Proposed guidance for providers on protections from scam mobile messages

Annex 10

Guidance

Published 29 October 2025

Contents

Section

This guidance, as well as the final text of any General Conditions and Non-Provider Conditions, is subject to our final decision, following our consultation process.

1. Overview

1.1 Scammers use mobile messaging services to reach victims at a mass scale and manipulate them into making payments or sharing sensitive information - often alongside scam phone calls, online messages, social media posts, paid-for adverts or emails. This activity causes significant financial and emotional harm to UK people and businesses and reduces their confidence in using communications services.

1.2 Ofcom has introduced rules to reduce the risk that people and businesses receive Person-to-Person (P2P) and Application-to-Person (A2P) scam messages (General Condition (GC) C.9 and Non-Provider Condition 3). The measures required under these rules are intended, in the round, to stop scammers from accessing mobile messaging services in the first place and, where they have gained access, to stop their activity.

1.3 This document constitutes guidance to assist mobile operators and aggregators comply with the requirements of GC C9 and Non-Provider Condition 3.

1.4 We will keep our guidance under review and will update it periodically as considered appropriate. Whether we consult on an updated version of this guidance will depend on the nature of the update; for example, we may not consult on changes that only update the guidance to identify new duties or amend references to legislation.

Introduction and background

1.5 Protecting consumers from harm is a priority for Ofcom and we remain concerned about harms from scams facilitated by calls and mobile messages. Ofcom has powers under the Communications Act 2003 (the Act) to ensure that telecoms services, such as mobile messaging services, are used effectively and efficiently and are not misused, for example to facilitate fraud or scams.

1.6 We have introduced measures to make it more difficult for scammers to use UK telecoms networks. These include rules for providers on their use of numbers[1] and on the provision of Calling Line Identification (CLI) facilities.[2]

1.7 We have also issued guidance setting out the measures we expect providers to take to comply with our rules, including:

- Guidance to help providers identify and block numbers that are associated with known organisations and that are never intended to make outbound calls.3 We record these numbers in the Do Not Originate list.[4]
- Guidance on the provision of CLI facilities and other related services.[5]
- Guidance clarifying the type of due diligence that UK providers should carry out when suballocating numbers to other providers.[6]

[1] GC B.1. Ofcom, General Conditions of Entitlement.
[2] GC C.6. Ofcom, General Conditions of Entitlement.
[3] Ofcom, 2022. Submitting numbers to the 'Do Not Originate' list: Guide for organisations.
[4] Ofcom, 2023. Do Not Originate List.
[5] Ofcom, 2022. Guidance on the provision of Calling Line Identification facilities and other related services
[6] Ofcom, 2022. Good practice to help prevent misuse of sub-allocated and assigned numbers.

- Guidance setting out the steps that providers are expected to take to identify calls from abroad that spoof UK landline Network Numbers and block them.[7]

1.8 We have monitored the evidence of harm from scam mobile messages and the implementation of industry-led initiatives to combat them.

1.9 [To summarise final decisions set out in our Statement.]

Regulatory framework

1.10 GC C9 and Non-Provider Condition 3 require providers to have systems and processes in place to help protect end-users from harms associated with scam mobile messages. These Conditions set out the minimum measures that providers must take; providers may also take additional measures beyond those set out in the Conditions or in this guidance to protect end-users from scam mobile messages.

1.11 The relevant GCs are set out in full in Section 2 below. Where relevant, we also identify the corresponding Non-Provider Condition.

1.12 Section 3 below explains the range of powers we have to take enforcement action in the event of a breach of our GCs (including GC C9) or Non-Provider Condition 3.

1.13 This guidance document includes a number of defined terms that readers may not be familiar with. These terms are set out in the consolidated GCs (or Non-Provider Conditions) and some are used in this document for ease of reference.

The purpose of this guidance

1.14 This document provides guidance on 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 Non-Provider Condition 3.

1.15 We expect to take this guidance into account when deciding whether to open an investigation into a provider relating to the implementation and ongoing operation of their anti-scam measures for mobile messaging services and, if so, the type of action that may be appropriate.

1.16 The steps set out and the examples presented in this guidance are not exhaustive. We expect the guidance to be used as a framework for how we might interpret the steps providers take to comply with GC C9 and Non-Provider Condition 3. We expect providers to take the steps that are reasonable and proportionate for their circumstances. Providers should record the steps they take to comply with GC C9 and Non-Provider Condition 3, including any reasons why they may have considered it appropriate to depart from this guidance.

1.17 In using this guidance, providers will also need to ensure they comply with their obligations under relevant data protection legislation and the Investigatory Powers Act 2016. Relevant data protection legislation is discussed in more detail in paragraphs 2.164-2.174 below.

[7] Ofcom, 2022. Tackling scam calls.

Who this guidance applies to

1.18 This guidance applies to providers involved in P2P and A2P messaging, as specified in GC C9 and Non-Provider Condition 3. The rules providers will need to comply with are specific to the channels over which mobile messages are sent and the provider's role in the delivery of mobile messages.

1.19 GC C9 and Non-Provider Condition 3 refer to providers within the scope of the specific Conditions as "Regulated Providers". In this guidance, we explain the type of providers each Condition applies to and then refer to "Regulated Providers" as "providers" for ease of reference. Depending on the context, providers within the scope of individual Conditions include:

- Mobile network operators (MNOs).[8]
- Mobile operators meaning MNOs and different types of Mobile Virtual Network Operators (MVNOs)[9], including 'thick' and 'thin' MVNOs.[10]
- Aggregators.[11]
- Tier 1 aggregators meaning aggregators that contract to pass traffic directly to an MNO.

1.20 We use the word "provider" to refer to both:

- Operators that are a "Communications Provider" within the scope of GC C9, as defined in the GCs as meaning "a person who (within the meaning of section 32(4) of the Act) provides an electronic communications network or an electronic communications service".
- Other operators that have access to numbers through their number allocations which, for whatever reason, may not be considered a "Communications Provider" within the scope of GC C9 in a specific context but which are within the scope of Non-Provider Condition 3.

1.21 Table 1 summarises the main requirements set out in [*proposed*] GC C9 and to whom they would apply.

Table 1: The [proposed] requirements and to whom they would apply

Intervention phase	Proposed requirements	Proposed to apply to
P2P mobile messaging		
Intelligence gathering	Have processes to receive scam reports, from customers and third parties, relating to telephone numbers and URLs that are being used for scams	Mobile operators

[8] A mobile provider that owns its own mobile network.
[9] A mobile provider that does not own the wireless network infrastructure over which it provides mobile services to its customers.
[10] 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.
[11] Aggregators contract with Business Sender, Messaging Service Providers and other aggregators to arrange for the delivery of large volumes of A2P Messages.

Intervention phase	Proposed requirements	Proposed to apply to
Restrictive measures	Volume limits for Pay As You Go customers. Identify and prevent mobile numbers they have assigned and reasonably believe to have sent scam messages from sending further messages.	Mobile operators
In-transit measures	Identify and block messages sent from telephone numbers reasonably believed to have sent scam messages. Identify and block messages reasonably believed to contain known scam URLs and telephone numbers by automated means. Review and record impact of identifying and blocking measures.	Mobile operators.
A2P mobile messaging		
Intelligence gathering	Have processes to receive scam reports, from customers and third parties, relating to telephone numbers and URLs that are being used for scams	Mobile operators and tier 1 aggregators.
Up-front due diligence requirements	Know Your Customer checks for new senders	Mobile operators and aggregators
	Prevent the use of fake alphanumeric sender IDs	Mobile operators and aggregators
	Have policies on protected IDs, generic IDs and special alphanumeric characters.	Mobile operators
Requirements for ongoing checks	Know Your Traffic checks	Mobile operators and aggregators
	Identify and block messages reasonably believed to contain known scam URLs and numbers by automated means	Mobile operators and tier 1 aggregators.
Incident management requirements	Quickly block messages from senders identified as scammers	Mobile operators and aggregators

2. The Guidance

Structure of this section

2.1 This section sets out guidance for providers to comply with protections for end-users from scam mobile messages under GC C.9. Where relevant we also identify the corresponding rule in Non-Provider Condition 3. The guidance covers how providers may meet their obligations to:

- Block suspicious numbers and messages and apply volume limits to address P2P messaging scams.
- Block suspicious messages and implement robust due diligence and incident management processes to prevent misuse of A2P services.
- Comply with several cross-cutting measures, including a right to challenge blocking decisions and requirements to keep operations under review, train staff, ensure good record keeping, comply with relevant data protection rules and ensure the continued transmission of legitimate messages.

Guidance to address P2P scam messages

2.2 Below we describe how mobile operators can comply with the obligations under GCs C9.2 to C9.5 to address P2P scams.

Receiving scam reports in relation to P2P scam messages

C9.2 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.

Who this obligation applies to

2.3 GC C9.2 applies to providers of Mobile Communications Services that transfer and/or terminate P2P Messages. This includes all mobile operators (MNOs and MVNOs).

Purpose of receiving scam reports

2.4 The purpose of receiving scam reports is to strengthen mobile operators' ability to detect scam messages, based on Sender IDs, URLs and phone numbers. By requiring mobile operators to implement robust systems for receiving scam reports from end-users and third parties, our rules should ensure they have timely access to relevant information. The ultimate goal of this requirement is to support the targeted, intelligence-led blocking of scam numbers and messages, as set out at GC C9.3.

Sources and mechanisms for receiving scam reports

2.5 Mobile operators are required to implement and maintain appropriate and effective policies, systems and processes to receive reports of scams from end-users and third parties on:

- Telephone Numbers (including Mobile Numbers and Sender IDs) that have been reported as sending P2P Messages intended to scam the recipients.
- URLs and telephone numbers that have been reported as being used as part of scam, including URLs and telephone numbers included in P2P Messages.

2.6 We expect mobile operators to implement adequate mechanisms to allow their own customers to report suspected scam messages, for example by ensuring customers can:

- Easily forward, or use reporting functionality built in to messaging applications, to report a suspected scam message to their own provider, or a reliable third party such as the 7726 service, that is then responsible for collating scam messages and providing the collected intelligence back to the customer's provider; and/or
- Access an internet web page form or email account that is regularly checked and allows them to report a suspected scam message.

2.7 We also expect mobile operators to offer advice to their customers on how they can report suspected scams if they receive them. This could be done by publishing information on their customer facing websites (e.g. Q&As) and/or ensuring that customer service operatives are trained to provide appropriate advice on how to report messaging scams.

2.8 We do not consider that having only a mechanism for enabling a mobile operator's own customers to report scams to be sufficient to comply with GC C9.2. Mobile operators should therefore also establish and maintain processes to use reports from third parties with expertise in identifying scams. This will enable mobile operators to act on scam reports that have been generated from users of other mobile operators, as well as their own.

2.9 Mobile operators are expected to obtain intelligence on scams from a range of sources that is not limited to scams that may have arisen in P2P Messages.

2.10 These sources could include:

- Consumer reports included in the 7726 database, which include scam reports from multiple mobile operators.
- Cyber Defence Alliance data, such as on scam URLs.
- The Global Signal Exchange.
- Cifas services (such as its National Fraud Database).

Tailoring intelligence requirements to a mobile operator's identifying and blocking capabilities

2.11 The type and extent of scam reports it may be appropriate to gather may depend on the type of provider. For example, thin MVNOs that rely on an MNO to block messages in transit are unlikely to need to obtain intelligence relating to scam URLs and telephone numbers included in the contents of a message. They would only likely need to use information under C9.2(a), i.e. Sender IDs that can be used for blocking numbers.

Scrutiny and validation of scam reports

2.12 Mobile operators must have a reasonable belief the numbers or messages identified in scam reports were intended for scam purposes when using information for the purposes of GC C9.3. Mobile operators should therefore undertake an appropriate level of validation of the information included in the scam reports.

2.13 To ensure responsible and effective use of scam reports, mobile operators are expected to take into account the following principles:

- Consent-based review: when using existing messages as a basis to inform scam reports, only use messages that have been reported by recipients, thereby indicating their agreement for the content to be reviewed for scam prevention purposes.
- Trusted intelligence sources: accept intelligence from third parties with proven expertise in identifying or aggregating scam-related data, provided they have a legitimate basis for doing so.
- Timeliness and automation: ensure that intelligence is current and robust, ideally gathered through automated systems that are regularly updated to reflect real-time developments in scam tactics.
- Validation and risk mitigation: use contextual testing and evaluation to verify the data's accuracy and minimise any 'false positives' (i.e. where legitimate messages may be identified as a scam) and refine the data before it is used to take action (as discussed in the paragraphs below).

2.14 Whether it may be appropriate to interrogate and validate scam reports (and the extent of that interrogation and validation) is likely to depend on the source and type of dataset underlying the intelligence. For example, reports based on 7726 data may contain incorrectly reported messages that are not actually a scam, including messages that may be commercial marketing or spam or that the end-user did not otherwise want to receive. Mobile operators are expected to interrogate such reports to filter out messages that they do not reasonably believe were intended to scam the recipients.

2.15 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. Depending on the type of scam report a provider is using, it may therefore be possible to presume it is valid without further interrogation.

2.16 Taking the steps set out in paragraphs 2.177-2.179 below in relation to the requirement to ensure the transmission of legitimate messages may help providers validate scam reports.

2.17 Providers may also 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.

Sharing scam reports with other providers and third parties

2.18 Sharing intelligence with other mobile operators and third parties can strengthen the quality and timeliness of intelligence. Sharing data helps to build a more robust and up-to-date understanding of scam activity. When relying solely on reports from customers on a single network, there is a risk of operating within an incomplete picture. In contrast, pooling

reports from customers across multiple providers is likely to create a more comprehensive and accurate dataset.

2.19 We therefore encourage mobile operators to establish intelligence sharing mechanisms for the purpose of significantly reducing the likelihood that consumers receive scam messages. Appropriate safeguards should be in place to ensure compliance with relevant data protection legislation and competition law. Examples of such safeguards include:

- Taking into account Information Commissioner's Office (ICO) guidance on how to comply with relevant data protection legislation.[12]
- Where possible, anonymising or removing any information that may identify the intended recipient.
- Sharing the minimum amount of information necessary for the specific purpose of significantly reducing the likelihood that consumers receive scam messages.
- Implementing internal confidentiality safeguards to ring-fence any information that is provided and ensure it is only provided to authorised individuals on a strictly need-to-know basis.

2.20 We note that the ICO's guidance on sharing personal information when investigation scams and fraud states that:

> "Effective data sharing between organisations and across different digital sectors is an important factor in preventing data-enabled scams and fraud.
>
> The UK GDPR and the Data Protection Act 2018 (DPA) do not prevent you from sharing personal information where it is appropriate to do so, or from taking steps to prevent harm."[13]

> "We are calling on organisations to share personal information responsibly to protect their customers from scams and fraud …
>
> We're warning that reluctance from organisations to share personal information to tackle scams and fraud can lead to serious emotional and financial harm.
>
> Data protection law does not prevent organisations from sharing personal information, if they do so in a responsible, fair and proportionate way."[14]

[12] See ICO, Sharing personal information when preventing, detecting and investigating scams and frauds [accessed on 24 October 2025]
[13] See ICO, Sharing personal information when preventing, detecting and investigating scams and frauds [accessed on 24 October 2025]
[14] ICO, Data protection is not an excuse when tackling scams and fraud [accessed on 24 October 2025]

Preventing P2P scam messages from being sent 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.

Who this obligation applies to

2.21 GC C9.3 applies to providers of Mobile Communications Services that transfer and/or terminate P2P Messages. This includes all mobile operators. In practice, we would expect MNOs and *thick* MVNOs to carry out any blocking under GC C9.3(b) and GC C9.3(c) but *thin* MVNOs would be required to ensure that their host MNO undertakes the required blocking on their behalf.

Purpose of scam blocking measures

2.22 The purpose of these measures is to ensure a more consistent and effective approach to number and message blocking across industry. These requirements set out that numbers should be blocked from sending messages, and messages should be blocked in transit, where it is reasonable to believe that they are being used/sent by scammers.

Blocking numbers used by scammers

2.23 Taking into account scam reports received (including in accordance with GC C9.2 and, where applicable, GC C9.6), mobile operators must implement and maintain appropriate and effective policies, systems and processes designed to 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.

2.24 We expect all mobile operators can comply with this obligation by feeding validated scam report information into existing fraud management systems to identify numbers that are suspected of sending scams and take appropriate steps to block them from sending further messages.

2.25 This requirement does not require mobile operators to scan message content before deciding to block a number.

Identifying and blocking scam messages in transit

2.26 Taking into account scam reports received (including in accordance with GC C9.2 and, where applicable, GC C9.6), mobile operators must implement and maintain appropriate and effective policies, systems and processes designed to:

- 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
- Block, via automated means and without undue delay, P2P Messages that contain URLs or telephone numbers which they reasonably believe were used part of a scam.

2.27 The obligation in GC C9.2(c) requires mobile operators to use automated tools to examine specific message content where necessary (i.e. URLs or phone numbers in messages). We are not recommending the use of a specific technology to do this and providers may adopt different tools to comply. For example, providers may decide to adopt tools that compare the content of messages against a database.

2.28 Mobile operators are expected to consider whether other indicators of malicious activity can be used to block messages before message contents are reviewed. For example, where a source Sender ID or Global Title15 is present in an internal blocklist, these should be used to block the message before the message content is analysed for policy violations. This can be achieved by appropriately ordering the application of firewall rules, where rules that examine message content are applied last.

2.29 We recognise that some degree of human review of messages is likely to be necessary to ensure automated tools are working as intended. This is not prohibited by our rules.

2.30 Mobile operators will also need to comply with relevant data protection legislation and take appropriate steps to ensure the continued transmission of legitimate messages (see paragraphs 2.164-2.179 below).

2.31 We recognise that some mobile operators 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 e.g. by tracking preset message volume and velocity thresholds that could flag suspicious behaviour. This form of monitoring is not required or prevented by our rules. We note that it is likely to be considered more intrusive and mobile operators should therefore ensure they comply with relevant data protection legislation.

P2P volume limits

C9.4 Regulated Providers must implement and maintain appropriate and effective policies, systems and processes setting limits on the volume of messages that their Pay As You Go Customers can send from a specific Mobile Number, in a specified period, to more than one 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 where that Pay As You Go

[15] 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.

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.

Who this obligation applies to

2.32 GC C9.4 and C9.5 apply to providers of Mobile Communications Services that transfer and/or terminate P2P Messages. This includes all mobile operators (MNOs and MVNOs).

The purpose of volume limit measures

2.33 The use of volume limits is intended to disrupt messaging scams by preventing scammers from sending large volumes of messages to different mobile numbers quickly and easily. By making bulk messaging via Pay As You Go SIMs more difficult and costly, these limits aim to reduce the number of scam mobile messages reaching consumers.

Setting a policy on volume limits

2.34 Mobile operators must implement and maintain appropriate and effective policies, systems and processes setting limits on the volume of messages that their Pay As You Go customers can send from a specific mobile number in a specified period to more than one mobile number, with the objective of preventing scam messages from being sent and/or received. The obligation to apply volume limits applies to Pay as You Go customers using any type of SIM, including SIMs made available or obtained electronically (eSIMs).

2.35 Under this obligation, a mobile operator can determine the details of its own volume limit policy. The policy may also differ depending on the particular product or service.

2.36 In considering what volume limit may be appropriate in any given circumstance, we would expect mobile operators to take into account:

- The volume and frequency of messages that a scammer might be expected to send.
- Whether it is likely to be more effective to impose strong limits for an initial period after a SIM is first used for messaging, if past trends suggest that scammers tend to send most of their messages shortly after a SIM is first acquired or activated.
- Typical use by legitimate users on the mobile operator's network, taking into account the type of customers the provider has and past use patterns.
- Whether hourly, daily, weekly or monthly volume limits are the most appropriate.
- Whether it is necessary to reset limits in light of the right to challenge process that providers must implement under GCs C18-19.

2.37 When considering the factors above, mobile operators may wish to consider industry-wide intelligence based on previous scamming campaigns, as well as its own intelligence based on previous scams identified on its network.

2.38 Once mobile operators have decided on an appropriate volume limit policy, they must record that limit in an internal policy. We discuss record keeping further below at paragraphs 2.156-2.162.

2.39 To ensure volume limits remain effective and do not interfere with legitimate use, mobile operators will also be expected to regularly review and assess the impact of their volume limits. This includes keeping any period after which a volume limit is reset under close

review and revising it if it becomes clear that setting the caps in such a way is not effective in preventing use by scammers. We discuss obligations relating to the review of anti-scam measures further below at paragraphs 2.142-2.150.

Implementing a block when the limit has been reached

2.40 Mobile operators must block, via automated means and without undue delay, Pay As You Go customers from sending any further P2P Messages where that Pay As You Go customer reaches any volume limit imposed by the mobile operator in line with the policy it has implemented under GC C9.4.

2.41 We expect mobile operators can comply with this obligation by configuring their existing fraud management systems to stop further messages from being sent after the volume limit has been reached.

2.42 We expect mobile operators to send a message to the SIM that has been blocked, explaining that the limit has been reached and will not be able to send further messages. We discuss mobile operators' obligations relating to a customer's right to challenge further below in paragraphs 2.135-2.141.

Guidance to address A2P scam messages

2.43 This sub-section describes how mobile operators and aggregators can comply with the requirements under GCs C9.6 to C9.16.

Processes for receiving A2P scam reports

C9.6[16]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 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.

Who this obligation applies to

2.44 GC C9.6 applies to any Communications Provider that transfers and/or terminates A2P Messages, except a Lower-Tier Aggregator. This includes mobile operators that enable A2P termination to their customers (whether they are an MNO or MVNO) and tier 1 aggregators. Aggregators that do not contract to pass traffic directly to a mobile operator will not need to comply with this Condition.

Purpose of receiving scam reports

2.45 The purpose of having processes to receive scam reports is to facilitate the ability of mobile operators and tier 1 aggregators to detect and block scam messages from reaching end-users (see paragraph 2.4 above).

[16] Non-Provider Condition 3.2 corresponds to GC C9.6.

Sources and mechanisms for receiving scam reports

2.46 Mobile operators and tier 1 aggregators 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 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.

2.47 The guidance we have set out at paragraphs 2.5 to 2.20 on how providers can meet their obligations under GC C9.2 is also applicable to A2P Messages. Providers are expected to obtain intelligence on scams from a range of sources that is not limited to scams that may have arisen in A2P Messages. They are also expected to source scam reports that have been generated from customers of other providers and trusted third parties, which could include:

- Reports included in the 7726 database.
- The Cyber Defence Alliance.
- The Global Signal Exchange.
- Cifas services (such as its National Fraud Database).

2.48 In addition, we would expect tier 1 aggregators to have arrangements in place with terminating providers to receive intelligence from terminating mobile operators.

Scrutiny and validation of scam reports

2.49 Providers must have a reasonable belief the numbers or messages identified in scam reports were intended for scam purposes when using information for the purposes of GC C9.7. Providers should therefore undertake an appropriate level of validation of the information included in the scam reports. We expect providers to adhere to the principles of consent-based reviews, using trusted intelligence sources, timeliness and automation and validation and risk mitigation, set out above in paragraph 2.13.

Sharing scam reports between different providers

2.50 As explained in paragraph 2.18 above, providers can strengthen the quality and timeliness of their intelligence by sharing intelligence with other providers and third parties. Sharing data helps each provider build a more robust and up-to-date understanding of scam activity. When providers rely solely on reports from their own customers, they risk working with an incomplete picture. In contrast, pooling reports from customers across all providers creates a more comprehensive and accurate dataset.

2.51 We therefore encourage 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. Examples of such safeguards are set out at paragraph 2.19 above.

Preventing A2P scam messages from being sent or received

C9.7[17]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.

Who this obligation applies to

2.52 GC C9.7 applies to any Communications Provider that transfers and/or terminates A2P Messages, except Lower-Tier Aggregators. This includes mobile operators that enable A2P termination to their customers (whether they are an MNO or MVNO) and tier 1 aggregators. Aggregators that do not contract to pass traffic directly to a mobile operator will not need to comply with this Condition.

Purpose of this requirement

2.53 The purpose of this measure is to ensure a more consistent and effective approach to message blocking across the sector. We expect providers to detect and block messages already in transit, that contain URLs or telephone numbers they reasonably believe have been used by scammers to facilitate scams.

Identifying and blocking scam messages in transit

2.54 Taking into account scam reports received (including in accordance with GC C9.6 and, where applicable, GC C9.2), 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 that they reasonably believe were used as part of a scam.

2.55 The guidance set out at paragraphs 2.26 to 2.31 above on how providers can meet the equivalent obligations in GC C9.3 in relation to P2P Messages is also applicable here.

2.56 In specific circumstances, an appropriate and effective policy may allow for A2P Messages from a limited number of Business Senders to not be subject to a provider's general identifying and blocking measures that are applied to other A2P Messages, provided certain conditions are met. This may be appropriate where, at a minimum:

- The provider has a direct and robustly verified relationship with a major Business Sender that it has established has a very low risk of fraud or has robustly verified that such a Business Sender has given permission for specified aggregators to use its alphanumeric Sender ID exclusively.
- The provider keeps appropriate records explaining why it considers it appropriate to take this approach for a specific Business Sender and why it considers its approach remains effective at blocking messages with scam URLs or telephone numbers.
- The provider keeps this process under regular review, including by monitoring scam reports and carrying out KYT checks for any indicators that the relevant Business Sender

[17] Non-Provider Condition 3.3 corresponds to GC C9.7.

poses a risk of sending scam messages or that the messages sent by the relevant Business Sender may be part of a scam.

Due diligence and on-going checks

C9.8[18] 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).

Who these obligations apply to

2.57 GCs C9.8 to C9.12 apply to any Communications Provider that transfers and/or terminates A2P Messages, including all Aggregators. This includes mobile operators and aggregators (whether they are acting at tier 1 or at lower tiers).

Purpose of these requirements

2.58 These requirements are designed to ensure that appropriate checks are carried out on A2P Business Senders and message traffic and that messages are prevented from being transferred and/or terminated if these checks have not been satisfactorily carried out by the provider or a person in their downstream chain.

2.59 Different parties in the chain of providers involved in the delivery of A2P Messages can take different actions to ensure these checks take place. The requirements recognise this by allowing providers to either carry out the required checks themselves, or satisfy themselves that they have been done via clear and unambiguous contractual terms with any party from which they receive messages.

Know Your Customer (KYC) checks

C9.10[19]The 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;

[18] Non-Provider Condition 3.4 corresponds to GC C9.8. Related GCs C9.9 to C9.12 are set out further below.
[19] Non-Provider Condition 3.6 corresponds to GC C9.10.

(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 carrying out such checks.

Purpose of this requirement

2.60 This requirement sets out the minimum KYC checks that must be conducted, but providers are welcome to take further measures they consider appropriate.

KYC checks

2.61 As part of assessing the risk of scams posed by new Business Senders, providers will need to know on whose behalf they are agreeing to convey messages. When onboarding new Business Senders directly, GC C9.8(a) requires providers to perform KYC checks. Where providers are not onboarding the Business Sender directly, they should take steps (set out at C9.9) to ensure that the downstream party that is onboarding the Business Sender conducts equivalent checks.

2.62 If, instead of directly onboarding a new Business Sender, the provider receives A2P Messages from another party, such as an aggregator or a Messaging Service Provider (MSP)[20], they must implement clear and unambiguous contractual terms with that party to ensure that equivalent checks take place. See guidance on this point below at paragraph 2.89.

2.63 As part of these checks, we require providers to collect and assess a range of information to inform a documented risk assessment relating to the Business Sender for any indication that the Business Sender poses a risk of sending scam messages. At a minimum, providers need to collect and assess the following information:

- Trading or registered names.
- Registered office or trading address.
- Nature of the service being provided by the business or organisation.
- Payment information.
- Existing telephone numbers and websites.
- Directors and persons of significant control (taking into account Companies House guidance).[21]
- Contact details of the senior individual with responsibility for authorising the messages.

[20] Companies that specialise in interfacing directly with Business Senders. MSPs often provide an Application Programming Interface that enables Business Senders to access different messaging services online and may generate messages on the Business Sender's behalf.

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

2.64 We also expect providers to verify that any information they receive about the Business Sender corresponds with information available publicly about the Business Sender. As part of collecting information on the nature of the Business Sender's business, providers must enquire about the type of message campaigns the Business Sender expects to use A2P messaging services for. This information can then be used to help corroborate the legitimacy of alphanumeric Sender IDs (see paragraphs 2.70-2.77 below) and target future KYT checks (see paragraphs 2.78-2.88).

2.65 The risk assessment should highlight whether any of the information that has been assessed contains an indication that the Business Sender poses a risk of sending scam messages. One or more of the following may be considered risk indicators:

- Inaccurate, vague or otherwise unclear information provided about the intended use of A2P messaging: for example, the intended use may not match the nature of the business or organisation.
- Incorrect or incomplete information (such as address information).
- Adverse information from a public database, such as the Cifas National Fraud and Insider Threat databases or the Financial Conduct Authority's (FCA's) list of unauthorised firms and individuals.
- Not using a UK IP address where the business purports to be based in the UK.
- Signing up outside of business hours (scammers may try to access providers' services outside of business hours to circumvent checks).
- Name, address, postcode, IP address, or other information matching a disabled or dormant account with the provider.
- The same email address being used to open multiple accounts.
- Use of a generic, non-business email address.
- Use of a virtual private network.

2.66 If the risk assessment identifies one or more risk indicators, the provider must:

- Cancel the onboarding of the sender; or
- Carry out enhanced checks on the sender to further inform the risk assessment and satisfy itself that the risk of scam activity is low.

2.67 Examples of enhanced checks include:

- Checking the Companies House register to confirm:
  - whether important information about the business has recently changed;
  - whether a person acting as a director of the business has been disqualified;
  - the key details of all individuals with influence over the business, including owners and directors;
  - the details of all individuals who receive any share of the revenue generated by the Business Sender; and
  - the names and details of any parent or ultimate holding company of the Business Sender.
- Asking for undertakings from the Business Sender that no other party is operating in the capacity of a shadow director, as defined under the Companies Act 2006.

- Checking against the Cifas National Fraud and Insider Threat databases that the business, or associated individuals are not registered.
- Checking against the FCA's Financial Services Register that the Business Sender and individuals the provider is dealing with have permission to carry out regulated financial activities, if relevant.[22]
- Checking against the list maintained on Ofcom's website of individuals and companies that have faced sanctions from what was the Phone-paid Services Authority (PSA) and its predecessors.[23]
- Checking if the Business Sender has links to any other active accounts or previously blocked accounts with the provider.
- Verifying details of the place of business, including ensuring the geographic location of the place of business matches the information provided by the Business Sender.
- Checking the Individual Insolvency Register to see if individuals with influence, including owners and directors, have gone bankrupt or signed an agreement to deal with their debts.
- Checking relevant industry registrations e.g. FCA firm reference number.

2.68 As set out at paragraph 2.51 above, we encourage mobile operators and aggregators to establish intelligence sharing mechanisms where there have been reports that the customer may have been involved in previous scam activity. We do not expect potential customers to be onboarded if the provider has credible evidence that the potential customer has previously been involved in scam activity or similar.

2.69 Records of risk assessments and evidence of checks must be retained for a period of at least three years after the end of the contractual relationship (as set out in table 3, below).

Checks on use of new alphanumeric Sender IDs

C9.11[24] 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.

The purpose of this requirement

2.70 Providers may offer Business Senders the option of sending messages that bear an alphanumeric Sender ID rather than a telephone number or short codes. This option is

[22] FCA, The Financial Services Register

[23] Ofcom, Complying with article 16 of the PRS Order. Ofcom is now responsible for enforcement with regard to Premium Rate Services.

[24] Non-Provider Condition 3.7 corresponds to GC C9.11.

attractive to legitimate senders, but scammers can also abuse them to impersonate trusted organisations and deceive mobile customers.

2.71 This requirement is designed to prevent scammers from using alphanumeric Sender IDs to support their efforts to trick potential victims. It is both an up-front requirement and an ongoing one, which we expect to be applied each time a new alphanumeric Sender ID is allocated. As well as preventing scammers from using alphanumeric Sender IDs, this requirement should also help providers to identify scammers.

Alphanumeric Sender ID checks

2.72 Use of an alphanumeric Sender ID may be requested when the Business Sender signs up to use the service, or after this point if they wish to use new alphanumeric IDs. Where a new alphanumeric Sender ID is requested, providers must review the request (and information obtained) to ensure it does not indicate that the Business Sender poses a risk of sending scam messages or breaching any relevant policies of terminating mobile operators in place relating to alphanumeric Sender IDs.

2.73 Providers must verify that the alphanumeric Sender ID a Business Sender is requesting to use aligns with the information provided by the sender during KYC checks. In particular, we would expect providers to use this information to verify to a high degree of confidence that the sender is authorised to represent themselves using business or brand names they may request to use in alphanumeric IDs. We would not expect a provider to allow a sender to use a brand name that they are not authorised to use to represent themselves.

2.74 Providers must also not allow a Business Sender to use an alphanumeric ID for any new use that is not consistent with the purpose for which they are seeking to send A2P messages, as recorded in KYC checks.

2.75 In line with GC C9.14, providers must ensure that senders from which they receive A2P Messages are required to promptly notify them of any changes in their Business Profile or change in the use of alphanumeric Sender IDs. We therefore expect that where a sender's business model has evolved and they will be using previously approved alphanumeric Sender IDs for a different purpose, they should notify the provider of this change. Providers should, as required under GC C9.8 and GC C9.12, review this information and update the associated risk assessment accordingly.

2.76 Separately, terminating providers are required to communicate a policy on alphanumeric Sender IDs throughout their A2P supply chain (see guidance in paragraphs 2.97-2.108 below). Aggregators must review requests to use alphanumeric IDs against these policies to ensure they comply. Providers may wish to automate some of these checks where it can support quicker identification, if these checks work as intended in accordance with GC C9.20.

2.77 Below we set out two examples of scenarios where providers would need to perform alphanumeric Sender ID checks and their outcomes:

- A Business Sender called the 'Office of Communications' would like to send messages with the alphanumeric ID 'Ofcom'. Upon review of the details provided about the organisation, it is clear that 'Ofcom' is the public-facing name of the organisation, that the name does not contravene any policies put in place by the terminating provider on protected IDs and is not on any other protected lists, having been registered by another organisation. The use is approved.

- A Business Sender called 'Village Hairdresser' would like to send messages with the alphanumeric ID 'ParcelDelivery'. The recorded purpose for which the sender is accessing A2P messaging is to send one-time passcodes for users to enter as part of two factor authentication of their online account. The stated purpose does not match the request alphanumeric ID, to an extent that it may be indicative of scam activity. The use is denied and the account investigated.

Know Your Traffic (KYT) checks

C9.12[25] 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 Condition 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 that 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.

The purpose of this requirement

2.78 These requirements are designed to ensure that providers are conducting effective KYT checks on an ongoing basis, to root out scammers from A2P channels. This should help address cases where a Business Sender's account has been hijacked, or a scammer has evaded KYC checks.

2.79 GC C9.12 sets out the minimum features of KYT checks that mobile operators and aggregators must ensure are conducted and providers are therefore welcome to take further measures they consider appropriate.

KYT checks

2.80 Providers are expected to monitor a range of risk indicators. While each indicator may not individually identify a potentially high-risk Business Sender, a combination of indicators is more likely to do so. We expect that the majority of monitoring can be conducted on an automated basis, subject to providers' complying with relevant data protection legislation (see paragraphs 2.164-2.174 below).

2.81 Monitoring and reviewing data on volume patterns that could be an indicator of scam activity may include:

[25] Non-Provider Condition 3.8 corresponds to GC C9.12.

- A significant and unprecedented increase in messages sent from a single Business Sender.
- A level of use that appear inconsistent with a Business Profile provided during KYC checks.
- A new or constant stream of messages being sent, which may be inconsistent with traffic patterns associated with other legitimate uses such as for One Time Passcodes, marketing campaigns, or reminders.

2.82 When monitoring for new and different use patterns of alphanumeric Sender IDs or telephone numbers, providers could take into account whether:

- Use of a new alphanumeric Sender ID has been denied because it does not align with the business purpose or because it contravenes a terminating provider's policy on protected sender IDs.
- There has been a significant and unprecedented increase in applications from a Business Sender for alphanumeric Sender IDs or new numbers to send messages from.
- Their intelligence shows use of alphanumeric Sender IDs which appears malicious or deceptive but have not yet been added to a provider's Sender ID policy.

2.83 Providers could monitor for changes in Business Profile information provided by Business Senders that may indicate potential scam activity by checking for:

- Significant or multiple changes to information that was originally provided in accordance with KYC checks.
- New details linked to the company appearing on registers (such as the Cifas National Fraud and Insider Threat databases, the Financial Conduct Authority).
- Changes where companies have been re-domiciled (in particular where the relevant country is known to be the origin point for a high level of scam messages).

2.84 Other activity that providers can consider to improve KYT checks may include:

- Monitoring the most used Sender IDs across their traffic.
- Spot checks on end-users and on downstream aggregators, to ensure due diligence is being conducted and up-to-date.
- Regular reviews with account holders.

2.85 Providers must review and update previous risk assessments held about Business Senders that they contract with, if they encounter information relevant to that assessment in the course of undertaking KYT checks.

2.86 Where a provider encounters indicators of scam activity from a Business Sender in the course of conducting KYT checks, the provider must seek evidence that messages from that sender are legitimate. Where messages have been passed from another company that is not the Business Sender, we expect providers to engage with relevant companies in their supply chain to seek further information. Where the provider holds the direct relationship with the Business Sender, we expect them to take appropriate steps to obtain relevant information from the sender to enable the provider to satisfy itself that the messages are legitimate.

2.87 Where a provider reasonably believes, based on their review of the evidence, that the Business Sender has sent A2P Messages that were intended to scam people, they must block that sender from sending further messages.

2.88 We also encourage mobile operators and aggregators to establish intelligence sharing mechanisms - for example, through contractual requirements and/or amnesties where aggregators report fraudulent traffic - 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. We also encourage providers to share information with other companies in their supply chain on tactics of detecting and assessing potential scam activities. See paragraphs 2.18-2.20 above.

Contractual requirements

C9.9[26] 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 IDs 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 C9.22 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:

[26] Non-Provider Condition 3.5 corresponds to GC C9.9.

(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 C9.20; and

(iii) take appropriate, effective and prompt action to address any non-compliance and, if applicable, satisfy itself the party will comply going forward.

The purpose of the contractual requirements

2.89 This requirement applies where mobile operators or aggregators receive messages from other parties that are not the Business Sender (for example, where one aggregator receives messages from another, or where an aggregator receives messages from an MSP).

2.90 These requirements are designed to ensure that the required checks are carried out at the onboarding Stage, no matter which party is onboarding the Business Sender, and that appropriate incentives exist to ensure compliance. In essence, the requirement is intended to ensure that the obligation to carry out the required checks is passed down the contractual chain.

Setting clear and unambiguous terms

2.91 Where the provider is not directly involved in onboarding a Business Sender, they must set clear and unambiguous terms for the party they receive the A2P Messages from to either: undertake the KYC, alphanumeric Sender ID and KYT checks identified in GC C9.8, or ensure that these checks have been conducted by a party in the downstream chain. These terms must include provisions covering the requirements in GC C9.9(a), including to ensure that parties take action in response to reports of scam messages coming from their services and to ensure records are retained.

2.92 Providers must also require the party from which they receive the A2P Messages to either: take appropriate steps to ensure that Business Senders notify that person when there are changes to their Business Profile; or otherwise ensure that the Business Sender will notify the party in the message chain with which they have a direct relationship of such changes. We expect the end result of these requirements will be that in all instances, when information that a Business Sender has provided in KYC checks changes, the party that conducted the KYC checks will be notified and can use insights to review and update any previous risk assessments, including in accordance with GC C9.12(b).

2.93 Downstream parties can help ensure that further downstream checks have been carried out by including similar requirements in their contracts.

Ensuring compliance

2.94 Providers are required to ensure that these contractual terms are complied with on an ongoing basis. We expect this to include monitoring the activities of parties they contract with and undertaking appropriate incident management (see guidance on our incident management requirements in paragraphs 2.114-2.125 below).

2.95 Providers must take action to address non-compliance when it is identified. It is for providers to decide what strategies they employ to achieve compliance and to be able to demonstrate that they are effective. This could include imposing financial penalties under

their contracts, or placing restrictions on downstream parties' ability to convey certain types of messages.

2.96 If, after actions have been taken to address non-compliance, that non-compliance continues and the provider is not satisfied that it is being addressed, we would expect that provider to cease to accept messages from the offending party.

Setting a policy on protected alphanumeric Sender IDs

C9.13[27] 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.

Who this obligation applies to

2.97 GC C9.13 applies to any provider that terminates A2P Messages. We therefore expect it to apply to mobile operators that enable A2P termination to their customers.

The purpose of this requirement

2.98 Some types of alphanumeric Sender IDs may pose greater risk to mobile customers than others, if scammers are successful in gaining access to them. These include recognised household brands or trusted organisations. In addition to directly copying these names, scammers seek to find ways to imitate such brands (for example, replacing a letter with a number). This requirement is designed to prevent scammers from impersonating an organisation.

Setting a policy on protected alphanumeric Sender IDs

2.99 Our rules require mobile operators that terminate A2P Messages to implement and maintain appropriate and effective policies, systems and processes to impose restrictions on the use of certain types of alphanumeric Sender IDs.

2.100 Downstream providers are not required to set a policy, but are expected to take into account terminating providers' policies when approving their use, in accordance with GC C9.11.

2.101 We expect policies under GC C9.13 to cover:

- **Protected Brand IDs**: the IDs that relate to high-risk known brands that the terminating provider determines must not be used by any party other than the authorised brand.
- **Generic IDs**: the IDs that the terminating provider prohibits because they are generic and could be used to mislead mobile customers about the sender.
- **Special alphanumeric characters**: an explanation of the alphanumeric character set that is approved for use or is prohibited.

2.102 Policies should be based on the terminating provider's assessment of the risk of harm posed by each alphanumeric Sender ID.

[27] Non-Provider Condition 3.9 corresponds to GC C9.13.

2.103 When considering which brand IDs should be listed as protected, we encourage terminating providers to:

- Consider high profile brands and organisations in sectors commonly targeted by scammers (for example banks, delivery companies and Government departments).
- Take account of existing initiatives designed to prevent impersonation. Such initiatives may include the SMS Sender ID Protection Registry operated by the Mobile Ecosystem Forum.

2.104 When considering which generic IDs to prohibit, we would encourage terminating providers to focus on IDs that do not represent a specific brand, sub-brand or recognised name of the sender, and in particular to consider generic IDs that may be designed to appear familiar or are linked to known scam tactics (such as creating a sense of urgency). This includes words that:

- May be more plausible to recipients, such as 'Customer service' or 'Accounts'.
- Might cause users to experience a sense of urgency, such as 'Alert', 'ActionNeeded' or 'Security'.
- Relate to banking or financial transactions, such as 'Payment', 'Bank' or 'Transfer'.
- Relate to online account security, such a 'SignIn', 'OTP', '2FA' or 'Code'.

2.105 When considering which alphanumeric characters to allow or prohibit, we encourage terminating providers to operate with a bias towards restricting the character set to those that are essential for legitimate business purpose. This could include, for example, prohibiting characters other than the standard alphabet, 0-9 numerals and essential punctuation. In particular, terminating providers should consider characters that could be used as substitutes for those in the standard alphabet, including those bearing accent punctuation or from non-Latin alphabets like the Greek alphabet.

2.106 As set out under GC C9.20, providers must keep their policies under review.

2.107 To comply with the requirement, we expect terminating providers to take reasonable steps to ensure that their policies are communicated down their value chain to aggregators and MSPs. Providers could consider incorporating their policy into their contractual agreements as one means of doing so.

2.108 To ensure these policies are enforced effectively and that all terminated messages are compliant, providers should consider implementing appropriate checks on their network. We also expect providers to have a feedback mechanism to alert downstream providers to messages they have passed on that include non-compliant alphanumeric Sender IDs.

Requiring notification of changes to Business Profiles

C9.14[28] Regulated Providers must take appropriate steps to ensure that Business Senders from which they directly receive A2P Messages are required to promptly notify any changes in their Business Profile, or changes in the use of any Alphanumeric Sender IDs, to them.

[28] Non-Provider Condition 3.10 corresponds to GC C9.14.

Who this obligation applies to

2.109 GC C9.14 applies to any Communication Provider that transfers and/or terminates A2P Messages (including all Aggregators) and that receive A2P Messages directly from the Business Sender. This includes mobile operators and aggregators that contract directly with Business Senders.

The purpose of this requirement

2.110 In order to assess whether changes to information about a Business Sender potentially indicate scam activity and determine whether risk assessments need to be updated, providers must ensure that they are notified of these changes.

Ensuring notification

2.111 To achieve this, we expect providers to set contractual obligations for Business Senders from which they receive messages directly, which place obligations on the Business Sender to notify the provider of changes to their Business Profiles. This includes any information that was collected during KYC checks that has since changed, including the purpose for which a Business Sender is accessing A2P messaging services.

2.112 Changes should be taken into account during KYT checks and previous risk assessments must be updated as appropriate in accordance with GC C9.12.

2.113 We note that where a provider does not receive messages directly from a Business Sender, but from an intermediary, C9.9 requires them to ensure that the onboarding party has contractual terms to the same effect.

Incident management requirements

C9.15[29] 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 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.

[29] Non-Provider Conditions 3.11 – 3.12 correspond to GCs C9.15 – C9.16

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 3 Working Days in all other cases:

(i) take appropriate steps to confirm the Business Sender(s) responsible for those messages;

(ii) implement appropriate measures to prevent the Business Sender(s) 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 C9.9(a); and

(ii) take appropriate and effective action to address the non-compliance and, if applicable, satisfy itself the party will comply going forward.

Who this obligation applies to

2.114 GC C9.15 and C9.16 apply to any Communications Provider that transfers and/or terminates A2P Messages, including all Aggregators. This includes mobile operators that enable A2P message termination and aggregators (whether they are acting at tier 1 or at lower tiers).

The purpose of incident management requirements

2.115 These requirements are intended to act as a framework of obligations for mobile operators and aggregators when they become aware of scam messages that have been transferred through A2P channels. They are designed to ensure that providers identify the source of the scam messages, and that the scammers responsible are denied access to the value chain. The requirements are further designed so that where downstream providers have not been complying with their regulatory or contractual obligations, which might have prevented the scam incident, appropriate steps are taken to address this. Together, these actions will make protections of the messaging channel more robust.

2.116 These requirements differ from the KYT requirements (identified in GC C9.12) in so far as those requirements require action to be taken where any indicators of scam activity are revealed by KYT checks, whereas these incident management requirements require action to be taken where the provider reasonably believes scam messages have been sent. In practice, a provider may have this reasonable belief because specific messages have been reported to them by end-users or by another provider.

Confirming the Business Sender responsible for sending scam messages

2.117 Where a provider has a direct relationship with a Business Sender and identifies a link to scam activity, we expect that the provider can directly confirm the Business Sender account responsible for sending a scam message. This must be done within one working day. We expect providers may need to confirm the Business Sender responsible for the identified messages, to rule out the possibility they originated from a different source, or because a Business Sender may send messages from more than one alphanumeric Sender ID.

2.118 Where a provider does not have a direct relationship with the Business Sender, we expect the provider will need to ask downstream providers to share information to confirm the Business Sender responsible for the messages. This must be done within 2 working days in cases involving no more than one aggregator or 3 working days in all other cases.

2.119 Providers without a direct relationship with a Business Sender must act to confirm the Business Sender responsible when they are aware of a Significant Scams Incident, which we define as a situation where it appears to the provider that a particular Business Sender has cumulatively sent or attempted to send, directly or indirectly, at least fifty A2P Messages that the provider reasonably believes were intended to scam the recipients.

Preventing the business sender from sending further messages

2.120 Where a provider has a direct relationship with a Business Sender linked to sending scam messages, they must implement appropriate measures to prevent the Business Sender from sending further A2P Messages via any network or service the provider provides, unless they have obtained evidence that they are satisfied demonstrates that either: the Business Sender was not responsible for sending the relevant A2P message; or the relevant A2P message was not intended to scam the recipients.

2.121 We would expect appropriate measures here to include pausing access to services and providing an opportunity for the Business Sender to explain any legitimate mitigating circumstances. If legitimate mitigating circumstances apply (such as having had an account hacked), the provider would be expected to seek proof and reassurances that reasonable measures are being taken to prevent future occurrences. Providers would also be expected to consider heightened checks in future (e.g. more frequent or intensive KYT checks on that Business Sender's account). If no legitimate circumstances apply, providers would also be expected to check whether the Business Sender has other accounts and put similar restrictions on these. They could also consider sharing intelligence with other trusted partners, taking into account the intelligence sharing guidance in paragraph 2.19 above.

2.122 Where a provider does not have a direct relationship with a Business Sender, they must implement appropriate measures to prevent the Business Sender (s) from sending further messages via any network or service the provider supplies, unless they have obtained evidence that they are satisfied demonstrates that either: the Business Sender was not responsible for sending the relevant A2P Messages; or the relevant A2P Messages were not intended to scam the recipients.

2.123 We would expect this to include the provider seeking confirmation from downstream providers that service has been paused or evidence of mitigating circumstances where it has not. Service could be paused within 2 working days where there is up to one aggregator

between that provider and the Business Sender (this could include up to one aggregator and one MSP) or 3 working days with more than 1 aggregator.

Establishing whether other parties have conducted appropriate checks and taking appropriate action

2.124 Where a provider does *not* have a direct relationship with a Business Sender, the provider must also, within 15 working days, establish whether the party involved in delivering the relevant A2P Messages to the provider is complying with the contractual requirements imposed on it under GC C9.9(a), take appropriate and effective action to address the non-compliance and, if applicable, satisfy itself the party will comply going forward.

2.125 To comply with this requirement, we would expect the provider to:

- Check whether the party that carried out the onboarding conducted appropriate up front and ongoing checks on the Business Sender and its traffic. This should include confirmation that KYC checks, checks relating to the use of alphanumeric Sender IDs and KYT checks were conducted, which could include relevant records of activity on that account.
- Seek credible reassurances where the downstream provider does not provide evidence that it conducted appropriate checks, that this will be addressed. If no credible reassurances are received, then the provider should consider pausing traffic until evidence is provided.
- Factor any past incidents and, where a downstream party appears to be higher risk, reflect this in their decision making.

General cross cutting measures

2.126 This section sets out guidance on a number of additional obligations that apply across all P2P and A2P messaging measures and therefore to all mobile operators and aggregators.

Right to challenge requirements

C9.17[30] Where a Regulated Provider has blocked a message under Condition C9.3(b), C9.3(c) or C9.7 using automated tools, Regulated Providers must, without delay, notify the person whose message they blocked or otherwise enable that person to become aware their message has been blocked.

C9.18 Regulated Providers must implement and maintain appropriate and effective policies, systems and processes that enable any person to challenge any blocking of their message or Mobile Number or other action the Regulated Provider takes under this GC that affects them. The policies must at least:

(a) explain the circumstances under which any blocking or other action may occur;

(b) explain how the person may challenge the action taken;

(c) explain the process the Regulated Provider will follow to investigate and determine any challenges made under this Condition, including the evidence it is likely to require

[30] Non-Provider Conditions C3.14 – C3.15 correspond to GCs C9.17 – C9.19.

from the person to demonstrate their Mobile Number or messages should not have been blocked;

(d) identify the different outcomes from challenging the actions taken;

(e) identify any conditions the Regulated Provider may attach to any of the outcomes identified in Condition C9.18(d), including any ongoing requirements placed on the person;

(f) identify a reasonable timeframe within which the Regulated Provider will reach the outcomes identified in Condition C9.18(d); and

(g) explain the process the person may follow to appeal any decision not to remove any blocking or other action taken.

C9.19 Regulated Providers must ensure that the policies, systems and processes in place under Condition C9.18 are well publicised and readily available, including ensuring that they are:

(a) in an easily accessible and reasonably prominent manner on their website;

(b) referred to in the terms and conditions for all relevant products and services; and

(c) provided free of charge on reasonable request in hard copy or other format.

Who this obligation applies to

2.127 GC C9.17 to C9.19 apply to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators.

The purpose of the right to challenge requirements

2.128 The right consists of two parts. First, providers must put processes in place to ensure senders are made aware their messages have been blocked using automated tools (proposed GC C9.17). Second, providers must have a clear, accessible and reasonably prominent policies explaining the right to challenge, including on their website (proposed GC C9.18 - C9.19). These requirements should ensure that there is a clear and accessible way to challenge the blocking of messages or numbers, particularly in cases where legitimate messages may have been erroneously blocked. By requiring providers to notify senders of messages that have been blocked and offering a straightforward complaints process, this measure is an important safeguard against potential interference with the right to freedom of expression under Article 10 of the European Convention of Human Rights (ECHR) in the event legitimate messages are blocked. It also supports fair treatment of customers, while maintaining the effectiveness of anti-scam tools.

Notifying senders that their message, or number, has been blocked

2.129 Providers that have blocked messages under C9.3(b) or (c) or C9.7 using automated tools must notify the person whose message they blocked of this fact or otherwise enable that person to become aware their message has been blocked, without delay.

2.130 Providers have discretion to decide how to do this. Examples may include:

- Sending a message to the sender to let them know their message has been blocked.
- Sending a form of error message or notification (such as an exclamation mark) to the sender to let them know their message has been blocked.

2.131 Providers may decide to implement different solutions depending on whether they are blocking messages sent by their own customers or from customers of another provider.

2.132 The requirement to notify only applies where messages have been blocked under GCs C9.3(b) and (c) and C9.7 as a result of the application of automated tools. It does not apply when blocking occurs under any other GCs or as a result of human review. It does not therefore apply to blocking under C9.3(a), blocking under C9.3(b) or (c) following a human review, applying volume limits under C9.5 or any blocking that may occur under C9.8/C9.12(c), C9.15 or C9.16 (although it would be open to providers to apply the notification requirement more widely). This is because:

- We expect senders will quickly know if their number or messages are being blocked under other GCs, including C9.3(a), C9.5 and C9.8/C9.12(c), C9.15 and C9.16.
- We consider the risk of false positives, and therefore the risk of interference with Article 10 ECHR, is higher in relation to GCs that require automated monitoring of the content of messages.
- 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. In such circumstances where a provider is likely to have the highest degree of confidence that a message is a scam, we do not consider it appropriate to require providers to inform a scammer their message has been blocked (which may also tip the scammer off and encourage them to try another provider or channel).[31]

2.133 Providers have discretion to decide whether, and in what circumstances, they may consider it appropriate to inform a person that it has blocked their number or message under other GCs or as a result of human review.

2.134 The scope of this requirement does not extend to notifying the intended recipient of the message that a message intended for them has been blocked. If a legitimate message is blocked and the sender has been made aware of this fact, then the sender will know that they must use other means (e.g. voice call, email or online messaging service) to contact the intended recipient.

[31] We recognise that any notification requirement may tip a scammer off, although we consider scammers are more likely to be tipped off following any human review on the basis a provider is likely to have the highest degree of confidence that a message is a scam following a human review.

Enabling persons to challenge any blocking of messages or mobile numbers

2.135 Providers are also required to implement and maintain appropriate and effective policies, systems and processes that enable a person to challenge any blocking of messages or a number or other action a provider may have taken under GC C9 that affects them.32

2.136 Any person can challenge any blocking decisions and not only the sender of a message.

2.137 The policies must at least include the requirements set out in table 2 below.

Table 2: Right to challenge requirements and guidance

Requirement under C9.18	Guidance on how providers could comply with the requirement
a) explain why any blocking or other action may have occurred	Provide reason(s) for the different circumstances in which a person's message or number may have been blocked.
b) explain how the person may raise a challenge	Provide advice on how a challenge can be raised: e.g. via a web form or email address.
c) explain the process the regulated provider will follow to investigate the challenge, including the evidence it is likely to require from the person to demonstrate their messages or mobile numbers should not have been blocked	Set out the steps that the provider will follow to conduct their investigation. We would expect the provider to specify the team that will conduct the investigation, how they will contact the person to relay the outcome and what information/evidence they will need to enable the investigation to proceed effectively.
d) identify the different potential outcomes following any challenge to the actions taken	We would expect one of the following scenarios to follow an investigation. The provider: • Removes the blocking, or takes other action, because it no longer reasonably believes that the relevant messages were intended to scam the recipients; • Maintains the blocking or other action taken because it continues to reasonably believe that the relevant messages (or mobile numbers from which they were sent) were intended to scam the recipients, or the person does not provide the provider with the information it requires to determine the challenge within a specified timeframe; or • Is notified that the person has withdrawn their challenge.

[32] Other action may include refusing to accept any more messages from a particular Business Sender or suspending or imposing a financial penalty on an aggregator that a provider considers to be responsible for scam messages.

Requirement under C9.18	Guidance on how providers could comply with the requirement
e) identify any conditions the regulated provider may attach to any of the outcomes identified in (d) above, including any ongoing requirements placed on the person	Where the person that has challenged a blocking decision is the party from which the provider has received messages, the provider may consider it appropriate to only continue to accept messages from that party if certain conditions are met. These conditions may, for example, relate to that party's processes, its customers or the volume of messages it may be allowed to send in the future.
f) identify a reasonable timeframe within which the regulated provider will reach the outcomes identified in (d)	We would expect the provider to identify a reasonable timeframe in which it aims to reach a decision following an investigation and to inform the person of that timeframe (e.g. within a certain number of working days). When considering timeframes for an investigation, we also expect providers to take into account specific circumstances, including the type and extent of the evidence that a number or message was legitimate or that the relevant messages are time-sensitive, such as appointment reminders.
g) explaining the process the person may follow to appeal any decision not to remove any blocking or other action taken	Point them in the direction of any processes that allow the person to escalate their challenge. This could include any existing complaints process used by the provider.

2.138 We expect providers to ensure the policies, systems and processes in place pursuant to GC C9 are widely communicated within their organisation, particularly in teams where queries about blocked messages and numbers will be received, such as customer contact teams.

2.139 Staff should also be appropriately trained, including on what information to provide to customers that exercise their right to challenge and how to ensure the provider acts in accordance with the policies, systems and processes it has implemented under GC C9.

2.140 Providers must also ensure the policies, systems and processes they have implemented under GC C9 are well publicised and readily available, including ensuring that they are:

- In an easily accessible and reasonably prominent manner on their website.
- Referred to in the terms and conditions for all relevant products and services.
- Provided free of charge on reasonable request in hard copy or other format. This includes providing the policy in a reasonably acceptable format, such as large print and Braille, in response to a request from a customer who needs such a format because of their disability.

2.141 Providers must ensure they act in accordance with their published policies, including by resolving any challenge within a reasonable timeframe.

Review of policies, systems and processes

C9.20[33] Regulated Providers must regularly review their policies, systems and processes, implemented under Condition C9 to:

(a) confirm that they remain appropriate and effective and are operating as intended;

(b) ensure the Regulated Provider is complying with its policies, systems and processes; and

(c) take appropriate and effective action to ensure that any issues identified are promptly addressed, including by making appropriate changes to their policies, systems and processes implemented under Condition C9.

Who this obligation applies to

2.142 GC C9.25 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators.

Purpose of reviewing policies, systems and processes

2.143 The purpose of this requirement is 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 ineffective.

Conducting reviews of anti-scam policies, systems and processes

2.144 Providers must regularly review their policies, systems and processes implemented under GC C9 to confirm that they remain appropriate, effective and are operating as intended. They must also ensure they are complying with their own policies, systems and processes.

2.145 The timing and extent of each review will depend on the circumstances, including the policy, system or process that is being reviewed and whether it is a scheduled review or an ad hoc review intended to address a specific issue that may have arisen. It will be appropriate to review some policies, systems and processes more regularly than other policies, systems and processes.

2.146 Examples of how providers could comply with these requirements include:

- Reviewing scam intelligence daily to support identification and blocking processes. Sources of scam reports should also be assessed periodically to maintain intelligence quality and identify new, valuable sources.
- Conducting an audit, at least annually, to evaluate the overall effectiveness of the anti-scam measures.
- Engaging solution vendors (e.g. firewall providers) and/or other competent third parties to support audits and inform reviews.

[33] Non-Provider Condition C3.16 corresponds to GC C9.20.

- Ensuring oversight by a senior individua for all reviews and audits.
- Communicating planned next steps clearly with relevant parts of the organisation following each review.
- Using a broad range of data sources to inform reviews. Providers should also engage with industry forums, law enforcement and anti-scam organisations to stay up-to-date on emerging threats and developments in cybercrime.
- Establishing cross-organisational working groups to coordinate learnings across teams and departments. This may include collaboration between specialist fraud teams and customer-facing functions.
- Facilitating coordination between MNOs and MVNOs to ensure insights into scam prevention are shared effectively.
- Structuring working groups to support rapid responses to emerging threats and enable efficient implementation of updated measures.

Ensuring that issues are addressed promptly

2.147 Providers must 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 implemented under GC C9.

2.148 We would expect providers to meet this obligation by ensuring that relevant teams and individuals are equipped to respond quickly to emerging threats.

2.149 As part of this, we would also expect providers to ensure that learnings from reviews are clearly documented and shared with appropriate teams. For example, providers should monitor rates of false positives and challenges to the blocking of legitimate messages and make appropriate changes to policies, systems, and processes to reduce the risk of false positives.

2.150 We would also expect to see clear lines of accountability and responsibility agreed and communicated to relevant teams and individuals, so it is clear who needs to take action and when.

Training staff

C9.21[34] Regulated Providers must ensure that all staff are made aware of, and 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 C9.18.

Who this obligation applies to

2.151 C9.21 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators.

[34] Non-Provider Condition C3.17 corresponds to GC C9.21.

Purpose of staff training

2.152 The purpose of this requirement is to ensure providers take the necessary steps to prepare their staff to implement the measures outlined in these Conditions. This training requirement goes beyond technical staff working in specialist fraud or network teams, extending more broadly to include customer-facing teams, so they are equipped to handle complaints and enquiries relating to blocked numbers and messages.

Steps to ensure staff are appropriately trained

2.153 Providers must ensure that all staff are made aware of, and 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 C9.18.

2.154 To comply with this obligation, we would expect providers to ensure that their staff (or others acting on their behalf) have the appropriate skills, competency and tools for the full design, deployment, operation and monitoring of the requirements under these Conditions. Relevant training is likely to be necessary. The scope of this obligation extends to any third parties or partners that providers may use to fulfil their obligations under Condition C9.

2.155 Providers are also expected to take appropriate steps to ensure that all staff who communicate with customers to enable customers to exercise their right to challenge are trained to identify such cases and provide guidance on how to navigate the process effectively.

Record keeping requirements

C9.22[35] 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 C9.23 to C9.25 below to be retained for at least the time period identified in those Conditions.

C9.23 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 C9.20;

(c) records of volume limits being applied under Condition C9.5; and

(d) records of the measures or action taken in response to an incident under Conditions C9.15 and C9.16.

C9.24 The following records must be kept for at least three years after the end of the relevant contractual relationship:

[35] Non-Provider Conditions C3.18 – C3.21 correspond to GCs C9.22 – C9.25.

(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).

C9.25 Records of communications between a Regulated Provider and any person regarding a challenge raised under Condition C9.18 must be kept for at least two years after the challenge was resolved or otherwise closed.

Who this obligation applies to

2.156 C9.22 to C9.25 apply to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators, but some providers will only need to comply with a subset of the requirements, as relevant to their business. For example, aggregators will not need to comply with record keeping related to P2P measures.

The purpose of record keeping requirements

2.157 The purpose of these record-keeping requirements is to ensure that providers possess written documentation of the measures taken to comply with the requirements of GC C9. Clear and up-to-date records, along with regular, timely reviews of compliance, will assist providers in tracking how they are complying with their obligations and ensuring that the measures they have taken are fit for purpose.

Record keeping requirements

2.158 Providers must implement and maintain appropriate record-keeping policies, systems and processes to demonstrate and ensure continued compliance with GC C9. These must be overseen by a designated senior individual and must, where applicable, provide for the records identified in C9.23 to C9.25, set out below, to be retained for at least the time period identified in those Conditions.

2.159 The record-keeping requirement includes but is not limited to keeping records of the categories of documents identified in table 3 below. In accordance with table 3, mobile operators within the scope of requirements relating to P2P messaging must keep records relating to:

- Policies, systems and processes implemented under Condition C9.
- Reviews of the effectiveness of those anti-scam measures.
- Application of volume limits.
- Communications relating to any challenges to blocking measures.

2.160 Mobile operators and aggregators within the scope of requirements relating to A2P messaging must keep records relating to:

- Policies, systems and processes implemented under Condition C9.
- Reviews of the effectiveness of those anti-scam measures.
- KYC checks and checks on alphanumeric sender IDs, including initial and updated risk assessments.
- Contractual terms and compliance with those contractual terms which they have agreed with parties from which they receive A2P Messages.
- Measures taken as a result of KYT checks.
- Measures taken in response to scam incidents.
- Communications relating to any challenges to blocking measures.

Required retention period for different categories of records

2.161 Providers must establish and maintain effective systems for keeping records. These systems are essential for providers to demonstrate compliance with GC C9. These must be overseen by a designated senior individual.

2.162 Crucially, the appointed individual must make sure that all the specific records mentioned in C9.23, C9.24 and C9.25 are kept for at least a specified length of time. The requirements in each case are summarised in the table 3.

Table 3: The minimum time periods required for providers to retain specific categories of records related to scam prevention policies

Retention period	Categories of records that Providers must keep
2 years	• Communications between a relevant provider and others regarding right to challenge (under C9.18). *(retention period starts after the challenge is concluded)*
3 years **(from end of contractual relationship)**	• KYC checks and checks on alphanumeric sender IDs (under 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. • Application of volume limits being applied under GC C9.5. • Measures or actions taken in response to scams incidents under C9.15 and C9.16.

Expectations of recording keeping requirements

2.163 We expect providers to keep written records that are durable, accessible, easy to understand and up-to-date. Written records may be made and kept in a durable medium of the provider's choice, provided they can be supplied to Ofcom easily and promptly, if required.

Data protection requirements

C9.26[36] Condition C9 applies subject to the requirements of the Relevant Data Protection Legislation.

Who this obligation applies to

2.164 GC C9.26 applies to any Communications Provider that transfers and/or terminates P2P Messages and/or A2P Messages, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators.

The purpose of this requirement

2.165 The purpose of this requirement is to ensure providers adhere to the relevant data protection obligations when they are seeking to comply with GC C9.

Providers will need to ensure compliance with relevant data protection rules

2.166 Our rules 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.[37]

2.167 Providers must therefore comply with the GCs in a way that ensures compliance with relevant data protection legislation. This includes:

- The UK General Data Protection Regulation 2018 (UK GDPR).
- The Data Protection Act 2018 (DPA).
- The Privacy and Electronic Communications Regulations 2003 (PECR).

2.168 We also expect providers to take into account any relevant guidance issued by the ICO.

a) The UK GDPR sets out 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:
b) Lawfulness, fairness and transparency;
c) Purpose limitation;
d) Data minimisation;

[36] Non-Provider Condition C3.22 corresponds to GC C9.26.
[37] See also ICO, 2022. Overview of Data Protection Harms and the ICO's Taxonomy.

e) Accuracy;
f) Storage limitation;
g) Integrity and confidentiality (security); and
h) Accountability.[38]

2.169 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.

2.170 Providers may also use third parties to carry out any data processing on their behalf. ICO guidance 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.[39] 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.

2.171 Other data protection legislation and guidance that are particularly relevant to our proposals 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 22 UK GDPR (relating to automated decision making) and, if so, ensure they comply with Article 22. Article 22 UK GDPR applies where a provider makes decisions based solely on automated processing of personal data, where the decision has legal or similarly significant effects. The ICO has also published guidance on content moderation[40] as well as on automated decision making and profiling.[41]
- Rules and guidance relating to monitoring of traffic data. Providers should, for example, ensure they comply with Regulations 7 and 8 of the PECR.

2.172 This is not intended to be an exhaustive list and providers are expected to take appropriate legal advice and ensure they comply with all data protection legislation that applies to them when complying with the GCs to which they are subject.

2.173 We are satisfied that our GCs can be implemented in accordance with data protection law. As noted above, the ICO has published guidance on content moderation and data protection, which 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

[38] Further information on these principles is available in ICO, A guide to the data protection principles [accessed 24 October 2025]. For example, providers should be transparent with users about the processing of personal data they carry out in order to comply with GC C9.
[39] ICO, controllers and processers [accessed 24 October 2025].
[40] ICO guidance on content moderation, in particular section on "What if we use automated decision-making in our content moderation?" [accessed 24 October 2025]. While this guidance 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.
[41] ICO guidance on automated decision making and profiling [accessed 24 October 2025].

technologies and processes. This includes advising service providers to carry out a data protection impact assessment to assess and mitigate data processing risks.

2.174 Providers should also ensure they comply with their obligations under other legislation that may be relevant, including the Investigatory Powers Act 2016.

Ensuring transmission of legitimate message requirements

C9.27[42] Regulated Providers must take appropriate steps to ensure the continued transmission of legitimate messages through networks.

Who this obligation applies to

2.175 GC C9.27 applies to any Communications Provider that transfers and/or terminates Person-To-Person Messages and/or A2P Messages, including all Aggregators. This includes all mobile operators (MNOs and MVNOs) and aggregators.

The purpose of the continued transmission of messages

2.176 This requirement is designed to reduce the risk of providers' systems wrongly blocking legitimate messages. While automated checks are often needed to help identify and stop scam messages, providers must take appropriate steps to ensure these checks do not inadvertently prevent legitimate messages from continuing to reach their intended destination.

Steps to mitigate the risk of legitimate messages being blocked

2.177 Providers must take appropriate steps to ensure the continued transmission of legitimate messages through networks. This means taking appropriate steps to keep rates of false positives low. Complying with other GCs and taking into account other aspects of this guidance will help ensure the continued transmission of messages through networks. This includes:

- Ensuring intelligence is current, robust and subject to contextual testing and evaluation.
- Using human review of intelligence to check that reported URLs and telephone numbers are, in fact, malicious and to ensure identifying and blocking techniques are working as intended.
- Establishing a clear and accessible policy for users to challenge any blocking decisions.
- Ensuring relevant staff receive appropriate training, which in this context we expect to include training on managing identifying and blocking systems and responding to incidents of scam (or potential scam) activity.
- Regularly review policies, systems, and processes to ensure they remain appropriate and effective. In this context, this should include monitoring the rates of false positives

[42] Non-Provider Condition C3.23 corresponds to GC C9.27.

and challenges to the blocking of legitimate messages and making appropriate changes to reduce the risk of false positives occurring.

2.178 However, providers are expected to take additional steps to comply with GC C9.27. Examples of such steps include the following (as applicable):

- Working with threat intelligence providers to identify message signatures and behavioural indicators associated with scam campaigns, particularly those that mimic legitimate communications. This intelligence could be used to target filters and reduce the risk of blocking genuine traffic.
- Collaborating with aggregators to understand expected traffic volumes, patterns, and message templates. This information should inform decisions and improve the accuracy of blocking systems.
- Applying quarantine functionality to temporarily hold messages that cannot be confidently classified as legitimate or illegitimate. This allows time for further traffic analysis and supports more accurate blocking decisions.
- Reviewing cases where legitimate messages were blocked in error and incorporating lessons learned into future message template reviews and firewall rules updates.

2.179 Providers may also wish to 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 end-user's number is not blocked. For example, where someone sends a scam message to a friend in order to warn them about the scam.

3. Enforcement of rules

3.1 We have a range of powers to take enforcement action for non-compliance with our rules relating to scam mobile messages.

3.2 We may decide to pursue more than one of these options in the particular circumstances of the case, as permitted by the relevant legislation.

3.3 When deciding whether to take enforcement action and what enforcement action may be the most appropriate, Ofcom will consider all relevant factors. This includes (but is not limited to), the available evidence that a provider is in breach of the relevant rule, including the extent to which a provider has taken into account the expectations in this guidance. We may obtain evidence through a variety of sources which may include:

- Statutory information requests.
- Ofcom's own monitoring or intelligence. For example, we may consider it appropriate to apply to be a new customer of a provider to check their KYC and onboarding process is robust and reflects any policy they may have provided to Ofcom.
- Intelligence provided by a third party.

3.4 Where applicable, any enforcement action will generally be carried out in line with Ofcom's Regulatory Enforcement Guidelines.[43]

General Conditions

3.5 We can take enforcement action under our GCs relating to scam mobile messages, including GC C9, as well as existing GCs including B1 and B4.4.

3.6 We may take action under more than one GC in the particular circumstances of the case. For example, a breach of GC C9 may also be considered a breach of GCs B1.6, 1.8 and/or 1.9.

3.7 Our powers to take enforcement action under our GCs relating to scam mobile messages include:

- Powers to impose significant financial penalties of up to 10% of annual turnover.[44]
- Powers to direct providers to take steps in order to comply with the relevant GC and/or remedy the consequences of the contravention. This could, for example, include directing a communications provider to (i) take certain action in relation to a number, sender or message; or (ii) compensate persons that have suffered loss or damage as a result of the non-compliance.[45] It is the duty of the person to comply with any such direction and that duty is enforceable in civil proceedings by Ofcom.[46]

[43] Regulatory Enforcement Guidelines for investigations.
[44] See sections 96A – 98 of the Act. We can impose any penalty we consider to be appropriate and proportionate up to the statutory cap and taking into account Ofcom's penalty guidelines.
[45] Section 96A(2)(d) and section 96C(2)(a) of the Act.
[46] Section 96C (5) and (6).

- Powers to suspend a communications provider's entitlement to provide electronic communications networks or electronic communications services, or to make associated facilities available.[47]
- Powers to issue a direction under GC B4.4 requiring communications providers to block access to certain numbers or communications services on the basis of fraud or misuse.[48]
- Powers to withdraw telephone number allocations if any of the conditions in section 61(1) of the Act are met including when withdrawal is in accordance with GC B1.18(d) or (e):
  - B1.18(d) gives us the power to withdraw numbers where "the Communications Provider has used a significant proportion of those Telephone Numbers, or has used such Allocation to a significant extent, inconsistently with … Condition [B1], or to engage in fraud or misuse". Depending on the nature and degree of harm that may be caused by a scam or potential scam, we may consider a single instance of misuse to constitute using an "Allocation to a significant extent, inconsistently with … Condition [B1], or to engage in fraud or misuse".
  - B1.18(e) gives us the power to withdraw numbers where "Ofcom has advised the Communications Provider in writing that a significant proportion of those Telephone Numbers has been used, or that such Allocation has been used to a significant extent, to cause harm or a nuisance, and the Communications Provider has failed to take adequate steps to prevent such harm or nuisance."

3.8 If we withdraw a +44 number, that number will no longer be allocated to a person meaning providers should not carry traffic related to that number, even if it does not transit or terminate in the UK. We may take enforcement action under GC B1.3 against any UK provider that continues to carry such traffic.

Non-provider Conditions

3.9 In the event of non-compliance with Non-Provider Condition 3, we have powers under section 59(6) of the Act to take enforcement action via civil proceedings against operators allocated numbers that may not be considered a communications provider within the scope of GC B1. We also have the power to withdraw numbers under section 61(4) of the Act.

Persistent misuse

3.10 Ofcom also has powers under sections 128 to 130 of the Act to take enforcement action against providers or other persons who persistently misuse an electronic communications network or services including issuing a penalty of up to £2m. Misuse of an electronic communications network or service involves using a network or service in ways which cause or are likely to cause someone else (including consumers) to unnecessarily suffer annoyance, inconvenience or anxiety. Misuse is persistent where it is repeated enough for it to be clear that it represents a pattern of behaviour or practice, or recklessness about

[47] Section 100 of the Act.
[48] See Annex A11 of our Regulatory Enforcement Guidelines for a summary of the relevant enforcement process.

whether others suffer the relevant kinds of harm. Any enforcement action for Persistent Misuse would take into account Ofcom's Persistent Misuse statement.[49]

3.11 Depending on the circumstances, we may take action against a provider or the person carrying out the misuse.[50]

Other action

3.12 Depending on the circumstances, we may consider it appropriate to take other action, including using soft enforcement tools. For example, we may consider it appropriate to maintain on our website a list of providers found in breach of our rules and/or a list of numbers and/or Sender IDs that have been associated with scams and that should not be used, transmitted or terminated in the UK.

[49] Statement of policy on the persistent misuse of an electronic communications network or electronic communications service.

[50] See paragraphs 1.19 – 1.20 of Ofcom's Persistent misuse statement.