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? – ~~Y~~ / ~~N~~ **OFCOM Advisory Committee NI (ACNI): General Comments** The OFCOM Advisory Committee NI (ACNI) have growing concerns about the prevalence and impact of scam text messages. The use of mobile messaging services to scam people has a significant and direct negative impact on both consumers and businesses alike leading to economic loss, stress and a lower confidence in services delivered via these channels. ACNI is concerned about the economic and personal harm caused by these scams especially for more vulnerable members of our society. At a time when we wish to encourage digital inclusion and increased financial capability it is distressing to hear stories where people have suffered significant financial loss, identity theft, and privacy breaches. For businesses, the risks are equally significant, as data breaches and compromised customer trust can lead to reputational damage and regulatory penalties. In Northern Ireland, where many local businesses and public services increasingly rely on digital interactions, the threat of scam texts undermines efforts to build a secure and trustworthy online environment. Increasingly public services and business are operating through a digital first approach and many use text messaging to verify users or authorise access to services. The spread of scam text messages erodes trust in legitimate communications from banks, healthcare providers, and public service bodies, making it harder for these institutions to engage with the public effectively. This is especially concerning for vulnerable populations, such as the elderly or those less familiar with digital threats, and who are often the primary targets of scammers. In relation to the **Call for Input** Yes, the document outlines the main methods scammers use, such as P2P and A2P messaging. However, specific challenges in NI arise due to the unique cross-border communications with the Republic

Question	Your response
	of Ireland. Scammers may exploit the differing regulatory frameworks across the two jurisdictions, making it harder to track and block scam activities that are cross border. Although Online Communications Services (OCS) are out of scope, there is a strong crossover between the fraudulent collection and harvesting of mobile numbers and the perpetration of scams using those numbers. OCS such as WhatsApp and Facebook are platforms that are exploited to entice users to provide mobile numbers and other personal details in response to scamming and smishing campaigns. It is therefore difficult to rule OCS completely out of scope. Indeed, it is likely that scammers will adopt multiple methods and channels to reach potential victims. It is likely that consumers will not pick up on subtle differences between OCS, SMS or RCS messaging and any differences will be of little comfort if they become the victim of a scam. Ruling that OCS is completely out of scope does present a risk of divergence in consumer protection and inconsistency of regulatory approach which could be exploited by scammers. Providing synergy and regulatory (and enforcement) consistency will be critical to ensure consumers receive the same level or protection and redress regardless of the messaging service used by scammers.
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~~ / N Ofcom research reports that suspicious / scam texts are more common than either suspicious mobile or landline calls. More than half of mobile phone users claim to have received at least one suspicious text in the previous three months. It appears there is increasing sophistication from scammers exploiting loopholes in SMS aggregators, which businesses widely use. Additionally, with the growth of RCS messaging, scammers are likely to take advantage of its features, such as end-to-end encryption, making it harder to track. It is important to appreciate the dual impact on consumers and businesses from scammers targeting SMS aggregators. Not only is there a substantial impact on consumers who fall victim of a scam but also the reputational risk for businesses who may have their identity used by scammers.

Question	Your response
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – ~~Y~~/ 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? – ~~Y~~ / N There is no direct evidence from Ofcom's recent reports to suggest that Northern Ireland is more affected than other UK regions by mobile messaging scams. However, specific factors like varying levels of public awareness, socio-economic factors, lower financial and digital literacy skills could play a role in how scams spread in Northern Ireland. As mentioned earlier it may be harder to track and block scam activities that are cross border. Data from services such as Consumerline or Scamwise NI could provide additional insight.
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? – ~~Y~~ / N It could be suggested that A2P or RCS channels may lead to the greatest harm, especially since legitimate businesses frequently use these routes. As a result, consumers may expect to receive messages from businesses which can be exploited by scammers. Scammers can easily mimic government, public sector or health sector organisations using these channels, which could harm consumers and eroding their trust and confidence in these services.
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~~ / N RCS adoption will likely rise, especially with Apple's adoption in iOS 18 (as detailed in Ofcom Call for Input)
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,	Confidential? – ~~Y~~ / N There should be significantly more focus on supporting consumers. A proactive approach to educating consumers on how to spot and report mobile messaging scams is required. Efforts to support consumers become more aware, alert and confident in dealing

Question	Your response
providing reasoning and evidence if possible.	with scam texts should be appropriately targeted to the most vulnerable in our society who have much less digital awareness or media literacy. It would be useful to gather evidence on the percentage of consumers who - (a) have sufficient knowledge of how to spot such scams; (b) know how to quickly and easily report such scams; and (c) are prepared to report rather than delete and ignore such scams. Given there are varying levels of financial and digital literacy across the UK any action must be tailored to the specific circumstances of each UK region. There should be greater awareness of existing measures. The 7726 (Action Fraud) reporting number is not widely advertised or known by consumers. Additionally, in NI consumers are also encouraged to report scams to Consumerline. It may not be clear to consumers why they are being encouraged to report a suspected scam to two separate services. Further research should be undertaken in relation to the actions undertaken by consumers when they receive (and recognise) a scam text. Do they ignore, block/report, ask a family member what to do or remain unsure about what course of action is most appropriate. This insight could support further efforts to inform and educate consumers about the most appropriate steps to take on receipt of a scam text message. Throughout this response we highlight the role consumer awareness, consumer education and consumers reporting scams can play in tackling this issue. These points are made in the realisation that it will be extremely difficult to fully prevent scammers using increasingly novel and sophisticated ways to scam consumers. However, this does not underplay the importance of Ofcom exploring '*upstream'* operational and technical solutions to target, disrupt and limit the ability of scammers to use text-based messaging services to target and reach consumers.
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	Confidential? – ~~Y~~/ N • Ensuring alignment in how scams are addressed across the border could prevent fraudsters from exploiting differences. Enhanced consumer education through region-specific campaigns could also increase awareness among NI consumers about how to recognise and report scams.

Question	Your response
	• It is also to be determined whether the move to eSIM will help in the fight against mobile messaging scams? • Should there be a mandatory requirement for CPs/MNOs to implement scam-blocking technology by default? Should mobile manufacturers have a similar requirement? • Much of the focus is upon consumer awareness and the use of technology to disrupt the actions of scammers. Enforcement should also be a clear deterrent. Ofcom has powers under sections 128 to 130 of the Communications Act to take enforcement action against a person who has persistently misused an electronic communications network or service, which can result in a penalty of up to £2m – it would be important to review how this power has been used to date (and could be used) to tackle text-based scams?
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – ¥ / N • Further evidence is required to ascertain the need for and effectiveness of SIM registration and IMEI suspension. (would deter the use of unregistered SIMs in scams) • Traffic monitoring, filtering and blocking should be mandatory. • The discussion around whether Sender ID registries should be voluntary or mandatory needs to be supported by evidence of which approach works best. How effective or ineffective is the voluntary approach in the UK compared to the mandatory approach in other jurisdictions? • Consideration should be given to introducing requirements for CPs/MNOs to implement spam-blocking by default. In particular, device-based tools should be provided by default rather than assuming consumers know, care or understand the need to download such tools. • Introducing stricter verification requirements for A2P messaging, especially in high-risk sectors like banking and government. • A consumer education which tackles areas such as scam awareness, digital skills and consumer proficiency specific to Northern Ireland.