Ofcom consultation on combating mobile messaging scams

Introduction

1. Mobile UK welcomes the opportunity to respond to Ofcom's consultation on combating messaging scams.

2. We agree with Ofcom that this criminal activity causes harm and undermines confidence in communications services. We welcome Ofcom's recognition that mobile operators already take significant steps to reduce the incidence and impact of messaging scams, including volume limits and SMS blocking. In 2025, mobile operators blocked more than **1.4 billion** text messages, approximately 5%[i] of the total number of SMS sent in a year.

3. The vast majority of blocked messages came through the person-to-person (P2P) route, and so Mobile UK also welcomes the steps being taken by the Government in the Crime and Policing Bill against the possession and supply of SIM farms.

4. As Ofcom mentions, operators also receive about 100 million reports to the 7726[1] Spam Reporting Service (SRS) each year. Following measures introduced at the device level, this number has risen steeply in recent years. Now that 'direct from device' reporting (e.g. *'this message looks like spam, do you want to report it?*) is more or less universal, reports received in January 2025 (10.1m) were more than ten times the number received in January 2023.

5. The benefit of the new approach is that operators get to hear of new scam texts more quickly. The disadvantage, though, is that the quality of reports has been eroded. Only a small minority of reports (perhaps less than 10%) relate to genuinely harmful text messages. The remainder is made up of unwanted spam, service messages, and even genuine messages being mistakenly reported. The SRS database is the source of intel for new scam text messages and remains a vital element of the anti-scam ecosystem.

6. While the SMS filters are very effective, it must be recognised that the risk of false positives (i.e. overblocking) is ever-present, and so operators need, and indeed have, tight processes for ensuring over-blocking is kept to a minimum and that customers have a route to resolution, if a legitimate message is ever blocked.

[1] 7726 is the original name for the operators' spam reporting service. Today, though, the great majority of reports come from single-click reporting directly from the device.

Comments on the proposed measures and guidance.

7. Mobile UK's overall stance to the consultation and to the proposals is supportive. We share Ofcom's determination to minimise messaging scams. Our response has therefore focused on a few key elements where we would urge Ofcom to adjust its proposed approach.

Cross-cutting measures

8. Mobile UK's strongest objection to Ofcom's proposals arises in the General Condition C9.17 "*Where a Regulated Provider has blocked a message under Conditions C9.3(b), C9.3(c) or C9.7 using automated tools, the Regulated Provider must, without delay, notify the person whose message they blocked or otherwise enable that person to become aware their message has been blocked.*"

9. Bearing in mind that the overwhelming majority of messages being blocked are being sent by the scammers, this proposal is impractical, disproportionate, and counter-productive. The scammers are already adept at modifying their scam messages to frustrate the SMS blocking systems. We should not be put in a position where operators must alert them proactively and enable them to react any more quickly than they already do.

10. We would urge that this requirement is removed.

11. It should be noted that we are not entirely clear how the 'challenge' process (new GCs C9.18-C9.19) will work in practice for offnet messages on the P2P channel. Is the customer supposed to challenge with their provider – who will not have done the blocking themselves, or the third-party who did the blocking – who will not be able to verify that this customer is legitimate? We note there is some flexibility offered (para. 5.128) but we would nonetheless welcome further discussion on this aspect.

Contractual requirements

12. In GC9.9, Ofcom has set out detailed requirements for contractual terms. We understand that this is to ensure that terms and conditions are passed down the contractual change.

13. The guidance (in paras 2.94 to 2.96) also sets down onerous requirements on the regulated parties to take action to enforce GC9.9, including imposing financial penalties on their counterparties, including other regulated parties.

14. This is a very burdensome requirement and a hard thing to impose on other commercial parties, who may even be competitors in some way or another, or where damning evidence has come through intelligence sharing (with the resulting risk of

operators appearing to 'gang up' on a third party). It is not always easy for operators to obtain the necessary evidence when some 'bad action' is suspected to have occurred.

15. Mobile UK suggests that enforcement and imposing financial penalties on regulated parties fall much more naturally into the domain of Ofcom. Operators should be able to refer potential non-conformance to Ofcom and not be drawn into assessing, imposing, and collecting financial penalties etc. on commercial partners.

GC 9.27 – duty to deliver messages

16. The bulk of the new general condition and guidance is placing a heavy burden on operators to take all necessary steps to ensure scam SMS are not sent on to the intended destination. Condition 9.27 requires that all 'good' SMS be delivered to their intended destination. The operator is thus forced to walk a tightrope of double jeopardy for non-compliance, and this is not proportionate.

17. Operators' business is to deliver the text messages they have contracted to deliver; they do not need a General Condition to ensure this happens. It is also relevant to point out that the vast majority of problematic SMS are sent through the P2P route, not A2P.

18. In good faith, Operators have voluntarily introduced SMS spam filters in the interests of the public good and the protection of customers. If the SMS firewalls return false positives, in other words, block texts they should not have blocked, operators will have to face the potential consequences with their commercial partners. They should not also be exposed to a potential Ofcom fine for non-delivery.

Concluding points

19. Mobile UK and its operator members are very supportive of taking all reasonable steps to combat scam text messaging; all members have signed up for Sector Fraud Charters 1 and 2.

20. We urge Ofcom, though, to reconsider the points we have raised in our response. These specific points in the proposals are not required or proportionate in the circumstances.

21. It should also be noted that the blocking of 2.6bn SMS since January 2022 has caused the scammers to react, not only within the domain of SMS, but they have also migrated to other platforms, such as WhatsApp etc.. For anti-scam work to be effective, the scammers must be met with resistance on all fronts, and the platform operators held to account in the same way that mobile operators are. We would

therefore expect Ofcom to be talking to the parties responsible for such platforms about measures to combat scam messaging there too.

22. Finally, if Ofcom is not minded to accept any of the changes we have suggested – and we very much hope they are minded – the implementation timetable should be extended to 12 months.

[i] Based on 28m, Ofcom Communications Market Report 2025