UK Finance

Ofcom Call for Input: Reducing Mobile Messaging Scams

Oct | 2024

Ofcom Call for Input: Reducing Mobile Messaging Scams

Representing 300 firms, we're a centre of trust, expertise and collaboration at the heart of financial services. Championing a thriving sector and building a better society. This includes helping lead the industry's collective fight against economic crime in the UK, including combatting fraud and cybercrime. This response is representative of our diverse membership and follows a series of member-led engagements.

Executive Summary

We are pleased to see Ofcom's Call for Input on reducing mobile messaging scams, which will contribute to wider the control framework applied in the communications environment. Our members are very supportive of Ofcom's engagement with further measures that could help to reduce the proliferation of fraud through mobile messaging scams, which continues to be a source of harm for victims.

- In addition to our response, we welcome further engagement with Ofcom on the consumer harm from scam texts and discussions around further measures to help reduce scams. Telecommunications were the source of 16% of the volume of APP Scam cases in 2023*. This is likely to be heavily SMS based, as smishing often overlooked when victims make their scam reports. The SMS received typically leads onto a vishing call.
- The industry welcomes Ofcom's exploration of new features that will help to reduce the perpetration of scams through mobile messaging scams. The FS sector is supportive of:
    - The SenderID Registry becoming mandated, as it can be comprehensive solution once all brands are onboarded. Courier brands for example are often impersonated and are the gateway, resulting in a huge loss to banking customers, there needs to be more of a focus in getting other brands onboarded to this solution.
    - mandatory registration of SIMs, and stronger governance around the requirements for registration, bulk sims in particular. This should include ID requirements and payments should only be acceptable where the registrant details match the purchaser.
    - improving the intelligence flow of spam reports from services like 7726, device manufacturers and OCS providers should all share their spam

reports. All of this is public reporting and should not be restricted bypaywalls that inhibit consumer protection.

- improving the blocking of dangerous URLs through a share/defend system, and

- It is necessary to consider that the routes used by fraudsters to perpetrate messaging scams will continue to evolve, and as measures to address vulnerabilities in all routes need to be undertaken holistically, fraudsters will adopt lower usage routes. There are three core areas of concern
    - The banking industry share's Ofcom's concerns over increased adoption of Rich Communication Services (RCS). Of particular concern is the potential capability through RCS for fraudsters to imitate legitimate brand names as well as the encrypted nature of RCS.
    - UK Finance accepts that OCS services are out of scope for this Call for Input. OCS messaging types also need to have controls imbedded. Experience demonstrates that phishing has migrated from email to SMS. Safer SMS will cause migration onto OCS, as seen in the Netherlands. There is a need for equivalence in OCS messaging control measures to mirror those implemented with SMS.
    - Standardisation/equivalence of regulation to mitigate across all messaging routes irrespective of Short Message Service (SMS) or Online Communications Services (OCS) infrastructure.
    - For the SMS blasters that can entirely circumvent existing SMS controls, whilst the MNOs do have a method for identifying this, it would be helpful to share if there was some detail around this and how governance around it could be built to ensure that FIs are covered if they are targeted.

- UK Finance is broadly supportive of the measures discussed in this call for input, however, there is a need for a more strategic view to implement these measures in a holistic way across all messaging infrastructures, rather than through a segmented lens of SMS Vs OCS.
- Currently reporting is *typically* led by the consumer or the Financial Services referring the smishing campaigns to the telcos to take down the number distributing the messages. This is retrospective and too late as the criminals messaging campaigns have landed and they are waiting for victims to respond. There is a need for Ofcom explore with the telcos how they can notify users who may have received the reported smishing text distributed

ifrom the identified sender by sending some form of alert to warn those receivers this was a scam message. And share advice on how to protect themselves or help the targeting person avoid responding. This is important especially as the industry is starting to see smishing campaigns that have evolved to no longer include URLs.

Section 3: The mobile messaging market and how scams are perpetrated

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.

Yes.

(Covers P2P and A2P sms, RCS, RCS emulators and spoofing sender IDs, SMS blasters OCS not in scope of document)

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.

The financial services industry is very concerned that there will be a rise in the adoption of RCS and OCS services for the perpetration of scams, this is because ntethe messaging traffic will typically be encrypted and operated over data rather than the Mobile Network infrastructure. It is important to note that as measures are implemented to address vulnerabilities within the mobile routes, fraudsters will likely migrate to lower usage routes, making them more prominent. A proactive and holistic approach to tightening up regulations and vulnerabilities in all messaging routes is therefore necessary, as the victims experience the same harms irrespective of the infrastructure the message reach the device.

Also, the consumer handsets need further regulation and controls to force the adoption of best practices, that will protect consumers from criminal activities such as ensuring:

- One time passcodes are obfuscated on locked devices.
- That messages are not automatically grouped or renamed, forcing them into existing messaging threads.
- There are usability features that balance the protection of users with genuine use e.g., new calls from unknown numbers can be supressed, but if you are expecting a call from your bank or law enforcement these would be from new phone numbers and be sent to voicemail.

Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?

RCS is free globally, and unregistered SIMs are used across the world which makes SIM farms more viable, traceability harder and means that criminals across the globe can more easily target UK consumers.

There are two particular concerns around RCS as a route for scam messages:

- Brand impersonation: This has been raised in the Philippines where RCS scam messages have been sent outside cellular network leveraging RCS. Though RCS may help brands become more recognisable in its communications through RCS brand registration, the concern is that this will provide consumers with a false sense of security if criminals are able to emulate brand IDs.
- As RCS will be using data and encrypted, there mobile operators will not be able to apply the current SMS firewalls to mitigate scam messages. The operators that create RCS infrastructure or outsource their RCS capabilities need to apply heuristic controls to stop suspicious traffic entering the consumer environment.

Section 4: Evidence on mobile messaging scams

Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?

SMS Samples, ask members, for nature: OTP bot

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.

There is an unknown volume of messaging that are reaching the public from OCS services, these services carry vast volumes of messages. The victim experience of receiving rogue messages are the same regardless of the infrastructure and as such they should be subject to equivalent regulation.

From an FS sector viewpoint, our understanding is that A2P (standard SMS) is causing the greatest harm at present, with an expectation that this will migrate and or increase with RCS due to the credibility of brand identification capabilities now this is available via iOS and Android.

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.

RCS availability is expected to increase exponentially, as increased scalability has been triggered via iOS adoption in UK in September. The FS sector shares Ofcom's concerns with potential emerging fraud threats that will come with RCS, as well as the opportunities. We anticipate that due to RCS brand credibility the criminals will migrate to RCS at pace due to the increased credibility, lower traceability, use of data rather than mobile networks which will not have SMS firewall protections.

Criminals are inventive at leveraging new technology that consumers are not familiar with, and exploiting gaps int technology as was seen with the SMS Blasters exploitation.

Section 5: Measures taken to disrupt mobile messaging scams

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.

We have outlined are views on the effectiveness of measures discussed below:

Further input on measures proposed

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

UK Finance and its members are supportive of further exploration of mandating SIM registration, this will increase traceability and act as a criminal deterrent. Even if false ID is used there will be common locations of criminals attempts that will aid disruption efforts of law enforcement. This is also mandatory in many regions of the world, linking IDs to Sim registration occurs in several regions etc.

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

We welcome originating providers having the option of blocking the IMEI of devices used for fraudulent communications.

In Australia, an industry code registered by the Australian Communications and Media Authority (ACMA) requires originating providers to investigate and undertake appropriate action to block fraudulent texts that originate from their own customers, including the option of blocking the IMEI of devices used for fraudulent communications

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?

Yes – all parties that can apply controls must have obligations once carrying a certain volume of messaging traffic etc. Additionally, MVNOs and aggregators should be required to use tools that monitor message patterns, including blocking of SMS with dangerous URLs within them.

This should be applied to the OCS service providers also, even if they have encrypted platforms the heuristic indicators can help mitigate scaled attacks.

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

There is a need for more consistent grades of messaging traffic, with priority on government, banking, regulators and law enforcement messages. This would also allow greater proportionality of controls for enterprise traffic.

There needs to be greater restrictions on traffic that have malformed names, generic names such as 'system upgrade' to prevent criminals leveraging entry points where there is no brand infringement rights to help protect consumers.

A large volume of the prolific and generic SenderIDs could be sourced from the SenderID registry, MNO rules or firewalls and the tier one aggregators.

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

Yes – Sharing of common links, rogue aggregators and 7726 public reporting access can help close the net on criminal activity.

The financial services sector could also explore supplying victim reports received directly.

Businesses that are targeted with impersonations are having their brands damaged, this is band for both the economy and trust in messaging. It is imperative that Ofcom seeks to tighten the intelligence flow across the messaging ecosystem to protect consumers, currently there are too many barriers. Victims that report messages to 7726, device manufacturers and OCS are not currently safeguarded adequately, the Financial services could provide extra layers of protection to victims that have received rogue messages. Currently this is a missed opportunity.

There is great opportunity for the Financial services(FS), Law Enforcement and Telcos to share more intelligence with each other. Information around the criminals trying to onboard the sim and distributing the smishing campaigns, combined with FS that see huge mule networks behind attacks to move the money, would be powerful. We recommend regular intelligence sharing meets and or Proof Of Concepts around

smishing samples to form a new data sharing agreements once we can evidence the power of it etc.

There should be mandatory communications provided to messaging users, to help them understand protection and reporting opportunities.

5.62 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

The FS sector is supportive of switching to a mandatory approach, as there needs to be a commercialised/functional approach to advancing the tools capabilities. The MEF sender ID registry has been very successful, but a mandatory approach is necessary to ensure widespread adoption that closes gaps in participation the ecosystem.

A mandatory approach will greatly improve clarity, and user awareness of the distinction between alphanumeric IDs that are genuine.

5.67 We are not aware of other tools, such as sender ID registries, designed to specifically protect brand IDs for RCS, but would welcome input from stakeholders if other mechanisms are used.

UK Finance has had engagement with some forms of RCS capable companies, which appear to be designed to protect brand IDs for RCS through an onboarding registration process. This is more prevalent in the USA, and we believe there are other tools such as the Mobile Ecosystem Forums.

5.85: We welcome input from stakeholders on how consumers could be better supported to report suspicious messages. For example, are there ways to make reporting tools more widely accessible to consumers, and could more be done to distinguish between suspected scam and spam messages (either through consumer facing services or through design of back-end systems used for analysis)?

For consumers to be better supported when reporting suspicious messages, there needs to be greater transparency and feedback to the user when they make the report via 7726. Feedback such as when the reported number has been investigated or removed, as well as the outcome of the investigation into the suspected scam message would help to increase user confidence. The reporting tool could provide

information about the suspected scam that was being attempted, increasing consumer awareness.

All public reporting tools must not have paywalls for other sectors that could help safeguard victims.

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;

Some Mobile Networks already has quite low limits on messaging, there have been small business exceptions such as window cleaners or horse betting syndicates that use personal SMS allowances as a business tool. This could be dealt with via a T's and C's upgrade.

Limits must be to be combined with sufficient business verification of legitimate business users, as well as an expanded mandated sender ID registry.

• Whether limits should be standardised.

There should be a low volume upper limit set/reviewed by the regulator periodically as a minimum, and the services can take a risk-based approach, below this to tighten if they wish to.

• What action should be taken if limits are breached; and

There needs to be alerts that trigger either a block or review where over a certain volume of SMS messages are sent. This will support proportionate controls. There should be best practices available from some Mobile Networks.

• What monitoring of limits should take place.

It would be logical to use historical traffic as an indicator of standardised norms on volumes and the current run rates. Also, comparisons of criminal usage in OTP bots etc to determine how criminals are circumventing the limits.

Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?

There are several measures Ofcom should seek to incorporate in its assessment, including:

- The intelligence from public report via 7726 needs to be shared across other sectors, including the links /numbers/ contents who's sent it for law enforcement pursuit. This was within the Home Office Telcom charter and still needs unlocking. Ofcom should mandate the consumer/public reporting options and information sharing requirements to safeguard victims. Public

reporting intelligence should not be paywalled, as this is not in the interest of the consumer.

- Messages that have legitimate sender IDs but have rogue phone numbers in content e.g. which are not on DNO list should be blocked by messaging providers.
- Improving reporting and blocking of scam texts and dangerous URLs – support for the NCSC share and defend system would encourage greater participation and improve consumer protection. However, to ensure intelligence around threat actors techniques are not lost the dangerous URLs would need to be shared with both Law enforcement and the Financial Services sector to maintain visibility of the threat landscape.
- Mandating 2FA and avoid knowledge-based questions unless they can't be commonly known, for example using the number and date of messages last sent would be better than mother's maiden name.

Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?

There must be sufficient grading of SMS traffic, for example having Bank. Govt and law enforcement in one lane, commerce in another lane and general traffic third lane to apply different rulesets that can impact misrepresentation such as impersonation.

A further priority area is proactive anticipation and mitigation of widespread criminal activity as RCS is further adopted, and its potential to provide an additional or amplified social engineering route for messaging scams. If managed services are used by MNOs to run RCS – they need to require due diligence on managed services to detect heuristic indicators of high risk and mitigate the activity, not simply state speak to managed services – as managed services will state that they are all encrypted. Services supplied needs to have fraud/risk controls.