Your response

Numeracle, Inc., is the industry pioneer and leader in verifying the identities of entities placing legal outbound communications and ensuring that verified identity information is transmitted securely to the communication's recipient. While thus far Numeracle's operations have been solely in the United States and Canada, we want to share our experiences as to what is working and what is not so that other countries can benefit from early efforts in the United States.

Numeracle believes the best way to fight illegal communications, including illegally spoofed messages and calls, is to identify those entities making legal communications and to transmit the verification of that identity end-to-end and present the information to the recipient of the communication. If the communications ecosystem identifies the legal and wanted calls and messages, it can then focus anti-robocall efforts on those who are unwilling or unable to identify themselves.

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

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? – No The full impact of Apple adding support for "Rich Communications Services" (RCS) remains to be seen but it seems reasonable to assume RCS availability and adoption will increase, perhaps substantially, in the next few years. The "rich" aspect of RCS as compared to the relatively limited appearance and functionality of SMS/MMS persuades that RCS should be more effective as a means for communicating to and interacting with consumers of RCS services. A 2019 Harvard Business Review Pulse Survey, "Mobile Messaging Blazes A Path To Consumers", reported that Subway Restaurants conducted pilot tests of RCS messaging and discovered, "the conversion rate for RCS messaging was 140% higher than for SMS in one deal and 51% higher in the other." More recently, reports of improvements in the call answer rates and call durations in the voice channel promoted using "branded calling" enhanced with the richer experience of name, logo, and reason for calling in the display of calls suggest there may also be substantial incentive for increasing use of RCS A2P channel for RCS Business Messaging. First Orion Benefits of Branded Communication
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? – No Verified Sender Identity registration in combination with subscriber registration will provide improved security and accountability. The signature over Chatbot metadata and data defined by GSMA is a similar functionality as STIR/SHAKEN call authentication defined by the IETF STIR working group and the ATIS/SIP Forum Joint Task Force on IP-NNI. STIR/SHAKEN also uses cryptographically-signed JSON structures called JSON Web Tokens (JWTs) containing information about the signer of the call attempt. Because there are RCS features that do not also include a Verified Sender (e.g., 1-to-1 Chat) but that operate from subscriber devices over the Internet through the Google Jibe Hub outside of carrier core voice and message signalling infrastructure, there may be benefit in exploring ways user digital identity may be combined with cryptographically-authenticated signalling for RCS features generally.

Question	Your response
	Similar to SIM registration, RCS message authentication combined with digital identity of subscribers will enhance traceback and enforcement efforts when the RCS P2P channel is abused. Beyond enforcement, RCS message authentication might also support A2P and P2A mutual authentication use cases beneficial to financial institutions, healthcare providers, and government agencies. There is evidence that number spoofing and scams have been perpetrated via RCS in the United States. (See https://www.androidpolice.com/rcs-spam-united-states/). There is some question whether the RCS Verified Sender Identity is a mandatory requirement for use of RCS Business Messaging except perhaps within business practices of individual communications service providers. Appendix A of GSMA's RCS Verified Sender product feature implementation guideline published in 2019 indicates that RCS Chatbot messages use digital signatures over a JSON structure containing Chatbot Name, Signature/Hash of icon file, Chatbot Address (called Service ID), and these signatures are created by an authorized Verification authority. It is worth noting that GSMA organization wrote the guidelines, but RCS Business Messaging (RBM) is a Google-specific implementation of GSMA standards and may deviate from the standard in terms of features supported and from the Verified Sender guidelines. Indeed, Step 5c of Appendix A of the GSMA guideline cautions, "c. NOTE: actual verification process is network internal and operator may take short cuts."
Question 8: Are there other measures that we should include in our assessment of the measures that can address mobile messaging scams?	Confidential? – No Mobile messaging scams, e-mail scams, web scams, and voice channel scams all share in common digital communications and the use of mimicry and obfuscation of identity. Without the ability to commit impersonation or otherwise hide the identity of the perpetrator, the scammer is thwarted in their attempts to use deception or extortion to extract money or other valuable assets from their victims. Every effort should be applied to developing ways to make it more difficult for scammers to hide who they are, and/or impersonate entities when using digital communications channels. Verified Sender Identity of RBM A2P messaging is a small step in the right direction. Digital identity in SIM registration is another. Practical, effective, risk-based Know Your Customer (KYC) processes to usefully identify businesses and individuals and provide

Question	Your response
	them with privacy-preserving digital identity tools and authoritative verifiable trust attribute credentials is the critical foundation which can be used to authenticate and verify communications between businesses, agencies, and individuals. There have been a few efforts of various legislative and regulatory bodies to establish and encourage digital identity-based authentication and verification mechanisms such as Verified Sender Identity registries and authenticated communications using technologies like DomainKeys Identified Mail (DKIM), BIMI, and STIR/SHAKEN. A more concerted effort by government and industry is needed to identify, understand, and leverage evolving digital identity infrastructures (e.g., eIDAS v2.0) and communications authentication and verification technologies and work towards more common methods of using these technologies and resources to restrain scammer ability to hide or impersonate identity in digital communications. It is worth noting that while telephone numbers are used as an address for routing calls and messages, a telephone number is an attribute of an identity but is not itself an identity. Where identifying the source of a communication attempt is important, because of rampant and potentially uncontrollable number spoofing, a telephone number is a hint that may or may not be strongly and verifiably associated with an identity. A digital signature applied using common cryptography carries the quality of non-repudiation. Many digital "wallets" make it simple for individuals to manage digital identity and transactions associated with their digital identity. Corporate digital "wallets" are not yet common, but the concept can still apply. The tools to marry KYC with identity with digital credentials and authenticated and verifiable communication exist in many forms.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – No Priority should be given to identifying opportunities to improve identity and related trust attribute information and increasing the use of message authentication and verification associated with business and person entities engaged in A2P, P2A, and P2P RCS messaging. The RBM Verified Sender Identity and business sender registries are a good starting point. More generalized corporate identity initiatives such as the Global Legal Entity Identifier Foundation (GLEIF) Legal Entity Identifiers

Question	Your response
	(LEIs) established by the Financial Stability Board of the G20 are another resource that could be investigated for suitability for improving verifiable identities associated with business digital communications and registries. Important regional or jurisdictional digital identity initiatives such as the EU eIDAS v2.0 "Electronic Identification, Authentication and Trust Services", and mobile Driver's Licenses, especially those that support W3C VC v1.1 (JWT) + OpenID for Verifiable Credential Issuance (OID4VCI) and OpenID for Verifiable Presentation (OID4VP) provide another substantial body of resources that might be well suited for assisting with SIM registration and P2P and P2A authentication and verification.

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