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 Ofcom correctly identifies call-to-action and phishing scams as two primary methods scammers use to reach UK consumers. Call to action messaging scams include various strategies including: HTTPS phishing, banking scams, prize and lottery scams, and service cancellation or suspension scams. These messages often reach consumers through SMS spoofing, SMS pumping or artificially inflated traffic (AIT), SMS trashing, SMS grey routes, SIM swapping, SMS roaming intercept fraud, and SMS malware (SMS hacking). Below are brief definitions and examples of each. **SMS Spoofing** occurs when the sender's information in a text message is falsified to make it appear as though the message is coming from a trusted source (e.g., a legitimate business, known contact, or familiar phone number). The goal of SMS spoofing is often to deceive the recipient into providing sensitive information, such as passwords or payment details, or to trick them into clicking on malicious links. **SMS pumping**, also known as Artificially Inflated Traffic (AIT), refers to a scam where a fraudster generates an abnormally high amount of SMS traffic by exploiting vulnerabilities in a telecom provider's network or billing system. The objective is often to drive up costs, as carriers and organizations are charged for each SMS sent, causing financial losses. The fraudster usually profits by receiving a share of the inflated traffic charges. **SMS trashing** refers to the practice of discarding or deleting legitimate SMS messages before they reach their intended recipients. This can happen due to a variety of reasons, such as fraudulent activities that intercept messages containing important information (e.g., one-time passwords or transaction alerts). SMS trashing can prevent critical communications from being received and can be used to disrupt services or communication channels. **SMS grey routes** involve the delivery of messages using unauthorized or unapproved channels to bypass standard billing agreements and avoid the proper costs associated with sending messages through legitimate routes. These routes are referred to as "grey" because they operate in a legal grey area – they are not outright illegal but violate the agreed upon regulations or practices of telecom operators. This often leads to poor quality or delayed message delivery.

Question	Your response
	SIM swapping is a type of fraud where a scammer gains control of a victim's mobile phone number by tricking a mobile carrier into transferring the victim's phone number to a SIM card controlled by the fraudster. Once the attacker gains control of the phone number, they can intercept SMS messages, including two-factor authentication (2FA) codes, and potentially access the victim's banking or social media accounts. **SMS roaming intercept fraud** occurs when scammers exploit vulnerabilities in mobile networks to intercept SMS messages sent to a mobile user while they are roaming in another country. This type of fraud is often used to capture sensitive information, such as one-time passwords or banking alerts, during the time the user's device is communicating with foreign networks. The intercepted information can then be used for unauthorized access to accounts or transactions. **SMS malware**, also known as SMS hacking, involves the use of malicious software that is delivered via text messages to infect a mobile device. Once the malware is installed, it can allow hackers to steal person information, track the user's activities, or control the device remotely. SMS malware often disguises itself as a legitimate app or link in a message and can spread through deceptive tactics like phishing.
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? –N According to Mobilesquared research shared in an Infobip blog post on SMS fraud, the most significant routes for mobile messaging scams over the next three years are Artificial Inflation of Traffic (AIT), Grey Routes, and Spam. AIT is identified as the highest threat, followed closely by Grey Routes, which evade proper oversight, and Spam, which continues to grow in scale. These routes exploit vulnerabilities in SMS networks and are likely to remain prevalent due to their profitability for fraudsters.
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – N According to the Android Police, "scammers have started sending spam texts to people in the US through spoofed phone numbers using end-to-end encrypted RCS messages, posing a new security concern." Sinch claims that there are 6 types of SMS spoofing that include: fake sender IDs, unsolicited bulk messages, harassment, corporate espionage, fake money transfers, and identity theft.

Question	Your response
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 At this time, iconectiv UK Limited has elected to not respond on this matter as we continue to research SMS and RCS scam messages.
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 The greatest harm from messaging scams largely depends on the type of channel being exploited. While all channels can be exploited, A2P SMS is more frequently abused and supports the greatest harm due to its scale, usage, and economic incentives. A2P SMS is frequently exploited for scams like SMS spoofing, SMS pumping (AIT), and phishing. Since A2P SMS is used by businesses and services to send notifications, alerts, marketing messages, and one-time passwords, it has become a significant target for fraudsters due to its widespread usage and financial value. A2P SMS supports large volumes of traffic from businesses to users, making it an attractive target. Scams like SMS pumping and grey routes take advantage of the commercial nature of A2P traffic by generating high volumes of fraudulent SMS that lead to inflated billing costs. The Impact of Fraud on A2P SMS Monetisation report issued by the Mobile Ecosystem Forum (MEF) estimated that fraudulent A2P traffic could account for up to 30% of all A2P SMS traffic, costing businesses and telecoms billions annually. The high economic stakes, combined with the volume of messages involved, make A2P SMS one of the most significant channels of harm.
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? – N The adoption and utilization of RCS (Rich Communication Services) are poised to accelerate significantly in the coming years. With Apple's recent decision to integrate RCS in the upcoming iOS 18 update, the technology will enjoy a broader global reach. RCS has already gained substantial traction among Android users, who are reaping the benefits of its features, including higher text limits, larger file transfers, and enhanced branding opportunities. According to Sinch, business adoption of RCS surged by 40% between June 2022 and June 2023. Furthermore, the global RCS subscriber base is projected to grow from 1.2 billion in 2022 to 3.8 billion by 2026, accounting for 40% of all mobile subscribers worldwide. The global RCS market, valued at $8.37 billion in 2023, is forecasted to reach $19.48 billion by 2028.

Question	Your response
	As communication trends evolve, subscribers are likely to see a reduction in traditional A2P SMS campaigns, with a gradual shift towards richer and more interactive channels like WhatsApp and RCS. These platforms offer enhanced features such as multimedia support, improved engagement, and personalized messaging, aligning better with modern user expectations. Mobile operators face several challenges with RCS, including ensuring the security of communications, as RCS offers advanced features that need to be protected from potential threats. Additionally, the implementation process can be complex, requiring significant infrastructure updates. Finally, enterprise adoption remains uncertain, as businesses weigh the benefits of RCS against the widespread use of established platforms like WhatsApp and other over-the-top messaging applications.
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 **<u>Volume Limits Effectiveness & Implementation</u>** Volume limits should be based on typical traffic patterns, with notifications or suspensions applied if limits are exceeded. These limits should be standardized across the industry, ensuring consistency. If limits are breached, traffic should be suspended once a specific percentage above the limits is reached. Monitoring of traffic and volume should occur in real-time at the MNO (Mobile Network Operator) level to detect and act on anomalies quickly. **<u>Driving Good Practice Among Aggregators</u>** To encourage good practices among aggregators, an agreed-upon set of industry standards should be developed, ideally by the MEF (Mobile Ecosystem Forum), which is well-positioned to lead this initiative. **<u>Effectiveness of KYC Checks in the Aggregator Supply Chain</u>** KYC (Know Your Customer) checks can be effective during the post-registration and onboarding processes. However, deeper inspections should be conducted as a standard procedure to ensure compliance, especially in supply chains with multiple parties involved. **<u>Collaboration for Fraud Reduction</u>** The true solution to mitigating fraud lies in ecosystem-wide collaboration. Each entity holds valuable information that, if shared across the network, could significantly reduce the number of fraudulent messages slipping through undetected.

Question	Your response
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	Confidential? – N Industry forums have discussed other measures that can assist in addressing messaging scams. These include: 1) trusted trunks, 2) A-B Matching ID Attestation Hub, and 3) In-Band Crypto-Signed Campaign IDs. The "Trusted Trunk" approach involves creating a verified list of specific A2P messaging entities, including aggregators and CPaaS providers, that are authorized by the enterprise sending the messages. This list would be established at the time of campaign or enterprise registration. By ensuring that only these designated entities can send messages on behalf of the enterprise, this strategy limits potential fraudulent actors from entering the messaging pipeline, ensuring trust and accountability. "A-B Matching" uses an ID Attestation Hub (IDAH) to verify various attributes of a business message. Essentially, the IDAH cross-checks ("matches") key elements of the message, such as the sender identity, campaign details, or routing information, against known, verified attributes. The hub confirms the legitimacy of the sender and the message, ensuring that the content and origin of the SMS align with the registered details of the business. The "In-Band" method involves embedding cryptographically-signed CampaignIDs directly into the message. These signatures are generated using secure cryptographic techniques that verify the integrity and authenticity of the campaign data. The receiving network can check the crypto-signature to confirm that the message originates from a legitimate source and that it hasn't been tampered with en route.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – N iconectiv UK Limited urges Ofcom to prioritize cooperation and partnership amongst all messaging ecosystem participants to jointly agree to solutions, taking account of the international scope of the messaging network.

Please complete this form in full and return to mobilemessagingscamsresponses@ofcom.org.uk.