Your response

Question	Your response
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.	**Confidential? – N** Yes. The routes described by Ofcom cover all the main methods by which mobile messaging scams are perpetrated.
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.	**Confidential? – Y Please treat items highlighted in yellow as confidential.** We believe that most mobile messaging scams currently originate by P2P SMS (including, but not limited to SIM farms) and A2P SMS: • Fraudsters can procure SIM farm kit easily and cheaply and obtain a PAYG SIM without the need to register their personal details or submit to identity checks, which makes P2P SMS particularly susceptible to abuse. • High volumes of A2P SMS are sent over the Three network (✂). Only a small percentage is likely to be fraudulent, but this is significant as a proportion of overall volumes. Based on volume, we anticipate that these routes are likely to remain the most important over the next 3 years
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	**Confidential? – N** No.
Question 4: Are you aware of other relevant data sources on the scale or nature of scam messages sent over SMS and RCS?	**Confidential? – N** We are not aware of other relevant data sources. In order to glean meaningful insight on the scale and nature of scam messages sent over RCS, we recommend that Ofcom engage directly with the internet platform provider, Google, which undertakes its own SPAM prevention and detection checks.
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.	**Confidential? – N** Fraudulent SMS, MMS or RCS messages can be the starting point of sophisticated scams which have devastating effects. We cannot meaningfully quantify the extent of the consumer harm caused by mobile messaging scams or attribute that harm to specific channels.

Question	Your response
	We have, however, set out our thoughts on volumes, which are ranked below from most to least prevalent: • P2P SMS (including, but not limited to, SIM farms) and A2P SMS • P2P RCS and A2P RCS Although we believe that P2P and A2P SMS are the routes which account for the most significant volumes, UK communications providers, including Three, make extensive efforts to monitor and filter/block SPAM and fraud in the SMS channel, thereby reducing harm to the end user. Whilst there is always more that can be done and we remain wholly committed to addressing such scams, the annual survey published by the ONS (referred to in paragraph 4.16 of Ofcom's Call for Inputs) reinforces our belief that the measures deployed cross-industry are increasingly effective, with only 1% of victims of fraud mentioning that they were first contacted by SMS. In common with other UK communications providers, Three has no visibility of the content of A2P or P2P RCS messaging services (which are provided to UK based customers from internet platforms operated by Google and are subject to end-to-end encryption), nor can we evaluate the volume of P2P RCS and A2P RCS scams. Our understanding of this service is limited and indirect. However, onboarding new A2P RCS agents (branded Sender IDs used for RCS campaigns) relies on a business verification process managed by MNOs. Aggregators, who manage the direct relationships with brands, may offer various operating models (API or CRM connector, self-service portal or full managed services). Whenever a full managed service is offered, aggregators build the campaigns on behalf of the merchants and have full visibility over the RCS campaigns (including content and call to action). This adds another layer of protection to the A2P RCS flow. For this reason, we believe that A2P RCS traffic accounts for the least harm overall.
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.	**Confidential? – Y - Please treat items highlighted in yellow as confidential.** Three customers using an Android device have been able to access RCS for some time. ✂, RCS coverage for Three customers will double overnight and will almost be on par with SMS. As such, we anticipate that RCS volumes will significantly increase from as early as January 2025. We cannot meaningfully forecast the rate at which P2P RCS volumes will grow but we do know that we are already enabling A2P

Question	Your response
	RCS use cases for large merchants ✂ and that this is only the beginning. ✂. It will take a while before RCS represents a material portion of A2P traffic. ✂

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.	**Confidential? N**
	
	Criminalising SIM farms
	
	We wholly support the criminalisation of SIM farms.
	
	Volume Limits
	
	We consider that it is for each individual communications provider to set volume limits and determine what action should be taken if such limits are breached. However, we endorse the approach set out in the CCSG's response to Ofcom's Call for Inputs and agree that Ofcom and providers should discuss fraud countermeasures in a moderated forum to develop a dynamic best practice approach.
	
	Due diligence checks in the aggregator chain
	
	Information Sharing
	
	We see value in greater information sharing between aggregators, including:
	
	• MNO sharing of information on blocked A2P traffic to aggregators, in order that they may also apply blocks and;
	• Timely updates from aggregators to MNOs if they have blocked suspicious campaigns and believe that some fraudulent traffic may have slipped through the net.
	
	What could be done to further drive good practice amongst the aggregator sector
	
	• We consider that aggregators should implement firewall protection solutions and have dedicated staff in place to monitor A2P/RCS SMS traffic (specifically large campaigns) to prevent fraud and spam.
	  ○ We believe that all aggregators should work with the MEF (and support the Sender ID Registry initiative) to ensure that they are sending messaging campaigns in a controlled manner.
	  ○ We note, with interest, the yellow and red card system referred to in Ofcom's Call For Inputs and agree that a yellow and red card system could be applied to Tier 2 partners by Tier 1 aggregators where Tier 2 partners are responsible for sending spam and smishing campaigns.

Question	Your response
	Standardisation • While we believe that best practice should be shared, we consider it should be left to aggregators to determine which firewall technologies or business processes best work for their organisation. Effectiveness of KYC checks across the aggregator supply chain, especially where there are many parties involved in the delivery of messages. • This is a shared responsibility between the originator of the campaign, the aggregator and all the actors in between. It would not be fair to expect that aggregators should own the end-to-end responsibility for this process. Hence, it is important for merchants and public sector bodies to have a good grasp of how the messaging campaigns they initiate are routed, through how many hops, etc. Aggregators are a conduit in the same way as MNOs, and they can only impose obligations on the party that they contract with but not all of the parties upstream (between the originators of the campaign and them). We welcome a stronger collaboration between the originators of the campaign and the MEF to ensure that those who communicate with their customers, patients, etc. do so in a controlled manner. 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. • MEF's Sender ID registry has this issue at the core of its initiative. Their scope of work could be extended, and the cross-industry collaboration strengthened. **Traffic Monitoring Tools** Should more parties, like MVNOs and aggregators, be making use of similar tools? • MNO's detection and monitoring activities also benefit MVNOs that share the SMS infrastructure of their parent networks. We consider that spam monitoring and detection tools should be deployed: i) by MVNOs not using their parent network's SMS infrastructure and; ii) to messages received by aggregators from their client in order to filter

Question	Your response
	traffic on their own messaging platforms, before such traffic is sent to the MNO. This additional layer of protection would enhance overall spam detection capabilities. How can existing tools and the human systems around them be better configured, or made more sophisticated? • Regular audits should be undertaken of existing configurations and new product features should timeously be implemented to facilitate better detection. Would more consistent implementations across parties, and better-quality information sharing improve blocking efforts, and how might these be achieved? • An information sharing approach is already in place via 7726 reporting, which each MNO accesses to review recent trends and further optimise their spam detection and filtering strategies. As those reports appear close to real-time, MNOs can timeously identify and respond to new threats. • While we believe that best practice should be shared, we consider it should be left to the parties to determine which firewall technologies or business processes best work for their organisation. Sender ID registry We consider that a mandatory approach to Sender ID registration would be impracticable due to the volume of Sender IDs used in the A2P SMS flow. ✂. Mandating the registration of Sender IDs would be so labour intensive that it would cripple the A2P flow for months until the process is completed. Each merchant or public sector body would first need to do an audit of the Sender IDs that they use in their channels, go through a rationalisation journey and only after that be in a position to register the Sender IDs. We consider that Ofcom should explore ways to make the MEF registry more effective and encourage wider adoption. However, we note that maintaining the registry with up-to-date Sender ID information creates an overhead for the MEF which would increase if the scope of Registry initiative were to expand.
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	**Confidential? – N** As mobile messaging scams are often the enabler of much more sophisticated frauds, we encourage closer cross-sector collaboration with the financial services sector.

Question	Your response
	Communication providers have invested significant resources to keep the A2P SMS channel clean. However, knowing it is impossible to completely eradicate fraud, we have developed and deployed 6 Verification APIs which facilitate real-time access to mobile operator data to achieve more effective fraud detection and prevention, business risk management and user identity verification. We consider that financial services institutions should work more closely with communications providers to jointly tackle more sophisticated frauds and explore more extensive use of the customer identity verification services on offer.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	**Confidential? – N** • Criminalisation of SIM farms • More effective cross-sector collaboration with financial services institutions.

For completeness, we would also like to take this opportunity to clarify a couple of the statements made by Ofcom in its Call For Inputs:

Paragraph 1.4 of the CFI states as follows (our emphasis added in bold):

> *"Mobile network operators are blocking around 30 million suspicious SMS messages per month in the UK.* ***However, scam SMS and RCS messages are still getting through****. Over half (56%) of mobile phone users report having received a suspicious text message in the past three months, though encouragingly this is down from 74% in 2022. There are significant areas where the data we have reviewed is not conclusive, so we are seeking further input from stakeholders.*

For the avoidance of doubt, communication providers do not have an ability to block RCS messages.

Paragraph 4.14 of the CFI states as follows (our emphasis added in bold):

4.14 SpamShield data has limitations meaning that it is difficult to draw firm conclusions about the scale of messaging scams using it in isolation. Some scam messages still get past Spamshield where it is in place, and SpamShield is not applied to all mobile messaging. For example, MVNOs with their own Short Message Service Centre (SMSC) do not use SpamShield and some MNOs do not put all A2P traffic through it, as discussed in the next chapter. ***It cannot scan the content of RCS messages due to encryption".***

We would emphasise that SpamShield is a firewall module present in our SMSC. RCS is a data product that doesn't rely on Three network elements. Accordingly, SpamShield cannot possibly scan the content of RCS messages as RCS traffic doesn't transit via our SMSC.