General

Ofcom call for inputs: reducing mobile messaging scams

BT Group response

7 October 2024

BT Group

Executive summary

Please note we consider sections highlighted in blue to be confidential

- Where BT/EE is acting as provider of a service (i.e. in Short Messaging Service – SMS) we are – in general – supportive of the measures described in Ofcom's call for inputs and have already introduced measures described on a voluntary basis.
- We are in favour of further initiatives in the SMS market (such as bans on SIM farms, more data sharing - both within the communications sector and between industries - and extension of existing limitations around sender IDs) but expect most of these to be outside the direct regulatory remit of Ofcom. In general, we do not believe that entirely novel regulatory initiatives in the SMS market in the UK (mandatory SIM registration, Sender ID registries) would deliver consumer benefits at this time given the high cost, complexity, and time involved in implementation.
- We do not hold sufficient data to estimate the impact of any given channel in delivering scam messages to end users as our information in SMS is limited to (i) traffic we block and (ii) malicious traffic reported by end users. Moreover, we do not hold reliable information on the extent to which scam SMS messages are successful in achieving their intended aims. We expect this to be available from third parties, such as banks.
- We hold limited information on the extent to which services not provided by us – such as Online Communications Services (OCS) or Electronic Communications Services (ECS) run by third parties – are leveraged by criminals to commit fraud.
- We note scams traffic across communications networks is often dynamic – putting up barriers on a given channel/route can lead to an increase in volumes elsewhere. It is important, therefore, that Ofcom – and others - use the full suite of their respective powers to take action against criminals operating in this space. , This is particularly important given, as underlined by Ofcom research, growth in scams messages appears to be focused on 'app-based' messaging which should, therefore, be the primary focus of any 'joined up' approach to scams messaging prevention.
- The suggestion that Rich Communications Services (RCS) might be an ECS does not align with how the service operates in the UK. We would welcome further discussion with Ofcom on this assessment. ✂
- ✂ Any new initiatives to help protect end users are likely to require the intervention of the owner/operator of the platform.

1. Future interventions in SMS should focus on areas already under consideration by Government

BT/EE has been at the forefront of efforts to prevent SMS scams reaching end users…

1.1 As part of BT's drive to 'Connect for Good', we are committed to working with our partners to help protect users of communications services from scams and fraud , not only because trust in our services means customers choose to continue to use them, but because protecting customers is the right thing to do.

1.2 Alongside our partners, we have worked hard in recent years to ensure that criminals – many of whom are linked to organised crime groups – are hampered in their efforts to use SMS platforms to contact end users . Measures now in place include:

- Advice on our website for consumers on how to spot/report an SMS scam;
- The 7726 platform which allows end users to report suspected scam SMS when encountered on any network. Data from this platform – which is now regularly shared with Ofcom – can be used to provide intelligence on trends and emerging threats in SMS;
- The Spam Shield filter, which was first deployed on our network in 2021. Its initial deployment lead to an initial 85% reduction in the total number of scam messages reported to us by EE customers;
- A Code of Conduct for aggregators/specific brands on use of Sender IDs in our A2P channel.

✂

… new measures in SMS should focus on those which have already received widespread stakeholder and policymaker interest

1.3 While we have taken substantive steps to prevent criminals from contacting customers via SMS, we know that some fraudulent traffic continues to get through. To address this traffic, we are in favour of policymakers taking further steps, with the aim of:

- Ensuring "trusted lanes" policies and "Codes of Conduct" are supported by all SMS providers (including aggregators);
- Delivering on policy initiatives which have already been suggested by MNOs around establishment of cross-MNO/cross-sector intelligence sharing and SIM farm bans given they already enjoy wider support across sector participants.

1.4 There are a set of measures discussed in Ofcom's document which we do not believe would be appropriate at this time – either because of the prohibitively high cost or because the administrative challenge involved to roll them out would likely lead to delays which would be unacceptable from a scams prevention perspective.

1.5 We set these three categories out below.

Ensuring existing policies are supported by sector participants

1.6 ✂

1.7 While we believe that Ofcom should make clear – for example via industry forums or guidance – that it supports such an approach being rolled out across the industry, we do not think it would be appropriate for these systems to be placed on a formal regulatory footing - i.e., introduced as new/existing General

Conditions , with associated enforcement action for breaches. Such an approach might add unnecessarily delays to processes and hinder our responsiveness to novel issues.

Interventions outside Ofcom's direct regulatory remit

1.8 Ofcom should consider using its influence with wider policy stakeholders – including the Government, other regulators, and market participants from other industries – to drive forward initiatives which have already been consulted on/are already being introduced via pilot projects. These measures include:

- Driving forward mooted legislation on banning SIM farms, which will then facilitate robust law enforcement action against criminal groups attempting to commit fraud in the UK. The UK Government had completed a consultation exercise on this prior to the 2024 General Election but it is not clear at the time of writing that legislation will be (re)introduced;
- Encouraging enhanced cross-MNO/cross-sector intelligence sharing which would allow a risk-based and intelligence-led approach to scams prevention. MNOs and sector participants from other industries currently approach blocking on a unilateral basis, meaning that threats need to be identified multiple times by multiple actors. While some sector participants are already working to deliver on these initiatives, we see opportunities to make this process more efficient – in particular, this requires data regulators to make clear in relevant guidance that fraud prevention is a legitimate reason for data sharing. This might be an appropriate work item for the Digital Regulators' Forum to consider.

Where we believe action would be inappropriate

1.9 We do not believe there is sufficient evidence to support the introduction of a (mandatory) Sender ID scheme at this time, given the likely high costs involved and the fact that there are more appropriate protections (set out above) which might achieve a similar effect. We have concerns about the complexities involved in the administration and operation of mandated schemes, and in particular that some senders might find that they are unable to send traffic if they have not appropriately engaged with new governance arrangements. This might ultimately prevent 'good faith' actors from sending successful communications to end users.

1.10 We have limited recent evidence on the costs, impacts, and any potential benefits of a SIM registry schemes as these have not been introduced in the UK. However, we note that international case studies suggest that these schemes do not necessarily prevent SIM fraud.[1] ✂. Moreover, careful consideration would be required regarding how such a programme might work in practice given it might result in service for some users (in particular if it meant retroactive registration of existing SIMs – ✂.) This must be considered against the current system, whereby SIMs known to be sending high volumes of 'bad' traffic can be blocked by respective MNOs.

2. The relative importance of any single route must be framed in its wider context

The interconnectedness of SMS infrastructure means there are a range of entry points for bad traffic into the ecosystem

2.1 Ofcom is correct in its characterisation of A2P and P2P channels as the channels through which SMS traffic (including malicious traffic) reaches end users, with P2P communications facilitated by interconnect between MNOs where users are on different networks. The two channels, however, are not entirely independent as implied by the Ofcom document, given that bad actors can switch to one channel should

[1] https://www.gsma.com/solutions-and-impact/connectivity-for-good/public-policy/wp-content/uploads/2013/11/GSMA_White-Paper_Mandatory-Registration-of-Prepaid-SIM-Users_32pgWEBv3.pdf

more stringent checks be introduced in another. This applies equally to traffic outside the SMS ecosystem (e.g. more checks on the SMS ecosystem might lead to malicious traffic moving to other platforms).

2.2 ✂

2.3 More broadly, while the openness of the UK telecommunications ecosystem has provided substantive consumer benefits through – for example, lowering barriers to switching and ensuring that communications services have remained affordable – it means that bad actors wishing to send malicious traffic over communications networks face fewer challenges in doing so. We think it is important that this trade-off is recognised and understood by policymakers given the range of interventions currently being considered in the messaging sector..✂[2]. ✂.

We do not have adequate data to define the harm in SMS –our information on other platforms is currently limited

SMS

2.4 In SMS, we do not have access to a definitive dataset which maps all end user interactions with suspicious communications nor detail on whether/when these have been successful (this information is most likely to sit with third parties, such as banks). Our data is limited to where end users have reported suspicious traffic, and information regarding where we have blocked traffic through one of our existing systems.

2.5 We note that Ofcom's most recent findings from its extensive research in this area implies that there been a decline in the number of SMS users receiving suspicious traffic since 2022.[3]

2.6 However, we believe better information sharing between sectors and participants would support provision of more granular information to allow policymakers in Ofcom and elsewhere to make more informed assessments of the impact of different interventions. We discuss this in greater detail above.

2.7 At time same time, data on the relative 'importance' of a specific channel is likely to be of limited value without data on wider scams performance (including reported frauds). This is due to the dynamic nature of the problem which means criminals often choose to migrate to a new approach in circumstances where existing channels are closed.

Third-party platforms (including RCS)

2.8 BT/EE provides network connectivity (either via the mobile network or – depending on the application – via the fixed network) to support users in accessing messaging services run by other platforms (such as RCS, WhatsApp, and iMessage, among others). In certain circumstances, SMS might be used in setting up these services – these SMS messages used for set up would be subject to existing protections already put in place by BT/EE. ✂.

[2] ✂

[3] https://www.ofcom.org.uk/siteassets/resources/documents/research-and-data/telecoms-research/scams-research/experiences-of-suspicious-calls-texts-and-app-messages-research-2024.pdf?v=373453

3. We are unable to introduce scams protection measures on RCS and other platforms administered by third parties

3.1 We note that the Call for Inputs suggests in Table 1 (page 13) that RCS services should be considered an Electronic Communications Service –ECS- (and therefore distinct from Online Communications Services), but that Ofcom has chosen not to set out further the reasoning for this. The suggestion that Rich Communications Services (RCS) might be an ECS does not align with how the service is operating/will operate in the UK. Ofcom should consider more comprehensively the extent to which the phone number is used for identification purposes and whether – if at all – it is used for routing. Such an approach – with appropriate engagement with interested parties – is required to ensure all parties are clear on the regulatory framework and associated obligations. Clarity for market participants on the regulatory regime is particularly important given that RCS use is expected to grow in the medium term.

3.2 ✂

3.3 We would welcome the opportunity to discuss these points further with Ofcom as appropriate.

Find out more at bt.com

Offices worldwide

Any services described in this publication are subject to availability and may be modified from time to time. Services and equipment are provided subject to British Telecommunications plc's respective standard conditions of contract. Nothing in this publication forms any part of any contract.

Registered office: 1 Braham Street, London E1 8EE

Registered in England No. 1800000

BT Group