particularly important in the light of our decision not to implement the proposed notification requirement.

7.61 We recognise that our proposed right to challenge had applied broadly to any action a provider takes under GC C9 that affects them, including challenges to the application of volume limits (under GC C9.5) as well as challenges relating to the application of due diligence checks, ongoing monitoring and incident management requirements (under GCs C9.8-C9.16). Taking into account the considerations above, we consider it necessary for the right to challenge to apply to blocking decisions taken under GCs C9.3 and C9.7, specifically. For example, we do not consider it necessary to require providers to offer a specific right to challenge:

- The application of a volume limit under GC C9.5, in accordance with a volume limit or fair use policy that providers have communicated to their customers.
- The result of any decision taken under GCs C9.8-C9.16 (requirements relation to conducting up-front due diligence, ongoing monitoring and incident management requirements), where we expect there will be existing commercial incentives and arrangements in place to manage any disputes.

Implementation challenges

7.62 We note the practical issues respondents raised about how providers can respond to challenges from an end-user that is not their customer. Any challenge will involve determining whether a message was intended to scam the recipient and, in most cases, we consider this is likely to be straightforward and unlikely to require obtaining data from another provider. For example, the provider that blocked the message should know why it blocked it and be able to review whether it was correctly blocked (it might carry out human review of potential false positives in a similar way).

7.63 We would expect the review of a challenge to include the manual verification of the relevant message's content or the rationale for blocking a number (taking into account relevant reports, such as to 7726, and associated traffic patterns). We would also expect providers to carry out basic checks on any relevant URLs to assess their origin and credibility. All providers would also be able to request information they may need from a challenger to be able investigate (e.g. name of sender, originating provider) and assess that information in the context of its own scam reports and other intelligence.

7.64 Taking into account the removal of the notification requirement, low rates of false positives and various steps providers can take to resolve a challenge themselves, we expect that there will be limited circumstances in which providers may consider it necessary to seek data from other providers to resolve a challenge.

7.65 For the same reasons (and in response to BT's comments) we consider the risk that the right to challenge would require the transfer of highly sensitive personal data between providers to be low. Where providers may consider it necessary to share information with another provider, we expect providers to follow the data sharing principles in paragraph 2.28 of our guidance.

7.66 Providers should also take account of the Information Commissioner's Office (ICO)'s guidance on sharing personal information when investigating scams and fraud, which explains that "Data protection law does not prevent organisations from sharing personal information, if they do so in a responsible, fair and proportionate way".[397]

7.67 Taking into account providers' incentives to deliver legitimate messages, we consider it appropriate for providers to have discretion in deciding how they will assess and determine challenges. We expect them to take reasonable steps to obtain appropriate evidence, take all relevant circumstances into account and take a consistent approach. This means that, where a provider has a reasonable belief that a number or message is associated with a scam and the challenger cannot sufficiently demonstrate it is legitimate (and there are no other factors that suggest that their activity could be legitimate), the provider has the discretion to retain the block (it may also consider whether to report the matter to the police, if appropriate). Alternatively, if there are various indicators that a number or message is legitimate but no definite proof of its legitimacy,[398] the provider has discretion to remove the block.

7.68 Overall, we consider that any practical issues (for example, relating to data sharing) should be limited and manageable.

Financial costs of our requirements

7.69 We note the concerns some respondents raised in relation to the potential costs of setting up a right to challenge process. We believe that many of the representations on costs that respondents made were premised on the expectation that providers would receive a significant number of challenges from mobile users who had received blocking notifications. As set out above, we would also have expected scammers to receive many notifications, which could pose a further risk that scammers might challenge blocking decisions vexatiously.

7.70 As explained above, we have decided not to implement the proposed notification requirement. We also understand existing rates of false positives and associated customer complaints to be low. While there may be an increase in challenges as a result of the consistent application of our blocking measures across industry, we do not expect any increase to be significant.

7.71 We are also imposing other safeguards, discussed in this section, that should help to mitigate the risk of false positives and therefore the risk of a large volume of challenges.

7.72 More generally, providers within the scope of GC C9.3 and C9.7 should already have well-established complaints processes, including where they are already subject to GC C4 relating to complaints handling and dispute resolution. We expect providers can absorb any right to challenge process into existing complaints processes, without incurring significant additional resource or cost.

7.73 We recognise that a challenge to a blocking decision could, in principle, be considered an expression of dissatisfaction within the scope of the definition of a 'Complaint' under GC C4. We do not, however, consider it necessary or proportionate to require providers to

[397] ICO, Data protection is not an excuse when tackling scams and fraud [accessed on 10 July 2026].
[398] For example, the sender ID or number aligns with known patterns used by a legitimate organisation, the message does not display typical characteristics of scams (e.g. no urgency or suspicious links) and the sender or number does not appear in scam reports.

consider challenges under GC C9 to be 'Complaints' for the purposes of GC C4 should they also fall in scope of that GC (nor do we consider it necessary or proportionate to require that challengers have the right to use an alternative dispute resolution scheme in relation to a challenge, specifically).

7.74 We have established a dedicated right to challenge process in GC C9.17, including an appeal process, which we consider provides an effective and targeted means of reviewing blocking decisions. While customers may potentially raise complaints under GC C4 about matters to which the right to challenge under GC C9.17 could also apply, the right to challenge process is available to any person affected by a block, rather than to individuals, small businesses and charities that fall within the definition of a 'Relevant Customer' under GC C4.

7.75 We further note that, given the likely very low number of false positives, the number of instances where a challenger remains unsatisfied at the end of a provider's appeal process should be even lower (and only a subset of those challenges are likely to be made by an individual, small business or charity potentially within the scope of GC C4). [399]

7.76 For these reasons, as well as the various safeguards we have put in place to further mitigate the risk of false positives arising and protect users' rights, we consider it appropriate for challenges under GC C9.17 to be treated as a request to review and, where appropriate (and possible) unblock a number or message, that are outside the scope of GC C4. We have added a footnote to GC C9.17 clarifying this.

7.77 Providers may, however, decide voluntarily to consider some challenges to be complaints within the scope of GC C4. We may also consider it necessary to review this position in future, depending on the extent of any evidence that persons challenging blocking decisions are dissatisfied with the outcome of providers' right to challenge processes, including their appeal processes.

7.78 Overall, we do not expect that there will be significant additional costs associated with the right to challenge requirement.

We expect the benefits of our right to challenge requirement to outweigh any costs and adverse impacts

7.79 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we have decided to retain the right to challenge. In making this decision, we have weighed the significant interference with individual rights that may occur if the fundamental right to challenge a blocking decision is removed against the potential costs and implementation challenges of implementing a right to challenge. Overall, we consider that the benefits of a right to challenge outweigh any costs or adverse impacts.

7.80 GC C9.17 requires providers to implement and maintain an appropriate and effective right to challenge policy and associated systems and processes. It also identifies the minimum requirements for that right to challenge policy.

---

[399] This scenario would only arise where (a) a false positive has arisen (which we already consider to be a very low risk); (b) a person has raised a challenge with their own provider: (c) that person is an individual, small business or charity within the definition of a 'Relevant Customer' in GC C4.1; and (d) that person is not satisfied with the outcome of the right to challenge process (which in itself includes an appeal stage). Businesses that do not benefit from C4 may also be more likely to challenge a blocking decision (where legitimate A2P messages are blocked).

7.81 The right to challenge will apply to any person that may have been impacted by blocking of messages or numbers (whether they are the sender, intended recipient or another third party, such as an aggregator). Therefore, it does not apply only in relation to the sender of a message. Affected persons can also challenge any blocking decision by any provider under GC C9.17.

7.82 GC C9.18 requires providers to ensure their right to challenge policy is well publicised and readily available on their website and in relevant terms and conditions.

7.83 We have decided to make amendments to GCs C9.17 and C9.18 to:

- Confirm that the right to challenge only applies to blocking decisions taken under GC C9.3 and C9.7. For this reason, GC C9.17 does not contain the requirement in proposed GC C9.18 that would enable any person to challenge "other action" that providers take under Condition C9 that affects them.
- Clarify that any affected person can raise a challenge relating to a number or message blocked under GC C9.3 and C9.7.
- Amend GC C9.17(f) to require providers to identify a "prompt" and reasonable timeframe within which the provider will reach an outcome following a challenge. We consider it important for an outcome to be reached promptly, given the potential impact of an incorrect blocking decision on individual rights.
- Confirm that providers are not required to treat challenges under Condition C9.17 as 'Complaints' for the purpose of GC C4.
- Remove the proposed requirement (in proposed GC C9.18(c)) for providers to provide their right to challenge policy free of charge on reasonable request in hard copy or another format. As explained above, we note that providers may absorb their right to challenge within established complaints processes, including where they are already subject to GC C4 relating to complaints handling and dispute resolution. Many providers that are subject to paragraph 18 of the Annex to GC C4 are already required to provide their Customer Complaints Code free of charge to Complainants upon reasonable request, in hard copy or other format. This obligation would also be less likely to be of use to challengers that are business senders.[400] For these reasons, we do not consider it necessary to include proposed GC C9.18(c) as part of the right to challenge but we have set out our expectations in paragraph 2.184 of our guidance.

7.84 We consider it appropriate for a right to challenge to be a requirement in the GCs with associated guidance. We recognise that, in other instances, a right to challenge process is identified in guidance (for example, in our CLI Guidance[401]). In other cases, however, it is written into the GCs (see for example GC C4). Given the potentially significant and serious risk of interference with individual rights where an individual has a legitimate message blocked, we consider it appropriate to include the right to challenge in the GCs. This will enable us to enforce any potential non-compliance directly.

7.85 We have also updated paragraphs 2.165-2.184 of our guidance on how we expect providers to assess and determine challenges, including: (a) the factors we expect them to take into

[400] We also note that GC C4 is focused on protecting a provider's own individual customers, small businesses and charities whereas any person (including larger businesses) has the right to challenge any provider under GC C9.17.

[401] See Ofcom, 2022. Guidance on the provision of Calling Line Identification facilities and other related services. In July 2026, we published our decision to amend this guidance to set out how we expect communications providers to tackle scams calls from abroad that spoof UK mobile numbers. See Ofcom, 2026.

account when assessing challenges made by both their own customers and customers of other providers; and (b) the principles we expect them to take into account if they do consider it necessary to share information with another provider.

7.86 The GCs relating to the right to challenge are now set out in GCs C9.17 and C9.18.

Review of policies, systems and processes

What we proposed

7.87 In our 2025 consultation, we proposed under GC C9.20 that providers must regularly review their policies, systems and processes to ensure they remain appropriate and effective and are operating as intended. We proposed that providers must ensure they are complying with their own policies, systems and processes and take appropriate and effective action to ensure that any issues identified are addressed promptly, including by making appropriate changes to their policies, systems and processes.

7.88 We did not consider this would impose significant additional costs beyond those of other P2P and A2P measures. We expected the need for some additional staff time to drive these costs.

Stakeholder responses

7.89 Some stakeholders expressed their support for our proposal to regularly review policies, systems and processes, as these promote accountability, effective oversight and a consistent approach to implementing protections across the sector.[402]

7.90 BT asked for clarification of our requirement to carry out reviews "regularly" and our proposed guidance that providers should carry out reviews at least annually. BT said Ofcom should set out clearly why it expects an annual review of procedures to be appropriate. It recommended that proposed GC C9.20 should be amended to require reviews "as appropriate".[403]

7.91 As explained in paragraph 5.16, [✂] raised some technical and cost concerns, saying that it would be challenging to extract the relevant data to assess the effectiveness of the volume limit.[404]

Our assessment

7.92 We welcome the general support for our proposed requirement relating to reviewing policies, systems and processes.

7.93 The requirement is intended to ensure that providers maintain the effectiveness of anti-scam measures. If providers do not stay vigilant and keep on top of new and emerging threats, their systems and processes are likely to become less effective.

7.94 We note BT's comments relating to the frequency at which providers should carry out reviews. Our proposed GC required reviews to be carried out regularly and our proposed guidance had referred to carrying out audits (by which we intended to describe more

[402] For example, iconectiv said it supports Ofcom's emphasis on regular reviews which helps promote accountability, enable effective oversight and support consistent application of controls across organisations. iconectiv UK response to October 2025 Consultation. Page 9; Citizens Advice Scotland response to October 2025 Consultation. Page 3; Which? response to October 2025 Consultation. Page 11.
[403] BT Group response to October 2025 Consultation. Page 14.
[404] Name withheld 1 response to October 2025 Consultation. Page 5.

formal and comprehensive audits) at least annually, as an example of ensuring compliance with the requirement.

7.95 Our proposed guidance also explained that the timing and extent of each review will depend on the circumstances, including the policy, system or process under review and whether it is a scheduled review, ad hoc or intended to address a specific issue that may have arisen.[405]

7.96 Taking into account stakeholders' comments, we remain of the view that providers should carry out some form of review regularly. We expect these reviews to include both:

- Informal reviews, as part of an ongoing evaluations of threats. We expect providers to carry these out on a continual or ad hoc basis, in response to any new threats, incidents or challenges that may arise.
- More formal and comprehensive reviews or audits, which we expect providers to carry out less frequently, for example annually, depending on the nature and extent of any informal reviews.

7.97 We consider it appropriate for providers to decide what reviews are reasonable and proportionate for their particular circumstances. This includes deciding how often to review their policies, systems and processes and the type of review they carry out. We also expect providers to be flexible about the timing and extent of any reviews depending on any new threats, incidents or challenges they may become aware of.

Financial costs of our requirements

7.98 We note [✂] comment on the cost required to review policies, in particular a volume limit. We address these issues in paragraph 5.41 on volume limits for PAYG SIMs. Overall, we do not expect our amended measures relating to reviewing policies, systems and processes to impose significant incremental costs on industry.

We expect the benefits of our requirement to regularly review policies, systems and processes to outweigh any costs and adverse impacts

7.99 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we have decided to implement our proposed requirement for providers to regularly review their policies, systems and processes (including all rules implemented under GC C9). However, we have updated our guidance to reflect the different types and frequency of reviews we expect providers to carry out to reflect the expectations set out in paragraph 7.96 above.

7.100 Overall, we consider the benefits of our measures relating to reviewing policies, systems and processes outweigh any costs or adverse impacts for industry and consider them to be proportionate.

7.101 Our requirement relating to reviewing policies, systems and processes is now set out in GC C9.19. Further information, including how providers are expected to comply, is set out in paragraphs 2.187-2.196 of our guidance.

[405] We also said that it will be appropriate to review some policies, systems and processes more regularly than other policies, systems and processes.

Training staff

What we proposed

7.102 In our 2025 consultation, we proposed that providers must ensure that all staff are made aware of, and appropriately trained on, the policies, systems and processes put in place under proposed Condition 9, including ensuring relevant staff are appropriately trained on the right to challenge processes implemented under Condition C9.18 (proposed GC C9.21).

7.103 We did not consider this would impose significant additional costs beyond those of other P2P and A2P measures.

Stakeholder responses

7.104 Several respondents supported our proposed requirement relating to training staff.[406] For example, iconectiv UK said it supported our emphasis on staff training, which would help promote accountability and support consistent protections.[407] The Campaign Registry stated that it conducts comprehensive staff security training, including security awareness and internal security policies.[408]

7.105 Utility Warehouse said that the proposed condition that "all staff" are aware and appropriately trained is an unrealistic and overly demanding requirement. It proposed the wording should be amended to "all relevant staff", which would also better align with the examples cited in our guidance and the wording in proposed GC C9.18.[409] UKCTA made the same suggestion.[410]

7.106 However, [✂] disagreed with the proposed training requirement, because it considered staff training would create a significant additional burden for aggregators, which it did not believe is justified.[411]

Our assessment

Rationale and benefits

7.107 We welcome the support for our proposed requirement relating to training staff among many stakeholders.

7.108 The requirement is intended to ensure that all staff that may have a role in ensuring compliance with General Condition C9 are made aware of, and appropriately trained on, the policies, systems and processes put in place under our proposed Condition C9. We agree with comments from Utility Warehouse and UKCTA that the requirement should not apply to "all staff", regardless of their role, which is likely to be unnecessary and unduly burdensome. Rather, it is intended to apply to "relevant staff".

7.109 Relevant staff includes any staff that are or may be involved in implementing Condition C9. This includes technical and other staff working in specialist fraud management or network teams, as well as staff that handle challenges and enquiries relating to blocked numbers

[406] [✂] response to October 2025 Consultation; VodafoneThree response to October 2025 Consultation. Page 8; iconectiv UK response to October 2025 Consultation. Pages 8-9; Pinnacle Teleservices response to October 2025 Consultation. Page 13.
[407] iconectiv UK response to October 2025 Consultation. Page 9.
[408] The Campaign Registry response to October 2025 Consultation. Page 11.
[409] Utility Warehouse response to October 2025 Consultation. Page 6.
[410] UKCTA response to October 2025 Consultation. Page 3.
[411] [✂] response to October 2025 Consultation.

and messages (including customer-facing teams that are the first point of contact for a challenge or enquiry and staff to whom challenges may be escalated). It also includes any third parties that carry out these functions on behalf of a provider.

Financial costs of our requirements

7.110 We note the comment that our proposed training requirement would impose a significant additional burden on providers. On the basis that the requirement is intended to apply to all relevant staff (as described above), we do not consider this requirement is likely to impose a significant incremental cost on industry. We also consider it necessary to ensure compliance with Condition C9. There is a real risk of non-compliance with Condition C9 (which is likely to significantly undermine our objective) if providers do not make staff performing functions relevant to the systems and processes implemented and maintained under C9 aware of, and appropriately trained on, its requirements.

We expect the benefits of our requirement on training staff to outweigh any costs and adverse impacts

7.111 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we have decided to implement our proposed training requirement, with a small amendment to refer to "all relevant staff". We have also updated our guidance to explain what we mean by "relevant staff". Overall, we consider that the benefits of our amended training requirement outweigh any costs or adverse impacts for industry and consider it to be proportionate.

7.112 Our amended requirement relating to training staff is now set out in GC C9.20. Further information including how providers are expected to comply is set out in paragraphs 2.200-2.201 of our guidance.

Record keeping and retention

What we proposed

7.113 In our 2025 consultation, we proposed that providers must implement and maintain appropriate records of scam prevention policies to ensure continued compliance with Condition C9. Our proposed record keeping requirements covered records relating to: general policies, systems and processes and formal reviews of those policies, systems and processes; records of the application of volume limits for PAYG SIMs; records of the measures or actions taken in response to an incident under Conditions C9.15 and C9.16; customer-related records; and records of challenges to blocking decisions.

7.114 We proposed that the record keeping requirements should be overseen by a designated senior individual. We proposed a minimum time period, ranging from 2 years to 5 years, depending on the specific category or records related to scam prevention policies.

7.115 In addition, we set out that we expected providers to incur most of the costs of our record keeping requirements as part of the additional ongoing staff and system costs that we specified under each P2P and A2P measure.

7.116 Our proposed record keeping requirements were set out in proposed GC C9.22-C9.25.

Stakeholder responses

7.117 Stakeholders were broadly supportive of our record keeping and retention proposals, but some respondents were concerned with the associated administrative burden and costs.

Support for record keeping proposals

7.118 Many stakeholders expressed support for introducing record keeping requirements, as proposed under GCs C9.22-C9.25. Stour and the CCP-ACOD agreed that providers should establish and maintain effective systems for keeping records, to demonstrate and ensure continued compliance with GC C9.[412] The CCP-ACOD also encouraged Ofcom to standardise audit requirements to include monitoring against unintended consequences, which would ensure greater accountability.[413]

7.119 Other respondents said that the record keeping proposals will assist providers in ensuring they are complying with their obligations and data protection legislation. [✂], iconectiv UK and Pinnacle agreed with our proposal, noting that including such safeguards would ensure proportionality and compliance with privacy laws.[414] Utility Warehouse added that they did not object to this proposal.[415]

Administrative burden and retention period concerns

7.120 Some respondents raised concerns about the administrative burden of complying with proposed GC C9.22, as well as the length of some of the proposed retention periods.

7.121 For instance, some respondents raised concerns about the need for aggregators to implement record keeping requirements, as noted in [✂] response that said record keeping would incur significant additional burdens for aggregators, which it did not believe was justified.[416]

7.122 Certain respondents were concerned that the proposed record keeping requirements would create significant costs for providers and that the proposed timeframes for record retention were disproportionately long. BT said the record keeping requirements would incur substantial costs[417] and would be too burdensome when considered alongside the guidance and timelines set out in proposed GC C9.23-C9.25, which contain nine different data retention requirements with varying retention periods.[418] techUK also argued that the proposal for a five-year retention period for some information is unreasonable, particularly when the records relate to personal data. They recommend that we outline the rationale for proposing a five-year retention period.[419]

7.123 Some stakeholders raised concerns about record keeping requirements on P2P channels. techUK disagreed with the proposal to keep records of communication with any person regarding a challenge for two years. It argued that this would be challenging on P2P channels as the volumes may be significant. It suggested Ofcom clarify what level of detail is required and justify why it is needed.[420]

---

[412] Stour Marine response to October 2025 Consultation. Page 4.
[413] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3; iconectiv UK similarly said it supports Ofcom's emphasis on robust record keeping helps promote accountability, enable effective oversight and supports consistent application of controls across organisations. iconectiv UK response to October 2025 Consultation. Page 9
[414] [✂] response to October 2025 Consultation; iconectiv UK response to October 2025 Consultation. Page 9; Pinnacle Teleservices response to October 2025 Consultation. Page 13.
[415] Utility Warehouse response to October 2025 Consultation. Page 6.
[416] [✂] response to October 2025 Consultation.
[417] BT Group response to October 2025 Consultation. Page 12.
[418] BT Group response to October 2025 Consultation. Page 15.
[419] techUK response to October 2025 Consultation. Page 4.
[420] techUK response to October 2025 Consultation. Page 5.

Other issues

7.124 Some stakeholders were unsure who would qualify as a "senior individual" able to oversee record keeping. Twilio requested we clarify the definition of a "senior individual", as described in proposed GC C9.22.[421]

Our assessment

Rationale and benefits

7.125 We continue to believe that requiring providers to retain the types of records we had proposed is important to enabling us to identify and assess potential non-compliance and therefore ensure our measures are effective.

7.126 We also consider it important for providers to retain the types of records we had proposed so they can monitor and ensure the ongoing effectiveness of their scam prevention measures. For example:

- If providers do not keep records of their general policies, systems and processes and formal reviews of those policies, systems and processes, it will be harder to understand how those policies have adapted to the changing threat landscape over time and assess what policies were most effective.
- If providers do not keep appropriate records of previous risk assessments and actions taken in relation to a particular customer or incident, they will have limited information available on which to update risk assessments and assess whether and how a particular customer's conduct may have changed (which may, for example, result in that customer being considered higher risk and subject to further monitoring). Providers would also have more limited information on the outcomes of challenges and false positives which they could otherwise use to help reduce the risk of further false positives.
- Records relating to the application of volume limits will provide important information for providers to identify numbers that repeatedly reach their volume limits (and the particular risk use of those numbers may pose). These records will also allow providers to monitor the effectiveness of their volume limits (including whether they are set at an appropriate level), which should help ensure they strike the right balance between blocking scam messages and enabling the transmission of legitimate messages.

7.127 In order to ensure we have the ability to request information to monitor any potential impacts on individual rights, we also consider it important to require providers to retain information relating to challenges, as well as information on false positives that are identified through the systems and processes they put in place under GC C9.26 (explained further below).

7.128 Providers may more generally consider it important to retain records relating to their existing customers or for auditing purposes.

7.129 Where records are retained, it is important that this is for a sufficient period, so providers can monitor the effectiveness of their policies and changes in customer behaviour over time. If retention periods are too short, then providers will have more limited and less reliable information available to reach robust conclusions on any changes or trends they observe.

[421] Twilio response to October 2025 Consultation. Page 12.

7.130 In future, we may also require information to be able to investigate potential non-compliance. In the course of such investigations, we may request historical information covering periods of several years, to be able to assess the seriousness of any potential non-compliance, including the extent of any consumer harm and whether non-compliance is an isolated incident or if there is a pattern of repeated conduct. Retention periods that are too short are likely to have a significant adverse effect on our ability to investigate non-compliance and carry out our enforcement functions. They would also limit our ability to monitor the effectiveness of our new requirements.

7.131 While providers can decide the format and location in which they retain records, it is important they are easily accessible if requested by Ofcom, and comprehensible.

Administrative burden and retention period concerns

7.132 We note the concerns raised by some stakeholders that our proposed retention periods are too burdensome and would drive substantial costs.

7.133 We issued our May 2026 requests in part to help us understand these concerns. We requested further evidence on MNOs' existing retention periods. The responses indicated that some providers are already retaining the types of records we set out for at least the periods we had proposed.[422]

7.134 For example, [✂] indicated that it already largely keeps all the types of records we have proposed for at least the periods we had proposed.[423] [✂] also confirmed that it keeps various records relating to scam prevention permanently and explained that this includes policies and processes relating to certain system configurations, as well as the "outputs of every review of scam prevention rules including manual checks, SpamShield [a firewall] configuration audits, audit reports, related email correspondence, and change implementation project records". That provider has confirmed that incidents formally logged are retained for five years and that information from the initial and ongoing checks on A2P partners is retained until the contract ends with the supplier.[424]

7.135 The responses to our May 2026 requests did, however, indicate that retention periods are generally much shorter where more significant volumes of data may be generated (for example, statistics on the application of volume limits). The responses also indicated some of our proposed record keeping requirements (including requirements relating to policies, systems and processes and the application of volume limits) did not make clear what specific types of records providers were required to retain.

7.136 We recognise some providers do not currently keep records in all the categories that we proposed, or for the time periods that we proposed, and that changing their processes to do so would drive some costs. However, in general we do not expect our requirements to result in the retention of significant volumes of documents. In particular, we only consider it necessary for providers to retain the following specific types of records:

---

[422] Responses to our May 2026 requests provided a varying level of detail relating to existing retention periods. Where providers identified existing retention periods relating to all our proposed record keeping requirements, their responses indicated that they were generally already retaining the types of records we proposed for at least the periods we had proposed.

[423] [✂] response to formal information request dated 29 May 2026, question 11.

[424] [✂] response to formal information request dated 2 June 2026, question 11.

- **Policies, systems and processes**: the requirement under what is now GCs C9.22(a) and (b) relates to overarching general policies, systems and processes and formal reviews of those policies, systems and processes.[425] We expect providers to retain such records in a limited number of documents and providers may set policies covering different GCs within a single overall policy. We do not consider it necessary for providers to retain more detailed and flexible rules that they apply, which they may update hourly or daily, or lists of scam URLs or numbers that have been blocked.
- **Volume limits for PAYG customers**: the requirement under what is now GC C9.25(b) to retain records of the application of volume limits under Condition C9.5 may generate a significant number of records, depending on how many times those limits are reached. We do not, however, consider it necessary for providers to retain all information relating to the specific application of volume limits; rather we consider it appropriate for them to retain a record of each instance a PAYG customer reaches a volume limit under Condition C9.5 (including the PAYG customer's number and the date on which the volume limit was reached). We recognise that some providers' systems may automatically delete relevant data, but providers should be able to periodically capture and store the relevant data as required, at minimal cost.
- **A2P scams incidents**: the requirement under what is now GC C9.22(c) to retain a description of an incident (including the date and time at which the incident was identified and the number of messages involved)[426] and records of the measures or action taken in response to an incident, under Conditions C9.15 and C9.16, will only apply if providers generate such records in response to potential scam indicators. We expect providers could retain this information in a template or form. We do not consider it necessary for providers to retain detailed operational or dynamic traffic data that they may generate in responding to an incident.
- **Customer-related records**: in relation to the requirements under what is now GC C9.23 to retain customer-related records, providers will need to perform KYC checks, checks on alphanumeric sender IDs and initial risk assessments when onboarding customers, which should generate a single or limited number of documents. Similarly, providers may generate updated risk assessments, actions from KYT checks[427] and requirements imposed under GC C9.9(a) and (b) (and thus need to retain these documents) only where they have identified potential scam indicators. We consider it important for customer-related records to be kept for existing customers and at least three years after the end of the contractual relationship.[428] However, providers should ensure their records are kept up to date, taking

[425] The type of policies we expect to be retained under this requirement include all versions of providers' policies on: their approach to receiving and validating scam reports; identifying and blocking scam numbers and messages; volume limits for PAYG customers; due diligence and ongoing monitoring relating to A2P messages; and identifying, monitoring and addressing false positives.

[426] We recognise that the GCs we consulted on did not require providers to retain a description of an incident. However, we consider providers are likely to have needed to retain a description of an incident as necessary context to retaining a record of measures or action taken in response to an incident. We therefore expect also requiring providers to retain a description of an incident will have a limited impact.

[427] Such actions are likely to occur where a provider encounters scam indicators from a business sender. Where the provider cannot satisfy itself that the relevant messages were legitimate we expect providers to retain records of: the actions taken (for example, blocking a sender from sending further messages); the date the actions were taken; and the name of the relevant business sender (and where relevant, the downstream provider that passed the messages to the provider).

[428] We note that Regulation 40 of The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 requires records to be kept for at least five years after a business relationship has come to an end.

into account the data accuracy principle in the UK Data Protection Regulation 2016 (UK GDPR).

- **Challenges to blocking**: in relation to the requirement under what is now GC C9.25(a) to retain information on challenges, we do not expect there to be high numbers of challenges, taking into account likely low levels of false positives and our decision to limit challenges to blocking decisions taken under GC C9.3 or C9.7. We also expect there to be far fewer challenges than there are complaints subject to record keeping requirements under GC C4.2(c) and paragraph 24 of the Annex to GC C4. We consider it appropriate for providers to retain records of communications between that provider and any person regarding a challenge raised under Condition C9.17, from the date the challenge was resolved or otherwise closed.[429] We expect this information can be retained in a similar way to existing record keeping practices relating to complaints (potentially within a template or form). The requirement to retain records relating to challenges relates to any query from any person about blocking activity, rather than a formal legal challenge.
- **False positives**: in relation to the new requirement under GC C9.24 to retain information on false positives, we consider the risk of false positives arising from implementing our measures to be very low, for the reasons set out in paragraphs 7.29. We consider it appropriate for providers to retain: a description of a false positive incident (including the date and time the incident first arose; its impact;[430] the likely cause;[431] and how and when it was identified);[432] and any measures or actions taken in response to that incident. [433] As explained in paragraph 7.166 below, we are giving providers the flexibility to comply with GC C9.26 by identifying, monitoring and addressing false positives where they reasonably believe a false positive may have arisen as a result of implementing our requirements, in acknowledgement that it may be operationally or technically challenging to determine if implementing our requirements was the sole reason why the false positive arose.

7.137 We note that not all providers will need to keep all of the records subject to the requirements. For example, MNOs are unlikely to onboard A2P customers and are therefore unlikely to generate, and have to retain, records such as KYC checks or checks on new uses of alphanumeric sender IDs, including initial and updated risk assessments.

---

[429] We note that this is the same type of information providers are already required to retain under paragraph 20 of the Annex to GC C4 relating to complaints. Taking into account the requirements of GC C4, we expect communications relating to challenges to include a clear record of the following information, or otherwise expect providers to ensure they have a clear record of the following information: (a) the date on which a challenge was received; (b) how the challenge was made (for example, by email or by phone); (c) the identity and contact details of the person making the challenge; (d) a description of what the challenge is about; (e) all communications made or received between the provider and the person making the challenge regarding the challenge including, as a minimum: the date on which the communication was made or received; how the communication was made or received (for example, by email or by phone); a description of what was contained in the communication (for example, advice given and/or action proposed to be taken and/or action agreed with the person making the challenge to be taken, to resolve the challenge); copies of any written communication; and (f) the date on which the challenge was resolved or otherwise closed.

[430] We expect this information to include how many messages were incorrectly blocked; the time period over which they were blocked; and the number of complaints or other known impacts.

[431] We expect this information to include information on whether the sole cause was likely to be implementing our requirements or whether a provider reasonably believes a false positive may have arisen as a result of implementing our requirements.

[432] We expect this information to include the time and date on which the incident was identified.

[433] We expect this information to include a record of any changes to rules, configurations or datasets; and the date and time on which such measures or actions were taken.

Financial costs of our requirements

7.138 Given the discussion above, including the types of documents that providers are already likely to retain, as well as the limited types and volume of documents they will be required to retain under these measures, we do not expect our amended record keeping requirements to impose a significant incremental cost on industry.

We expect the benefits of our record keeping and retention requirements to outweigh any costs and adverse impacts

7.139 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we continue to consider it proportionate to require providers to retain the general types of information included in our proposed record keeping requirements. We further consider it proportionate to require providers to retain information on their false positives rates.

7.140 However, having reviewed responses to our 2025 consultation and our May 2026 requests, we have decided to make the following changes to the length of the retention periods and specific types of records we will require providers to retain:

- **Volume limits for PAYG customers**: we have decided that providers must retain a record of each instance a PAYG customer reaches a volume limit under Condition C9.5 (including the PAYG customer's number and the date on which the volume limit was reached). We have also significantly reduced the period for which providers need to retain records of applying volume limits, under what is now GC C9.25(b), to at least 12 months. For the reasons set out in paragraph 7.126 above, we do not consider it appropriate to reduce this period further. We note that this 12-month retention period is the same period as the requirement under GC C3.3 relating to the retention of billing records. The amended requirement is now set out in C9.25(b).
- **A2P scams incidents**: we have amended the requirement relating to the retention of records on incidents under Conditions C9.15 and C9.16, to also require providers to retain a description of the incident (including the date and time the incident was identified and the number of messages involved). The amended requirement is now set out in GC C9.22(c).
- **Challenges to blocking**: we have decided to implement our consultation proposal to require providers to retain records of communications between that provider and any person regarding a challenge raised under Condition C9.17, from the date the challenge was resolved or otherwise closed. However, we have decided to reduce the retention period to 12 months. While we do not expect many challenges (and have amended GC C9.17 so that the right to challenge only applies to blocking decisions made under GC C9.3 and C9.7), this 12-month period aligns with the existing retention period for complaints under paragraph 24 of the Annex to GC C4. The amended requirement is now set out in GC C9.25(a).
- **False positives**: we have decided to require providers to retain the following information relating to false positives for two years: (a) a description of a false positive incident (including the date and time the incident first arose; its impact; the likely cause; and how and when it was identified); and (b) any measures or actions taken in response to that incident. This new requirement is now set out in GC C9.24.

7.141 We have updated our guidance to clarify the specific types of records we expect providers to retain under each requirement (in accordance with paragraph 7.136 above).

7.142 We consider our amended record keeping measures strike an appropriate balance between, on the one hand, reflecting how providers should ensure the effectiveness of their measures and enabling us to identify and assess potential non-compliance (including

potential impacts on individual rights), and on the other hand, the potential burden for providers. We anticipate that the benefits of our amended record keeping measures will outweigh any costs or adverse impacts for industry and consider them to be proportionate. We also consider our amended record keeping measures to be consistent with the principle of storage limitation under the UK GDPR.

7.143 The amended record keeping requirements are summarised in the Table 7.2 below and have been reflected in our updated guidance. We have also updated our guidance to explain that:

- The "designated senior individual" that needs to oversee record keeping requirements should be a senior individual with delegated authority or responsibility for compliance with GC C9 and/or fraud management.
- Providers can decide the format and location in which they retain records but we expect them to be easily accessible if requested by Ofcom, and comprehensible.

7.144 It remains open to providers to retain records for longer than our requirements, taking into account their own policies and relevant data protection principles.

7.145 Our amended record keeping requirements are set out in GCs C9.21-C9.25. Further information including how providers are expected to comply is set out in paragraphs 2.204-2.225 of our guidance.

Table 7.2: Retention periods

Retention period	Categories of records that providers must keep
12 months	• Communications relating to challenges under GC C9.17 (retention period starts after the challenge is concluded). • Instances where PAYG customers reach a volume limit set under GC C9.4.
2 years	• Description of false positive incidents and measures or actions taken in response under GC C9.26.
3 years from end of contractual relationship	• KYC checks and checks on alphanumeric sender IDs (under GC C9.8), including initial and updated risk assessments. • Actions from Know Your Traffic Checks. • Requirements imposed on entities under GC C9.9(a). • Actions taken for ongoing compliance/addressing non-compliance with entities under GC C9.9(b).
5 years	• Policies, systems, and processes implemented under GC C9. • Reviews of effectiveness of the policies, systems, and processes, including any resultant actions or changes under GC C9.19. • Descriptions of incidents and measures or actions taken in response to scams incidents under GCs C9.15 and C9.16.

Ensuring the transmission of legitimate messages / identifying, monitoring and addressing false positives

What we proposed

7.146 In our 2025 consultation, we set out under proposed GC C9.27 that providers must take appropriate steps to mitigate the risk that legitimate messages passing through their blocking tools are prevented from reaching their intended destination. While complying with other GCs (and accompanying guidance) would also help providers to ensure the continued transmission of messages through networks, proposed GC C9.27 was intended to impose a clear and separate obligation to take additional steps to mitigate the risk of blocking legitimate messages.

Stakeholder responses

7.147 Many stakeholders disagreed with our proposed requirement to ensure the transmission of legitimate messages, stating that it would be unnecessary and create compliance concerns.

Whether the proposed requirement is necessary

7.148 Several respondents said that the requirement went against Ofcom's bias against intervention. BT said we had not identified a failure on the part of providers to transit or terminate legitimate messages.[434]

7.149 Many respondents said it was not necessary to introduce a formal requirement to ensure continued transmission, given operators already have commercial incentives to transmit messages.

7.150 Virgin Media O2 and Sky said it already is in operators' best interest to deliver legitimate traffic and that such regulatory obligations are not appropriate.[435] Mobile UK said the proposed condition would place a heavy burden on operators and, given they already have commercial incentives to deliver messages, proposed GC C9.27 was not necessary.[436] UKCTA stated that all legitimate providers have the objective of ensuring the transmission of legitimate messages.[437]

7.151 Other respondents recognised that the proposed GC C9.27 attempted to minimise over-blocking, but that it was unnecessary to formalise the requirement, as providers are already continuously assessing whether messaging campaigns are legitimate.[438] BT argued that the proposed GC C9.27 would undermine blocking efforts, which benefit consumers ([✂]).[439]

7.152 Some respondents (including Sky and UKCTA) stated that proposed GC C9.27 was unnecessary because providers are already required to take steps to ensure the transmission of legitimate messages under other GCs.[440]

---

[434] BT Group response to October 2025 Consultation. Page 15.
[435] Virgin Media O2 response to October 2025 Consultation. Page 4; Sky response to October 2025 Consultation. Page 3.
[436] Mobile UK response to October 2025 Consultation. Page 3.
[437] UKCTA response to October 2025 Consultation. Page 3.
[438] VodafoneThree response to October 2025 Consultation. Page 7; BT Group response to October 2025 Consultation. Page 15.
[439] BT Group response to October 2025 Consultation. Page 16.
[440] Sky response to October 2025 Consultation. Page 3; UKCTA response to October 2025 Consultation. Page 3.

Compliance concerns

7.153 Certain respondents expressed concerns that the proposed GC would ask operators to balance the obligation to block scam mobile messages with ensuring the transmission of legitimate messages and that it could be difficult to comply with both requirements simultaneously. Mobile UK and Virgin Media O2 said that this would force operators to walk a tightrope and they would potentially face penalties for non-compliance on both sides. It considered that this was not proportionate.[441] Sky suggested that potential enforcement action for over-blocking under proposed GC C9.27 would be counter-productive while industry is being asked to become more effective at collaborating to identify scams.[442]

7.154 Some respondents raised concerns with implementing the proposed GC on A2P channels, specifically. Mobile UK argued that, in the event of an operator incorrectly blocking a message (e.g. spam), operators should not potentially have to face enforcement action.[443]

7.155 BT added that, through the proposed GC C9.27, Ofcom had attempted to disproportionally place its duties under the Human Rights Act 1998 onto operators. It argued that, while Ofcom attempted to ensure proposed GC C9.27 would protect the right to free expression under Article 10, it had provided no clear guidance on what is considered a "legitimate" message. Therefore, it considered that Ofcom had not appropriately discharged its duty to balance the relevant ECHR provisions proportionately.[444]

Our assessment

Rationale and benefits

7.156 The proposed requirement to ensure the transmission of legitimate messages was included primarily as a safeguard to mitigate the risk of false positive blocking, as our proposals had the potential to interfere with individual rights, specifically freedom of expression.

7.157 While we consider that false positive rates from blocking under our rules are likely to be very low (and lower than we had understood at consultation), we recognise that it is not possible to eliminate all false positives and some will therefore still arise: for example, as a result of human error.[445] Therefore, we consider it important that providers take appropriate steps to identify false positives when they arise and minimise the risk they continue to occur, to reduce the risk of interference with individual rights.

7.158 The responses to our May 2026 requests indicate that providers currently have varying levels of oversight over false positives. While some providers have implemented various manual checks to proactively identify false positives (at least daily), other providers do not currently appear to have any systems and processes in place to proactively identify false positives and, typically, appear to become aware of these only following complaints.

7.159 We further consider it important for Ofcom to have oversight over false positive rates and the ability to monitor any significant changes that may impact individual rights.

---

[441] Mobile UK response to October 2025 Consultation. Page 3; Virgin Media O2 response to October 2025 Consultation. Page 3.
[442] Sky response to October 2025 Consultation. Page 3.
[443] Mobile UK response to October 2025 Consultation. Page 3.
[444] BT Group response to October 2025 Consultation. Page 16.
[445] For example, we understand from [✂]

7.160 For these reasons, we continue to consider it necessary to implement a specific requirement to mitigate the risk of false positive blocking.[446]

7.161 However, we acknowledge the opposition to the proposed requirement among respondents, in particular due to the existing commercial incentives for providers to deliver legitimate messages and the potential conflict between, or need for, rules to block scam messages on the one hand and a rule to deliver legitimate messages on the other.

7.162 In the light of stakeholder comments that our proposed requirement is unnecessary and creates significant compliance concerns, we consider we can achieve our objective with a less onerous requirement and have decided to amend our proposal to instead require providers to:

- Implement and maintain appropriate and effective policies, systems and processes to identify and monitor false positives that may arise as a result.
- Take appropriate, effective and prompt action where they identify false positives.

7.163 A requirement to establish and maintain systems and processes to identify and monitor false positives should ensure providers have appropriate oversight over false positives. This should allow providers to monitor trends and identify any unexpected increase in false positive rates that may indicate an issue that could potentially lead to providers blocking a significant number of legitimate messages.

Description of the amended requirement

7.164 We consider it particularly important for providers to identify and monitor false positives where senders may not otherwise become aware that a provider has blocked their message. Given our decision not to implement the proposed notification requirement, which would have required providers to notify senders when they block messages under GCs C9.3(b) and (c) and C9.7 by automated means, this scenario is more likely to arise under our new measures. The amended requirement therefore only applies to providers that are subject to GCs C9.3(b) and (c) and C9.7.

7.165 In relation to the type of false positives we consider it appropriate for providers to identify, we note that:

- False positives may arise (and may be more likely to arise) as a result of providers implementing blocking rules that go beyond our requirements to block messages that contain URLs or telephone numbers associated with scams (for example, when they block messages using probabilistic search methods).
- Providers may find it technically or operationally challenging to isolate false positives that have arisen as a direct result of implementing our measures from those that have arisen from implementing other rules. For example, where providers block messages on the basis

[446] We recognise that identifying, monitoring and addressing false positives may be implicit in some of our other requirements, for example, the requirement to validate scam reports where appropriate under GCs C9.2 and C9.6; the requirement to maintain and implement "appropriate and effective" blocking rules under GCs C9.3 and C9.7 and have a reasonable belief before blocking; the right to challenge blocking decisions under what is now GC C9.17; the requirement under what is now GC C9.19 to regulatory review policies, systems and processes to confirm that they remain appropriate and effective and are operating as intended; and the requirement under what is now GC C9.20 to ensure relevant staff are appropriately trained. However, given the importance of minimising false positives and Ofcom having oversight over false positives rates, we consider it appropriate for requirements relating to false positives to be clearly set out in a GC that is directly enforceable by Ofcom.

of a range of potential indicators, including but not limited to the presence of a number or URL in a message, implementing our requirements may contribute to, but not be the sole reason for, the provider generating a false positive.

7.166 As a result, we consider it appropriate to give providers the flexibility to comply with the requirement by identifying and monitoring false positives where they reasonably believe a false positive may have arisen as a result of implementing our requirements (i.e. due to the presence of a number or URL in a message). The amended requirement is now numbered GC C9.26.

7.167 Providers are expected to implement processes to proactively identify potential false positives. In doing so:

- Providers can use automated tools and/or human review to help identify false positives through periodic reviews of blocked messages or traffic patterns.
- Providers should recognise that they may be less likely to detect false positives in relation to certain types of traffic: for example, on P2P messaging, where some end-users may not be aware that a provider has blocked a message and may also be less likely than business senders to challenge blocking decisions. Providers should take this into account in their approaches to monitoring for false positives.

7.168 We do not consider it appropriate for providers to rely on challenge mechanisms, queries or complaints as their primary means of identifying false positives, given that the number of challenges they receive may not reflect the true incidence of erroneous blocking.

7.169 Where providers identify false positives, we also consider it important they take appropriate, effective and prompt action. This is particularly important given the significant number of legitimate messages that they could potentially block in a short space of time if things go wrong (for example, due to human error).[447] We expect providers to take action where they:

- Identify individual false positives.
- Observe an unexpected increase in false positive rates.

7.170 Appropriate action is likely to include ensuring the same legitimate messages or type of legitimate messages (e.g. campaigns) are not blocked. This may require providers to amend rules in blocking tools and feeding false positives back into validation checks. We expect providers to carry out root cause analysis to understand why erroneous blocking has occurred and make appropriate changes to systems, processes, and/or controls, including updating rules, filters, or datasets, to prevent a recurrence. Providers should also ensure that they document the findings of such reviews and share them with relevant teams.

7.171 We do not expect providers to unblock messages that they have blocked erroneously after finding them to be false positives (which could cause confusion to end-users). However, providers may do so where appropriate (and possible), for example following a challenge under GC C9.17.

Compliance concerns

7.172 We consider that the amendments we have made to the requirement we initially proposed will address stakeholders' concerns. Requiring providers to identify, monitor and address false positives, rather than ensure the transmission of legitimate messages, should not

[447] For example, we understand from [✂]

impact or conflict with either providers' commercial incentives or other rules requiring providers to block scam messages.

7.173 We also consider the amended requirement to be a narrower and more targeted form of our proposed requirement (which is likely to have required providers to establish systems and processes to identify false positives). The guidance we consulted on said that providers should monitor rates of false positives (paragraph 2.149 of our 2025 consultation) and therefore we do not consider we are introducing a requirement significantly different to that on which we consulted.

7.174 More generally, the amended requirement will only apply to providers that are subject to GCs C9.3(b) and (c) and C9.7. Where it may be operationally or technically challenging to determine if implementing our requirements was the sole reason why a false positive arose, providers also have the flexibility to comply with GC C9.26 by identifying, monitoring and addressing false positives where they reasonably believe a false positive may have arisen as a result of implementing our requirements.

Financial costs of our requirements

7.175 We recognise that this amended requirement to identify, monitor and address false positives is likely to mean some providers have to implement and maintain new systems and processes. These costs are likely to vary across providers, depending on the extent of any proactive checks they currently have in place.

7.176 However, taking into account how providers currently identify false positives, we do not expect our amended requirement to impose a significant incremental cost on industry.

We expect the benefits of our requirement to identify, monitor and address false positives to outweigh any costs and adverse impacts

7.177 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we have decided to implement an amended requirement for providers subject to GCs C9.3(b) and (c) and C9.7 to: implement and maintain appropriate and effective policies, systems and processes to identify and monitor false positives; and take appropriate, effective and prompt action where they identify false positives.

7.178 We consider our amended and narrower requirement addresses the concerns raised by stakeholders while still allowing us to mitigate the risk to individual rights, by:

- Minimising the risk that false positives arise.
- Allowing Ofcom to have visibility of false positive rates and the ability to monitor any significant changes that may impact on individual rights, if necessary.

7.179 Overall, we consider the benefits of our amended requirement in mitigating risks to individual rights outweighs any costs or adverse impacts for industry and consider it to be proportionate.

7.180 The amended requirements relating to false positives are set out in GC C9.26. Further information, including how providers are expected to comply, is set out in paragraphs 2.229-2.245 of our guidance.

Data protection

What we proposed

7.181 In our 2025 consultation, we proposed that all activities must continue to comply with relevant data protection legislation (proposed GC C9.26).

7.182 We did not consider this would impose significant additional costs beyond those of other P2P and A2P measures.[448]

Stakeholder responses

7.183 Many respondents expressed their support for the requirement to ensure providers adhere to relevant data protection legislation when they are seeking to comply with GC C9.[449] iconectiv UK agreed that our measures can operate in a manner that is compatible with data protection obligations, while delivering meaningful consumer protection benefits.[450]

7.184 Utility Warehouse said that the proposed conditions should only be applied in circumstances where it does not impact a provider's ability to abide by data protection legislation.[451]

7.185 Amnesty International UK said it supported Ofcom's proposal to implement safeguards for its P2P and A2P measures and recommended that Ofcom should not rely on existing generic data protection rules to mitigate relevant risks. It added that restrictions on the purpose for which data can be used should be defined more clearly to avoid potential abuses.[452]

Our assessment

Rationale and benefits

7.186 We welcome several stakeholders' support for our proposed requirement for providers to comply with relevant data protection legislation.

7.187 Data protection legislation contains various individual data rights. In particular, the UK GDPR sets out the following seven key principles that sit at the heart of data protection law (and which providers will need to consider as part of ensuring their processing complies with data protection rules): lawfulness, fairness and transparency; purpose limitation; data minimisation; accuracy; storage limitation; integrity and confidentiality (security); and accountability.[453] Compliance with data protection legislation is also a relevant consideration when assessing whether any interference with Article 8 and 10 ECHR rights may be proportionate.

7.188 We consulted with the ICO in relation to our consultation proposals in accordance with Article 36(4) of the UK GDPR. We have continued to consult with the ICO prior to making this statement (including in relation to responses to our consultation and our amendments

[448] Although we noted that some providers may consider it necessary to obtain internal or external advice from data protection lawyers.
[449] [✂] response to October 2025 Consultation. iconectiv UK response to October 2025 Consultation. Page 8; Pinnacle Teleservices response to October 2025 Consultation. Page 14; Utility Warehouse response to October 2025 Consultation. Page 6.
[450] iconectiv UK response to October 2025 Consultation. Page 9.
[451] Utility Warehouse response to October 2025 Consultation. Page 6.
[452] Amnesty International UK response to October 2025 Consultation. Page 2. We discuss Amnesty UK's response in more detail under our rights assessment in Section 8.
[453] Further information on relevant data protection legislation is set out in our detailed rights assessment in Annex 4 and in our guidance.

to cross-cutting measures). We are satisfied that our measures can be implemented in accordance with data protection law.

Financial costs of our requirements

7.189 Stakeholders did not indicate that data protection law may prevent them from implementing our measures or refer to any costs of ensuring compliance with data protection legislation. We do not expect a requirement to comply with relevant data protection legislation when implementing our measures to impose a significant incremental cost on industry.

We expect the benefits of our data protection requirements to outweigh any costs and adverse impacts

7.190 Taking into account all relevant factors (including the reasons set out above and our assessment of our overall package of measures in section 8), we continue to consider that the benefits of requiring compliance with relevant data protection legislation outweighs any costs or adverse impacts for industry and we consider it to be proportionate. We have therefore decided to implement our proposed requirement to require compliance with data protection legislation.

7.191 However, we have decided to make some amendments to our guidance in response to Amnesty International UK's comments.

7.192 First, we have expanded our guidance to refer to the importance of complying with any other relevant legislation, including data protection legislation, consumer law (including under the Consumer Rights Act 2015 and the Digital Markets, Competition and Consumers Act 2024) and the Investigatory Powers Act 2016 (relating, amongst other things, to the acquisition and retention of communications data). We have also suggested that providers may want to consider the Guiding Principles on Business and Human Rights,[454] which explains how businesses can avoid infringing on the human rights of others and address adverse human rights impacts with which they are involved.

7.193 Second, to help providers comply with relevant data protection legislation and other potentially relevant legislation, we have updated our guidance to make clearer that we expect providers to inform users of the circumstances in which their messages may be blocked and explain how they can do this. We have made clear that these steps will help ensure providers comply with the fairness and transparency principles under the UK GDPR. We have also made clear in our guidance that robust validation of scam reports and ensuring records are kept up to date will help ensure compliance with the data accuracy principle under the UK GDPR and we have provided a link to the ICO's recently updated guidance on purpose limitation.[455]

7.194 The requirement to comply with relevant data protection legislation is set out in GC C9.27. Further information including how providers are expected to comply is set out in paragraphs 2.248-2.260 of our guidance.

---

[454] United Nations Human Rights Office of the High Commissioner: Guiding Principles on Business and Human Rights

[455] ICO, Guidance on purpose limitation (March 2026) [accessed on 8 July 2026]

Our guidance for providers of mobile messaging

7.195 Alongside our 2025 consultation we published proposed guidance for providers of mobile messaging services on how they could comply with the measures we proposed.[456]

7.196 We have summarised stakeholder responses on parts of our guidance relating to specific GCs where we discuss those GCs in sections 5, 6 and 7 of this statement. In the paragraphs below, we summarise and respond to more general comments on our guidance.

General stakeholder responses

7.197 Several stakeholders, including The Campaign Registry, the CCP-ACOD, iconectiv UK, Pinnacle Teleservices, Stour Marine and Which? made general comments supporting out proposed guidance.[457] [✂] also said that establishing a consistent approach and providing guidance would be beneficial to providers that already undertake blocking measures.[458]

7.198 While expressing overall support, some stakeholders noted that further clarification may be required in certain areas of the guidance to support effective and fair compliance.

7.199 Which? suggested that Ofcom should explicitly clarify that the guidance is not legally binding and that providers may depart from it in individual cases.[459]

7.200 Amnesty International UK did not explicitly refer to our proposed guidance but said it was concerned about monitoring and scanning of messages that goes beyond targeting monitoring of known scam URLs and numbers. It suggested that the infrastructure required to implement our proposals and the creation of new datasets could open new vectors for surveillance. In this context, Amnesty UK noted that our consultation had not discussed how our proposed measures would work in the context of existing surveillance and intelligence powers.[460]

Our assessment and decisions

7.201 We welcome the general support for our guidance, which sets out the steps providers are required or expected to take to protect end-users from scam P2P and A2P messages. It is intended to help providers ensure that they comply with their obligations under GC C9 and we continue to consider it is appropriate to publish this guidance.[461]

7.202 In response to Which?'s comment, we have amended paragraph 1.5 of our guidance to confirm it is not legally binding. However, our guidance explains that we will take it into account when deciding whether a provider may be compliant with our rules. It states that we expect providers to take the steps that are reasonable and proportionate for their circumstances. It also states that providers should record the steps they take to comply with our rules, including any reasons why they may have considered it appropriate to depart from our guidance.

---

[456] Ofcom, 2025. Proposed guidance for providers on protections from scam mobile messages.
[457] Which? response to October 2025 Consultation. Page 2; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 2; The Campaign Registry response to October 2025 Consultation. Page 14. iconectiv UK response to October 2025 Consultation. Page 10; Pinnacle Teleservices response to October 2025 Consultation. Page 5; Stour Marine response to October 2025 Consultation. Page 6.
[458] [✂] response to October 2025 Consultation.
[459] Which? response to October 2025 Consultation. Page 2.
[460] Amnesty International UK response to October 2025 Consultation. Page 2.
[461] Ofcom, 2026. Scam mobile messages: guidance on protecting people and businesses.

7.203 In response to Amnesty UK's concerns, our proposed guidance recognised that some providers may carry out other types of monitoring not required by our rules, which may be more intrusive, and explained that providers should therefore ensure they comply with relevant data protection rules. We have decided to update our guidance to make more prominent the information it contains on anti-scam measures beyond those that our rules require (paragraph 1.13 of our guidance). As explained in paragraph 7.192 above, we have also expanded the guidance to refer to the importance of complying with other relevant legislation.

8. Assessment of package of measures and our decisions

8.1 In this section, we assess our package of measures in the round, and consider:

- The benefits to consumers and businesses of our package of measures.
- The potential impact of our package of measures on the rights to privacy and freedom of expression under Article 8 and 10 ECHR. In particular, we consider the extent to which our requirements may interfere with these rights and assess whether our requirements are proportionate to that interference.
- The proportionality of our overall package of measures.

8.2 We also summarise all the changes we have decided to make to the GCs we proposed in our 2025 consultation.

8.3 Finally, we explain why we have decided not to introduce mandatory sender ID registration at this time.

Overarching benefits for consumers and businesses

8.4 In section 3, we set out the harms that victims of mobile messaging scams experience, as well as the harms that these scams cause for mobile users more broadly. In sections 5, 6 and 7, we explain how we expect our requirements to reduce the number of messaging scams that consumers and businesses receive, while also safeguarding legitimate users of mobile messaging. We consider that these rules, taken together should in turn lead to a significant reduction in the harms associated with messaging scams.

8.5 In particular, we consider that this reduction in harm from mobile message scams should benefit consumers by reducing the risk of financial loss and related impacts, such as administrative burden, stress and reduced confidence in money management and financial institutions. Even where they are not the direct victims of scams, consumers stand to benefit from a reduction in the nuisance associated with receiving fraudulent or misleading communications and feel safer when using financial and digital services.

8.6 We also expect that reducing mobile messaging scams will benefit businesses and institutions by reducing the indirect costs they incur, such as reputational harm and the potential erosion of customer trust when these organisations are routinely impersonated in scam messages. In addition, financial institutions may incur lower costs from investigating scam-related incidents, handling associated customer complaints and other customer support, reimbursing customers for their losses, and lower volumes of scam traffic on their networks.

8.7 In relation to our A2P measures specifically, we expect it will be harder for criminals to use alphanumeric sender IDs, including with close imitations of legitimate business names or fabricated or obscure names. We consider that this is likely to reduce attempts to impersonate legitimate and trusted brands and make such attempts at impersonation less successful. Where criminals cannot closely imitate brand names using alphanumeric sender IDs, mobile users may be better able to spot impersonation attempts that do evade detection, because they will be less-convincing imitations. As a result, mobile users may be less likely to fall victim to the underlying scam.

8.8 We consider that, beyond reducing harm from scams themselves, our measures will improve trust in business messaging. By significantly reducing the likelihood that mobile users receive A2P message scams, we consider that those users may develop more trust in the legitimate messages that they receive from genuine brands over A2P routes. This, in turn, may make A2P messaging more effective and valuable to legitimate business senders.

Rights assessment

Potential interference with Article 8 and 10 ECHR rights

8.9 We recognise that the measures we are putting in place may impact individuals' rights under Articles 8 and 10 ECHR.[462] We set out these rights in full in Annex 4. In summary:

a) Article 8 ECHR sets out the right to respect for private life and correspondence. Our measures could result in interference with this right where, for example, providers are required to review the content of a message to check if it contains a known scam URL or number, or to check if a message identified as indicative of a scam is in fact legitimate before it is delivered.
b) Article 10 ECHR sets out the right to freedom of expression, including the right to receive and impart information without unnecessary interference by a public authority. Our measures could result in interference with this right where, for example, legitimate measures are blocked (false positives).

8.10 We consider GCs C9.2, C9.3, C9.6, C9.7, C9.8, C9.12, C9.15 and C9.16 could potentially interfere with Article 8 and/or 10 rights and in Annex 4 we explain how these specific GCs may interfere with those rights.

8.11 We do not consider that Article 8 rights protect messages which seek to facilitate scam activity. Similarly, we do not consider blocking mobile numbers that have sent scam messages or blocking messages that contain scam URLs or telephone numbers to engage Article 10 ECHR.

8.12 We consider Article 8 and 10 rights are most likely to be interfered with where the content of legitimate messages is reviewed and/or those legitimate messages are subsequently blocked. We consider any interference with such rights is more likely to arise where: providers do not carry out appropriate validation of scam reports to ensure they are in fact a scam; providers do not have appropriate systems and processes in place to mitigate the risk of human error when inputting rules in scam prevention systems; and/or providers do not have appropriate systems and processes in place to identify and monitor false positives and take appropriate, effective and prompt action when they are identified. We also consider interference with individual rights is more likely to occur under GCs C9.3(b) and (c) and C9.7 where automated tools are used to block messages and senders may not otherwise become aware that a provider has blocked their message.

8.13 Any interference with Article 8 and 10 rights must be lawful, pursue a legitimate social aim and not be disproportionate. In essence, restrictions on these rights must be necessary and the measure's contribution to its objective must outweigh its adverse impacts. Compliance with data protection legislation is a relevant consideration when assessing whether any interference with Article 8 and 10 rights may be proportionate.

[462] These rights have been implemented in UK law under the Human Rights Act 1998.

Our provisional view

8.14 In our consultation, we said that there is a substantial public interest in reducing the likelihood that consumers and small business end-users receive scam mobile messages. We also said that our measures will be effective in achieving this objective and address the harms set out in section 3.

8.15 Our provisional view was that the risk of potential adverse impacts on Article 8 and 10 rights arising was low and we explained that we were proposing to implement various safeguards to mitigate the risk of those potential impacts. We balanced these potential adverse impacts on rights under Articles 8 and 10 ECHR against the significant public interest in our proposals and our provisional view was that these potential adverse impacts were proportionate to our objective.

Stakeholder responses

8.16 Some respondents commented on our assessment of the potential impacts of our proposed measures on individual rights under Articles 8 and 10 ECHR. We also reached out to various human rights organisations to make them aware of our proposals and see if they had any comments or concerns.[463]

8.17 Many respondents recognised the possibility of legitimate messages being blocked, both under existing industry measures and as a result of our proposals. Some referred to the risk of false positives arising as "material",[464] whereas others considered this risk to be limited.[465]

8.18 Many respondents generally agreed with our rights assessment and the cross-cutting measures we had proposed to mitigate any potential adverse impact on individual rights.[466] In particular, Amnesty International UK agreed that "dealing with scams is a legitimate policy objective to justify certain interferences with the rights to privacy and free expression, as long as these are proportionate" and said that it did "not see the proposals to expand the scanning of number-based messaging systems as excessively problematic".[467] CCP-ACOD also emphasised the importance of ensuring legitimate communications are not unintentionally disrupted, consumers receive transparent explanations and accessible means of redress.[468]

8.19 However, some respondents (including some MNOs) did not agree that our package of cross-cutting measures was proportionate in striking the right balance between mitigating the risk of false positives on the one hand and against the significant harm from scam

---

[463] We reached out to Liberty, Privacy international, Big Brother Watch, Open Rights Group, Amnesty International UK. Amnesty International UK subsequently provided a response.
[464] CCUK response to October 2025 Consultation. Page 5; See also Sky response to October 2025 Consultation. Page 4
[465] Sky response to October 2025 Consultation. Page 4; Utility Warehouse response to October 2025 Consultation. Page 6.
[466] Stour Marine response to October 2025 Consultation. Pages 4-5; Name withheld 1 response to October 2025 Consultation. Page 4; iconectiv UK response to October 2025 Consultation. Pages 8-9; Pinnacle Teleservices response to October 2025 Consultation. Pages 13-14; The Campaign Registry response to October 2025 Consultation. Pages 11-12; Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 3.
[467] Amnesty International UK response to October 2025 Consultation. Page 1.
[468] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 5; See also Pinnacle Teleservices response to October 2025 Consultation. Pages 14-15.

messages on the other, and considered our proposed cross-cutting measures went further than necessary.[469]

8.20 For example, VodafoneThree disagreed that we needed to require providers to notify certain senders in the event their message was blocked and considered other cross-cutting measures (including our proposed right to challenge) were sufficient to mitigate risks from potential over blocking.[470]

8.21 BT said that our cross-cutting measures were not "proportionately justified" by our ECHR analysis. It said there was no evidence that the cross-cutting measures we proposed would protect users from scams or infringement of their individual rights and that we were attempting to transfer our public duty under the Human Rights Act 1998 (HRA) onto private operators. It added that Ofcom's lack of guidance to providers (including on what considerations to take into account when dealing with challenges or on what constitutes a "legitimate message" that providers should take reasonable steps to transmit) meant Ofcom had not appropriately discharged its duty under the HRA.[471]

8.22 BT suggested that concerns relating to potential impacts on individual rights could be addressed by alternative means. These could include an information remedy that makes clear certain categories of messages will be blocked or periodic reviews of systems to ensure they are transmitting/terminating legitimate messages.[472]

8.23 Simwood suggested that any proportionality assessment involving the balancing of these competing interests, and the weighing of the impact of over blocking versus fraud, and invasion of privacy, was a matter for Parliament and not a sectoral regulator.[473] It also said that the fact of today's "industry practice" of blocking messages does not mean that statutory rights to privacy have been upheld or that providers' actions are lawful.[474]

8.24 Some respondents made more specific comments:

- Amnesty International UK was concerned with general monitoring and scanning of messages that goes beyond targeting monitoring of known scam URLs and numbers. It suggested that the infrastructure required to implement our proposals and the creation of new datasets could open new vectors for surveillance. In this context, Amnesty International UK noted that our consultation had not discussed how our proposed measures would work with existing surveillance and intelligence powers. Amnesty International UK also recommended that Ofcom does not rely on existing generic data protection rules. It added that restrictions on the purpose for which data can be used should be defined more clearly to avoid mission creep and potential abuses.[475]
- Pinnacle Teleservices said that it is important to distinguish between domestic and international messaging contexts when assessing proportionality and jurisdictional applicability, as messages originating and terminating within the UK are subject to a different regulatory and legal framework than internationally originating traffic.

[469] Sky response to October 2025 Consultation. Page 4; CCUK response to October 2025 Consultation. Page 5.
[470] VodafoneThree response to October 2025 Consultation. Page 7.
[471] BT Group response to October 2025 Consultation. Pages 2, 3 and 14.
[472] BT Group response to October 2025 Consultation. Page 3.
[473] Simwood response to October 2025 Consultation. Page 3.
[474] Simwood response to October 2025 Consultation. Page 3.
[475] Amnesty International UK response to October 2025 Consultation.

Our assessment

8.25 We have set out the legal basis for our measures in section 2 (and the relevant legal framework is set out more fully in Annexes 4 and 5). We also consider our measures pursue a legitimate social aim, in particular the prevention of crime, the protection of potential victim's health, public safety and the economic well-being of the country.

8.26 We continue to consider there to be substantial public interest in requiring providers to implement measures to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages.

8.27 As noted above (and set out more fully in Annex 4), we have identified some potential adverse impacts of our measures on the right to privacy and the right to freedom of expression under Articles 8 and 10 ECHR.

8.28 We continue to consider it appropriate to implement various safeguards to mitigate the risk of those potential impacts and explain more fully in Annex 4 how we consider those safeguards mitigate potential impacts on Article 8 and 10 rights.

8.29 We welcome the general support for implementing safeguards to mitigate the risk of interference with individual rights under Articles 8 and 10 ECHR.

8.30 We also acknowledge the concerns raised by some respondents that some of our proposed cross-cutting measures may not be proportionate, taking into account the limited risk of interference with individual rights and significant harm from scam messages. Taking these concerns into account, and for the reasons set out in section 7, we have decided to amend some of our proposed cross-cutting measures. In particular, we have decided to remove the proposed notification requirement. We have also amended the proposed requirement to ensure the transmission of legitimate messages to instead require providers to implement and maintain appropriate systems and processes to identify, monitor and address false positives that arise under GCs C9.3(b) and (c) and C9.7.

8.31 For the reasons set out in more detail in Annex 4, we consider that the risk of potential adverse impacts to individual rights under Article 8 and 10 ECHR from implementing our amended measures to be low. In particular, we consider there is a very low risk of false positives arising (and lower than we had understood at consultation) and our amended measures will further help mitigate the risk of false positives arising.[476]

Our amended measures will help mitigate the risk of adverse rights impacts

8.32 We have made various changes to our measures which we consider further mitigate any potential adverse rights impacts. In particular:

a) We have strengthened our guidance relating to who should be considered an appropriate third party from which to obtain scam reports and how we expect providers to validate scam reports and reduce the risk of human error when inputting rules into scam prevention systems. We understand issues in underlying scam reports (which have not been appropriately validated) and/or systems and processes to prevent human error may be the cause of most false positives and consider these changes to our guidance will help mitigate the risk of false positives arising. [477]

[476] We discuss false positives rates in more detail in paragraph 7.29 of section 7.

[477] In response to our May 2026 requests, no provider indicated that false positives are likely to arise (or how they may arise) in relation to incorrectly identifying known scam URLs or numbers in messages. Rather, they

b) We have amended GC C9.26 to ensure it is more targeted at requiring providers to identify and monitor false positive rates and take appropriate, effective and prompt action where false positives are identified under GCs C9.3(b) and (c) and C9.7. These changes should:

   i) Ensure providers have appropriate systems and processes in place to mitigate impacts on individual rights when false positives arise whilst also mitigating the risk of the same or similar false positives arising in the future. We recognise that processes to identify false positives may require further review of the content of messages but consider this proportionate to mitigate impacts on individual rights associated with false positives.
   ii) Enable Ofcom to request records relating to false positives rates which will provide us with oversight and an ability to monitor any significant changes that may impact on individual rights.

8.33 We recognise that, in principle, our removal of the proposed notification requirement could adversely impact individual rights to the extent senders and intended recipients may not know an individual message has been blocked. However, as explained in section 7, we consider the risk of legitimate messages being blocked in error (false positives) is very low, meaning a notification requirement would have had very limited benefit in protecting individual rights. To help mitigate the risk that users may not know an individual message has been blocked, we have updated our guidance to make clearer that we expect providers to inform users of the circumstances in which their messages may be blocked and explain how they can do this. GC C9.26 should also ensure providers take proactive steps to identify false positives rather than only relying on challenges.

Response to more specific comments

8.34 Taking into account concerns raised by BT, we have updated our guidance to explain how we expect providers to inform users of the circumstances in which a message may be blocked, the types of factors we expect providers to take into account when dealing with challenges and how we expect providers to identify, monitor and address false positives under GCs C9.3(b) and (c) and C9.7. Amended GC C9.26 will also provide Ofcom with oversight of false positive rates and an ability to monitor any significant changes that may impact on individual rights, taking into account our obligations under the HRA.

8.35 In response to points made by Amnesty International UK, we have made various updates to our guidance which we respond to in paragraphs 7.191-7.193 (relating to compliance with relevant data protection legislation) and paragraph 7.203 (relating to comments on our guidance) of section 7. More generally, we consulted with the ICO in relation to our consultation proposals in accordance with Article 36(4) of the UK GDPR. We have continued to consult with the ICO prior to making this statement. We are satisfied that our measures can be implemented in accordance with data protection law.

8.36 In response to Pinnacle Teleservices's comments relating to jurisdictional considerations, we have explained in paragraph 2.48 that our rules can apply to providers outside the UK to the extent they fall within the scope of the relevant definitions and there is a territorial connection to the UK. This could be because, for example, a +44 call is being routed into the UK where the intended recipient is based.

---

indicated false positives are more likely to arisen as a result of suspicious looking URLs (that have not been validated as a scam) or human error in identifying suspicious key words or shared sender IDs.

8.37 In response to Simwood's comment that our proportionality assessment under the HRA is a matter for Parliament, Ofcom has various duties relating to telephone numbers including specific powers to impose rules relating to mobile messaging. We have taken into account our relevant duties and powers in deciding what measures it would be proportionate to impose. These rules are summarised in paragraphs 2.42-2.50 and set out more fully in Annex 5 of this statement.

We consider any interference with Article 8 and 10 rights is proportionate

8.38 We have balanced the potential adverse impacts on rights under Articles 8 and 10 ECHR of the final measures identified in this statement against the significant public interest in implementing them. For the reasons set out above, and explained more fully in Annex 4, we consider any potential adverse rights impacts are proportionate to our objective.

Proportionality assessment for our package of measures

We consider our overall package of measures is necessary to achieve our policy objective and does not give rise to disproportionate adverse impacts

8.39 Under our regulatory principles, we will only intervene if we consider it appropriate and proportionate to do so. This is based on our duty under section 3(3)(a) of the Act to have regard to the principles under which regulatory activities should be proportionate and targeted only at cases where action is needed. Below we assess the proportionality of our package of measures in the round, including by taking into account the evidence we present on each measure in sections 5, 6 and 7.

8.40 As set out in section 2, our policy objective is to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages. Section 3 sets out the harm that scam messages cause and section 4 sets out our view that this objective cannot be achieved without further regulatory intervention, given persisting gaps in existing anti-scam measures. Scammers deliberately exploit multiple vulnerable aspects of UK mobile operators and aggregators' networks and therefore no single intervention would be sufficient to address these vulnerabilities in a comprehensive way.

8.41 To respond to this challenge, we are requiring the package of complementary measures set out in sections 5, 6 and 7, which we consider would, altogether, be an effective means of achieving our objective. By collectively targeting the specific weaknesses identified in current anti-scam protections (as demonstrated for each measure), we expect the package will introduce greater frictions and costs into scammers' operations across P2P and A2P channels and ensure vulnerable aspects of providers' networks are more secure. In turn, we expect that this will reduce the volumes of fraudulent messages reaching UK consumers and help to address the associated harms identified in section 3.

8.42 We also consider that this package of measures is necessary because, as discussed above, we do not think our objective can be achieved without further intervention, due to the scale of mobile messaging scams, harms to consumers and existing gaps in anti-scam measures. We also consider that these measures establish a minimum industry standard, which is important to ensure consumers are protected.

8.43 We recognise that our package of measures may introduce some additional costs for industry and could have some adverse impacts on consumers and businesses, as discussed in sections 5, 6 and 7 for each measure. As costs will vary depending on each individual

provider's existing anti-scam practices, we do not estimate a collective financial impact on industry. However, as this package of measures largely builds on existing anti-scam processes already deployed by many providers, we do not expect it to impose significant costs in the round. Nonetheless, taking the expected benefits, costs, and potential adverse impacts of each measure together in the round, we anticipate that these costs and impacts will be proportionate to the expected benefits. In particular, the measures are designed to deliver a material reduction in scams and related harms by strengthening protections against the vulnerabilities in providers' networks that scammers exploit.

8.44 We do not expect our package of measures to have a material negative impact on competition and innovation. This is because, in general, the expected costs are unlikely to be material relative to the scale of operations of the parties concerned; and in cases where certain providers face higher additional costs than others, we expect this to be driven by some providers already incurring these costs through their existing anti-scam measures. In the market for A2P services, there are a large number of competing providers and we do not have any reason to expect that introducing our measures, which are important in setting minimum standards to protect consumers, will have a negative impact on competition. We also consider that our measures will ensure that providers apply consistent measures to protect consumers and businesses from scams, creating a level playing field and supporting more effective competition.

8.45 We also consider that our requirements are the least onerous approach to achieving our objective because we have not identified alternative, less costly, measures that would be as effective. We also consider that our measures seek to improve implementation and consistency of measures that have already been adopted by many mobile operators and aggregators across the industry, further indicating they should not be unduly onerous.

8.46 Overall, and taking into account our duties, we therefore consider that our package of measures is necessary and will be effective in achieving our policy objective in the least onerous way without giving rise to disproportionate costs and adverse impacts in the round.

8.47 We have also had regard to our public sector equality duties and Welsh language obligations and have set out our equality and Welsh language impact assessments in Annex 3.

We have taken account of our growth duty

8.48 In formulating our requirements, we are required to have regard to the statutory 'growth duty': an obligation to consider the desirability of promoting economic growth, alongside the accompanying statutory guidance.[478]

8.49 In our view, our package of measures will support economic growth by reducing fraud-related costs and increasing trust in communications services. In section 3, we highlighted the harms associated with mobile messaging scams. These include financial losses incurred by both victims and the financial institutions that may reimburse them and a general erosion of trust in digital communications and organisations that are regularly impersonated in scams. Reducing these harms will improve consumer welfare and support more effective digital engagement. In addition, our A2P requirements will reduce the likelihood that consumers receive A2P messaging scams, which we consider will help build

[478] Section 108 of the Deregulation Act 2015.

trust in business communications, reduce avoidable costs and support more efficient economic activity.

8.50 We recognise that our requirements will increase the regulatory burden on some mobile operators and aggregators. However, as discussed under individual measures above, we do not consider that the requirements will impose significant costs on providers. We therefore consider that any increase in regulatory burden will be limited and that firms will also benefit from our rules introducing a level playing field in how providers must combat scam messages.

8.51 Therefore, when we take account of the potential impact on growth, we consider that our rules are proportionate and will not impose undue regulatory burden on providers that could otherwise counteract the positive impacts that the requirements will generate for growth.

Our decisions

8.52 Taking into account all relevant factors (including our policy objectives, relevant legal duties, assessments of each measure in sections 5, 6 and 7 and the assessments in this section and associated annexes), we have decided to proceed to implement a range of measures to tackle scam mobile messages through new GC requirements and guidance. These measures are summarised below.

Setting volume limits

8.53 We have decided to implement a requirement for operators to implement and maintain appropriate and effective processes relating to the volume of messages that their PAYG customers can send from a SIM, in a specified period.

Receiving scam reports, and identifying and blocking scam numbers and messages

8.54 We have decided to implement the blocking requirements on P2P channels set out in section 5, which includes having processes in place to receive scam reports, blocking numbers used by scammers, and blocking scam messages in transit.

8.55 We have additionally decided to implement the blocking requirements set out in section 6 on mobile operators and tier 1 aggregators in A2P channels, which includes having processes in place to receive scam reports and block scam messages in transit.

Up front due diligence, ongoing checks and incident management for A2P messaging

8.56 We have decided to implement requirements set out in section 6 for up-front due diligence, ongoing checks and incident management for all parties operating in the A2P market.

Cross-cutting measures

8.57 We have decided to implement the requirements set out in section 7 that enhance the above measures and safeguard human rights.

8.58 As set out in section 7, we have decided not to implement the proposed requirement to notify mobile users when certain messages are blocked.

New GCs and guidance

8.59 Our new GCs are set out in full in the Notification of our decision to set General Conditions at Annex 1, including the defined terms (we reuse existing definitions as far as possible).

8.60 Our guidance is linked to in Annex 6.

8.61 Below is a summary of the key amendments to the GCs we proposed in our 2025 consultation:

- The definition of 'P2P Messages' has been updated to further clarify that our rules apply only to messaging services that fall within the scope of public electronic communications services[479]. We have also removed the reference to P2P messages being sent "between individuals", taking into account the fact some P2P messages may be sent from SIM farms.
- GCs C9.2 and C9.6 have been amended to require providers to "regularly" and "proactively" ensure they receive scam reports, including from "appropriate" third parties.
- GCs C9.2, C9.3(a), C9.17 to C.9.25 and C9.27 have been amended to clarify obligations on thin MVNOs. In particular, we have:
    - inserted a new provision, GC C9.2(a), requiring providers that assign mobile numbers, including thin MVNOs, to receive scam reports relating to customers to whom they have assigned numbers;
    - amended GC C9.1 to ensure that GC C9.3(a), relating to the blocking of customers' numbers used for scam activity, applies to providers that assign mobile numbers, including thin MVNOs; and
    - amended GC C9.1 to ensure that the cross-cutting requirements in GC C9.17 to C.9.25 and C9.27 apply to providers that assign mobile numbers, including thin MVNOs.
- GC C9.4 has been amended to require providers to apply volume limits to messages sent to any mobile number (instead of the previous wording referring to messages sent to "more than one mobile number").
- The definition of 'Pay As You Go Customer' for the purposes of GCs C9.4 and C9.5 has been amended to clarify that MNOs are responsible for complying with our volume limits measures in relation to both their own customers and their thin MVNOs' customers. It has also been amended to ensure it captures all types of pre-paid SIMs including where a customer is required to have a pre-pay credit balance to continue to use the service or service outside of any inclusive allowance.
- We have updated our definition of 'A2P messages' to clarify that our rules relate to any messaging services that are sent using a public electronic communications service and/or network[480].
- The definition of 'Aggregator' has been amended to exclude any provider acting as such an intermediary that, while it may contract directly with business senders, it is acting in a

[479] For the avoidance of doubt, the 'P2P Messages' definition is not intended to bring messaging services that are Number-Independent Interpersonal Communications Services (as defined in section 135(3B) of the Act) in scope of GC C9.

[480] For the avoidance of doubt, the 'A2P Messages' definition is not intended to bring 'Number-Independent Interpersonal Communications Services' (as defined in section 135(3B) of the Act) in scope of GC C9 or Condition 3 of the Non-Provider Conditions. We have however maintained the 'A2P messages' definition for the Non-Provider Conditions that we proposed in our 2025 Consultation given such conditions are imposed on operators that are not communications providers (see paragraphs A5.20 to A5.22 in Annex 5).

capacity where its business sender customers must have a separate contractual relationship with a third party to transfer A2P messages.

- The definition of 'Business Sender' has been amended to refer to "any person" rather than "any organisation" to ensure it captures any person (whether an individual, sole trader, partnership, company or other organisation).
- GC C9.13 has been amended to make clear that the objective of the policies, systems and processes relating to Protected Alphanumeric Sender IDs is to prevent their use for scams.
- GC C9.16 relating to incident management involving more than one aggregator has been amended to increase the time providers have to identify the business senders responsible for certain scam messages and take appropriate action to prevent further messages being sent from 3 to 5 working days.
- Proposed GC C9.17 (relating to the proposed requirement to notify senders when messages are blocked via automated means under GCs C9.3(b) and (c) and C9.7) has been removed.
- The numbering of GCs C9.17-C9.27 has changed and the final GCs have different numbers to those we consulted on.
- What is now GC C9.17 relating to the right to challenge has been amended to:
    - Clarify that it applies only to the blocking of messages or numbers under GC C9.3 and C9.7. The scope in GC C9.1 has also been amended to only capture providers caught by C9.3 and C9.7 and confirm it does not therefore apply to lower-tier aggregators;
    - Clarify that any affected person can raise a challenge relating to a number or message blocked under GC C9.3 and C9.7;
    - Clarify that providers are not required to treat challenges under Condition C9.17 as 'Complaints' for the purpose of GC C4;
    - Require providers to identify a "prompt" and reasonable timeframe for reaching a decision on a challenge; and
    - Remove the proposed requirement (in proposed GC C9.18(c)) for providers to provide their right to challenge policy free of charge on reasonable request in hard copy or other format (which we have instead included in guidance).
- What is now GC C9.20 relating to training requirements has been amended so that the training obligations apply to "relevant" staff, rather than all staff.
- What are now GCs C9.21 to C9.25 relating to record-keeping requirements have been amended to:
    - Clarify the type of information that must be retained relating to the application of volume limits for PAYG customers and reduce the retention period to 12 months;
    - Clarify the type of information that must be retained relating to challenges and reduce the retention period to 12 months;
    - Clarify the type of information that must be retained in relation to scam incidents;
    - Introduce record-keeping requirements relating to false positives for providers subject to C9.26.
- What is now GC C9.26 has been amended to require providers to identify, monitor and address false positives arising under GCs C9.3(b) and (c) and C9.7 (instead of the previous broader requirement under proposed GC C9.27 to ensure the transmission of legitimate messages). GC C9.1 has also been amended to clarify that thin MVNOs and lower-tier aggregators are not caught by this requirement.

Non-Provider conditions

8.62 Our GCs only apply to communications providers, as defined in the GCs. As explained in the legal framework in Annex 5, Ofcom can also impose conditions on persons other than communications providers (Non-Provider Conditions) that have applied for or been allocated numbers (including through sub-allocation). The Non-Provider Conditions that we can set include obligations corresponding to numbering-related GCs we have imposed in connection with the allocation, transfer and use of telephone numbers.

8.63 We proposed imposing Non-Provider Conditions corresponding to our proposed GCs for A2P messaging services and cross-cutting measures (proposed GCs C9.6-C9.27), to close any potential loophole under which an operator may potentially seek to argue that they are not subject to applicable GCs because they are not, or are no longer, providing an electronic communications service or an electronic communications network[481] and should not therefore be considered a communications provider on whom we can impose GCs.

8.64 We did not receive any responses to our consultation in relation to these proposals and have decided to impose Non-Provider Conditions corresponding to our amended GCs.

8.65 The Non-Provider Conditions should ensure that all operators (including aggregators) who have been allocated numbers, either by Ofcom or through sub-allocation, and are involved in the transfer and/or termination of A2P messages, are required to comply with our rules relating to A2P scam mobile messages (regardless of whether they may not be considered a communications provider within the scope of our GCs).

8.66 Our Non-Provider Conditions are set out in full in Annex 2 and reflect the changes we have made to the GCs in Annex 1, as far as possible. We have added defined terms to these Non-Provider Conditions corresponding to the relevant terms used in the GCs, as far as possible.

Legal tests

8.67 We consider the legal tests are met in relation to our new GCs and Non-Provider Conditions:

a) **Not unduly discriminatory**: Our GCs apply equally to all persons that are defined as providing specific A2P and/or P2P messaging services and the Non-Provider Conditions apply to persons that are allocated telephone numbers and provide A2P messaging services. We recognise that different GCs apply to different types of providers. For example, some GCs apply to all MVNOs whereas others only apply to MVNOs that transfer and/or terminate messages; some apply to tier 1 aggregators but not lower-tier aggregators; and some apply to MSPs to the extent they are carrying out similar functions to aggregators whereas other MSPs are outside the scope of our rules altogether. For the reasons set out in this statement, we consider there to be an objective justification for the scope of each of our GCs. We also note that all our GCs apply equally to all persons within defined categories. We therefore consider our proposals are not unduly discriminatory.

b) **Proportionate**: As explained above, we consider that our package of measures is necessary and will be effective in achieving our policy objective in the last onerous way, without giving rise to disproportionate costs and adverse impacts in the round.

[481] Both as defined in section 32 of the Act.

c) **Transparent:** the GCs and Non-Provider Conditions are set out in Annexes 1 and 2, respectively. Our reasons for introducing new rules and what they are intended to achieve are explained above. Issuing guidance alongside the GCs and Non-Provider Conditions will further clarify our expectations and likely approach to compliance and enforcement. As far as possible, we have reused existing definitions in the GCs and the wording of the Non-Provider Conditions corresponds to the wording of the proposed GCs. We therefore consider our interventions to be transparent.

8.68 In making our decisions, we have considered and acted in accordance with our general duties under section 3 of the Act, the requirements set out in section 4 of the Act and our general duty in relation to telephone numbers under section 63 of the Act.

8.69 We have also had regard to the UK Government's Statement of Strategic Priorities for telecommunications, management of radio spectrum and postal services in accordance with section 2B of the Act, as well as the desirability of promoting economic growth in section 108 of the Deregulation Act 2015.

8.70 The legal framework under which we are operating is set out more fully in Annex 5.

We are not introducing A2P sender ID registration at this time

Sender ID registration

8.71 In our October 2025 consultation, we recognised that a mandatory sender ID registration for A2P messages could be an effective means to tackle messaging scams, but considered that our other A2P proposals would be a less onerous means to achieving our objective. As such, we did not propose to introduce such a measure at this time.

Stakeholder responses

8.72 Some respondents disagreed with the case for a mandatory, centralised sender ID registry and supported our position. BT said that a sender ID registry system would be expensive, burdensome, and would reduce the ability of individual providers to tackle new, emerging threats.[482] The MEF said that a regulator-run registry would require public funding and be slow to design and deploy.[483] techUK stated that mandatory sender ID registries have proved to be cumbersome and risk disrupting A2P traffic flows.[484]

8.73 Other respondents were in favour of Ofcom exploring a mandatory, centralised sender ID registry. Which? said that a mandatory registry would address industry's inconsistent application of anti-fraud measures.[485] Twilio, CCUK, and The Campaign Registry said that a centralised or shared registry would be a single, reliable source for verifying sender IDs.[486] Similarly, XConnect recommended that we reconsider a sender ID registry.[487]

8.74 We also received comments about sender ID registry systems in other countries that were mostly in favour of a similar model in the UK. Which? said that the implementation costs in

[482] BT Group response to October 2025 Consultation. Page 9.
[483] MEF response to October 2025 Consultation. Page 5.
[484] techUK response to October 2025 Consultation. Page 4.
[485] Which? response to October 2025 Consultation. Pages 8-9.
[486] Twilio response to October 2025 Consultation. Pages 8-9; CCUK response to October 2025 Consultation. Page 2; The Campaign Registry response to October 2025 Consultation. Page 7.
[487] XConnect response to October 2025 Consultation. Page 2.

the UK would not be particularly high, as Australia's scheme costs less than 1% of total annual industry revenues.[488] Twilio said that internationally, there is increasingly a move towards regulator-led, centralised or nationally coordinated sender ID registries, such as in Ireland and Singapore.[489] CCUK also raised successful international precedents in Australia, Singapore, and India.[490] BT stated instead that such systems have appeared complex and expensive to introduce in international examples, and have not necessarily reduced the volume of scams immediately.[491]

8.75 Certain respondents supported a sender ID registry but advocated instead for an industry-led model. VodafoneThree said that Ofcom could encourage wider adoption of the MEF registry.[492] [493] The MEF suggested that wider adoption of a mandatory registry, combined with declared use cases, would be more effective than a regulator-run model.[494]

Our assessment

8.76 We consider that a centralised sender ID registry could be onerous to both business senders and to aggregators and MSPs. BT and techUK said that it would be burdensome, and the MEF stated that it would take time to implement. We recognise these comments and, in line with our consultation position, we believe that there would be significant up front and ongoing costs associated with both registering IDs and maintaining a registry. Charging models for a registry could vary, such as charging businesses directly when registering IDs, or charging mobile operators and aggregators to register IDs on behalf of their customers. Where the costs are charged to companies registering IDs, this is likely to increase costs for aggregators and/or the business end-users that use A2P mobile messaging. These costs could particularly affect small and medium sized businesses, which would have to register to use a sender ID even though they are not likely to be spoofed by scammers. Anybody responsible for setting up and maintaining the registry would generate costs in administering a sender ID registry that people and businesses would ultimately bear. We therefore consider that this approach would represent a more significant intervention than our measures to prevent alphanumeric sender IDs from being abused.

8.77 We recognise such a registry could make it harder for criminals to use alphanumeric sender IDs by requiring them to be registered centrally before they can be used, with proof that each sender ID is being used for legitimate purposes. Countries including Australia, Ireland, Italy and Singapore have centralised registration rules.[495] In response to Which?, Twilio, CCUK, and The Campaign Registry's comments that a mandatory, centralised registry could

---

[488] Which? response to October 2025 Consultation. Page 9.
[489] Twilio response to October 2025 Consultation. Pages 8-9.
[490] CCUK response to October 2025 Consultation. Page 2.
[491] BT Group response to October 2025 Consultation. Page 9.
[492] VodafoneThree response to October 2025 Consultation. Page 6.
[493] A voluntary Sender ID model is operated in the UK. The MEF, a trade body, runs a cross-sector Sender ID registry initiative called the 'Sender ID Protection Registry' and it charges brands a fee to sign up. Brands are only protected if they have registered their Sender IDs under a voluntary registry. In contrast, a mandatory, centralised registry is government or regulator-run, imposes set-up and ongoing costs on brands, and can require the blocking of all unregistered alphanumeric Sender IDs. Ofcom, 2024. Call for input: Reducing mobile messaging scams. Pages 32-34.
[494] MEF response to October 2025 Consultation. Page 5.
[495] See for example Singapore's approach at IMDA, Full SMS Sender ID Registration is to be required by January 2023', Ireland's approach from ComReg, ComReg launches SMS Sender ID Registry to help prevent text scams, Australia's at ACMA, The SMS sender ID register, and in Italy through AGCOM, Guida alla registrazione al Registro degli Alias.

address inconsistencies, we consider that such a registry could be an effective means to achieve our policy objective, and that it could help to address opacity in the A2P supply chain. Such an approach could be particularly effective in preventing brand impersonation tactics used by scammers. We also noted that some respondents viewed international examples such as Australia as evidence that a centralised sender ID registry could be successful in the UK.

8.78 At this stage, although we consider such an approach could be an effective way to meet our objective, our view is that we can achieve our objective through the other, less onerous A2P measures set out above. These include requirements for parties onboarding new business senders to check the alphanumeric sender IDs that they intend to use against the legitimate business purposes described in KYC checks, and the maintenance of policies by mobile operators in relation to the use of certain protected or generic alphanumeric IDs and the use of special alphanumeric characters.

8.79 We recognise that certain respondents instead proposed wider or mandatory adoption of an industry-led registry. We remain supportive of additional industry-led initiatives that help to further protect mobile users and businesses from Sender ID abuse.

8.80 Having considered stakeholder responses, we have decided not to take forward a centralised sender ID registry at this time.

9. Implementation periods

9.1 In this section we set out our assessment of stakeholder responses to our proposed implementation periods for the new GCs and guidance and our decision.

What we proposed

9.2 In our consultation, we proposed an implementation period of:

- Six months from the publication of our final decision for our requirements concerning P2P messaging (GCs C9.2-9.5 and C9.17-9.27)[496].
- Twelve months from the publication of our final decision for our requirements concerning A2P messaging (GCs C9.6-9.27 and Non-Provider Condition 3).

Stakeholder responses

9.3 We received mixed responses from stakeholders about the proposed implementation periods. A number of respondents supported our proposals (or suggested they should be shorter), but other respondents indicated that a longer implementation period of at least 12 months would be appropriate for both P2P and A2P proposals.

P2P measures implementation period

9.4 A number of respondents said they required 12 months to implement the P2P proposals, including where cross-cutting requirements would apply, if Ofcom proceeded with the cross-cutting proposals as we set them out in our 2025 consultation.[497]

9.5 techUK and VodafoneThree suggested that Ofcom align its implementation period for the P2P measures with the A2P measures at 12 months. Both respondents said that the P2P requirements would require changes to systems and work with third-party suppliers, making 6 months unrealistic.[498] VodafoneThree stated that more time would be needed to comply with the P2P proposals, in particular GC C9.4 and C9.5 (which require operators to implement volume limits for PAYG SIMs). It said additional time may be required to introduce new systems.[499]

9.6 More generally, BT indicated it would need 2-3 years to comply with all cross-cutting measures (including in relation to P2P messages), such as the right to challenge. However, it said that, if Ofcom did not require providers to apply the cross-cutting measures to all of the requirements, then the proposed timelines would be sufficient.[500]

9.7 [✂] also stated that a longer period would be required for certain providers to implement the P2P proposals.[501]

---

[496] We proposed that GCs C9.17-9.27 would take effect after 6 months with respect to the transmission of P2P messages and after 12 months for A2P messages.
[497] Sky response to October 2025 Consultation. Page 5; Virgin Media O2 response to October 2025 Consultation. Page 5; Mobile UK response to October 2025 Consultation. Page 4.
[498] VodafoneThree response to October 2025 Consultation. Page 5; techUK response to October 2025 Consultation. Page 6.
[499] VodafoneThree response to October 2025 Consultation. Page 4-5.
[500] BT Group response to October 2025 Consultation. Page 16.
[501] Name withheld 1 response to October 2025 Consultation. Page 5.

A2P measures implementation period

9.8 The MEF suggested that providers would require more time to implement the A2P requirements, especially GC C9.7 (blocking) and C9.9 (in particular, ensuring that providers pass requirements through the supply chain).[502] It suggested a centralised industry threat intelligence model to ensure consistent implementation within the proposed timeframe.

9.9 [✂] stated that a longer period would be required for certain providers to implement the A2P proposals.[503]

9.10 Stour stated that 12 months was reasonable for the A2P proposals at a technical level, but at a high cost. It also said that a phased approach of technical, operational and contract measures would be more reasonable.[504]

9.11 Two respondents stated that the A2P proposals could be implemented quicker than 12 months.[505]

General comments

9.12 A number of respondents were broadly in support of our proposed implementation periods for both P2P and A2P.[506] The CCP-ACOD stated that Ofcom should go further and implement the proposals without delay.[507] Which? and iconectiv UK agreed with our proposed implementation periods and said they are proportionate.[508]

9.13 The Federation of Communication Services noted there may be inconsistencies in the implementation periods different types of providers would require and stated that smaller providers and their customers would need support, given the costs.[509] Stour and The Campaign Registry suggested a phased approach to implementation so that more complex measures can be introduced over a longer period.[510]

Our reasoning and decisions

9.14 Following consideration of stakeholders' responses to our consultation, we have decided to retain our proposed implementation periods of:

- Six months from our statement for our requirements concerning P2P messaging (GCs C9.2-9.5 and C9.17-9.27[511]). They will come into effect on Monday 18 January 2027.
- Twelve months from our statement for our requirements concerning A2P messaging (GCs C9.6-9.27 and Non-Provider Condition 3). They will come into effect on Thursday 15 July 2027.

---

[502] MEF response to October 2025 Consultation. Page 14.
[503] Name withheld 1 response to October 2025 Consultation. Page 5.
[504] Stour Marine response to October 2025 Consultation. Page 5.
[505] Utility Warehouse response to October 2025 Consultation. Page 7; The Campaign Registry response to October 2025 Consultation. Page 14.
[506] Pinnacle Teleservices response to October 2025 Consultation. Page 18-19; [✂] response to October 2025 Consultation; [✂] response to October 2025 Consultation.
[507] Communications Consumer Panel and ACOD response to October 2025 Consultation. Page 2.
[508] Which? response to October 2025 Consultation. Page 13; iconectiv UK response to October 2025 Consultation. Page 11.
[509] FCS response to October 2025 Consultation. Page 1.
[510] Stour Marine response to October 2025 Consultation. Page 5; The Campaign Registry response to October 2025 Consultation. Page 14.
[511] We will require that GCs C9.17-9.27 take effect after six months with respect to P2P messages and after 12 months for A2P messages.

9.15 We have decided to retain different implementation periods for P2P and A2P messaging requirements as we consider that providers must undertake greater and more complex technical and contractual to comply with some of our A2P requirements.

9.16 We note the concerns of respondents that have suggested that our proposals could and should be implemented faster to minimise the further harm consumers will experience from scam mobile messages. As set out in section 3, the scale of the harm is substantial and we want to ensure that our intervention takes effect as soon as reasonably possible.

9.17 We have considered respondents' requests for a longer implementation period for the P2P requirements. We acknowledge that, in some cases, these measures may require providers to procure new systems and sources of intelligence, including implementing new volume limits for PAYG customers and enhancing blocking capabilities.

9.18 Many providers already apply these measures in some form and thus our requirements build on existing systems and processes that providers already have in place. We have not seen any evidence to indicate that it is not technically or operationally possible for providers to implement our P2P proposals in 6 months.

9.19 Some respondents to our 2025 consultation raised concerns about the implementation period for applying cross-cutting measures to the P2P requirements, in particular the right to challenge blocking (in combination with blocking notifications). We consider that the changes we have made to our cross-cutting requirements (see section 7), particularly our decision not to implement the blocking notification requirement, will significantly reduce the challenge of applying the cross-cutting measures to the P2P requirements.

9.20 We recognise that mobile operators and aggregators may need to make changes to their systems, processes and contractual arrangements to comply with our A2P requirements. Amending or implementing new contractual and/or technical arrangements is likely to take more time than mobile operators will require to implement the P2P measures. However, we have not seen any evidence to indicate that it is not technically or operationally possible for providers to implement our A2P proposals in 12 months.

9.21 Taking into account the changes we have made to the proposals in our 2025 consultation, we consider that an implementation period of six months for our P2P requirements and twelve months for our A2P requirements strikes an appropriate balance between allowing sufficient time for providers to make the necessary changes to comply with the new rules and ensuring that consumers benefit from protection as soon as possible. Taking into account all relevant factors (including the reasons set out above and assessment of our overall package of measures in section 8), we consider these implementation periods remain appropriate and proportionate.

A1. Notification to set General Condition C9

Notification of Ofcom's decision to set General Conditions relating to protections for end-users of public electronic communications services and the allocation, adoption and use of telephone numbers under section 48(1) of the Act (the Notification)

Background

A1.1 On 29 October 2025, Ofcom published a notification pursuant to sections 48(1) and 48A(3) of the Act, proposing to:

- set General Condition C9, as set out in Schedule 1 to that notification; and
- add new definitions and amend one definition in the General Conditions, as set out in Schedule 2 to that notification.

A1.2 Ofcom's reasons for making the proposal, and the effect of this proposal, were set out in sections 3-5 of the consultation document accompanying that notification.

A1.3 Ofcom invited representations about the proposals by 28 January 2026.

A1.4 A copy of the notification was sent to the Secretary of State in accordance with section 48C(1) of the Act.

A1.5 By virtue of section 48A(6) and (7) of the Act, Ofcom may give effect to the proposals, with or without modification, only if:

a) they have considered every representation about the proposal made to them within the period specified in the notification; and

b) they have had regard to every international obligation of the United Kingdom (if any) which has been notified to them for this purpose by the Secretary of State.

A1.6 Ofcom received responses to the notification and has considered every such representation made to them in respect of the proposals set out in the notification (and the accompanying consultation document).

A1.7 The Secretary of State did not notify Ofcom of any international obligation of the United Kingdom for the purpose of section 48A(6) of the Act.

Decision

A1.8 In accordance with section 45 and 48(1) of the Act, and as set out in the Schedules to this Notification, Ofcom has decided to:

a) set General Condition C9;

b) add new definitions and amend one definition in the General Conditions

A1.9 For the reasons explained in the explanatory statement accompanying this Notification, Ofcom has decided that the provisions set out in set out in Schedule 1 of this Notification shall enter into force as follows:

- General Conditions C9.1-C9.5 and C9.17-C9.27 relating to Person-to-Person messages shall come into force on 18 January 2027.
- General Conditions C9.1 and C9.6-C9.27 relating to Application-to-Person messages shall come into force on 15 July 2027.

A1.10 Ofcom's reasons for reaching this decision, and the effect of this decision, are set out in sections 3-9 of the explanatory statement accompanying this Notification.

A1.11 Ofcom considers that it has complied with the requirements of sections 45 to 49C, 51(1)(a) and 58 of the Act, insofar as they are applicable.

A1.12 In reaching these decisions, as explained in section 8 of the statement accompanying this Notification, Ofcom has considered and acted in accordance with its general duties under section 3 of the Act, the six requirements set out in section 4 of the Act and its general duty in relation to telephone numbers under section 63 of the Act. We have also had regard to the UK Government's Statement of Strategic Priorities for telecommunications, management of radio spectrum and postal services in accordance with section 2B of the Act, as well as the desirability of promoting economic growth in section 108 of the Deregulation Act 2015. We have also consulted the Information Commissioner's Office on these decisions to the extent they relate to the processing of personal data in accordance with Article 36(4) of the UK General Data Protection Regulation.

A1.13 A copy of this Notification and the accompanying statement document have been sent to the Secretary of State in accordance with section 48C(1) of the Act.

A1.14 In this Notification:

"the Act" means the Communications Act 2003;

"Ofcom" means the Office of Communications; and

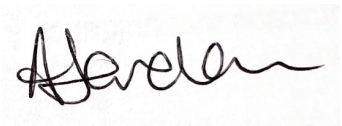
"General Conditions" means the general conditions set under section 45 of the Act by Ofcom, as amended from time to time.

A1.15 Words or expressions shall have the meaning assigned to them in this Notification, and otherwise any word or expression shall have the same meaning as it has in the Act and General Conditions.

A1.16 For the purposes of interpreting this Notification: (i) headings and titles shall be disregarded; and (ii) the Interpretation Act 1978 shall apply as if this Notification were an Act of Parliament.

A1.17 The Schedules to this Notification shall form part of this Notification.

Signed by



Amy Jordan,

Policy Director, Infrastructure and Connectivity

A person authorised by Ofcom under paragraph 18 of the Schedule to the Office of Communications Act 2002.

15 July 2026

Schedule 1 – Annex 1

We have imposed the following General Condition C9.

C9 Protections from scam mobile messages

This condition requires regulated providers to have systems and processes in place to help protect end-users from harms associated with scam mobile messages. It sets out the minimum measures that providers must take, including: having processes in place to receive reports on, and block, numbers used for scams and messages containing scam numbers and URLs; carrying out Know Your Customer and Know Your Traffic checks; and taking appropriate action against persons identified as responsible for scam messages. Regulated providers may take additional measures beyond those set out here to protect end-users from scam messages.

Scope

C9.1 The provisions of this **Condition** apply as follows:

(a) **Conditions** C9.2(b) and (c), C9.3(b) and (c), C9.4 and C9.5 apply to any **Communications Provider** that transfers and/or terminates **P2P Messages**;

(b) **Conditions** C9.2(a) and C9.3(a) apply, in the context of **P2P Messages**, to any **Communications Provider** that has assigned **Mobile Numbers**;

(c) **Conditions** C9.6 to C9.7 apply to any **Communications Provider** that transfers and/or terminates **A2P Messages**, except **Lower-Tier Aggregators**;

(d) **Conditions** C9.8 to C9.12 and C9.14 to C9.16 apply to any **Communications Provider** that transfers and/or terminates **A2P Messages**, including all **Aggregators**;

(e) **Condition** C9.13 applies to any **Communications Provider** that terminates **A2P Messages**;

(f) **Conditions** C9.17 and C9.18 apply to any **Communications Provider** that

(i) transfers and/or terminates **P2P Messages** and/or **A2P Messages**, except **Lower-Tier Aggregators**; and/or

(ii) in the context of **P2P Messages**, has assigned **Mobile Numbers;**

(g) **Conditions** C9.19 to C9.25 and C9.27 apply to any **Communications Provider** that

(i) transfers and/or terminates **P2P Messages** and/or **A2P Messages**, including all **Aggregators**, and/or

(ii) in the context of **P2P Messages**, has assigned **Mobile Numbers**; and

(h) **Condition** C9.26 applies to any **Communications Provider** that transfers and/or terminates **P2P Messages** and/or **A2P Messages**, except **Lower-Tier Aggregators.**

and each person to whom a provision applies is a '**Regulated Provider'** for the purposes of that provision.

Person-To-Person Messages

Processes for receiving Scam Reports

C9.2 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) **Scam Reports** from **End-Users** and appropriate third parties, in relation to:

(a) **Customers** they have assigned **Mobile Numbers** to;

(b) **Telephone Numbers** that the **End-User** and/or third party believes sent **P2P Messages** intended to **Scam** the recipients; and

(c) **URLs** and **Telephone Numbers** that the **End-User** and/or third party believes were used as part of a **Scam**, including **URLs** and **Telephone Numbers** included in **P2P Messages.**

Preventing Scam messages being sent and/or received

C9.3 Taking into account **Scam Reports** received, **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes designed to:

(a) prevent, without undue delay, **Mobile Numbers** they have assigned to a **Customer** from sending **P2P Messages** where they reasonably believe those **Mobile Numbers** have sent **P2P Messages** intended to **Scam** the intended recipients;

(b) block, without undue delay, **P2P Messages** sent from **Telephone Numbers** where they reasonably believe those **Telephone Numbers** to have sent **P2P Messages** intended to **Scam** the intended recipients; and

(c) block, via automated means and without undue delay, **P2P Messages** that contain **URLs** or **Telephone Numbers** which they reasonably believe were used as part of a **Scam**.

C9.4 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes setting limits on the volume of **P2P Messages** that their **Pay As You Go Customers** can send from a specific **Mobile Number**, in a specified period, to any **Mobile Number**, with the objective of preventing **Scam** messages from being sent and/or received.

C9.5 **Regulated Providers** must block, via automated means and without delay, **Pay As You Go Customers** from sending any further **P2P Messages** when that **Pay As You Go Customer** reaches any volume limit imposed by the **Regulated Provider** in line with the policy it has implemented under **Condition** C9.4, for the duration of the time specified in the policy.

Application-To-Person Messages

Processes for receiving Scam Reports

C9.6 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) **Scam Reports** from **End-Users** and appropriate third parties in relation to **URLs** and **Telephone Numbers** that the **End-User** and/or third party believes were used as part of a **Scam**, including **URLs** and **Telephone Numbers** included in **A2P Messages**.

Preventing Scam messages being sent and/or received

C9.7 Taking into account **Scam Reports** received, **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to block, via automated means and without undue delay, **A2P Messages** that contain **URLs** or **Telephone Numbers** which they reasonably believe were used as part of a **Scam**.

Requirements relating to due diligence and ongoing checks

C9.8 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to ensure that:

(a) for any **A2P Messages** that they transfer and/or terminate, **Know Your Customer Checks**, checks relating to the use of any **Alphanumeric Sender IDs** and on-going **Know Your Traffic Checks** are conducted in accordance with **Conditions** C9.10 to C9.12, either by the **Regulated Provider**:

(i) carrying out these checks themselves; or

(ii) taking the steps in Condition C9.9; and

(b) they do not transfer and/or terminate **A2P Messages** or enable the use of the relevant **Alphanumeric Sender IDs** unless they are reasonably satisfied with the outcome of these checks or with the checks carried out under **Condition** C9.9(a).

C9.9 **Regulated Providers** must:

(a) implement and maintain clear and unambiguous contractual terms with any party from which they receive **A2P Messages** (that is not a **Business Sender**), requiring that party to:

(i) conduct **Know Your Customer Checks** on **Business Senders** at the **Onboarding Stage**, or take appropriate steps to ensure these checks have been conducted at the **Onboarding Stage**;

(ii) conduct checks when allowing a **Business Sender** to use a new **Alphanumeric Sender ID** to ensure that any proposed use of the **Alphanumeric Sender ID** is consistent with the **Business Profile** and purposes disclosed during **Know Your Customer Checks**, or take appropriate steps to ensure these checks have been conducted;

(iii) conduct on-going **Know Your Traffic Checks** on **Business Senders** or take appropriate steps to ensure these checks are conducted;

(iv) not transfer **A2P Messages** or enable the use of the relevant **Alphanumeric Sender IDs** unless they are reasonably satisfied with the checks carried out

under **Conditions** C9.9(a)(i)-(iii);

(v) take appropriate, effective and prompt action in response to any reports of **A2P Messages** coming from their service that are suspected of being sent with the intention to **Scam** the recipients;

(vi) retain records in line with **Conditions** C9.21 to C9.25; and

(vii) take appropriate steps to ensure that **Business Senders** notify the party of changes to a **Business Sender**'s **Business Profile**, or otherwise ensure that the party with the direct relationship to the **Business Sender** will be notified of such changes.

(b) implement and maintain appropriate and effective policies, systems and processes to:

(i) ensure ongoing compliance with the contractual obligations imposed under **Condition** C9.9(a);

(ii) monitor and assess compliance with these obligations, taking into account **Conditions** C9.16 and C9.19; and

(iii) take appropriate, effective and prompt action to address any non-compliance and, if applicable, satisfy itself the party will comply in future.

C9.10 **Know Your Customer Checks** must include:

(a) due diligence checks against **Business Profiles** for any indication that the **Business Sender** poses a risk of sending **Scam** messages;

(b) assessing the proposed use of any **Alphanumeric Sender IDs** for any indication that the **Business Sender** poses a risk of sending **Scam** messages, where applicable taking into account policies in place under **Condition** C9.13;

(c) confirmation of the contact details of a senior individual that is responsible for authorising the messages to be sent or transferred and/or terminated; and

(d) carrying out appropriate risk assessments to identify whether enhanced checks are appropriate to any cases, and if so, carrying out such checks.

C9.11 Checks when allowing the use of any new **Alphanumeric Sender IDs** must include:

(a) due diligence checks to verify that the proposed use of **Alphanumeric Sender IDs** aligns with the information disclosed during **Know Your Customer Checks** on the **Business Profile**, including the stated purposes for seeking to access **A2P Message** services; and

(b) where applicable, reviewing the proposed use of the **Alphanumeric Sender ID** against policies in place under **Condition** C9.13.

C9.12 **Know Your Traffic Checks** must include:

(a) monitoring and reviewing data on volume patterns; identifying new or different use of **Alphanumeric Sender IDs** or **Telephone Numbers**; and checking any information on or notifications of changes in **Business Profiles**, for any indicators of **Scam** activity, taking into account policies in place under **Condition** C9.13 and information obtained under **Conditions** C9.9(a)(vii) and C9.14 (whichever is applicable);

(b) using any insights from **Condition** C9.12(a) to review and update any previous risk assessments, as appropriate; and

(c) where any indicators of **Scams** are identified under **Condition** C9.12(a):

(i) seeking appropriate evidence as to whether or not the **A2P Messages** are legitimate; and

(ii) blocking those **A2P Messages** where the **Regulated Provider** reasonably believes, based on their review of any evidence provided, that the relevant **A2P Messages** were intended to **Scam** the intended recipients.

C9.13 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes that impose restrictions on the use of **Protected Alphanumeric Sender IDs** in **A2P Messages** they terminate and communicate such policies to parties from whom they received **A2P Messages,** with the objective of preventing their use for **Scams**.

C9.14 **Regulated Providers** must take appropriate steps to ensure that **Business Senders** from which they directly receive **A2P Messages** are required to promptly notify them of any changes in their **Business Profile**, or changes in the use of any **Alphanumeric Sender IDs**.

Incident management requirements

C9.15 Where a **Regulated Provider** becomes aware of a **Business Sender** that they **Onboarded** sending or attempting to send, directly or indirectly, an **A2P Message** that the **Regulated Provider** reasonably believes was intended to **Scam** the recipient, the **Regulated Provider** must take the following steps within 1 **Working Day**:

(a) confirm the identity of the **Business Sender** responsible for those messages; and

(b) implement appropriate measures to prevent the **Business Sender** from sending further **A2P Messages** via any network or service the **Regulated Provider** provides unless the **Regulated Provider** has obtained evidence which they are satisfied demonstrates either:

(i) the **Business Sender** was not responsible for sending the relevant **A2P Message**; or

(ii) the relevant **A2P Message** was not intended to **Scam** the recipients.

C9.16 Where a **Regulated Provider** becomes aware of a **Significant Scams Incident** involving a **Business Sender** that they did not **Onboard**, the **Regulated Provider** must:

(a) within 2 **Working Days** in cases involving no more than one **Aggregator** or 5 **Working Days** in all other cases:

(i) take appropriate steps to confirm the identity of the **Business Sender** responsible for those messages; and

(ii) implement appropriate measures to prevent the **Business Sender** from sending further **A2P Messages** via any network or service the **Regulated Provider** provides unless they have obtained evidence which they are satisfied demonstrates either:

1. the **Business Sender** was not responsible for sending the relevant **A2P Messages**; or
2. the relevant **A2P Messages** were not intended to **Scam** the recipients;

(b) promptly within 15 **Working Days**:

(i) establish whether the party involved in delivering the relevant **A2P**

Messages to the **Regulated Provider** is complying with the requirements that **Regulated Provider** imposed on them under **Condition** C9.9(a); and

(ii) take appropriate and effective action to address the non-compliance and, if applicable, satisfy itself the party will comply in future.

Cross-cutting requirements

Right to challenge

C9.17 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes that enable any affected person to challenge any blocking of a **Mobile Number** or message under **Conditions** C9.3 or C9.7.[512] The policies must:

(a) explain the circumstances under which any blocking may occur;

(b) explain how the person may challenge the blocking.

(c) explain the process the **Regulated Provider** will follow to investigate and determine any challenges made under **Condition** C9.17, including the evidence it is likely to require from the person to demonstrate the **Mobile Number** or messages should not have been blocked;

(d) identify the different potential outcomes that may follow any challenge;

(e) identify conditions the **Regulated Provider** may attach to an outcome following a challenge, including any ongoing requirements that may be placed on the person;

(f) identify a prompt and reasonable timeframe within which the **Regulated Provider** will reach an outcome following a challenge; and

(g) explain the process the person may follow to appeal any decision not to remove any blocking taken.

C9.18 **Regulated Providers** must ensure that the policies, systems and processes in place under **Condition** C9.17 are well publicised and readily available, including ensuring that they are:

(a) easily accessible and reasonably prominent on their website; and

(b) referred to in the terms and conditions for all relevant products and services.

Review of policies, systems and processes

C9.19 **Regulated Providers** must regularly review their policies, systems and processes, implemented under **Condition** C9 to ensure that:

(a) they remain appropriate and effective and are operating as intended;

(b) the **Regulated Provider** is complying with its policies, systems and processes; and

(c) any issues identified are promptly and effectively addressed, including by making appropriate changes to their policies, systems and processes

[512] For the avoidance of doubt, **Regulated Providers** are not required to treat challenges under **Condition** C9.17 as '**Complaints**' for the purpose of **Condition** C4 (relating to complaints handling and dispute resolution processes).

implemented under **Condition** C9.

Training staff

C9.20 **Regulated Providers** must ensure that all relevant staff are appropriately trained on the policies, systems and processes in place under **Condition** C9, including ensuring relevant staff are appropriately trained on the right to challenge processes implemented under **Condition** C9.17.

Record keeping

C9.21 **Regulated Providers** must implement and maintain appropriate record keeping policies, systems and processes to demonstrate and ensure continued compliance with **Condition** C9. These must be overseen by a designated senior individual and must, where applicable, provide for the records identified in **Conditions** C9.22 to C9.25 below to be retained for at least the time period identified in those **Conditions**.

C9.22 The following records must be kept for a period of at least five years:

(a) records of policies, systems and processes implemented under **Condition** C9;

(b) records of reviews of the effectiveness of policies, systems and processes implemented under **Condition** C9, including any actions taken or changes made to those policies, systems and processes under **Condition** C9.19; and

(c) records of the description of an incident under **Conditions** C9.15 and C9.16 (including the date and time the incident was identified and the number of messages involved), and measures or actions taken in response to that incident.

C9.23 The following records must be kept for a period of at least three years after the end of the relevant contractual relationship:

(a) records of **Know Your Customer Checks** and checks relating to the use of **Alphanumeric Sender IDs** carried out under **Condition** C9.8, including initial and subsequent risk assessments;

(b) records of actions taken as a result of **Know Your Traffic Checks** carried out under **Condition** C9.8;

(c) records of requirements imposed on parties under **Condition** C9.9(a); and

(d) records of actions taken to ensure ongoing compliance and address any non-compliance under **Condition** C9.9(b).

C9.24 Records relating to **False Positives** under **Condition** C9.26 must be kept for a period of at least two years and must include:

(a) a description of a **False Positive** incident (including the date and time the incident first arose; its impact; the likely cause; and how and when it was identified); and

(b) any measures or actions taken in response to that incident.

C9.25 The following records must be kept for a period of at least one year:

(a) Records of communications between a **Regulated Provider** and any person regarding a challenge raised under **Condition** C9.17, from the date the challenge

was resolved or otherwise closed; and

(b) records of each instance a **Pay As You Go Customer** reaches a volume limit set by the **Regulated Provider** under **Condition** C9.4 (including the **Pay As You Go Customer**'s **Mobile Number** and the date on which that volume limit was reached).

Identifying, monitoring and addressing False Positives

C9.26 Where a **Regulated Provider** is required under **Conditions** C9.3(b), C9.3(c) or C9.7 to block messages, the **Regulated Provider** must implement and maintain appropriate and effective policies, systems and processes to identify and monitor **False Positives**, and take appropriate, effective and prompt action when **False Positives** are identified.

Data protection

C9.27 **Condition** C9 applies subject to the requirements of the **Relevant Data Protection Legislation**.

Schedule 2 – Annex 1

We have decided to insert the following definitions in alphabetical order in the 'Definitions' section of the General Conditions.

The terms in **bold** below are defined terms in the General Conditions and any which are not separately defined in the table below have the same meaning as in the Communications Act 2003 or, if not defined there, our General Conditions of Entitlement or the National Telephone Numbering Plan.

Terms to be inserted
'**Aggregator'** means an intermediary that transfers (either directly or indirectly) **A2P Messages** between **Business Senders** and **Mobile Service Providers** that could terminate those messages to recipients (excluding intermediaries that contract directly with **Business Senders** but are acting in a capacity where that **Business Sender** is required to have separate contractual relationship with a third party to transfer **A2P Messages**).
'**Alphanumeric Sender ID'** means a sender identification displayed on a message recipient's handset, consisting of any characters, such as a code, custom name or brand name, used by a **Business Sender** when sending **A2P Messages**.
'Application-To-Person Message' or **'A2P Message'** means a message from a **Business Sender**, sent (either directly or indirectly) to **Mobile Numbers** using a software application and using a **Public Electronic Communications Service** and/or **Public Electronic Communications Network.**
'**Business Sender**' means any person, other than a **Regulated Provider**, that communicates with members of the public via **A2P Messages**. This includes, but is not limited to banks, schools, public bodies and retailers.
'**Business Profile**' means information relating to the **Business Sender** including information relating to: the trading or registered name; registered office or trading address; the nature of the services being provided (and the purposes for which they are seeking to access **A2P Messages**); payment / bank account information; existing telephone numbers; websites; and the name of directors and persons of significant control (taking into account the Companies House's guidance on people with significant control (PSCs): How to identify and record the people who own or control your company).
'False Positive' means, for the purposes of **Condition** C9, an instance where a **Regulated Provider** reasonably believes that a **P2P Message** or **A2P Message** may have been incorrectly identified and blocked pursuant to **Conditions** C9.3(b), C9.3(c) or C9.7 on the basis the **Regulated Provider** had reasonably believed it was intended to scam the recipient.
''**Know Your Customer Checks**' means the checks set out in **Condition** C9.10.
'**Know Your Traffic Checks'** means the checks set out in **Condition** C9.12.
'**Lower-Tier Aggregator'** means an **Aggregator** that is acting in a capacity in which it does not contract directly with a **Mobile Service Provider** that directly terminates **A2P Messages** to recipients.
'**Onboarding**' (and other forms of the word) means where a **Regulated Provider** undertakes or is involved in the **Onboarding Stage**.
'**Onboarding Stage'** means the period during which a party is preparing to start providing their service to a new **Business Sender** and they are collecting and verifying all the information needed to facilitate this.

'**Pay As You Go Customer**', means, for the purposes of **Condition** C9, a **Customer** who accesses a **Mobile Communications Service** (either directly from a **Regulated Provider** or indirectly via another **Communications Provider** using that **Regulated Provider**'s **Public Electronic Communications Network**) and is required to have a pre-pay credit balance to continue to use that service or service outside of any inclusive allowance.
'**Person-to-Person Message'** or '**P2P Message'** means a message sent from one **SIM** to another, using a **Mobile Communications Service** or otherwise using a **Public Electronic Communications Service**.
'**Protected Alphanumeric Sender IDs**' means **Alphanumeric Sender IDs** which have restrictions or conditions placed on their use because they relate to known brands (such as 'Royal Mail' or 'HMRC'), contain special alphanumeric characters (such as those outside the standard alphabet, 0-9 numerals and essential punctuation) or are generic IDs (such as 'Alert', 'Security' or 'Customer Service').
'**Scam**' (and other forms of the word) means any deceptive act or scheme designed to trick a person into disclosing personal or financial information or to trick them out of their money or other valuables, including but not limited to conduct that may be considered fraud under the Fraud Act 2006.
'**Scam Report**' means a report made by any person about a **Scam** message (or other forms of **Scam**), including complaints from **End-Users** and reports from law enforcement, regulatory or consumer bodies or other third parties.
'**Significant Scams Incident**' means a situation where it appears to the **Regulated Provider** that a particular **Business Sender** has cumulatively sent or attempted to send, directly or indirectly, at least fifty **A2P Messages** that the **Regulated Provider** reasonably believes were intended to **Scam** the recipients.
'**SIM**' for the purposes of **Condition** C9, stands for Subscriber Identity Module (SIM) and includes SIMs available or obtained electronically.
'**Short URLs**' means a **URL** with a smaller number of characters than a specified, original **URL** that uses **URL** redirection to refer to the same resource.
'**URLs**' stands for Uniform Resource Locator, and means a reference that specifies the location of a resource accessible by means of the internet, including **Short URLs**.

We have decided to amend the following definition in the 'Definitions' section of the General Conditions:

Terms to be amended
'Non-provider Numbering Condition' ~~means the conditions[513] that apply to persons other than Communications Providers made under section 59 of the Act, including in relation to Global Titles and the use of Unbundled Tariff Numbers~~ means the conditions[514] that apply to persons other than **Communications Providers** made under section 59 of the **Act**, including in relation to **Global Titles**, the use of **Unbundled Tariff Numbers** and **A2P Messages**.

[513] ~~Non-Provider Condition~~
[514] Non-Provider Condition

A2. Notification to set Condition 3 in the Numbering Conditions Binding Non-Providers

Notification of Ofcom's decision to set Numbering Conditions Binding Non-Providers relating to the allocation, adoption and use of telephone numbers under section 48(1) of the Act (the Notification)

A2.1 On 29 October 2025, Ofcom published a notification pursuant to sections 48(1) and 48A(3) of the Act, proposing to:

- set the following Numbering Conditions Binding Non-Providers: Conditions 3.1 to 3.23, as set out in Schedule 1 to that notification; and
- add new definitions in the Numbering Condition Binding Non-Providers, as set out in Schedule 2 to that notification.

A2.2 Ofcom's reasons for making the proposal, and the effect of this proposal, were set out in sections 3-5 of the consultation document accompanying that notification.

A2.3 Ofcom invited representations about the proposals by 28 January 2026.

A2.4 A copy of the notification was sent to the Secretary of State in accordance with section 48C(1) of the Act.

A2.5 By virtue of section 48A(6) and (7) of the Act, Ofcom may give effect to the proposals, with or without modification, only if:

a) they have considered every representation about the proposal made to them within the period specified in the notification; and

b) they have had regard to every international obligation of the United Kingdom (if any) which has been notified to them for this purpose by the Secretary of State.

A2.6 Ofcom received responses to the notification and has considered every such representation made to them in respect of the proposals set out in the notification (and the accompanying consultation document).

A2.7 The Secretary of State did not notify Ofcom of any international obligation of the United Kingdom for the purpose of section 48A(6) of the Act.

Decision:

A2.8 In accordance with section 45 and 48(1) of the Act, and as set out in the Schedules to this Notification, Ofcom has decided to:

- set the following Numbering Conditions Binding Non-Providers: Conditions 3.1 to 3.23, as set out in Schedule 1 to this Notification; and

- add new definitions in the Numbering Condition Binding Non-Providers, as set out in Schedule 2 to this Notification.

A2.9 For the reasons explained in the explanatory statement accompanying this Notification, Ofcom has decided that the obligations set out in Schedule 1 of this Notification shall enter into force on 15 July 2027.

A2.10 Ofcom's reasons for reaching this decision, and the effect of this decision, are set out in Sections 3-9 of the explanatory statement accompanying this Notification.

A2.11 Ofcom considers that it has complied with the requirements of sections 45 to 49C and 59 of the Act, insofar as they are applicable.

A2.12 In reaching these decisions, as explained in section 8 of this statement, Ofcom has considered and acted in accordance with its general duties under section 3 of the Act, the six requirements set out in section 4 of the Act and general duty in relation to telephone numbers under section 63 of the Act. We have also had regard to the UK Government's Statement of Strategic Priorities for telecommunications, management of radio spectrum and postal services in accordance with section 2B of the Act, as well as the desirability of promoting economic growth in section 108 of the Deregulation Act 2015. We have also consulted the Information Commissioner's Office on these decisions to the extent they relate to the processing of personal data in accordance with Article 36(4) of the UK General Data Protection Regulation.

A2.13 A copy of this Notification and the accompanying statement document have been sent to the Secretary of State in accordance with section 48C(1) of the Act.

A2.14 In this Notification:

"the Act" means the Communications Act 2003;

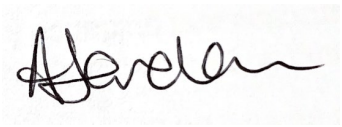
"Ofcom" means the Office of Communications.

A2.15 Words or expressions shall have the meaning assigned to them in this Notification, and otherwise any word or expression shall have the same meaning as it has in the Act.

A2.16 For the purposes of interpreting this Notification: (i) headings and titles shall be disregarded; and (ii) the Interpretation Act 1978 shall apply as if this Notification were an Act of Parliament.

A2.17 The Schedules to this Notification shall form part of this Notification.

Signed by



Amy Jordan,

Policy Director, Infrastructure and Connectivity

A person authorised by Ofcom under paragraph 18 of the Schedule to the Office of Communications Act 2002.

15 July 2026

Schedule 1 – Annex 2

We have decided to insert the following in the Numbering Condition Binding Non-Providers after Condition 2:

Condition 3: Application-To-Person (A2P) Messages - Protections from scam messages

Scope

3.1 This **Condition** applies as follows:

a) **Conditions** 3.2 to 3.3 apply to any person that transfers and/or terminates **A2P Messages**, except **Lower-Tier Aggregators**;

b) **Conditions** 3.4 to 3.8, 3.10 to 3.12, 3.15 to 3.21 and 3.23 apply to any person that transfers and/or terminates **A2P Messages**, including all **Aggregators**;

c) **Condition** 3.9 applies to any person that terminates **A2P Messages**;

d) **Conditions** 3.13 to 3.14 and 3.22 apply to any person that transfers and/or terminates **A2P Messages**, except **Lower-Tier Aggregators**;

each person to whom a provision applies is a '**Regulated Provider'** for the purposes of that provision.

Processes for receiving Scam Reports

3.2 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and, where appropriate, validate) **Scam Reports** from **End-Users** and appropriate third parties in relation to **URLs** and **Telephone Numbers** that the **End-User** and/or third party believes were used as part of a **Scam**, including **URLs** and **Telephone Numbers** included in **A2P Messages**.

Preventing Scam messages being sent and/or received

3.3 Taking into account **Scam Reports** received, **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to block, via automated means and without undue delay, **A2P Messages** that contain **URLs** or **Telephone Numbers** which they reasonably believe were used as part of a **Scam**.

Requirements relating to due diligence and on-going checks

3.4 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes to ensure that:

a) for any **A2P Messages** that they transfer and/or terminate**, Know Your Customer Checks**, checks relating to the use of any **Alphanumeric Sender IDs** and on-going **Know Your Traffic Checks** are conducted in accordance with **Conditions** 3.6 to 3.8, either by the **Regulated Provider**:

(i) carrying out these checks themselves; or

(ii) taking the steps in **Condition** 3.5; and

b) they do not transfer and/or terminate **A2P Messages** or enable the use of the relevant **Alphanumeric Sender IDs** unless they are reasonably satisfied with the outcome of these checks or with the checks carried out under **Condition** 3.5(a).

3.5 **Regulated Providers** must:

(a) implement and maintain clear and unambiguous contractual terms with any party from which they receive **A2P Messages** (that is not a **Business Sender**), requiring that party to:

(i) conduct **Know Your Customer Checks** on **Business Senders** at the **Onboarding Stage**, or take appropriate steps to ensure these checks have been conducted at the **Onboarding Stage**;

(ii) conduct checks when allowing a **Business Sender** to use a new **Alphanumeric Sender ID** to ensure that any proposed use of the **Alphanumeric Sender ID** is consistent with the **Business Profile** and purposes disclosed during **Know Your Customer Checks**, or take appropriate steps to ensure these checks have been conducted;

(iii) conduct on-going **Know Your Traffic Checks** on **Business Senders** or take appropriate steps to ensure these checks are conducted;

(iv) not transfer **A2P Messages** or enable the use of the relevant **Alphanumeric Sender IDs** unless they are reasonably satisfied with the checks carried out under **Conditions** 3.5(a)(i)-(iii);

(v) take appropriate, effective and prompt action in response to any reports of **A2P Messages** coming from their network that are suspected of being sent with the intention to **Scam** the recipients;

(vi) retain records in line with **Conditions** 3.17 to 3.21; and

(vii) take appropriate steps to ensure that **Business Senders** notify the party of changes to a **Business Sender**'s **Business Profile**, or otherwise ensure that the party with the direct relationship to the **Business Sender** will be notified of such changes.

(b) implement and maintain appropriate and effective policies, systems and processes to:

(i) ensure ongoing compliance with the contractual obligations imposed under **Condition** 3.5(a);

(ii) monitor and assess compliance with these obligations, taking into account **Conditions** 3.12 and 3.15; and

(iii) take appropriate, effective and prompt action to address any non-compliance and, if applicable, satisfy itself the party will comply in future.

3.6 **Know Your Customer Checks** must include:

(a) due diligence checks against **Business Profiles** for any indication that the **Business Sender** poses a risk of sending **Scam** messages;

(b) assessing the proposed use of any **Alphanumeric Sender IDs** for any indication that the **Business Sender** poses a risk of sending **Scam** messages, where applicable taking into account policies in place under **Condition** 3.9;

(c) confirmation of the contact details of a senior individual that is responsible for authorising the messages to be sent or transferred and/or terminated; and

(d) carrying out appropriate risk assessments to identify whether enhanced checks are appropriate to any cases, and if so, carrying out such checks.

3.7 Checks when allowing the use of any new **Alphanumeric Sender IDs** must include:

(a) due diligence checks to verify that the proposed use of **Alphanumeric Sender IDs** aligns with the information disclosed during **Know Your Customer Checks** on the **Business Profile**, including the stated purposes for seeking to access **A2P Message** services; and

(b) where applicable, reviewing the proposed use of the **Alphanumeric Sender ID** against policies in place under **Condition** 3.9.

3.8 **Know Your Traffic Checks** must include:

(a) monitoring and reviewing data on volume patterns; identifying new or different use of **Alphanumeric Sender IDs** or **Telephone Numbers**; and checking any information on or notifications of changes in **Business Profiles**, for any indicators of **Scam** activity, taking into account policies in place under **Condition** 3.9 and information obtained under **Conditions** 3.5(a)(vii) and 3.10 (whichever is applicable);

(b) using any insights from **Condition** 3.8(a) to review and update any previous risk assessments, as appropriate; and

(c) where any indicators of **Scams** are identified under **Condition** 3.8(a):

(i) seeking appropriate evidence as to whether or not messages are legitimate; and

(ii) blocking messages where the **Regulated Provider** reasonably believes, based on their review of any evidence provided, that the relevant **A2P Messages** were intended to **Scam** the intended recipients.

3.9 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes that impose restrictions on the use of **Protected Alphanumeric Sender IDs** in **A2P Messages** they terminate and communicate such policies to parties from whom they received **A2P Messages**, with the objective of preventing their use for **Scams.**

3.10 **Regulated Providers** must take appropriate steps to ensure that **Business Senders** from which they directly receive **A2P Messages** are required to promptly notify them of any changes in their **Business Profile**, or changes in the use of any **Alphanumeric Sender IDs**.

Incident management requirements

3.11 Where a **Regulated Provider** becomes aware of a **Business Sender** that they **Onboarded** sending or attempting to send, directly or indirectly, an **A2P Message** that the **Regulated Provider** reasonably believes was intended to **Scam** the recipient, the **Regulated Provider** must take the following steps within 1 **Working Day**:

(a) confirm the identity of the **Business Sender** responsible for those messages; and

(b) implement appropriate measures to prevent the **Business Sender** from sending further **A2P Messages** via any network or service the **Regulated Provider** provides unless the **Regulated Provider** has obtained evidence which they are satisfied demonstrates either:

(i) the **Business Sender** was not responsible for sending the relevant **A2P Message**;

or

(ii) the relevant **A2P Message** was not intended to **Scam** the recipients.

3.12 Where a **Regulated Provider** becomes aware of a **Significant Scams Incident** involving a **Business Sender** that they did not **Onboard**, the **Regulated Provider** must:

(a) within 2 **Working Days** in cases involving no more than one **Aggregator** or 5 **Working days** in all other cases:

(i) take appropriate steps to confirm the identity of the **Business Sender** responsible for those messages; and

(ii) implement appropriate measures to prevent the **Business Sender** from sending further messages via any network or service the **Regulated Provider** provides unless they have obtained evidence which they are satisfied demonstrates either:

1. the **Business Sender** was not responsible for sending the relevant **A2P Messages**; or
2. the relevant **A2P Messages** were not intended to **Scam** the recipients;

(b) promptly within 15 **Working Days**:

(i) establish whether the party involved in delivering the relevant **A2P Messages** to the **Regulated Provider** is complying with the requirements that **Regulated Provider** imposed on them under **Condition** 3.5(a); and

(ii) take appropriate and effective action to address the non-compliance and, if applicable, satisfy itself the party will comply in future.

Right to challenge

3.13 **Regulated Providers** must implement and maintain appropriate and effective policies, systems and processes that enable any affected person to challenge any blocking of a **Mobile Number** or message under **Condition** 3.3. The policies must:

(a) explain the circumstances under which any blocking may occur;

(b) explain how the person may challenge the blocking;

(c) explain the process the **Regulated Provider** will follow to investigate and determine any challenges made under **Condition** 3.13, including the evidence it is likely to require from the person to demonstrate the **Mobile Number** or messages should not have been blocked;

(d) identify the different potential outcomes that may follow any challenge;

(e) identify conditions the **Regulated Provider** may attach to an outcome following a challenge, including any ongoing requirements that may be placed on the person;

(f) identify a prompt and reasonable timeframe within which the **Regulated Provider** will reach an outcome following a challenge; and

(g) explain the process the person may follow to appeal any decision not to remove any blocking taken.

3.14 **Regulated Providers** must ensure that the policies, systems and processes in place under **Condition** 3.13 are well publicised and readily available, including ensuring that they are:

(a) easily accessible and reasonably prominent on their website; and

(b) referred to in the terms and conditions for all relevant products and services.

Review of policies, systems and processes

3.15 **Regulated Providers** must regularly review their policies, systems and processes, implemented under **Condition** 3 to ensure that:

(a) they remain appropriate and effective and are operating as intended;

(b) the **Regulated Provider** is complying with its policies, systems and processes; and

(c) any issues identified are promptly and effectively addressed, including by making appropriate changes to their policies, systems and processes implemented under **Condition** 3.

Training staff

3.16 **Regulated Providers** must ensure that all relevant staff are appropriately trained on the policies, systems and processes in place under **Condition** 3, including ensuring relevant staff are appropriately trained on the right to challenge processes implemented under **Condition** 3.13.

Record keeping

3.17 **Regulated Providers** must implement and maintain appropriate record keeping policies, systems and processes to demonstrate and ensure continued compliance with **Condition** 3. These must be overseen by a designated senior individual and must, where applicable, provide for the records identified in **Conditions** 3.18 to 3.21 below to be retained for at least the time period identified in those **Conditions**.

3.18 The following records must be kept for a period of at least five years:

(a) records of policies, systems and processes implemented under **Condition** 3;

(b) records of reviews of the effectiveness of policies, systems and processes implemented under **Condition** 3, including any actions taken or changes made to those policies, systems and processes under **Condition** 3.15; and

(c) records of the description of an incident under **Conditions** 3.11 and 3.12 (including the date and time the incident was identified and the number of messages involved), and measures or actions taken in response to that incident.

3.19 The following records must be kept for a period of at least three years after the end of the relevant contractual relationship:

(a) records of **Know Your Customer Checks** and checks relating to the use of **Alphanumeric Sender IDs** carried out under **Condition** 3.4, including initial and subsequent risk assessments;

(b) records of actions taken as a result of **Know Your Traffic Checks** carried out under **Condition** 3.4;

(c) records of requirements imposed on parties under **Condition** 3.5(a); and

(d) records of actions taken to ensure ongoing compliance and address any non-compliance under **Condition** 3.5(b).

3.20 Records relating to **False Positives** under **Condition** 3.22 must be kept for a period of at

least two years and must include:

(a) a description of a **False Positive** incident (including the date and time the incident first arose; its impact; the likely cause; and how and when it was identified); and

(b) any measures or actions taken in response to that incident.

3.21 Records of communications between a **Regulated Provider** and any person regarding a challenge raised under **Condition** 3.13 must be kept for at least one year from the date the challenge was resolved or otherwise closed.

Identifying, monitoring and addressing False Positives

3.22 Where a **Regulated Provider** is required under **Condition 3.3** to block messages, the **Regulated Provider** must implement and maintain appropriate and effective policies, systems and processes to identify and monitor **False Positives**, and take appropriate, effective and prompt action when **False Positives** are identified.

Data protection

3.23 **Condition** 3 applies subject to the requirements of the **Relevant Data Protection Legislation**.

Schedule 2 – Annex 2

We have inserted the following definitions, in alphabetical order, in the 'Part 1: Definitions and Interpretation' section of the "Numbering Condition Binding Non-Providers[515]":

The terms in **bold** below are defined terms in the General Conditions and any which are not separately defined in the table below have the same meaning as in the Communications Act 2003 or if not defined there, our Numbering Condition Binding Non-Providers or the National Telephone Numbering Plan.

Terms to be inserted
'**Aggregator'** means an intermediary that transfers (either directly or indirectly) **A2P Messages** between **Business Senders** and **Mobile Service Providers** that could terminate those messages to recipients (excluding intermediaries that contract directly with **Business Senders** but are acting in a capacity where that **Business Sender** is required to have separate contractual relationship with a third party to transfer **A2P Messages**).
'**Alphanumeric Sender ID'** means a sender identification displayed on a message recipient's handset, consisting of any characters, such as a code, custom name or brand name, used by a **Business Sender** when sending **A2P Messages**.
'**Apparatus'** includes any equipment, machinery or device and any wire or cable and the casing or coating for any wire or cable.
'Application-To-Person Message' or **'A2P Message'** means a message from a **Business Sender**, sent (either directly or indirectly) to **Mobile Numbers** using a software application**.**
'**Business Sender**' means any person, other than a **Regulated Provider**, that communicates with members of the public via **A2P Messages**. This includes, but is not limited to banks, schools, public bodies and retailers.
'**Business Profile**' means information relating to the **Business Sender** including information relating to: the trading or registered name; registered office or trading address; the nature of the services being provided (and the purposes for which they are seeking to access **A2P Messages**); payment / bank account information; existing telephone numbers; websites; and the name of directors and persons of significant control (taking into account the Companies House's guidance on people with significant control (PSCs): How to identify and record the people who own or control your company).
'**Condition**' means a Condition in Part 1
'False Positive' means, for the purposes of **Condition** C9, an instance where a **Regulated Provider** reasonably believes that a **A2P Message** may have been incorrectly identified and blocked pursuant to **Condition** 3.3 on the basis the **Regulated Provider** had reasonably believed it was intended to scam the recipient.
'**Know Your Customer Checks**' means the checks set out in **Condition** 3.6
'**Know Your Traffic Checks'** means the checks set out in **Condition** 3.8
'**Lower-Tier Aggregator'** means an **Aggregator** that is acting in a capacity in which it does not contract directly with a **Mobile Service Provider** that directly terminates **A2P Messages** to recipients.

[515] Numbering Conditions Binding Non-Providers

'**Onboarding**' (and other forms of the word) means where a **Regulated Provider** undertakes or is involved in the **Onboarding Stage**.
'**Onboarding Stage'** means the period during which a party is preparing to start providing their service to a new **Business Sender** and they are collecting and verifying all the information needed to facilitate this.
'Mobile Communications Service' means a **Public Electronic Communications Service** consisting in the conveyance of **Signals** by means of a **Public Electronic Communications Network** through the agency of **Wireless Telegraphy** to or from **Apparatus** which is designed or adapted to be capable of being used in motion.
'**Mobile Number'** means a **Telephone Number**, from a range of numbers in the **National Telephone Numbering Plan**, that is used to identify **Apparatus** designed or adapted to be capable of being used while in motion.
'Mobile Service Provider' means a **Communications Provider** that provides a **Mobile Communications Service**.
'**Protected Alphanumeric Sender IDs**' means **Alphanumeric Sender IDs** which have restrictions or conditions placed on their use because they relate to known brands (such as 'Royal Mail' or 'HMRC'), contain special alphanumeric characters (such as those outside the standard alphabet, 0-9 numerals and essential punctuation) or are generic IDs (such as 'Alert', 'Security' or 'Customer Service').
'**Relevant Data Protection Legislation'** means the General Data Protection Regulation (EU) 2016/67930[516], the Data Protection Act 2018 and the Privacy and Electronic Communications (EC Directive) Regulations 2003
'**Regulated Provider**' means a person other than a **Communications Provider** and has the meaning given to it in **Condition** 3.1.
'**Scam**' (and other forms of the word) means any deceptive act or scheme designed to trick a person into disclosing personal or financial information or to trick them out of their money or other valuables, including but not limited to conduct that may be considered fraud under the Fraud Act 2006.
'**Scam Report**' means a report made by any person about a **Scam** message (or other forms of **Scam**), including complaints from **End-Users** and reports from law enforcement, regulatory or consumer bodies or other third parties.
'**Signals**' includes: (a) anything comprising speech, music, sounds, visual images or communications or data of any description; and (b) signals serving for the impartation of anything between persons, between a person and a thing or between things, or for the actuation or control of apparatus;

[516] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (United Kingdom General Data Protection Regulation) (Text with EEA relevance).

'**Significant Scams Incident**' means a situation where it appears to the **Regulated Provider** that a particular **Business Sender** has cumulatively sent or attempted to send, directly or indirectly, at least fifty **A2P Messages** that the **Regulated Provider** reasonably believes were intended to **Scam** the recipients.
'Short URLs' means a **URL** with a smaller number of characters than a specified, original **URL** that uses **URL** redirection to refer to the same resource.
'**URLs**' stands for Uniform Resource Locator, and means a reference that specifies the location of a resource accessible by means of the internet, including **Short URLs**.
'**Wireless Telegraphy**' means the emitting or receiving, over paths that are not provided by any material substance constructed or arranged for the purpose, of electromagnetic energy of a frequency not exceeding 3,000 gigahertz that: (a) serves for conveying messages, sound or visual images (whether or not the messages, sound or images are actually received by anyone), or for operating or controlling machinery or apparatus; or (b) is used in connection with determining position, bearing or distance, or for gaining information as to the presence, absence, position or motion of an object or of a class of objects.
'Working Day' means the hours between 09.00 – 17.00 on Monday to Friday, with the exception of Bank Holidays and public holidays.

A3. Impact assessments

A3.1 Section 7 of the Act requires us to carry out and publish an assessment of the likely impact of implementing rules which would be likely to have a significant impact on businesses or the general public, or when there is a major change in Ofcom's activities. We included this assessment in our 2025 consultation, in particular in section 5 and Annex 3.

A3.2 More generally, impact assessments form part of good policymaking and we therefore expect to carry them out in relation to a large majority of our rules. We use impact assessments to help us understand and assess the potential impact of our policy decisions before we make them. They also help us explain the policy decisions we have decided to take and why we consider those decisions best fulfil our applicable duties and objectives in the least intrusive way. Our impact assessment guidance sets out our general approach to how we assess and present the impact of our decisions.[517]

A3.3 In section 3 of this statement, we explain the harms which arise from scam mobile messages and in sections 5-8 we set out our rules aimed at addressing this harm and assess their impact and proportionality. In summary, we expect our rules to have an overall positive impact for stakeholders, consumers and citizens, in particular by introducing greater frictions and costs into scammers' operations across P2P and A2P channels and ensuring key vulnerable aspects of UK providers and aggregators' networks are more secure. In turn, we expect this would reduce the volumes of fraudulent messages reaching UK consumers and help to address the harms associated with messaging scams.

A3.4 We also consider that these benefits outweigh the costs and risks of adverse impacts and that our rules are proportionate.

Equality impact assessment

A3.5 We have given careful consideration to whether our rules will have a particular impact on persons sharing protected characteristics (broadly including race, age, disability, sex, sexual orientation, gender reassignment, pregnancy and maternity, marriage and civil partnership and religion or belief in the UK and also dependents and political opinion in Northern Ireland), and in particular whether they may discriminate against such persons or impact on equality of opportunity or good relations. This assessment helps us comply with our duties under the Equality Act 2010 and the Northern Ireland Act 1998.[518]

A3.6 When thinking about equality we think more broadly than persons that share protected characteristics identified in equalities legislation and think about potential impacts on various groups of persons (see paragraph 4.7 of our impact assessment guidance).

A3.7 In particular, section 3(4) of the Act also requires us to have regard to the needs and interests of specific groups of persons when performing our duties, as appear to us to be relevant in the circumstances. These include:

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

[517] See Ofcom impact assessment guidance.
[518] Further detail is set out in section 149 of the Equality Act 2010 and section 75 of the Northern Ireland Act 1998.

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

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

A3.8 We examine the potential impact our policy is likely to have on people, depending on their personal circumstances. This also assists us in making sure that we are meeting our principal duty of furthering the interests of citizens and consumers, regardless of their background and identity.

A3.9 We have not identified any adverse impacts on specific groups of persons that are likely to be affected in a different way to the general population.

A3.10 In making our decisions that relate to customers' ability to challenge blocking of their messages by their provider, we have considered the risk that certain groups may find it harder to engage with processes providers may establish to comply. In seeking to mitigate this risk, we require providers' policies to be easily accessible and prominent on their websites [519] and we explain in our guidance that we expect this policy to be provided in any format upon reasonable request (for example, if a visually impaired customer requires a braille version).

A3.11 By reducing the number of scam messages that people receive, we consider that our rules are likely to have a particularly positive impact on any groups of persons that may be more susceptible to scam messages. Where any groups of persons may be more susceptible, a significant reduction in the likelihood these groups receive scam mobile messages will ensure that they are less likely to encounter them and to risk suffering harm.

A3.12 We also consider that certain groups may experience harms associated with scam mobile messages differently. There is evidence, for example, that female and ethnic minority victims are significantly more likely to experience some types of emotional and health harms associated with fraud and cybercrime compared to males and non-ethnic minority people respectively.[520] Any reduction in these types of harms from our rules would therefore have a particularly positive impact on these groups.

A3.13 Lastly, our rules will support people to have more confidence in A2P messages they may receive. For example, we have identified people receiving a high volume of communication from for example healthcare providers, such as those with long-term health conditions, as being particularly likely to benefit from our rules where they may need to take action in response to A2P messages.

A3.14 In our 2025 consultation, we asked if stakeholders agreed with our equality impact assessment set out in Annex 3 to that document.

A3.15 All stakeholders who responded to this question in our 2025 consultation agreed with our assessment of how our rules impact persons with protected characteristics.

A3.16 The Campaign Registry agreed that our proposals are likely to have a positive equality impact by reducing exposure to scams, which they noted can disproportionately affect vulnerable and less digitally confident users.[521]

---

[519] GC C9.18 requires providers to ensure that the policies, systems and processes in place under Condition C9.17 are well publicised and readily available.

[520] Experiences of victims of fraud and cyber crime.

[521] The Campaign Registry response to October 2025 Consultation. Page 15.

Welsh language assessment

A3.17 The Welsh Language (Wales) Measure 2011 made the Welsh language an officially recognised language in Wales. Ofcom is required to take Welsh language considerations into account when formulating, reviewing or revising policies which are relevant to Wales (including decisions which are not targeted at Wales specifically but are of interest across the UK).

A3.18 Where the Welsh Language Standards are engaged, we consider the potential impact of a policy on: (i) opportunities for persons to use the Welsh language; and (ii) treating the Welsh language no less favourably than the English language. We also consider how a policy could be formulated so as to have, or increase, a positive impact, or not to have adverse effects or to decrease any adverse effects.

A3.19 Our policy objective is to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages. Overall, we expect our rules to have a positive impact on all UK customers, including Welsh language speakers, by disrupting scam activity and reducing exposure to scam mobile messages. This should help minimise the anxiety and emotional distress experienced by victims, including those who speak Welsh.

A3.20 We do not consider many of our new rules will have any impact on our Welsh language obligations. This includes our rules that would require providers to identify and block scam telephone numbers. Welsh language considerations may be more relevant where our rules require providers to review the content of messages (which may be in Welsh), identify scam URLs or to engage with Welsh language speakers that may want to challenge any blocking of their legitimate messages.

A3.21 When setting a GC, we must apply the relevant tests under the Act, including ensuring that any measure is proportionate. We do not consider it proportionate to formulate our rules in such a way that they will have specific positive impacts on opportunities to use the Welsh language when engaging with providers: for example, by requiring providers to use tools to detect malicious sender IDs and URLs and review message content in Welsh, or by publishing their right to challenge policy in Welsh (noting that most providers subject to our rules are likely to engage with their customers in Welsh).

A3.22 However, we have set out in our guidance that providers may wish to consider the extent to which scam reports identify malicious sender IDs and URLs in Welsh and whether their identifying and blocking measures may be able to identify and block numbers and messages sent from, or that contain, those malicious sender IDs or URLs.

A3.23 In our 2025 consultation we asked if stakeholders agreed with our Welsh language impact assessment set out in Annex 3 to that document.

A3.24 All stakeholders who responded to this question in our 2025 consultation agreed with our assessment of how our rules impact Welsh language speakers.

A3.25 The Campaign Registry said they could see no obvious impact on Welsh speakers or the use of the Welsh language.[522]

[522] The Campaign Registry response to October 2025 Consultation. Page 15.

A3.26 BT agreed that Welsh language scams are not currently a major problem, citing only [✂] record of Welsh language messages (spam rather than scam) being reported to 7726 and this was spam rather than a scam.[523]

[523] BT response to October 2025 Consultation.

A4. Further detail on our rights assessment

A4.1 Ofcom is required by section 6 of the Human Rights Act 1998 to act in a way which is compatible with the European Convention on Human Rights (ECHR). Ofcom needs to balance a range of fundamental rights under the ECHR when carrying out its functions including the right to respect for private and family life (Article 8 of the ECHR) and the right to freedom of expression (Article 10 of the ECHR). [524]

A4.2 Article 8(1) explains that everyone has the right to respect for his private and family life, his home and his correspondence. Article 8(2) states that there shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others.

A4.3 Article 10(1) explains that everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. Article 10(2) states that the exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.

A4.4 In section 8, we summarised how our measures could adversely affect individual rights under Articles 8 and 10 ECHR.

A4.5 Any interference with these rights must be lawful, pursue a legitimate social aim and not be disproportionate. In essence, restrictions on these rights must be necessary and the measure's contribution to its objective must outweigh its adverse impacts. Compliance with data protection legislation is a relevant consideration when assessing whether any interference with Article 8 and 10 rights may be proportionate.

A4.6 In section 8, we explained why we considered the risk of potential adverse impacts to individual rights under Article 8 and 10 ECHR from implementing our amended measures to be low and that potential adverse rights impacts are proportionate to our objective of reducing the likelihood that consumers and small business end-users receive scam mobile messages.

A4.7 In the paragraphs below, we provide further detail on our rights assessment. We first identify key data protection considerations that are relevant to our measures and rights assessment. Second, we identify which measures are more likely to interfere with Article 8 and 10 rights. Third, we identify the potential interference with those rights. Fourth, we set

[524] These rights have been implemented in UK law under the Human Rights Act 1998.

considerations relevant to our assessment of whether our measures are proportionate to this potential interference.

Data protection considerations

A4.8 All of our measures are individually likely to involve the processing of personal data, either because the sender, intended recipient or other individuals are identifiable from the content or metadata of a message, or because the content or metadata of a message is connected to other information, which renders someone identifiable. Such processing, in particular automated processing, can lead to a number of possible data protection harms, such as loss of control of personal data, invisible processing or unwarranted surveillance.[525]

A4.9 Providers will therefore need to continue to ensure their processing of personal data complies with relevant data protection legislation including the General Data Protection Regulation (EU) 2016/67930 ('UK GDPR'), the Data Protection Act 2018 ('DPA') and the Privacy and Electronic Communications (EC Directive) Regulations 2003 ('PECR').

A4.10 The UK GDPR sets out the following seven key principles that sit at the heart of data protection law (and which providers will need to consider as part of ensuring their processing complies with data protection rules). These are: [526]

a) Lawfulness, fairness and transparency;[527]
b) Purpose limitation;[528]
c) Data minimisation;
d) Accuracy;[529]
e) Storage limitation;
f) Integrity and confidentiality (security); and
g) Accountability.

A4.11 Providers may use third parties to carry out data processing on their behalf. Guidance issued by the Information Commissioner's Office (ICO) is clear that, where third parties are used, it is for the service provider and that third party to identify their respective roles and obligations under data protection law, and ensure that all the requirements of that law are met.[530] Providers will also need to comply with the rules on "restricted transfers" in the UK GDPR if transferring personal data outside the UK for the purposes of implementing the GCs, ensuring that appropriate safeguards are in place with respect to all such transfers.

---

[525] Also see Information Commissioner's Office, 2022. Overview of Data Protection Harms and the ICO's Taxonomy.

[526] Further information on these principles is available in ICO, A guide to the data protection principles [accessed 10 July 2026]. The UK GDPR provides a higher level of protection for the processing of particularly sensitive categories of data relating to race, sexual orientation, sex life, health data, political opinions, trade union membership, religious or philosophical beliefs, biometric or genetic data (known as special category personal data) and criminal conviction and offence data. See also ICO. What data protection rights do people have? [accessed 10 July 2026].

[527] For example, providers should be transparent with users about the processing of personal data they carry out in order to comply with GC C9.

[528] See ICO, guidance on purpose limitation (March 2026) accessed on [10 July 2026].

[529] For example, robust validation of scam reports and ensuring records are kept up to date will help ensure compliance with the data accuracy principle.

[530] ICO. Controllers and processers [accessed 10 July 2026].

A4.12 Other data protection legislation and guidance that are particularly relevant to our measures include:

- Rules and guidance relating to the monitoring of content, in particular automated monitoring. Providers should consider whether they are likely to be caught by Article 22A UK GDPR relating to automated decision making which applies where a provider makes decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. We note that ICO Guidance on "Content moderation and data protection" (in particular on "What if we use automated decision-making in our content moderation?")[531] indicates that content moderation will not involve solely automated decision-making where it involves a database matching tool. Similarly, ICO guidance on "What does the UK GDPR say about ADM?"[532] explains that a human can set a simple rule that is applied automatically, but the system is not actually making its own separate decision. We expect our measures requiring providers to identify known, validated scam URLs and numbers in messages to be implemented using a database matching tool (where a human sets a rule that is applied automatically), rather than a system making decisions based on the likelihood of something happening. It is however providers' responsibility to ensure they comply with relevant data protection rules, taking into account how they implement our measures and associated ICO guidance. Where Article 22A applies, providers must ensure they comply with the restrictions and safeguards in Articles 22B-D UK GDPR.[533] The ICO has also published guidance on automated decision making and profiling.[534]
- Rules and guidance relating to monitoring of traffic data. Providers should, for example, ensure they comply with Regulations 7, 8 and 29 of the PECR.

A4.13 We are satisfied that our measures can be implemented in accordance with data protection law.[535] As noted above, the ICO has published guidance on content moderation and data protection that explains how data protection law applies to content moderation technologies and processes, including where these are solely automated, and provides advice to help service providers comply with the UK GDPR and the DPA when utilising these technologies and processes. This includes advising service providers to carry out a data protection impact assessment to assess and mitigate data processing risks.

Relevant measures

A4.14 Some of our measures may interfere with Article 8 and 10 rights, in particular the following measures:

a) GCs C9.2 and C9.6, which require providers to implement and maintain appropriate and effective policies, systems and processes to regularly and proactively ensure they receive (and where appropriate, validate) reports of scams from end-users and appropriate third parties relating to:

[531] See ICO. Content moderation and data protection, in particular on What if we use automated decision-making in our content moderation? [accessed 10 July 2026]. While the ICO's guidance on automated-decision-making in content moderation is aimed at organisations who are carrying out content moderation to meet their obligations under the Online Safety Act, it explains that it also applies to organisations who are carrying out content moderation for other reasons.
[532] ICO guidance on What does the UK GDPR say about ADM? [accessed 10 July 2026]
[533] ICO. What are the ADM safeguards?
[534] ICO. Guidance on automated decision making and profiling [accessed 10 July 2026].
[535] We have also consulted with the ICO through our consultation process and prior to making the final decisions in this statement in accordance with Article 36(4) of the UK GDPR.

- Customers they have assigned mobile numbers to;
- Telephone numbers that the end-user and/or third party believes sent P2P messages intended to scam the recipients; and
- URLs and telephone numbers that the end-user and/or third party believes were used as part of a scam, including URLs and telephone numbers included in P2P or A2P messages.

b) GC C9.3(a) requires providers to prevent, without undue delay, mobile numbers they have assigned from sending P2P messages where they reasonably believe those mobile numbers have sent P2P messages intended to scam the recipients.

c) GC C9.3(b) requires providers to block, without undue delay, P2P messages sent from telephone numbers where they reasonably believe those telephone numbers have sent P2P messages intended to scam the recipients.

d) GC C9.3(c) and C9.7 require providers to block, via automated means and without undue delay, P2P or A2P messages that contain URLs or telephone numbers which they reasonably believe were used as part of a scam.

e) GCs C9.8/9.12 require providers to monitor and review data on volume patterns as part of KYT checks and take appropriate action in response to any indicators of scam activity based on those checks (which could result in A2P messages being blocked).

f) In response to becoming aware of a message that the provider reasonably believes was intended to scam the recipient, GCs C9.15 and C9.16 require providers to (i) take appropriate steps to confirm the sender responsible for the messages; and (ii) prevent, or take appropriate measures to prevent, the sender from sending further A2P messages.

A4.15 We accept that providers could seek to reduce the likelihood that consumers and small business end-users receive scam mobile messages services by taking steps that are not required by our measures or taken in order to comply with our measures. This is a commercial matter for providers and not therefore within the scope of this assessment.

Article 8 right to privacy

Potential interference

A4.16 GCs C9.2 and C9.6 require providers to gather intelligence in reports made about a scam (or potential scam) message, including complaints from customers and reports from law enforcement, regulatory or consumer bodies or other appropriate third parties (the intelligence gathering stage).

A4.17 Providers are required to use (and, where appropriate, validate) that intelligence to identify:

a) Telephone numbers they reasonably believe to have sent P2P messages intended to scam the recipients.

b) URLs or telephone numbers they reasonably believe were used as part of a scam, including URLs or telephone numbers included in P2P or A2P messages (the validation stage).

A4.18 For example, providers are expected to interrogate reports such as 7726 data to filter out messages (such as commercial marketing messages) that the provider does not reasonably believe were intended to scam the recipients. Providers may use automated tools or human review to carry out this validation.

A4.19 As a preliminary point, we do not consider Article 8 rights protect messages which seek to facilitate scam activity.

A4.20 Our view is that the intelligence gathering and validation stages are unlikely to impact on the right to privacy under Article 8. This is because the intelligence that providers are required to gather is based on one or more of the following:

a) Intelligence or messages provided by customers to the provider or a third party. In other words, the recipient of the messages has effectively agreed to the content of their message being reviewed for potential scam prevention purposes.
b) Publicly available URLs, which in themselves will not contain any private information.
c) Intelligence provided by third parties that have expertise in, and a legitimate basis for, identifying or aggregating scams, provide a rich source of timely information and can provide detailed information on current and emerging threats. Further information on this is provided in our guidance.

A4.21 The next stage requires providers to identify and block mobile numbers and messages in accordance with GCs C9.3 and C9.7.

A4.22 Any identifying and blocking under GCs C9.3(a) or (b) could be carried out using automated tools or as a result of human review. Our view is that identifying and blocking mobile numbers or messages under GCs C9.3(a) and (b) is less likely to impact on the right to privacy under Article 8 because there should be no need for providers to review the content of messages. There may, however, be some impact on the right to privacy under Article 8, to the extent providers are required to review message traffic data and associated metadata.

A4.23 Identifying known scam URLs and telephone number in messages under GCs C9.3(c) and C9.7 will, however, interfere with the right to privacy under Article 8. This is because providers are required to use automated tools to review the content of private messages.

A4.24 We are not recommending the use of a specific kind of technology. This means that providers may adopt different tools to comply with our measures. For example, providers may decide to adopt tools that compare the content of messages against a database. Various factors may impact on the right to privacy, including the type of technology that is used and how it operates, as well as how any underlying database is compiled.

A4.25 While GCs C9.3(c) and C9.7 require providers to use automated tools, they do not prevent human review and we recognise that some degree of human review of messages is likely to be necessary to ensure the automated tools are working as intended. Review of content by human moderators may have a more significant impact on users' privacy, although we note that, if human review is focused on checking that reported URLs and telephone numbers are in fact malicious, there will be less need for humans to review private messages.

A4.26 The degree of interference will also depend on the nature of the content of the message. For example, consumers may be less likely to have an expectation of privacy in relation to scam messages or commercial marketing. We note that Amnesty International UK has also commented on "the low expectations of privacy and security in [number-based systems like SMS] due to legacy constrains [sic] and regulations, including mandatory access by law enforcement …".[536]

[536] Amnesty International UK response to October 2025 Consultation. Page 1.

A4.27 GCs C9.8 and C9.12 require providers to monitor A2P volume patterns for both indicators of a risk of scams and for scam indicators. This is likely to involve reviewing message traffic data and associated metadata which can impact on the right to privacy under Article 8. Where any indicators are identified, providers are required to take appropriate action by obtaining, or taking appropriate steps to obtain, relevant information from the sender to enable the provider to satisfy itself that the messages are legitimate.

A4.28 There may be further impacts on the right to privacy under Article 8 if a provider reviews the content of messages to determine whether the messages are legitimate or not, and those messages are in fact legitimate.

A4.29 GCs C9.15 and C9.16 do not require providers to carry out any form of monitoring of traffic data or the content of messages. These measures are therefore unlikely to impact on the right to privacy under Article 8.

Proportionality of potential interference

A4.30 For the reasons set out below, we consider that the interference with the right to privacy (and particularly under GCs C9.3, C9.7, C9.8/9.12) to be proportionate.

A4.31 In particular, we have decided to include various safeguards in our rules to limit any impact on the right to privacy under Article 8.

A4.32 First, we explain in guidance that providers are expected to consider whether other indicators of malicious activity can be used identify and block messages before message content is reviewed. For example, where a source sender ID or Global Title is present in an internal blocklist, our guidance explains that these should be used to block the message before the message content is reviewed. This can be achieved by providers appropriately ordering the application of firewall rules, where rules that examine message content are applied last.

A4.33 Second, in relation to GCs C9.3(c) and C9.7, we require providers to identify messages which contain known scam URLs and telephone numbers they have gathered from reports from end-users and appropriate third parties about a scam (or potential scam) message. We also explain in guidance that providers should:

a) Take appropriate steps to mitigate the risk of false positives, including by validating reports such as 7726 data to filter out messages (such as commercial marketing messages) that the provider does not reasonably believe were intended to scam the recipients. Providers are also required under GC C9.26 to take appropriate, prompt and effective action when they do identify false positives to mitigate the risk of further false positives arising.
b) Ensure the intelligence they have gathered and use to identify known scam URLs and telephone numbers in messages is current, robust and subject to contextual testing and evaluation.

A4.34 GCs C9.3(c) and C9.7 (and our accompanying guidance) should therefore ensure **any review of messages is intelligence-led, focused and targeted**. It should also allow providers to train their systems to identify specific numbers and URLs without needing to capture or process other content in the same way. Our measures do not, for example, require providers to carry out indiscriminate or a more general assessment of the contents of all messages based on broader probabilistic search methods. In other words, our measures should require providers to implement an exact data base matching tool (where a human sets a rule that is applied automatically), rather than a system making decisions

based on the likelihood of something happening. We recognise that some providers may carry out other types of monitoring based on their own review of messages on their network that have not been reported by end-users or third parties. This form of monitoring is not required or prevented by our measures. We note that it is likely to be considered more intrusive and our guidance explains that providers should therefore ensure they comply with any other relevant legislation, including data protection legislation.

A4.35 Third, we **require providers to carry out *automated* monitoring in order to identify known scam URLs and telephone numbers in messages** (which we consider to be less intrusive than human review of private messages). Automated tools can be used to search messages for embedded URLs and telephone numbers without any human needing to read the content. In practice, some degree of human review is likely to be necessary, for example, to ensure identifying and blocking techniques are working as intended and identify and monitor false positives. However, we expect any human involvement in the review of messages for known scam URLs and telephone numbers to be limited and for the primary purpose of mitigating the risk of false positives. The safeguards identified in paragraph A4.33 above should also ensure the accuracy and effectiveness of intelligence and reduce the amount of content that providers will need humans to review.

A4.36 Fourth, in relation to GCs C9.8 and C9.12 (which may involve a provider reviewing the content of A2P messages to determine whether they are legitimate or not), providers are not required to proactively review the content of messages where they have identified any indicators of a risk of scams, or scam indicators; rather, they are required to seek appropriate evidence from the sender to enable the provider to satisfy itself that the messages are legitimate. We also expect message senders will be informed of this possibility in advance (for example, in contractual arrangements) or before the content of a message is disclosed.

A4.37 Fifth, in relation to all our measures, we **require providers to comply with relevant data protection legislation**. Providers will therefore be required to consider and manage the risks associated with the processing of personal data involved in implementing our measures. We have highlighted in our guidance the fundamental principles of data protection legislation, as well as specific provisions of such legislation, and explained that we expect providers to take into account relevant ICO guidance (see discussion from paragraph A4.8 above).

A4.38 We consider that safeguards under data protection law, as explained in various ICO guidance, will help ensure that the processing of data can be done responsibly, with people's information rights being respected. In particular, we consider the requirement to ensure any review of messages is intelligence-led, targeted and automated supports the UK GDPR principles of data minimisation and fairness, including by ensuring humans are not indiscriminately reviewing the content of private messages.

A4.39 Sixth, we are requiring providers to comply with various other cross-cutting measures relating to reviewing policies, training staff and record keeping (described in section 7). In particular:

a) Providers are required to ensure they regularly review their policies, systems and processes to ensure they remain appropriate and effective and are operating as intended; ensure they are complying with their own policies systems and processes; and ensure that any issues identified are promptly and effectively addressed.

b) Providers are required to ensure relevant staff are appropriately trained on the policies, systems and processes in place under Condition C9. Our guidance also explains that we expect training to cover managing identifying and blocking systems.
c) Providers are required to keep records to demonstrate how they comply with Condition C9, including the requirement to ensure compliance with data protection legislation.

A4.40 More generally, providers have reputational and commercial incentives to ensure any monitoring is carried out in a way that limits impacts on the right to privacy under Article 8, as well as under data protection legislation (particularly in relation to their own customers). These commercial incentives should encourage providers to strike a reasonable balance in their implementation of our measures, including the technical configuration of their automated tools and their use of human moderators.

Article 10 right to freedom of expression

Potential interference

A4.41 Interference with freedom of expression could arise where either:

a) Mobile numbers are blocked by a provider, but those numbers have not been used to send P2P messages intended to scam the recipients.
b) Messages are blocked by a provider where those messages were not intended to scam the recipients.

A4.42 In other words, there is a risk of blocking legitimate mobile numbers and messages. This could occur as a result of GCs C9.3, C9.7, C9.8/9.12(c), C9.15 and C9.16. We consider the risk of false positives to be higher where providers use automated tools (which they are required to use under C9.3(c) and C9.7 but may use to comply with other GCs). Where a provider has a higher tolerance for false positives, more numbers and messages may be incorrectly blocked.[537]

A4.43 We also consider interference with individual rights is more likely to occur under GCs C9.3(b) and (c) and C9.7 where automated tools are used to block messages and senders may not otherwise become aware that a provider has blocked their message.

A4.44 As a preliminary point, we do not consider blocking mobile numbers that have sent scam messages or blocking messages that contain scam URLs or telephone numbers to engage Article 10 ECHR.

A4.45 Overall, we consider the risk of interference with the right to freedom of expression to be low, on the basis that:

a) The requirements to block mobile numbers and messages under GCs C9.3 and C9.7 should be based on current and robust intelligence of known scam messages, URLs or telephone numbers that is subject to contextual testing and evaluation. Providers are also required to identify, monitor and address false positives by making appropriate changes to systems, processes, and/or controls to prevent recurrence. Providers should therefore have a high degree of confidence that any blocking is focused and targeted on known scam numbers and messages. This should ensure any blocking is accurate and effective, which should significantly reduce the risk of false positives.

[537] Over-blocking could potentially arise in relation to the most highly protected forms of content, such as political speech.

b) Evidence from stakeholders indicates that false positive rates as a result of implementing GCs C9.3(b) or (c) or C9.7 are likely to be significantly lower than the already low rates from current blocking practices. [538]
c) Any false positives that may still arise under GCs C9.3 and C9.7 are more likely to relate to commercial speech in the form of marketing messages (or spam), which attract the least level of protection under Article 10.
d) Any blocking under GCs C9.3(a) or (b) could be carried out using automated tools or as a result of human review. Given that humans can better understand context and nuance, we consider the risk of a legitimate message being blocked as a result of an incorrect human review to be low, and lower than the risk of messages being blocked by automated tools.
e) While any blocking under GCs C9.3(c) and C9.7 would need to be carried out using automated tools, our rules do not prevent any human review and recognise that some degree of human review of messages is likely to help reduce the risk of legitimate messages being blocked. For example, human review could check that reported URLs and telephone numbers are, in fact, malicious and to ensure identifying and blocking techniques are working as intended.
f) The requirements under GCs C9.8/9.12(c), C9.15 and C9.16 do not require any blocking. Any blocking that does occur under these GCs would result from the provider satisfying itself that the relevant numbers have sent scam messages or the relevant messages contain scam URLs or telephone numbers. If any legitimate messages are blocked, this is likely to be the result of an incorrect human review, which we consider to be low risk.

A4.46 We recognise that there could be a small amount of mobile numbers or messages that are incorrectly blocked. Such errors could arise for various reasons, for example:

a) **System or human errors**: An error may occur in a provider's systems and processes (such as the intelligence it has gathered or any database on which it relies, or where blocking tools are not working as intended). This may be the result of human error, for example, in failing to carry out appropriate validation of scam reports or incorrectly inputting a rule into its scam prevention systems.
b) **Spoofing**: In a P2P channel, a scammer may spoof a legitimate mobile number which recipients may report, leading to that legitimate number being categorised as malicious. In an A2P channel, a scammer may use a spoofed Alphanumeric Sender ID (e.g. a bank's name), meaning reports associated with the message may wrongly identify a legitimate Alphanumeric Sender ID as malicious.
c) **Warnings**: An individual may copy a scam URL or telephone number to send to a friend, to warn them about a scam. While the individual's message may be blocked (and interfere with the right to freedom of expression), it should mean an actual scam message containing the relevant URL of telephone number is also blocked, therefore mitigating the risk of the intended recipient being scammed from the relevant message.

A4.47 We have explained in our guidance that providers should consider if there are specific scenarios where a legitimate message may contain a scam URL or telephone number and take appropriate steps to ensure that the end-user's number is not blocked (paragraph 2.40).

[538] See paragraph 7.29.

Proportionality of potential interference

A4.48 For the reasons set out below, we consider that any potential interference with the right to freedom of expression is proportionate.

A4.49 As noted above, we consider the risk of interference to be low. We have also decided to include various safeguards in our rules to limit any potential impacts to freedom of expression.

A4.50 First, we require providers subject to GCs C9.3(b) and (c) and C9.7 to implement appropriate systems and processes to identify and monitor false positives. This should ensure all providers subject to C9.3(b) and (c) and C9.7 have appropriate oversight over false positives meaning they can take appropriate, prompt and effective action when both (a) individual false positives are identified; and (b) providers observe an unexpected increase in false positive rates which may indicate an issue that could potentially lead to providers blocking a significant number of legitimate messages. Appropriate action is likely to include ensuring the same legitimate messages or type of legitimate messages (e.g. campaigns) are not blocked by amending rules in their scam prevention systems and feeding false positives back into validation checks.

A4.51 Second, we **require providers to implement a right to challenge process** for blocking decisions under GC C9.3 and C9.7 (see section 7). Our guidance explains that we expect providers to inform users of the circumstances in which their messages may be blocked and explains how providers can do this. The availability of an accessible complaints process should also allow customers to quickly and easily contact any provider to challenge a blocking decision under GC C9.3 or C9.7. We consider this right to challenge process supports the UK GDPR principles of fairness and transparency.

A4.52 Third, and as explained above, we **require providers to comply with relevant data protection legislation**. We have identified the fundamental principles of data protection legislation in our guidance, as well as specific provisions of such legislation, and explained that we expect providers to take into account relevant ICO guidance.[539]

A4.53 Fourth, we require providers to comply with various other cross-cutting measures relating to reviewing policies, training staff and record keeping (described in section 7). In particular:

a) Our guidance explains that we expect providers to keep rates of false positives and challenges to the blocking of legitimate messages under review, and make appropriate changes to their policies, systems and processes to reduce the risk of false positives occurring.
b) Providers are required to ensure relevant staff are appropriately trained on the right to challenge processes. Our guidance also explains that we expect training to cover managing identifying and blocking systems and responding to incidents of scam (or potential scam) activity.
c) As noted above, providers are required to keep records to demonstrate how they comply with Condition C9, including the requirement to ensure compliance with data protection legislation. We are not requiring providers to retain any messages that have been blocked, which we consider to be consistent with the UK GDPR principle of storage limitation.

[539] We have also consulted with the ICO through our consultation process and prior to making the final decisions in this statement in accordance with Article 36(4) of the UK GDPR.

A4.54 More generally, providers have reputational and commercial incentives to ensure any blocking is carried out in a way that limits the number of legitimate numbers or messages that are blocked (particularly in relation to their own customers). These include meeting users' expectations and avoiding the cost of dealing with complaints and appeals.

A5. Legal Framework

A5.1 In this Annex, we set out a brief overview of our powers and duties that are relevant to our decisions in this statement. It is not a full statement of all the legal provisions which may be relevant to Ofcom's functions or to numbering. The applicable legal framework mainly derives from our duties and powers in the Communications Act 2003 (the Act).

A5.2 When considering the decisions set out in this statement we have considered and acted in accordance with the legislative provisions set out below.

Ofcom's duties

General duties

A5.3 The Act places a number of duties on us that we must fulfil when exercising the regulatory powers and functions we have been given.

A5.4 Section 3(1) of the Act states that it shall be our principal duty, in carrying out our functions:

- to further the interests of citizens in relation to communication matters;[540] and
- to further the interests of consumers in relevant markets, where appropriate by promoting competition.[541]

A5.5 In performing our duties under section 3(1) of the Act, we are required to have regard to the principles under which regulatory activities should be transparent, accountable, proportionate, consistent and targeted only at cases in which action is needed, as well as any other principles appearing to us to represent best regulatory practice (section 3(3) of the Act).

A5.6 Section 3(4) of the Act provides that we must have regard, in performing our duties, to a number of matters, as they appear to us to be relevant in the circumstances, including:

- the desirability of promoting competition in relevant markets;
- the desirability of promoting and facilitating the development and use of effective forms of self-regulation (except in relation to our Online Safety functions);
- the desirability of encouraging investment and innovation in relevant markets;
- the desirability of ensuring the security and availability of public electronic communications networks and public electronic communications services;
- the vulnerability of children and of others whose circumstances appear to us to put them in need of special protection;
- the needs of persons with disabilities, of the elderly and of those on low incomes;[542]

[540] "Citizens" means all members of the public in the United Kingdom (section 3(14) of the Act).
[541] "Consumer" is defined in section 405(5) of the Act and includes people acting in their personal capacity or for the purposes of, or in connection with, a business.
[542] We also have public sector equality duties in section 149 of the Equality Act 2010. 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

- the desirability of preventing crime and disorder;
- the opinions of consumers in relevant markets and of members of the public generally;
- the different interests of persons in the different parts of the United Kingdom, of the different ethnic communities within the United Kingdom and of persons living in rural and in urban areas; and
- the extent to which, in the circumstances of the case, the furthering or securing of the matters mentioned in section 3(1) is reasonably practicable.

A5.7 In addition, section 3(5) of the Act requires that, when performing our duty to further the interests of consumers, we must have regard, in particular, to the interests of those consumers in respect of choice, price, quality of service and value for money.

A5.8 Where it appears to us that any of our general duties conflict with each other in a particular case, we must secure that the conflict is resolved in the manner we think is best in the circumstances (section 3(7) of the Act).

A5.9 Section 4(2) of the Act requires us to act in accordance with six requirements when carrying out certain functions, such as when setting conditions, which are in summary:

- to promote competition in the provision of electronic communications services, networks and associated facilities and the supply of directories;
- to promote the interests of all members of the public in the United Kingdom;
- to take account of the desirability of Ofcom carrying out of its functions in a manner which, so far as practicable, does not favour one form of or means of providing electronic communications networks, services or associated facilities over another (i.e. to be technology neutral);
- to encourage the provision of network access and service interoperability to such extent as Ofcom considers appropriate for the purposes securing efficiency and sustainable competition; efficient investment and innovation; and the maximum benefit for the persons who are customers of communications providers and of persons who make associated facilities available;
- to encourage compliance with certain standards in order to facilitate service interoperability, end-to-end connectivity, and secure freedom of choice for the customers of telecoms providers; and
- to promote connectivity and access to very high capacity networks by members of the public and businesses in the United Kingdom.

A5.10 Under section 2B(2)(a) of the Act, we are required to have regard to the UK Government's Statement of Strategic Priorities (SSP) for telecommunications, management of radio spectrum and postal services.[543]

---

minimise disadvantages suffered by people due to their protected characteristics; and take steps to meet the needs of people with protected characteristics. We have similar public sector equality duties in section 75 of the Northern Ireland Act 1998. We have set out our equality impact assessment in Annex 3.

[543] DSIT, Statement of Strategic Priorities for telecommunications, the management of radio spectrum, and postal services, 2026. We note, in particular, that Strategic Priority 2 states that "Ofcom should continue to use its levers to identify and address the vulnerabilities in telecoms networks that are exploited by criminals to scam consumers".

A5.11 Under section 108 of the Deregulation Act 2015, we are required to have regard to the importance of promoting economic growth. In order to consider the promotion of economic growth, Ofcom will exercise its regulatory functions in a way that ensures that: a) regulatory action is taken only when it is needed; and b) any action taken is proportionate. The government's statutory guidance on this duty recognises a well-protected and healthy population and environment leads to higher productivity and growth, and therefore in many cases there is no tension between a regulator's protection duties and the growth duty.[544]

A5.12 Lastly, we are also required under Article 36(4) of the UK General Data Protection Regulation to consult the Information Commissioner's Office on proposals that relate to the processing of personal data.

Our duties relating to telephone numbers

A5.13 Ofcom has a general duty under section 63 of the Act in carrying out its telephone numbering functions to, among other things:

a) secure that what appears to us to be the best use is made of the numbers that are appropriate for use as telephone numbers; and
b) encourage efficiency and innovation for that purpose (section 63(1) of the Act).

A5.14 It is also our duty, in carrying out our numbering functions, to secure that there is no undue discrimination by communications providers against other communications providers in relation to the adoption of telephone numbers for purposes connected with the use by one communications provider, or their customers, of an electronic communications network or electronic communications service provided by another (section 63(2) of the Act).

Our powers relating to the proposed conditions

General Conditions

A5.15 Ofcom's power to set general conditions is set out in section 45(2)(a) of the Act. A general condition may be applied generally to every person providing an electronic communications network (ECN) or electronic communications service (ECS), or to every person providing an ECN or ECS of a particular description specified in the condition (section 46(2) of the Act). Persons who provide an ECN or ECS are defined in section 405 of the Act as "communications providers" (CPs).

A5.16 Pursuant to section 45 of the Act, we are authorised to set certain general conditions (GCs), including consumer protection and numbering related GCs.

A5.17 Section 51 of the Act identifies the types of consumer protection related GCs we can impose on CPs. These include GCs making such provisions as we consider appropriate for the purpose of protecting the interests of end-users of public ECS (section 51(1)(a) of the Act). Section 51(2) includes a non-exhaustive list of the type of conditions we can impose under s. 51(1)(a) which includes the power to set GCs that:

- relate to the supply, provision or making available of goods, services or facilities in association with the provision of a public ECS (section 51(2)(a));

[544] Department for Business & Trade, 2024. Growth Duty: Statutory Guidance - Refresh.

- require the provision, free of charge, of specified information, or information of a specified kind, to end-users (section 51(2)(d)); and
- require a CP, in specified circumstances, to block access to telephone numbers or services in order to prevent fraud or misuse, and enable them to withhold fees payable to another CP in those circumstances (section 51(2)(f)).

A5.18 Public electronic communications services (as referred to in the Act) include:

- number based interpersonal communications services which are services that (i) enable direct interpersonal and interactive exchange of information by means of ECNs between a finite number of persons, where the persons initiating or participating in the communication determine its recipient; and (ii) connect with or enable communication with numbers from a national/international numbering plan (section 32(2) and (2A)(b) and 32A of the Act); and
- services consisting in, or having as their principle feature, the conveyance of signals (section 32(2) and (2A)(c) of the Act).

A5.19 Section 58 of the Act identifies the types of GCs we can impose relating to the allocation, adoption and use of telephone numbers. These include GCs which:

- regulate the use by a CP, for the purpose of providing an ECN or ECS, of telephone numbers not allocated to that provider (section 58(1)(b) of the Act);
- impose restrictions on the adoption of telephone numbers by a CP, and on other practices by CPs in relation to telephone numbers allocated to them (section 58(1)(c) of the Act);
- impose requirements on a CP in connection with the adoption[545] by him of telephone numbers (section 58(1)(d) of the Act);
- require CPs to secure compliance with such rules relating to the use of telephone numbers by their customers as we may set out in GCs or determine in accordance with provisions made by the GCs (section 58(1)(i) of the Act).

Conditions imposed on non-providers

A5.20 Pursuant to section 59 of the Act, Ofcom also has the power to impose conditions on persons other than communications providers ('non-providers') in relation to the allocation of telephone numbers to those persons, the transfer of allocations to and from those persons, and the use of telephone numbers by those persons. These conditions are referred to as Numbering Conditions Binding Non-Providers.

[545] Section 56(6) of the Act explains that adoption of a telephone number by a CP are references to his doing any of the following in relation to a number allocated (whether or not to that provider) by Ofcom: (a) allocating or transferring that number to a particular customer or piece of apparatus; (b) using that number for identifying a service or route used by that provider or by any of his customers; (c) using that number for identifying a communication as one to be transmitted by that provider; (d) designating that number for use in selecting a service or the required elements or characteristics of a service; or (e) authorising the use of that number by others for any of the following purposes identified in section 56(5) of the Act: identifying the destination for, or recipient of, an electronic communication; identifying the origin, or sender, of an electronic communication; identifying the route for an electronic communication; identifying the source from which an electronic communication or electronic communications service may be obtained or accessed; selecting the service that is to be obtained or accessed, or required elements or characteristics of that service; or identifying the communications provider by means of whose network or service an electronic communication is to be transmitted, or treated as transmitted.

A5.21 The conditions that may be set include conditions imposing obligations corresponding to any of the obligations that may be imposed on communications providers by General Conditions making provision for, in connection with: the allocation of telephone numbers; the transfer of allocations; or the use of telephone numbers.

A5.22 A person who is not a communications provider, but applies for the allocation of a telephone number, or is allocated such a number, including through sub-allocation under the General Conditions, has a duty to comply with any conditions set under section 59 of the Act.

Legal tests for setting conditions

A5.23 Section 47(2) of the Act governs the circumstances in which we can set general conditions and Numbering Conditions Binding Non-Providers. It states that a condition can be set where the condition is:

a) not such as to discriminate unduly against particular persons or against a particular description of persons;
b) proportionate to what the condition or modification is intended to achieve; and
c) in relation to what it is intended to achieve, transparent.

A5.24 We are required under section 48A(3) of the Act to publish a notification:

a) stating that we are proposing to set the relevant conditions;
b) setting out the effect of those conditions;
c) giving our reasons for making the proposal; and
d) specifying the period within which representations may be made to Ofcom about our proposal.

A5.25 Sections 47 to 49 of the Act apply in relation to the setting of conditions under section 59 relating to non-providers and the modification and revocation of such conditions as they apply in the case of general conditions.[546]

A5.26 In accordance with section 48 of the Act, we have today published notifications of our decision to set General Conditions and Non-Provider Conditions set out in Annexes 1 and 2.

Impact assessments

A5.27 Annex 3 of this consultation identifies the relevant legal provisions relating to impact assessments, including under section 7 of the Act, section 149 of the Equality Act 2010 and section 75 of the Northern Ireland Act 1998. Annex 4 sets out our rights assessment including the relevant legal provisions under Article 8 and 10 ECHR.

[546] Section 59(4) of the Act

A6. Accompanying guidance

A6.1 Our accompanying guidance for Communications Providers can be found here.