Which?

2 Marylebone Road
London NW1 4DF
020 7770 7000
which.co.uk

Thomas Brooks
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

Consultation Response

Which? response to Ofcom's consultation on *Combatting Mobile Messaging Scams*

Submission date: 16/01/2026

Summary

Which? welcomes the opportunity to respond to Ofcom's consultation on combatting mobile messaging scams. Mobile messaging scams are pervasive: mobile users reported an estimated 100 million suspicious messages to mobile operators through the 7726 service in the year to April 2025. Mobile messaging scams are also very harmful, accounting for approximately £65 million per year in consumer fraud losses.

While Which? welcomes Ofcom's intervention in this space, we believe that the regulator must go further in a number of areas in order to properly tackle mobile messaging scams. In particular:

- **Volume limits:** Ofcom should provide guidance on an acceptable SMS volume limit and on an acceptable reset period for SMS volume limits.
- **Information sharing:** Ofcom should mandate that operators not only have processes in place to receive scam reports, but also that they proactively seek scam intelligence from third parties. Ofcom should also mandate that operators have to share scam intelligence received from their users with other operators.
- **Know Your Customer checks:** Ofcom should update its guidance to require enhanced due diligence checks for customers who are based in high risk countries. Providers should also conduct enhanced checks on customers whose IP address does not correspond to the stated location of their business.
- **Sender IDs:** Ofcom should introduce a mandatory Sender ID registry to combat fake Sender IDs, as this will be more effective than Ofcom's current solution.
- **Know Your Traffic checks:** Ofcom should update its guidance to state that, when providers do not receive a response from business senders to a request for clarification on a suspicious communication, they should infer that the communication was fraudulent and prevent that sender from sending further messages.
- **Cross-cutting measures:** Ofcom should oblige providers to make consumers aware of their right to alternative dispute resolution if they wish to contest a provider's

decision, such as blocking messages.
- **A drafting amendment** to proposed Condition C9.3 to strengthen the duty to prevent scam messages being sent and/or received. It is not sufficient that processes should only be 'designed' to achieve the desired effect, so this word should be removed.

Full response

Question 1: Do you agree with our conclusions on the types and scale of harm that scam messages cause, based on the available evidence?

Ofcom has identified three kinds of consumer harm that are caused by mobile messaging scams: financial harm, time harm, and emotional harm, as well as harms to business and to the wider economy. With respect to financial harm, Ofcom estimates that financial losses from mobile messaging scams are approximately £65 million per year (consultation, 3.20). Ofcom references several studies that demonstrate the emotional harm caused by fraud, including reports produced by the Home Office and Visa, but it does not provide any estimates relating to time harm or emotional harm, although it does say that "we believe that the emotional impact on victims is significant, in line with the impact of fraud more generally" (consultation, 3.22).

Which? is concerned that the impacts of scams on victims have long been underestimated. Our research, published in May 2023, found that being a scam victim is associated with significantly lower levels of life satisfaction, lower levels of happiness and higher levels of anxiety. Using the approach in HM Treasury's guidance on wellbeing analysis, we estimated that this lower level of life satisfaction is equivalent to an average impact of approximately £2,500 per victim. With 3.7 million incidents of fraud experienced in 2019-20, we estimated that the total losses in wellbeing associated with fraud victimisation amount to £9.3 billion per year.

Ofcom also fails to mention the possibility of physical harm, despite numerous studies showing that fraud victimisation can result in physical harm. A study conducted by the Social Market Foundation in 2023 found that 9% of fraud victims reported an impact on their physical health as a result of fraud victimisation. A study by the Identity Theft Resource Centre in 2018 noted that nausea and sleep problems are particularly associated with fraud, but victims have also reported symptoms such as aches, pains, and skin conditions.
As such, while we agree with Ofcom's conclusions on the types and scale of harm that scam messages cause, we believe that the emotional impact on fraud victims is actually underestimated, and is greater than the financial impact, not "broadly in line", as Ofcom has stated. Moreover, Ofcom has failed to note the substantial evidence of the physical harm that scams can cause. In our view, this strengthens the case for interventions in this market which are designed to prevent fraud from happening at all.

Question 2: Do you agree with our assessment of the extent and effectiveness of existing measures?

Ofcom considers that its existing general conditions have created friction in the supply chain for scammers (consultation, 4.9). It also outlines a series of measures taken by industry which have created friction for scammers. On the whole, Ofcom finds that these measures are often applied inconsistently across the industry, limiting their overall effectiveness (consultation, 4.64).

We agree with Ofcom's assessment of the limited effectiveness of existing measures. Mobile messaging scams are amongst the most common which are reported via Which?'s scam alerts service. Between 30 November 2024 and 1 December 2025, consumers submitted 2,400 reports of 'text scams' (as defined by the person submitting the report) to Which?'s Scam Sharer tool. This accounts for approximately 20% of all the reports received by the Scam Sharer tool during that time period. This evidence suggests mobile messaging scams remain a widespread problem for consumers.

Question 3: Do you agree with our provisional conclusions on the case for further intervention to combat scam messages?

Ofcom has concluded that existing measures to address mobile messaging scams are, collectively, not sufficient to address future harm from scam mobile messages, or to achieve Ofcom's policy objective to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages (consultation, 4.62). Although the use of mobile messaging has declined in recent years, the latest figures show that 28 billion such messages are in fact sent annually, which indicates a large potential for harm even if only a tiny proportion of those are fraudulent.

Which? agrees with Ofcom's provisional conclusions on the case for further intervention. We believe that, given the harm that mobile messaging scams cause to consumers, and the general upward trend in the number of scams (up from 3.4 million incidents March 2017 to 4.1 million incidents in June 2025 per the Crime Survey for England and Wales), there is a clear case for regulatory intervention in this space. Ofcom's own research from 2025 as reported by Which? shows that one in 10 survey respondents received daily suspicious text messages, a third reported receiving them weekly, and two-thirds reported receiving them monthly.

Moreover, failing to intervene in the mobile messaging sector will likely make it a more attractive vector for scammers. This is because Ofcom has signalled an intention to strengthen counter-fraud protections in other areas, including by introducing measures to combat scam calls from abroad and by implementing the Online Safety Act to tackle fraudulent paid for adverts and other kinds of fraudulent online content. If it becomes more difficult for scammers to perpetrate fraud via voice calls and online platforms as a result of these interventions, but it does not become more difficult for scammers to perpetrate scams via mobile messaging services, the likelihood is that scammers will shift their focus to mobile messaging services as the most viable platform to scam UK consumers. In order to prevent this, Ofcom must strengthen protections in the mobile messaging space in tandem with strengthening protections in other areas.

Moreover, as Ofcom points out numerous times in the consultation document, the previous regulatory approach, which has relied largely on voluntary measures such as the Fraud Sector Charter for telecommunications, has not been sufficient to reduce scams. This is because the voluntary measures have not been adopted consistently by all industry players. The best way to address this problem is, as Ofcom suggests, to make counter-fraud measures compulsory, rather than voluntary. Therefore, we agree with Ofcom's conclusion that it is justified in intervening in this market to prevent scams. In addition, it should be considered that, in contrast to the duties on banks, there is currently no right for victims who have lost money as a result of a failure by a telecoms provider to block a scam message to obtain reimbursement from that provider, meaning that telecoms providers currently have fewer incentives to prevent fraud than banks.

Question 4: Do you agree with our proposal to require mobile operators to implement volume limits on P2P messaging?

Ofcom is proposing that mobile operators must establish and implement appropriate and effective procedures relating to 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 (consultation, 5.12). This policy proposal is framed as a response to four main problems: some operators not setting any limits at all; some operators setting limits, but too high to be effective; some operators resetting their limits at short intervals, which reduces the effectiveness of the measure; and some operators not enforcing their limits in an effective way. These four issues are all a subset of the overall problem that Ofcom has diagnosed in relation to industry measures, i.e. that measures are applied inconsistently. It is the existence of this inconsistency which Ofcom has cited in justification of its decision to introduce new requirements for operators in this sector.

The main issue with Ofcom's proposal is that it will only address two of the four problems that Ofcom has identified with volume limits. Ofcom's proposal will oblige providers to set volume limits, thereby addressing the problem of some providers not currently setting such limits. Ofcom's proposal will also oblige providers to automatically block messages which exceed volume limits, which will address the issue of some operators not enforcing limits effectively.

Ofcom has said that operators should undertake an evidence-based assessment of what a good limit would look like, but has not provided any parameters or guidance in relation to an effective limit. Its proposal will not therefore address the issue of providers setting limits which are too high to be effective.

Similarly, Ofcom is proposing that operators can continue to implement limits that reset at short intervals. Ofcom says that it expects operators to keep such limits under review and to revise them if it becomes clear that setting the caps in such a way is not effective in preventing use by scammers. Ofcom will presumably enforce against a provider which does not revise an ineffective volume limits policy, though it makes no mention of this in the consultation document. Such a process would be time consuming and would continue to expose consumers to potentially fraudulent messages. As it stands therefore, Ofcom's suggested policy does not address the problem of providers resetting volume limits at short intervals.

In Which?'s view, Ofcom's current proposals do not therefore adequately address the main problem that Ofcom has diagnosed: inconsistency of practice among operators. In order to address this, we suggest that Ofcom provide guidance relating to an acceptable volume limit and an acceptable period after which a volume limit can be reset. Ofcom could consult with operators during the implementation period of these proposals to gather an evidence base to inform its guidance on these subjects. The guidance should be based on an assessment of the legitimate factors that justify the use of bulk message sending.

Without minimum standards for volume limits and reset periods, there is a risk that volume limits will continue to be applied inconsistently, and that they will therefore continue to be ineffective. As a result of this, Ofcom may fail in its policy objective to significantly reduce the likelihood that consumers and business end-users receive scam mobile messages.

Question 5: Do you agree with our proposal to require mobile operators to identify and block scam messages and telephone numbers on P2P channels?

Scammers often include links to fake websites in fraudulent messages, with the aim often being to convince consumers to share their personal information with the scammers. Data from Which?'s Scam Sharer tool from 30 November 2024 to 1 December 2025 indicates that links to parking fine websites and the website of the UK Government were especially common.

Ofcom is proposing that mobile operators be required to implement and maintain appropriate and effective policies, systems and processes to receive reports of scams from customers and third parties relating to telephone numbers that the customer, or third party, believes sent messages intended to scam the recipients, and URLs and telephone numbers that the customer, or third party, believes were used as part of the scam (consultation, 5.33). This intervention is designed to address the fact that, according to Ofcom's information gathering, not all mobile operators have processes in place to collect useful data that can make their tools to block scammers' numbers and messages more effective (consultation, 5.31).

Which? agrees with Ofcom's proposal overall. Which? has recently published a paper which analyses responses to the Home Affairs Select Committee's unpublished 2023 inquiry into fraud. Our paper found that the telecoms sector had the lowest level of engagement with the inquiry in relation to data sharing. Out of the eight signatories to the 2022 Telecoms Fraud Charter (which promises, amongst other things, that telecoms providers will share information with other telecoms providers, banks and law enforcement to detect and reduce fraud), only two, BT and EE submitted evidence to the inquiry. We are therefore pleased to see Ofcom include provisions relating to the sharing of information about scams.

However, we believe the existing language, which requires operators to "maintain appropriate and effective policies, systems and processes to receive Scam Reports from

End-Users and third parties” (guidance, 2.2) is too passive. Ofcom’s guidance later clarifies that, as well as having systems in place which allow their users to easily report scams, operators are expected to proactively obtain intelligence on scams from other sources. This is an important requirement which should be foregrounded. We therefore suggest that Ofcom amend the wording on the proposed requirement to: “Have processes to receive scam reports from users and to proactively obtain scam intelligence from third parties, relating to telephone numbers and URLs that are being used for scams.”

Moreover, the current guidance merely states that “mobile operators are expected to obtain intelligence on scams from a range of sources that is not limited to scams that may have arised in P2P messages” (guidance, 2.9), before going on to list some examples, including the Global Signal Exchange and the Cifas National Fraud Database. Which? believes that Ofcom should be more prescriptive here. Currently, there is no guidance for operators around how frequently they ought to be requesting this information. If operators do not request third party information frequently, they will not receive the most up-to-date fraud information, which could limit the effectiveness of the policy. To make the proposed policy more effective, Which? believes that operators should have to request third party information on a monthly basis.

Moreover, Which? believes that Ofcom should broaden the list of named sources contained within its guidance (specifically at 2.10). Which?’s October 2024 policy research paper, *How data sharing can protect victims and prevent fraud*, found that most victims (63%) report fraud to their banks. The next most popular reporting routes were Action Fraud (19%) and the police (17%). None of these organisations or institutions are currently mentioned in Ofcom’s guidance. Which? believes that Ofcom should update the guidance to state that operators should regularly request scam reports from financial services institutions and law enforcement.

Finally, Which? believes that Ofcom’s proposal can go further in terms of sharing information between operators. The guidance states that Ofcom does not consider that having only a mechanism for enabling a mobile operator’s own customers to report scams to be sufficient to comply with its proposed policy (guidance, 2.8). It goes on to state that operators should therefore obtain intelligence from third parties. It does not however suggest that operators share the intelligence they receive from their customers with other operators. Which? believes that Ofcom’s guidance should require operators to share the fraud information they receive from their customers with other operators, as well as banks and other third parties. This will ensure that operators are receiving as much usable scam intelligence as possible.

Question 7: Do you agree with our proposals to require mobile operators and aggregators to perform KYC checks and KYT checks, to implement measures regarding alphanumeric sender IDs and to ensure incident management processes are followed for A2P messaging?

Ofcom has proposed the following requirements for mobile operators and aggregators:

- **due diligence:** conduct effective KYC checks at the onboarding stage to prevent scammers from using A2P services to contact potential victims;
- **preventing the use of fake sender IDs:** maintain a policy on protected brand IDs (ensuring that only authorised brands can use certain high-risk IDs), generic IDs (prohibiting certain generic IDs such as ‘customer service’), and special alphanumeric characters (explaining which characters are permitted and which are not (e.g. non-Latin alphabetic characters)) to prevent fraudsters from using fake alphanumeric sender IDs and take appropriate steps to ensure that business senders notify them of changes to their business or use of alphanumeric sender IDs;
- **Know Your Traffic checks:** review data on volume patterns, new or different use of alphanumeric sender IDs or telephone numbers, and any notifications of changes in business senders’ profiles;
- **Incident management:** apply incident management processes where scam activity is identified to both block senders of scam messages from being able to send further messages and to ensure any compliance failures by other parties are addressed; and
- ensure that requirements are passed through the supply chain where needed.

Due diligence

In terms of KYC checks, Ofcom is proposing that operators check:

- information relating to the trading or registered name, and registered office or trading address;
- the nature of the services being provided (and the purposes for which a business sender is seeking to access A2P messaging channels); and
- payment information, existing telephone numbers, websites, directors and persons of significant control.

Which? is generally in favour of Ofcom’s proposals in relation to KYC checks, but feels that there are some areas in which the proposals can be strengthened.

Firstly, Ofcom’s guidance on KYC checks cites “not using a UK IP address where the business purports to be based in the UK” (guidance, 2.65) as a risk indicator. Which? has seen examples of scams where fraudsters have claimed to be based in one country, but have provided a business address listed in another country which does not correspond to the organisation whom the individual claims to represent. It is therefore not sufficient to only check that an operator who claims to be based in the UK has a UK IP address. We recommend that Ofcom updates the risk indicator list to include “not using an IP address which corresponds to the geography in which the business purports to be based” as a possible indicator of fraudulent activity which ought to trigger enhanced due diligence checks.

Secondly, under HMRC's anti money laundering guidance (2025), businesses must carry out enhanced due diligence when entering a transaction with a person resident in a high risk third country. Various reports and studies have demonstrated high scam activity in specific regions, including China, Southeast Asia, and West Africa. The Philippines was the most commonly reported international dialling code associated with potentially fraudulent text messages in the reports made to Which?'s Scam Sharer tool between 30 November 2024 and 1 December 2025. Ofcom should undertake an assessment of which countries are disproportionately responsible for mobile messaging fraud and update its guidance to oblige operators to carry out enhanced due diligence measures when entering a transaction with a person in a high risk country.

Preventing the use of fake sender IDs

Scammers commonly use fake sender IDs to lure consumers into a false sense of security when perpetrating mobile messaging scams. Which?'s Scam Sharer tool has received numerous reports of potential scam messages sent from fake sender IDs. Commonly spoofed sender IDs include DWP, Evri, Tribe HR, Royal Mail, and HMRC.

In terms of preventing the use of fake sender IDs, Ofcom is proposing that providers:

- ensure that the proposed use of alphanumeric IDs is consistent with the nature of the business applying to use them, as set out in response to KYC checks;
- do not allow a sender to use a brand name that they are not authorised to use to represent themselves;
- ensure that business 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 the alphanumeric sender IDs;
- implement and maintain appropriate and effective policies, systems and processes on the use of:
    - specific protected IDs: alphanumeric sender IDs which must only be used by high-profile organisations and brands they relate to, or close imitations of these which should not be used by any sender;
    - generic IDs: Alphanumeric sender IDs which do not help to identify the sender, but could be used by scammers to add credibility to their messages, e.g. 'Delivery', 'Alert' or 'Urgent'; and
    - special alphanumeric characters within alphanumeric IDs, such as those outside of the standard Aa-Zz alphabet and 1-9 number set, including obscure punctuation, or non-Latin alphabet characters, which can be used to closely mimic legitimate business names.

Ofcom also considered introducing a mandatory Sender ID registry, but has decided not to take that forward. Which? disagrees with this decision. In our view, a mandatory sender ID registry would be much more effective at tackling the core problem identified by Ofcom: the inconsistent application of counter-fraud measures within industry. The policy would therefore give Ofcom a much better chance of achieving its overall policy aim, which is to reduce the risk of consumers receiving scam messages. We do not believe that the introduction of a mandatory sender ID register would be unduly onerous for operators.

Ofcom has repeatedly stated that inconsistent application of counter-fraud measures is a problem, but mandating duties for all providers in relation to sender ID will not address such inconsistency as effectively as the introduction of a mandatory sender ID registry. Under Ofcom's current proposals, providers are expected to monitor 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); and 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). If these proposals are implemented, the risk of their being applied inconsistently remains. Under a Sender ID registry however, such checks would be conducted by the regulator. Such checks are likely to be more thorough and more consistent than checks carried out by operators. Moreover, businesses are more likely to comply with a regulator's requests for information, such as information about where companies are domiciled.

The main reason Ofcom cites for not implemented a sender ID registry is the "significant up front and ongoing costs associated with both registering IDs and maintaining a registry" (consultation, 5.152). However, the example of other markets suggests that the implementation costs of a sender ID registry would not be particularly high. In December 2024, the Australian Government estimated that its sender ID scheme would increase regulatory costs across the entirety of the telecoms sector by A$21.5 million per year (approximately £10.7 million). Ofcom's 2024 call for evidence also cites the example of Singapore, whose national Sender ID registry came into effect in January 2023, and where organisations are charged a one off set up fee of S$500 (£290) and an ongoing annual fee of S$200 (£116) to participate in the national sender ID register. The economic impact assessment commissioned by the Irish Government in 2024 for its sender ID registry estimated one off costs of €150,000 for mobile network operators and €123,000 for aggregators.

By contrast, Ofcom's Q1 2025 Telecommunications Market Data Update estimates that mobile telephony services generated £3.5 billion in retail revenues in Q1 2025. The increased regulatory cost as a percentage of overall telecoms revenues could therefore be relatively modest; the industry cost of Australia's scheme does not amount to even 1% of total annual industry revenues. Which? believes that a modest cost such as this would be more than justified, given the substantial harm which scams cause to consumers.

Know Your Traffic checks

Ofcom expects providers to monitor a range of indicators of scam activity (guidance, 2.80). Where providers encounter indicators of scam activity, they must seek evidence that messages from the sender are legitimate (guidance, 2.86). Where a provider believes, based on reviewing the evidence, that the messages were intended to scam people, they must block the sender from sending further messages (guidance, 2.87).

The current guidance is ambiguous as to what providers should do if the sender does not respond to the provider's request for information. Which? believes that Ofcom's guidance could be strengthened by making it clear that, if the provider does not receive a response from the sender regarding the legitimacy of the communications, the provider should infer that the messages were intended to scam people and block the sender from sending further messages. Elsewhere in Ofcom's proposals, the regulator has set a deadline of one working day for senders to provide evidence that they were not responsible for sending scam messages (for example at consultation 5.83). Which? proposes that Ofcom should give providers the same time period - one working day - to respond to a request for information. This policy would need to be made clear in providers' contracts with business senders, and providers would need to clearly communicate with business senders that they will be blocked unless they provide the required information in the given timeframe. In a situation where a business sender does not provide the information within the three working day limit, but does then provide information demonstrating that their message was legitimate, providers should be required to unblock the business sender immediately.

Incident management requirements

Ofcom's proposals require action to be taken where the provider reasonably believes scam messages have been sent by a business (guidance, 2.116). They must confirm who sent the suspected scam messages within one working day if they hold a direct relationship with them, and within three working days if they do not (guidance, 2.117 and 2.118). Unless there are mitigating circumstances, providers should place restrictions on the accounts of businesses found to have sent fraudulent messages (guidance, 2.121). Which? agrees with this proposal.

Contractual relationships

Where a provider is not directly involved in onboarding a business sender, Ofcom will require that they must set clear and unambiguous terms for the party from whom they receive the A2P messages to either undertake KYC, alphanumeric sender ID and KYT checks, or ensure that these checks have been conducted by a party in the downstream chain (guidance, 2.91). Ofcom expects providers to cease accepting messages from a party which has been found to be non-compliant with contractual requirements on a regular basis (guidance, 2.96). Which? agrees with this proposal.

Question 8: Do you agree with our proposals to require mobile operators and tier 1 aggregators to identify and block scam messages on A2P channels?

Ofcom has proposed that providers must implement 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 (guidance, 2.54).

Which? agrees with this proposal in general. However, as we highlighted in our response to question 5, there is an issue around the messaging of this requirement. Ofcom should make it clear in the wording of the proposal that it is not sufficient to simply receive scam intelligence, but that operators must also proactively request information relevant to blocking scams from a wide range of sources on a regular basis. Moreover, operators should be required to share their intelligence with other operators, with banks, and with law enforcement.

Question 10: Do you agree with our cross-cutting measures, including our proposed approach to persons being notified of their blocked messages or numbers in certain circumstances; the right to challenge; record keeping; staff training; and ensuring that regulated providers continue to comply with relevant data protection legislation?

Ofcom is proposing to require providers to establish policies, systems and processes to support the right to challenge the blocking of a measure by automated means (consultation, 5.125). Providers should also establish and maintain effective systems for keeping records to demonstrate and ensure continued compliance (consultation, 5.135). Providers must ensure that all staff are appropriately trained on the policies, systems and processes put in place (consultation, 5.139).

Which? agrees with Ofcom's proposals. Consumers should be notified if their messages have been blocked (i.e. due to volume limits), and they should have the right to challenge any decision to block their messages (for instance, if they were sharing a scam URL as a warning to their contacts).

We also suggest that Ofcom's guidance should oblige providers to make their customers aware of their rights to alternative dispute resolution if they believe that they have been harmed in some way by a measure such as message blocking.

Question 12: Do you agree with our proposed new GC C9?

Which? disagrees with one aspect of Ofcom's proposed new GC C9. Under Ofcom's currently proposed GC C9.3, providers must implement and maintain appropriate and effective policies, systems and processes which are "designed" to prevent mobile numbers from sending scam messages, to block messages from the numbers of suspected scammers, and to block messages which contain known scam URLs. In Which?'s view, it is not sufficient that processes should only be 'designed' to achieve the desired effect. We therefore propose that Ofcom remove the word 'designed' from the draft text. We note that other proposals under the new GC C9 do not contain this word. For example:

- 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…
- 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…
- 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 Customer reaches any volume limit imposed by the Regulated Provider…

In the interests of clarity, Which?'s proposed GC C9.3 would read as follows:

Taking into account Scam Reports received, Regulated Providers must implement and maintain appropriate and effective policies, systems and processes to:

a) prevent, without undue delay, Mobile Numbers they have assiged to a Customer from sending P2P messages where they reasonably believe those Mobile Numbers have sent P2P Messages intended to Scam the 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.

Question 13: Do you agree with the guidance we have proposed, including our expectations on how providers could comply with the new requirements, if implemented?

In general, Which? agrees with the guidance that Ofcom has proposed. However, Which? feels that Ofcom could clarify in section 1 of the guidance that the guidance is not statutory. Moreover, Which? feels that Ofcom should add wording emphasising that it can depart from the guidance based on individual circumstances. There is precedent for Ofcom making such statements. For example, Ofcom states in its guidance under General Condition C1 - contract requirements that "this guidance is not binding on Ofcom, and while we will take it into account, we will determine compliance with Condition C1 on the basis of the individual circumstances of the given case." In Which?'s view, such a statement would be helpful for Ofcom if it is seeking to take enforcement action which arguably goes further than the wording in the guidance, but which still falls within a reasonable interpretation of the new General Condition C9 on preventing mobile messaging scams.

Question 14: Do you agree with the proposed implementation periods for our proposals?

Ofcom is proposing a six month implementation period for its P2P messaging proposals and a 12 month implementation period for its A2P messaging proposals. Which? recognises that providers need time to prepare for new duties, and we believe that the time period set out by Ofcom is sensible.

We think it is important that Ofcom bear in mind its own calculation that mobile messaging scams cause £65 million in financial losses from UK consumers every year (consultation, 3.20). Given the scale of the financial harm caused, it is imperative that Ofcom does not allow its implementation timeline to slip, as has regrettably been the case for Ofcom's implementation of the Online Safety Act. Ofcom must also ensure that providers do not delay implementation of the new rules, as was the case for the implementation of the One Touch Switch programme, which was delayed from April 2023 to September 2024 due to delays on the part of providers. Ofcom must therefore undertake robust and proactive monitoring to provide assurance that operators will implement these proposals according to the agreed timeline.

About Which?

Which? is the UK's consumer champion, here to make life simpler, fairer and safer for everyone. Our research gets to the heart of consumer issues, our advice is impartial, and our rigorous product tests lead to expert recommendations. We're the independent consumer voice that works with politicians and lawmakers, investigates, holds businesses to account and makes change happen. As an organisation we're not for profit and all for making consumers more powerful.

For more information contact:

Matt Niblett
Senior Policy Advisor
matt.niblett@which.co.uk

January 2026