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, we agree that the chapter covers all the routes scammers use to scam people, i.e., SMS via A2P or P2P and RCS.
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 Currently, SMS is an important route as most services in the UK, including government, telecom, entertainment, delivery companies, and banks, use SMS to share updates with their customers. We collaborate with a major UK mobile network operator (MNO), which provides us with 3.58 million SMS messages flagged by SpamShield that were sent to 2.23 million mobile numbers in the UK between December 2023 and February 2024. We present the distribution of over 39k unique sender IDs abused by scammers to send illicit messages and identify eight categories, including spam [1]. We show that scammers impersonate organisations/companies and family/friends to deceive users by sending SMS via the P2P route [1,2] or spoofing A2P sender IDs [3] to steal sensitive financial information. With the growing implementation of RCS, we expect the perpetration of mobile messaging scams to shift to RCS over the next three years. Previous research indicates that scammers migrate to platforms following the target victims [4,5]. In line with prior research, we expect scammers to migrate to RCS along with general population. As of November 2023, Google reported 1 billion active users with RCS enabled in Google Messages, and Apple has recently rolled out RCS with its iOS 18 update. In our current research, we collaborate with a major UK MNO that provides us with four months (May 2024 - July 2024) of 7726 user reports. Performing textual analysis, we estimate that approximately 15% of all reports are RCS messages. This indicates that scammers have already started the perpetration of mobile messaging scams to shift to RCS. (Note: This research is currently in the process of submission to a conference; it is not publicly available.) [1] Agarwal, Sharad and Harvey, Emma and Marie Vasek. “Poster: A Comprehensive Categorization of SMS Scams.” In Proceedings of ACM Internet Measurement Conference (IMC) 2024.

Question	Your response
	[2] Agarwal, Sharad and Harvey, Emma and Mariconti, Enrico, and Suarez-Tangil, Guillermo, and Vasek, Marie. "'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom." In Proceedings of 34th USENIX Security Symposium 2025 (USENIX Security 25). USENIX Association. [3] https://www.helpnetsecurity.com/2022/09/20/revolut-data-breach-phishing/ [4] Carlson, Eric L. "Phishing for elderly victims: as the elderly migrate to the Internet fraudulent schemes targeting them follow." Elder LJ 14 (2006): 423. [5] Moore, Tyler and Han, Jie and Clayton, Richard. "The postmodern Ponzi scheme: Empirical analysis of high-yield investment programs." In Financial Cryptography and Data Security: 16th International Conference, FC 2012, Revised Selected Papers 16, pp. 41-56. Springer Berlin Heidelberg, 2012.
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – N We do not have evidence of scammers' tactics for accessing RCS messaging. However, industry articles have pointed to scammers using programmable scripts and device farms that automatically send iMessage and RCS texts in bulk [1]. We also believe this could be done by simulating messaging apps using virtual machines. [1] https://www.netcraft.com/blog/darcula-smishing-attacks-target-usps-and-global-postal-services/
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 The chapter already discusses the two major data sources - 7726 user reporting service (including Apple and Google's one-click) and SpamShield. We have identified additional data sources, including online discussion forums such as Reddit and X (formerly known as Twitter). Using particular keywords like 'smishing' and 'sms scam' results in many user-reported scam messages over SMS and RCS. Other data sources include forums such as smishtank.com, 800notes.com, scammer.info, telecom community forums, and fraud reports submitted by victims to their banks and Action Fraud. Additionally, working groups like the Anti-Phishing Working Group (APWG) run data-sharing services like the eCrime exchange service (https://apwg.org/ecx/) who have recently started collating phishing SMS messages. We also believe that Google and Apple are

Question	Your response
	the most significant sources of scam messages over RCS. Google processes user-reported messages to enhance spam detection [1]. [1] https://support.google.com/messages/answer/9061432
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 We collaborate with a major UK mobile network operator, which provides us with 3.58 million SMS messages flagged by their firewall. These messages originated from over 42k unique sender IDs and were sent to 2.23 million mobile numbers between December 2023 and February 2024 [1]. We discover eight different categories of scam messages, including spam. The 'Wrong number' scam and 'Hi mum and dad' scam messages abuse a significant majority of mobile numbers as sender IDs (P2P) to initiate the message and continue their interaction with victims to lure them into providing financial details [1,2]. An arrest by the DCPCU shows that these scammers use SIM boxes to broadcast and communicate with the victims [3]. We also access four months of 7726 user reports (including Google's one-click reports). We find that P2P SMS forms the majority of cases in these reports too. As SpamShield serves as a firewall only for SMS, we want to understand the abuse of RCS for scam messages. To this end, we search for messages above the 160-character limit originating from a mobile number in 7726 user reports. We estimate that 14.7% of all reports are unique RCS messages. While this number is comparatively lower, 7726 reports only get RCS text messages forwarded manually by users. Google does not share the RCS text messages blocked or reported by the users in their messaging app to mobile network operators' 7726 data feed. (Note: our analysis of 7726 user reports is in the process of submission and is not publicly available.) [1] Agarwal, Sharad, and Emma Harvey, and Marie Vasek. "Poster: A Comprehensive Categorization of SMS Scams." In Proceedings of ACM Internet Measurement Conference (IMC) 2024. [2] Agarwal, Sharad and Harvey, Emma and Mariconti, Enrico, and Suarez-Tangil, Guillermo, and Vasek, Marie. "'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom." In Proceedings of 34th USENIX Security Symposium 2025 (USENIX Security 25). USENIX Association. [3] https://www.linkedin.com/posts/dcpcu_police-operations-investigations-activity-7088103726455877632-8hQV

Question	Your response
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 Users are becoming more privacy-conscious and have started migrating to secure communication channels. RCS provides encrypted messaging communication to users and has been enabled by default on all mobile phones using Google's messaging apps. Apple has also implemented RCS in the release of iOS 18. As Google reports in the previous chapter, users have already started adopting RCS. As users shift from SMS to RCS, scammers have also started migrating to RCS to lure victims into scams. Prior research indicates that scammers tend to follow victims (as explained in Q.2). Our study supports this as we find that 14.7% of 7726 user reports are RCS messages, and scammers have started abusing RCS to deceive victims. Due to encryption, the same measures as SpamShield cannot be implemented for RCS, making it challenging to identify and stop 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.	Confidential? – N SMS Volume limits 1. Limits on SMS should be set based on the type of SIM card, i.e., pay-as-you-go and pay monthly. In order to avoid abuse, pay-as-you-go should have a much smaller limit than the pay monthly ones. The pay-as-you-go SMS limit should be extended based on usage over time, which, in principle, is similar to a credit limit. Businesses could request the MNOs directly for larger limits, where required, for commercial purposes. There should be a clear distinction in limits for individual and business purposes. With the pay monthly, mobile network operators can already identify the entity/person abusing the SIM cards as they perform credit checks before issuing a SIM card. However, implementing limits for individuals might have negative consequences, such as scammers registering businesses in the country or using stolen identities to set up SIM cards. 2. Having standardised limits would help avoid scammers from abusing a particular mobile network operator's service over others. 3. If limits are breached, mobile network operators should check the reason and suspend service for SIM cards for illegitimate usage as it would violate their terms and conditions. If the body of the SMS is potentially malicious, the mobile network operator should further investigate

Question	Your response
	and report this to law enforcement agencies to take appropriate action. 4. Mobile network operators should monitor the SMS sending patterns of the users, such as if they are sending SMS to various mobile numbers simultaneously or whether SpamShield has previously flagged the body of the message. This monitoring will help identify abuse of SIM cards, and the services could immediately be suspended. SIM registration requirements In most cases, scammers abuse pay-as-you-go monthly SIM cards and virtual mobile numbers to send scam messages. Ofcom should suggest that mobile network operators perform SIM registration for pay-as-you-go and virtual mobile numbers. This would help identify the users if they abuse SIM cards. Additionally, this would increase the cost for scammers to procure SIM cards, making it difficult for them to send scam messages. However, there is a trade-off for individuals who do not have IDs for KYC verification. IMEI suspension We believe that the IMEI suspension could effectively mitigate scams in the UK. Linking a SIM to an IMEI number could help mobile network operators identify the kind of device being used and suspend services if the device is a stolen phone or a SIM farm. This would significantly increase the cost for the scammers as once an IMEI is detected for abuse, scammers cannot use the same device with multiple SIM cards to send scam messages. This would also support the measure to limit SMS by creating an IMEI watchlist, which could help detect a device using multiple SIM cards in a short span of time. Intelligence Sharing We are unaware of aggregators and MNOs currently sharing intelligence data with each other. We suggest sharing intelligence signals data feeds like flagged SMS content, malicious domains, and scammer mobile numbers via common secure repositories such as NCSC Shared and Defend. Sharing incident data feeds could also help other operators and aggregators to take faster actions and be prepared in advance. A2P routes impervious to scams 1. Ofcom should utilise the ‘code of practice’-style documents governing aggregators’ use of bulk messaging services by the two MNOs, as mentioned in the chapter, and create a standard code of practice that every MNO

Question	Your response
	should follow. The ‘whitelisting’ or ‘trusted traffic’ policies should be standardised across the aggregator sector. 2. KYC checks across the aggregator supply chain could effectively stop sender ID spoofing and should be a part of the standard practice to stop scam campaigns. Effectiveness of measures to protect customers We analyse two months of SpamShield data from one major UK MNO that indicates that they have been quite successful at protecting customers by blocking over 89% of harmful SMS messages [1]. [1] Agarwal, Sharad, and Emma Harvey, and Marie Vasek. “Poster: A Comprehensive Categorization of SMS Scams.” In Proceedings of ACM Internet Measurement Conference (IMC) 2024. Traffic monitoring tools 1. Our research indicates that scammers do abuse MVNOs and virtual mobile numbers to deceive victims through P2P scam messages [1]. As already mentioned in the chapter, it is known that scammers also abuse aggregators to conduct A2P scams. We suggest that MVNOs and aggregators use tools like SpamShield to stop scams over SMS. Implementing traffic monitoring at the aggregator level could help stop scams before they reach the MNOs. 2. Tools like SpamShield should use threat intelligence data from various antivirus vendors and threat intelligence companies to detect and block harmful texts containing malicious URLs. Deep inspecting SMSs could help identify and block unidentified scammer numbers. Rules known to work on SpamShield filtering should be implemented on SpamShield by Mavenir to work across all MNOs instead of each MNO configuring the firewall rules themselves. 3. Better information sharing among MNOs, MVNOs and aggregators could help identify and stop harmful texts before they harm the public. As soon as any operator or aggregator detects malicious text, they should share the information with others to block similar text messages or SMS containing the same malicious URLs. Consistent implementations of monitoring tools could help stop known threats across all networks. SpamShield provides the flexibility to set new rules based on intelligence signals, which could be easily shared among all mobile network operators and aggregators. Operators and aggregators

Question	Your response
	could use a central repository or database, such as NCSC's Share and Defend, to share identified intelligence signals. [1] Agarwal, Sharad and Harvey, Emma and Mariconti, Enrico, and Suarez-Tangil, Guillermo, and Vasek, Marie. "'Hey mum, I dropped my phone down the toilet': Investigating Hi Mum and Dad SMS Scams in the United Kingdom." In Proceedings of 34th USENIX Security Symposium 2025 (USENIX Security 25). USENIX Association. Identify suspicious RCS messages in transit RCS messages use mobile numbers as sender IDs. Mobile network operators should share the list of identified harmful mobile numbers with companies like Google so they can block RCS messages going out from those mobile numbers. Similar to SMS, scammers broadcast RCS messages to lure multiple victims simultaneously, and therefore, using message frequency and hash of the text could help identify and block suspicious RCS messages. Sender ID We suggest that Ofcom let MEF continue with the registry but enforce the pricing structure to make it affordable for brands to register with them for sender identity protection. If this path is decided, Ofcom and MNOs should make the brand registration for MEF mandatory to stop sender ID spoofing. Efficacy of these additional policies Currently, various brands have been using different aggregator services that provide them with more than one sender ID. We suggest that the allow listing policies should be updated so that MNOs can utilise the MEF sender ID registry to whitelist the sender IDs and block the other suspicious ones. This would provide MNOs the ability to cross-check against the registry for brands before starting campaigns or allowing SMS messages through SpamShield filters. Effectively support consumer education Two academics, Stajano and Wilson, explain seven lures to understand why victims fall for scams [1]. We apply these to the initial 'Hi mum and dad' scam messages and the complete conversations with scammers. We find that scammers use kindness, distraction, and time/urgency principles to deceive victims into 'Hi mum and dad' [2]. Users of messaging applications should be made aware of the lures identified to stop them from falling prey to such scams.

Question	Your response
	Elderly people are generally susceptible to scams [3]. There should be programs set up to educate them about technology. The stakeholders, such as banks, should work with MNOs and the government to make people aware of scams and the routes scammers abuse to lure victims. If someone is too kind online, it probably is not true. [1] Stajano, Frank, and Paul Wilson. “Understanding scam victims: seven principles for systems security.” Communications of the ACM 54, no. 3 (2011): 70-75. [2] Agarwal, Sharad and Harvey, Emma and Mariconti, Enrico, and Suarez-Tangil, Guillermo, and Vasek, Marie. “‘Hey mum, I dropped my phone down the toilet’: Investigating Hi Mum and Dad SMS Scams in the United Kingdom.” In Proceedings of 34th USENIX Security Symposium 2025 (USENIX Security 25). USENIX Association. [3] James, Bryan D., and Boyle, Patricia A. and Bennett, David A. “Correlates of susceptibility to scams in older adults without dementia.” Journal of elder abuse & neglect 26, no. 2 (2014): 107-122. Handset-based solutions We suggest that handset-based solution providers such as Truecaller or antivirus apps such as Norton share data with the MNOs when a scam message or malicious URL is detected. This could help MNOs stop scam messages from being further distributed. The flagged RCS messages in the Google messaging app should also be shared with MNOs to block mobile numbers initiating those messages. Consumer Reporting Tools Currently, the reporting system does not separate spam from scam messages. While sending spam messages is against MNOs’ terms and conditions, the harm caused by scam messages is significantly more. We suggest adding options in the one-click reporting system so a user can report spam and scams separately. However, MNOs cannot completely depend on users to make the right choice. Hence, a classification algorithm should be implemented to confirm the user-reported category before adding it to the database. Additionally, classifiers should be implemented for users’ reporting via 7726, which could distinguish spam from scam messages. This would help mobile operators take appropriate actions for each category of messages.

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 1. Currently, a search on Google can help anyone in the UK procure a SIM farm/box. We suggest bringing back the Criminal Justice bill that has a provision to penalize the supply and use of SIM farms for any illegitimate use. 2. We suggest data sharing among mobile operators, aggregators, and companies like Google and Apple that provide the RCS messaging. Sharing intelligence signals could significantly curb scams over SMS and RCS messaging.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – N We suggest that pay-as-you-go SIM registration requirements, making sender ID registry, and data sharing among MNOs and aggregators be set out as the priority areas.

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