Vodafone Response to
Ofcom Call for Input:
Reducing mobile messaging scams

Evidence and options for addressing consumer harm

1. Introduction

Vodafone welcomes the opportunity to provide input to Ofcom's Call-For-Input (CFI) regarding reducing mobile messaging scams. We proactively seek to reduce such scams, in order to minimise the impact both on our own and other Mobile Network Operators' (MNOs') customers. We operate a firewall which seeks to eliminate scams using our SMS services, and monitor reports from mobile customers in order to refine our blocking.

2. Answers to Questions

Question 1:

Do you agree that the routes described in this chapter cover all of the main methods that scammers use mobile messaging services to scam people? If not, please explain other methods.

An unfortunate artefact of the different regulatory regime that applies for messaging services is that the scope of this CFI is inevitably compromised. Consumers do not care that there is a regulatory distinction that SMS and RCS are considered to be Public Electronic Communications Services hence regulated by Ofcom, whereas applications such as Whatsapp! and iMessage sit outside that regime. Indeed, the threading together of messages from different platforms into a single application on mobile devices means that in many cases users will be unaware of whether an individual message has been delivered by a given service – we have concrete evidence of this by the volume of reports for e.g. iMessages which are reported via the 7726 SMS reporting platform.

We therefore believe that any analysis of the danger of fraudulent messaging is ultimately doomed if it is restricted to the sector of the market regulated by Ofcom. To be effective, the analysis should cover all mobile messaging platforms, and for example Apple and Meta should be engaged to give their perspective.

We also believe that Ofcom should include MMS within the study, once again on the basis that few consumers would recognise the distinction between SMS and MMS. We have not seen scam usage of MMS on any mass scale since Flubot in 2022, but it still presents a risk. It should be noted that Flubot switched to using MMS once the MNOs had been able to make a significant impact blocking the perpetrators' SMS with Spam Shield (our firewall implementation) and using other means.

Question 2:

Which routes do you think are the most important today and will be over the next 3 years for the perpetration of mobile messaging scams? Please provide evidence for your views.

It's difficult to answer this question with any certainty, but as ✂.

iMessage too will likely remain a problem whilst Phishing as a Service (PhaaS) platforms such as ✂ exist, allowing fraudsters easy access to send RCS and iMessage scams. We expect similar ongoing issues with Whatsapp!.

SMS will remain a problem to some degree, mainly over the P2P channel, but we believe that this can be constrained by more effective use of SMS firewalls by all MNOs and Mobile Virtual Network Operators (MVNOs) that have their own SMS infrastructure.

In 2021 Vodafone was seeing ✂ scam SMS per day from its SIMs; effective firewall deployment has driven this down to ✂ scam SMS per day, demonstrating that our measures have had a very positive effect in reducing phishing over SMS.

Question 3:

Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?

✂

The SIMs used for this activity are geographically clustered, indicating highly organised activity. Initially the SIMs were used in a limited number of devices, but since Vodafone has been taking action to bar the SIMs and block the devices, a lot of the threat actors have begun spoofing IMEIs. We have also seen evidence of threat actors rapidly porting the relevant numbers to third party MNOs in order to circumvent our blocking service to them.

Question 4:

Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?.

We would firstly highlight that RCS/iMessage should be included in the analysis, and we disagree with Ofcom's decision to exclude the latter from scope. We can see some reports against RCS/iMessage scams in the 7726 database, but Google and Apple should be approached in relation to the spam databases they hold, as what we have vis is likely to be the tip of the iceberg.

An internet search for "RCS scams" yields Reddit pages showing screenshots of scams sent over RCS by UK mobile numbers to mobile customers of overseas networks, for example in the US. Vodafone and the other UK MNOs do not have visibility of reports against our numbers by non-UK mobile customers, but Google would have this visibility for RCS, as would Apple with regards to iMessage.

The RCS and iMessage scams reported to 7726 are largely related to Royal Mail or Evri phishing, mostly following the same content and URL templates, suggesting a ✂ is being used. However, there are likely to be other types of phishing RCS/iMessage that we have no visibility of.

For SMS, the bulk of the scams we see are sent via P2P channel, with a small minority over A2P. The nature of these scams currently include:

- Delivery scams, mainly purporting to be from Evri (mainly P2P) ;
- Wrong number ("Pig Butchering") scams, mainly sent over A2P, using numbers rather than alphanumeric senders so that replies can be received;
- Hi Mum/Hi Dad scams (exclusively P2P)
- Albanian Boss scams, purporting to be the manager of an escort, claiming the victim has wasted his escort's time, and threatening violence if a payment is not made immediately. (P2P)
- Bank scams, asking the victim to reply N, or call a number if they don't recognise a payment, or didn't request an OTP (mainly P2P)
- iPhone location scams – "your lost iPhone is found – click here to locate or lock your phone" (P2P)

The SMS and RCS scams we see are almost exclusively sent by numbers, with a very small minority sent with alphanumeric sender IDs. The iMessage scams we can see are sent by a mixture of UK or overseas mobile numbers, and email addresses.

Question 5: What is your understanding of which channels are supporting the greatest harm (such as A2P or P2P SMS, or RCS)? Please provide any supporting evidence.

For SMS, we consider that the ✂. The monthly reporting shared with Ofcom by the MNOs might highlight which networks' SIMs are delivering the highest volume of scam SMS.

We do not have visibility of the real levels of RCS or iMessage scams, so if Ofcom wishes to get an holistic view of the scope for consumer harm, then it is imperative that it asks Google and Apple for reporting equivalent to the reporting the MNOs are sharing each month so the levels and nature of scam traffic can be compared and understood.

Question 6:

What do you think will happen to RCS availability and adoption in the next few years? Please provide supporting evidence and or reasons for you views.

We think it inevitable that ✂. Scams follow the presence of potential victims, so we would expect the level of scams using RCS to increase too.

Question 7:

Do you have views on the effectiveness of the measures discussed in this chapter? For measures where we have identified specific issues, please comment on these in your answer, providing reasoning and evidence if possible.

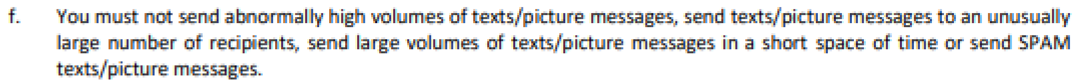
Taking each of the points raised in the CFI in turn:

5.9 We believe consideration should be given to whether and how volume limits could be made more effective as a tool for disrupting scammers, without disrupting legitimate use.
We would welcome views on how this could be done and the issues involved, including on:

- **How limits should be set and what constitutes a reasonable need;**
- **Whether limits should be standardised;**
- **What action should be taken if limits are breached; and**
- **What monitoring of limits should take place.**

Vodafone limits new PAYG and VOXI SIMs to ✂. Similar limits are in place for MMS, limited to ✂. The SMS usage cap was implemented in 2021 and made an immediate impact, with PAYG and VOXI usage for scams plummeting as a result.

The ✂ was determined after analysis to find a level that would limit the fraudsters' ability to send mass SMS, but not impact legitimate users. Since its implementation we have received zero related complaints, and users who hit the cap are automatically in breach of the terms of our Acceptable Use Policy[1], including:



f. You must not send abnormally high volumes of texts/picture messages, send texts/picture messages to an unusually large number of recipients, send large volumes of texts/picture messages in a short space of time or send SPAM texts/picture messages.

We cannot comment on other MNOs' current SMS limits, so do not know if standardising them across MNOs would have a positive effect. If Ofcom has visibility of the current limits across the MNOs, as well as the levels of reports against each networks' SIMs, this might assist in decision making. However, rather than a mandated hard limit, a cap could be mandated with wording such as *"each MNO must implement an SMS/MMS cap that prevents a fraudster sending x messages within a single hour, while limiting the negative*

[1] https://www.vodafone.co.uk/cs/groups/configfiles/documents/contentdocuments/acceptable-use-policy-may-2024.pdf

impact on legitimate message senders". We note that it might not be technically possible for all MNOs to apply an hourly cap.

Vodafone does not ✂. Multiple detection processes are run in parallel, but separately, to the caps to bar SIMs suspected of sending scam messages. These use datapoints such as ✂ to make an informed decision on whether a SIM is likely sending scam SMS, before barring them as quickly as possible.

5.13 We would welcome views on whether SIM registration requirements merit any further exploration in the UK.

Superficially, proper SIM registration requirements, including ID checks, would significantly reduce the volume of PAYG SIMs that are used to send scam messages, or receive OTP messages to set up Google/Apple (and other online service) accounts. However, it is inevitable that fraudsters would find their way around most protections, for example by using dupes and stolen identities to apply for the SIM cards. Further, we believe that such measures would be unpopular with legitimate customers. We therefore believe the regulatory case is difficult to establish.

5.17 We would be interested in respondents' views on whether a similar approach to IMEI suspension could be effective in the UK.

✂

5.32 We would welcome input from stakeholders on how else intelligence is shared amongst aggregators and operators and any ways in which this could be improved.

Together with other MNOs, Vodafone is part of the Messaging Scams Group (MSG) which meets regularly to share intelligence and decide actions to combat scams. ✂.

5.34 We would welcome views from respondents on what more can be done to make the A2P route more impervious to scams. In particular we are interested to understand views on:

● What could be done to further drive good practice amongst the aggregator sector;

● Whether more standardisation would help to close the loopholes that scammers have sought to exploit;

● How effective KYC checks are across the aggregator supply chain, especially where there are many parties involved in the delivery of messages; and

● How best to mitigate associated supply chain uncertainties, such as by building on the contractual obligations and dedicated connections described above, taking steps to reduce the number of parties in the supply chain, or other methods.

We must firstly stress that a minority of scam SMS originates from A2P sources. This said, we would support a review of whether regulation of aggregators would be beneficial; there is clearly a difference in the effectiveness of some aggregators over others at addressing the issues raised in this CFI. To drive it down further, some MNOs may need to ✂ if they don't already.

5.48 We are interested in exploring whether and how the use of these tools can be made more effective across industry. We would particularly welcome views from stakeholders on:

● Should more parties, like MVNOs and aggregators, be making use of similar tools?

● How can existing tools and the human systems around them be better configured, or made more sophisticated?

● Would more consistent implementations across parties, and better-quality information sharing improve blocking efforts, and how might these be achieved?

Transparent best practice sharing across all the MNOs would be very useful. As all four MNOs are ✂: there is thus potential ✂, suggesting improvements and rules that could benefit all networks.

For MVNOs with their own SMS infrastructure, similar SMS firewalling should be implemented otherwise it's likely their SIMs will be heavily targeted by fraudsters realising they can send more scam SMS.

5.50 We would welcome further input from stakeholders on what can be done, and on what is being done, to identify suspicious RCS messages in transit.

Vodafone does not have visibility of RCS messages in transit: any identification would need to be carried out by Google and Apple.

5.62 (regarding sender ID registries) For the UK, we are interested in stakeholders' views on the best way forward. Broadly, there appear to be two main approaches:

- **Firstly, to continue with the registry run by the MEF and to seek to make it more effective (such as through wider adoption by brands that haven't yet signed up, or by moving closer to a real time approach); or**
- **Secondly, to switch to a mandatory approach as adopted by other countries described above, which would need to be run by an appropriate organisation.**

We have not seen evidence that the current MEF approach is proving ineffective, so would favour making enhancements to this rather than starting with a new regulated model. If brands shared their aggregator partner and sender IDs with the MNOs, and their contract with said aggregator was appropriately robust, then the use of their sender IDs could be controlled even more effectively.

5.74 We would welcome suggestions of any of other approaches which could be used to effectively support consumer education on mobile messaging scams.

It could be appropriate for Ofcom and/or the MNOs to set up dedicated pages on their websites to highlight the latest scam message campaigns that have been seen, in order to raise awareness. However, we must be realistic that these are unlikely to be consumers' most desired web visits.

5.79 We welcome input from stakeholders on any ways in which handset-based solutions could be improved or used further to help consumers..

Our understanding is that Google and Apple's one-touch spam reporting solutions ✂.

Question 8:

Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?

We remain open to additional measures, but do not have any to contribute at this stage. However, we must stress that any formulation of measures must take an holistic approach including all messaging platforms (including those which have been ruled out-of-scope for this CFI), otherwise spam and scam traffic will just migrate to platforms with weaker controls.

Question 9:

Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?

We believe that the priority should be fully understanding the size of the RCS and iMessage (and maybe WhatsApp) scam issue - Ofcom's engagement with Google and Apple is likely a good first step to determining priority areas. It is worth noting that iMessage and RCS allow free of charge international messaging, so it might be found that UK SIMs are creating accounts that are used to scam overseas mobile customers at scale.

In terms of SMS, we believe that better intelligence and best practice sharing between the MNOs should be a priority. This would allow all MNOs to take other ideas to be implemented to further reduce scam traffic by making full use of the tools available.

Vodafone UK
October 2024