Mobile Messaging Scams Team
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

Dear Sir or Madam,

Re: Reducing Mobile Messaging Scams

Thank you for your 29 July 2024 call for input on how to reduce mobile messaging scams.

The Mobile Ecosystem Forum (MEF) is a global trade association headquartered in London with members in 45 countries. We seek to provide an international perspective on matters that impact our members and the communications ecosystem as a whole. MEF members collaborate to develop and support best practices, codes of conduct, and anti-fraud schemes that benefit consumers, mobile network operators, and organisations that engage with the public through their phones.

MEF are leaders in developing methods by which the communications industry and its partners actively tackle scam and spam messages. Our initiatives include:

- The UK's SMS SenderID Protection Registry;
- Our Business SMS Code of Conduct, which covers methods for stakeholders to police fraudulent messages; and
- Our Business SMS Fraud Framework, which explains how businesses can mitigate 14 types of fraud.

Our comments to the consultation are given in the following pages, using the format of your standard response form. The key observations are as follows.

- The fall in the number of scam SMS messages reported by consumers demonstrates the effectiveness of proactive anti-fraud controls such as the voluntary SMS Sender ID registry that MEF operates in the UK.
- Similar proactive controls are needed for Rich Communications Services (RCS) and online communication services (OCS) or fraudsters will migrate to whichever messaging channels can be most easily exploited.
- Voluntary methods of tackling impersonation fraud such as the UK's SMS Sender ID registry are preferable because they place most burden on the organisations that have most reason to ensure they are not being impersonated.
- If larger businesses and public sector institutions do not voluntarily engage with secure methods of identifying themselves when communicating with the public then it will be appropriate to compel them to act, but the work involved in authenticating the identity of the originator of a message should be understood to be a burden for the organisation originating the message as well as a burden for communications providers.
- It is anticipated that organisations will use Rich Call Data for outgoing voice calls in future, a development similar to the use of Rich Communications Services in that both are capable of presenting consumers with logos and other information to help

them identify the origin of the communications they receive, resulting in increased commonality in the know your customer (KYC) controls needed for both voice calls and messaging.

- Although they are considered separately at present, KYC expectations need to be harmonised across SMS, RCS, online communication services and voice calls.
- The extent to which the UK's SMS Sender ID registry has been successful at reducing the number of scam messages that impersonate major brands demonstrates how easy it is for scammers to otherwise subvert KYC checks.
- The experience of countries like India is that controls over the use of A2P SMS leads fraudsters to compensate by making more use of P2P SMS and RCS.
- It is regrettable that the provisions in the Criminal Justice Bill that would have impeded scammers' use of SIM farms did not become law.
- A comprehensive strategy for tackling the criminal exploitation of all kinds of radio devices to disseminate scams is preferable to disjointed piecemeal responses to specific techniques that scammers use.
- The marked rise in the use of SMS blasters across East Asia highlights the need for controls to prevent their unsanctioned import and use within the UK, in addition to improvements in how we detect and locate SMS blasters.
- Consideration should be given to using the new powers created by the Online Safety Act to reduce the number of adverts for radio equipment typically used by scammers that are propagated using popular social media platforms.
- The experiences used to train anti-fraud professionals in developed economies is unhealthily narrow; a great deal more could be learned from the methods used to tackle scams by government agencies, communications providers and other businesses in African and Asian countries where consumers tend to rely even more heavily on mobile messaging than they do in the UK.
- More use could be made of honeypots to detect and measure the extent of scams across all communications channels; the results produced would be more timely and reliable than information from the public, whilst the cost of operation would likely be significantly less than the amount that has to be dedicated to reviewing reports of scams supplied by the public.
- Fraudsters adapt their methods to circumvent new controls, so it is wise to prioritise the speed of implementation over the pursuit of perfection when designing technical measures to protect consumers from crimes that occur on a daily basis.

Yours sincerely,

Eric Priezkalns
Director of Anti-Fraud and Integrity, Mobile Ecosystem Forum

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 include all the main methods that scammers currently use to scam the public. Some of the methods described, such as SMS blasters, may not be common enough to qualify as one of the 'main' methods at this time. However, the lack of resources dedicated to identifying methods like these also means their actual use may be grossly underestimated. The way we measure the scale of scams is too patchy and too anecdotal to accurately estimate the extent of methods used by criminals with any level of confidence.
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 It is likely that RCS messaging sent on a person-to-person (P2P) basis is in the process of catching and potentially overtaking application-to-person (A2P) SMS as the most common channel for transmitting scam messages to phone users in bulk. However, it is problematic to measure the use of P2P RCS by scammers because the channel is encrypted and because there is limited publicly-available data on potential controls at either the beginning (SIM registration) or the end (content received on the handset) of the sequence of events involved in using this channel. Only Google would be in a position to reasonably estimate the rate at which P2P RCS is being used for scams and the effectiveness of any controls designed to detect and prevent scams. The majority of spearphishing-type scams which require a high degree of interaction between the scammer and a victim will have likely already migrated to online communications services (OCS) that fall outside of the scope of this consultation. This is largely because of the effectiveness of steps that have already been taken by communications providers to deny service to bad actors. The experience in India is that there has been an enormous rise in the use of P2P SMS by scammers, in parallel with the decline in the use of A2P SMS for scams. The UK should anticipate a similar increase in scam activity via P2P SMS if tough controls over A2P SMS are not mirrored by similar controls over P2P SMS. Google's decision to temporarily disable RCS for Business Messaging (RBM) in India during 2022[1,2] is also important for understanding the risk of established fraudsters switching to RCS for the sending of messages in bulk. Although there is no suggestion that RBM was used in India to propagate scams, it is important to emphasise that there is only the blurriest of lines that divides outright scams from unsolicited advertising (spam) that contains misinformation. Scammers pretend to run legitimate businesses. They try to appear the same as other users

[1] www.theverge.com/2022/6/1/23150243/google-rcs-ads-india-spam-verified-business

[2] commsrisk.com/the-good-news-behind-google-stopping-indian-rich-business-messaging-spam/

Question	Your response
	of bulk messaging services. There is significant overlap between anti-spam and anti-scam controls that both seek to determine the identity and to evaluate the reputation of a prospective sender of messages in bulk. Indians are far more likely to be users of Android than iOS, and Indian MNOs gave free access and imposed inadequate KYC controls on businesses that sought early access to RBM. The result was that bulk senders of adverts transitioned to RBM more rapidly than would be expected in countries where Apple has a higher share of the handset market. Coupled with India's tough controls over A2P SMS, spammers were highly motivated to flood the new channel with advertising messages. This is indicative of what could happen in the UK if the availability and popularity of RCS grows without being subject to robust controls over who may send messages in bulk. A wide spread of East Asian countries including the Philippines, Vietnam and Thailand have identified an increased need to tackle the use of SMS blasters by scammers. A similar pattern of spreading use now appears to be emerging in Europe, beginning with France and Norway before the first identified use of SMS blasters by scammers within the UK. Meanwhile, the New Zealand Police have just reported the first instance of an SMS blaster being used for fraud in that country. We anticipate the UK and Europe will experience a rapid growth in the illegal use of SMS blasters as a consequence of them becoming progressively cheaper, lighter, smaller and more portable, and because of the effectiveness of anti-scam controls implemented by network operators and by businesses working upstream from them, unless similarly robust controls are proactively adopted over the use of radio equipment. The extreme difficulty of detecting and locating SMS blasters makes them an appealing way for scammers to circumvent know your customer (KYC) and anti-fraud controls that are implemented by communications providers and which rely upon the analysis of network traffic. The use of SIM farms to spread scams should be evaluated alongside SMS blasters as they both involve radio devices although one requires a SIM and a connection to a mobile network and the other does not. Both also involve criminal syndicates which can be based out of the country hiring a stooge to operate the equipment in-country, which drives up the cost of their criminal enterprise but gives the syndicate protection from prosecution. The extent to which fraudsters will use both SIM farms and SMS blasters should hence be understood in the context of: ● the ease and cost of obtaining the radio equipment; ● the portability of the equipment and the sophistication of technology developed by manufacturers to evade detection; ● the amount invested in the expensive methods needed to detect and locate the radio equipment; ● the amount of law enforcement resources applied to arresting and prosecuting the stooges caught operating the radio equipment and the

Question	Your response
	difficulty of prosecuting the criminal enterprise that employed those stooges; ● the effectiveness of controls to counter other, cheaper ways of disseminating scams. Based on the experience of countries like Thailand, which has tasked police and customs officials to do more to find imported radio devices used by scammers[3], we expect the rate at which criminal syndicates will turn to the use of radio devices to disseminate scams will be profoundly influenced by the effectiveness of controls to inhibit scammer methods that do not involve radio devices. The use of radio equipment to disseminate scams greatly increases the cost to the criminal enterprise but the detection and confiscation of this equipment is also very costly to law enforcement. This can result in a potential 'sweet spot' where the private sector has done all that is reasonable to tackle scams but criminals can still generate enough profit to justify the cost of using radio equipment to disseminate their scams.
Question 3: Do you have any evidence specifically on what tactics scammers are using to access RCS messaging?	Confidential? – N See above for analysis of what might occur if too few KYC checks are applied before an entity is allowed to send messages in bulk. P2P messaging through RCS will suffer the same endemic weaknesses as P2P SMS in jurisdictions where consumers can obtain SIM cards without needing to provide evidence of their identity.
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 Data to estimate the scale and nature of scam messages sent by SMS and RCS is patchy at best. We do not have confidence in the estimates most commonly cited by others because: ● members of the public do not reliably discriminate between illegal scam messages and other messages which are spammy but legal; ● estimates generated by extrapolation from industry data usually starts with a sample that is too small or too obviously biased to be considered representative; ● very little academic research has been devoted to this subject. However, the experience of other countries is informative because criminal gangs operate scams at an international level. Much of this response is informed by the experience of how scammers behave and the mitigations that have been implemented in Asian and African countries.

[3] www.facebook.com/royalthaipolice/posts/pfbid0bwS7YJYVkioAY7xjrMhdzsrWPzbZgjVL7G5Qr4x5AuqJFdsQve4n6o3YpERKKTywl

Question	Your response
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 evidence from India and other countries is that the amount of harm supported by a communications channel exhibits a simple and predictable relationship to the popularity of that channel with end users and the effectiveness of controls to prevent misuse of the channel. Criminals gravitate to the channels that have the most end users and the least effective anti-scam controls.
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 Market data from research business Mobilesquared tells us that the number of RCS users in the UK has more than doubled since 2020 and is now thought to exceed 20 million, or slightly over one-third of the number of SMS users. The number of RCS messages increases geometrically when there is an arithmetic progression in the number of RCS users. There has been a 28-fold increase in the number of RCS messages received by British users since 2020. This only equates to 0.7 RCS messages per user per year according to our most recent data, but it is easy to see how exponential growth will continue as it becomes increasingly likely that both the sender and recipient of a message will be capable of using RCS. We expect a further acceleration in the growth of RCS when Apple upgrades iPhones to use RCS. Forecasting the future popularity of RBM from historic data is problematic because the popularity of A2P SMS for messaging is linked to its ubiquity. A2P SMS will remain a popular method for businesses to reach customers until there is a 'tipping point' when enough consumers have RCS-enabled phones to make it attractive for businesses to use the additional features provided by RBM. Another factor that will influence the popularity of RBM is the ability to counter imposter frauds by communicating additional information that serves to validate the identity of the business which sent the message. As such, the popularity of RBM with organisations that send large numbers of outbound messages will be itself influenced by how many scam messages are delivered by A2P SMS, and by the extent of regulatory and social pressure to mitigate fraud.
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	Confidential? – N All of the measures currently in effect within the UK have a role to play in mitigating scams. A more difficult question concerns how to evaluate the extent to which each measure contributes to the goal of eliminating scams, and hence which changes would most increase the cumulative effectiveness of all the controls in place. However, that question can seem simple compared to

Question	Your response
in your answer, providing reasoning and evidence if possible.	evaluating whether to introduce new measures that have not been tried before, sometimes because of the complex legal questions that arise. **Ofcom rules on numbers** Ofcom's rules on number allocation, adoption and use are good and sensible. They should, however, be treated as security hygiene; they eliminate some of the simplest and easiest methods that criminals might otherwise use, but they do not serve as obstacles that organised crime will struggle to circumvent. A criminal enterprise that is prepared to pay somebody to travel to a foreign country and drive around a hired car containing a radio transmitter that circumvents any network by connecting directly to a victim's phone is not going to be stopped by rules concerning the use of telephone numbers. To use a metaphor, it is wise to lock the front door but that does not mean a determined criminal will not gain entry by breaking a window. Sometimes there is a tendency to assume scammers belong to a 'cottage industry' with limited resources and little ability to adapt to new controls. It is our belief that this underestimates the extent to which serious organised criminal syndicates are responsible for scams, as evidenced by the hundreds of thousands of people that are currently being forced to work in scam compounds in East Asia[4]. To further the point, it is right that Ofcom's Good Practice Guide sets an expectation that providers should undertake know your customer (KYC) checks, but that does not mean that all providers are equally stringent in applying KYC before deciding whether to accept a new customer. The more stringent a provider is at due diligence, the more businesses they will turn away, potentially to a competitor that is less stringent in their approach. The industry needs to work with Ofcom to pursue continuous improvement and alignment of KYC checks so there is a level playing field for all providers. This is vital to maintaining confidence that none are able to game the system by exploiting a lack of scrutiny over the way KYC checks are performed or the process for deciding which potential customers should be rejected. Consistent KYC checks are essential because serious organised criminal syndicates have the resources to create plausible front companies and bribe industry insiders. MEF offers to run a regular informal industry conclave that compares and encourages consistency in KYC if Ofcom would be willing to play a steering role. MEF has relevant experience as an impartial intermediary through the work done for our Business Messaging Code of Conduct and the SMS Sender ID registry we operate in the UK. The question of how to establish appropriate standards for KYC needs to be seen in the round. This is because of the technological convergence of the infrastructure that underpins different forms of communication, such as voice calls and messaging, and the growing reliance of other business sectors that need

[4] For example, see the 2023 report of the Office of the United Nations High Commissioner for Human Rights as available from bangkok.ohchr.org/online-scam-and-trafficking-sea/

Question	Your response
	communications networks to transact with their customers. KYC expectations need to become consistent across all technological platforms used by all organisations. Ofcom's rules on the use of numbers should be seen as part of that context. Expectations should be communicated not just to the providers responsible for vetting potential customers, but also to the types of businesses that expect to send large numbers of messages or make large numbers of calls to phone users. This would help to discourage any gaming of the system that may occur if a provider seeks to gain a commercial advantage by negotiating how to minimise the KYC burden on the customer, perhaps by recommending that weaker regulatory expectations have been established for one communications channel than another. Effective KYC increasingly needs to peer behind the veil of incorporation to determine who ultimately owns or controls a legal entity. Recidivist criminals are adept at creating fronts that seem to be legitimate new businesses, but which are conduits for the same kinds of illegal and harmful traffic that the criminals have profited from before. Terminating the service of a front entity found responsible for bad traffic does not prevent bad actors from repeating their methods by creating a new legal entity. It would be helpful for Ofcom to provide ongoing and routinely updated guidance with how far KYC checks should investigate the ownership and management of companies that purchase bulk messaging services. Particular emphasis needs to be placed on when it becomes appropriate to seek the involvement of law enforcement agencies to continue the investigation of who ultimately owns and controls businesses, especially when these people are believed to live outside of the UK. **Criminalising SIM farms** It is a shame that the legislation to criminalise illegitimate uses of SIM farms was not brought into effect due to the Criminal Justice Bill not completing its passage through Parliament. It is our belief that SIM farms have not historically been responsible for the majority of scam SMS messages received in the UK, but their use for illegitimate purposes will rapidly increase due to the effectiveness of other controls that prevent the misuse of A2P messaging. Evidence from countries like India, Australia, Philippines and Thailand is that criminals devote more resources to establishing SIM farms that exploit standard retail SIMs for P2P messaging as a reaction to being denied access to A2P messaging services. For example, the Telecom Regulatory Authority of India (TRAI) reports there has been a ten-fold increase in unsolicited P2P SMS following the introduction of regulations that appear to have successfully curbed the abuse of A2P SMS. **Volume limits** Limits on the use of consumer SIMs to send messages are a way to increase the costs incurred by criminals who originate large numbers of P2P messages by forcing them to acquire more SIMs to send the same number of messages.

Question	Your response
	However, these limits will never be able to eliminate the misuse of SIMs unless they are set so low that they also increase the cost of services for some genuine consumers. Irrespective of whichever limits may be imposed, it is vital that there is rigorous and independent monitoring of compliance with any standard. Otherwise there is a risk that some providers will neglect to consistently impose the mandatory limit, effectively giving themselves a commercial advantage over other providers. It is well known that providers have had 'fair use' limits that are mentioned in the contractual terms provided to customers but which have not been effected in practice. Staff working for providers have themselves complained about the revenue and cost implications of not curbing excessive usage by customers. In such circumstances, 'fair use' limits may be treated by communications providers as an optional legal backstop that they use to counter the very worst abuses of their services, but with no intention to systematically monitor all customer usage, as would be necessary to consistently impose limits in practice. If providers enforce new volume limits proposed by Ofcom as loosely as they have enforced their own fair use limits then criminals will soon gravitate to those providers with no effective limits, irrespective of what is written into the provider's contract. In other words, any volume limit will only be effective if communications providers have consistently implemented technology and processes to monitor when limits are exceeded. Ofcom should give consideration to a more moderate alternative to strict limits on the volume of usage. In response to the aforementioned increase in unwanted P2P SMS in India, TRAI is currently consulting on whether higher charges should apply when a customer's usage exceeds a standard industry-wide threshold. The reasoning behind this proposal is that it would never lead to a situation where a genuine consumer was unable to send a message, but it would drive up the costs incurred by spammers and scammers that routinely maximise the use of each SIM they acquire. The limit before applying the higher rate may be set lower than a limit to stop providing service because there would no longer be a risk of a genuine consumer being denied service when they most need it. Differential pricing, if consistently applied, may also have the merit that providers would be incentivised to purchase and implement whatever additional technology or processes would be required to monitor volumes of usage and charge customers accordingly. **SIM registration requirements** We respectfully disagree with Ofcom's characterisation that the SIM registration requirements of other countries have 'typically' been designed to counter terrorism or fraud. Those are legitimate reasons to impose SIM registration and these justifications are often cited by authorities in other countries. However, SIM registration has implications for personal privacy that go well beyond countering terrorism and fraud, and there are many examples of countries imposing SIM registration obligations to pursue other objectives.

Question	Your response
	It is important to provide some context for why countries may enforce laws that require the registration of SIMs, and why the essential motive for mandatory SIM registration often differs from the explanation given to the public. One of the most common examples relates to imposition of limits on free speech. There are countries where the majority of people who have access to the internet obtain that access solely through their mobile phone. In such countries, registration of SIMs can be a necessary component of a strategy designed to prevent the expression of opinions that would be considered legal in the UK. Some countries that strictly enforce SIM registration are motivated by the more prosaic goal of securing the government's tax revenues. This occurs where governments generate a significant component of their revenues by imposing termination fees on inbound international telecoms traffic. These taxes can be avoided by parties who use a SIM farm as an in-country relay station for international communications. The international leg of the communication occurs over the internet, whilst the in-country leg is a mobile call charged at the usual domestic retail rate advertised for consumer use. Mandatory SIM registration and limits on the number of SIMs that an individual may possess makes it more difficult to obtain all the SIMs needed for these SIM farms. Tax revenues generated from such international termination fees are in general decline as customers are motivated to use OCS as a substitute, but there is an apparent shift in the taxation policies of these countries where either OCS use is taxed directly, or new taxes are imposed on adjacent services like mobile money. The pursuit of these tax revenues continues to be a key motivation for enforcing laws concerning SIM registration. There is a long and complicated history surrounding the question of whether SIM cards can legally be used to bypass termination fees within the UK but this history is also pertinent to determining whether it would be appropriate to introduce SIM registration requirements in the UK. The legality of using SIM cards in this manner was somewhat concluded in March 2023 by the Supreme Court decision in *R (VIP Communications Ltd) v Secretary of State for the Home Department*[5]. The circumstances of that case were that Ofcom had, at one point in time, taken a position where there would no longer be any effective prohibition against the use of SIM cards acquired on a retail basis for the purpose of avoiding wholesale termination fees. The Home Secretary intervened, on the grounds of national security, to direct Ofcom to exercise its power to regulate the use of radio devices so that Ofcom would not allow any specific instance of SIM cards being used in this manner within radio devices referred to as "commercial multi-user gateways" (COMUGs). The Supreme Court decided that the Home Secretary's direction was legal, though the decision was only reached after an earlier appeal overturned a contrary decision by a lower court. Other readers of this response may more commonly refer to COMUGs as GSM gateways or 'simboxes', and would recognise that the historical use of these

[5] www.supremecourt.uk/cases/docs/uksc-2021-0019-judgment.pdf

Question	Your response
	devices was mostly bypass of termination fees, as countered by other governments through legislation that prohibits the bypass of these fees and mandates SIM registration. This use of COMUGs is underlined by manufacturers advertising how to use COMUGs to evade termination fees, and by them developing features designed to make it more difficult for their use to be detected by MNOs. These devices are also found in SIM farms where they serve the different purpose of obfuscating the true origin of scam communications. The Supreme Court's decision established that the Home Secretary has the right to direct to Ofcom to not approve any use of COMUGs on national security grounds because it was predicated on the substantive threat that occurs when multiple-leg communications enabled by COMUGs cannot be reliably traced to their origin. This inability to trace the true origin of a call or message is pertinent to the criminal syndicate's use of SIM farms to obfuscate the origin of scams as well as the use of the same kinds of devices by terrorists and other threats to national security. Tracing the origin of the communication is obstructed because the CLI presented on the receiving phone is not tied to a known owner of the SIM associated with that number, nor represents the true source of the originating leg of the communication. Without the changes in law that were envisioned by the Criminal Justice Bill, the introduction of mandatory SIM registration would beg the question of why the Home Secretary would continue to be entitled to prohibit the use of any COMUGs for multi-leg communications on national security grounds. The factual substance underpinning the Supreme Court's decision would drastically change if all SIMs were registered to known users. In such circumstances, purchasers of SIMs that are installed in COMUGs could be subjected to the same obligation to assist in the tracing of calls as currently applies to any other business involved in the supply of communications services. The primary rationale for the UK's current *de facto* ban on COMUGs, which is that the CLI seen by the recipient of communication cannot reliably be traced to the user of the SIM, would no longer apply if there is a registration process that ensures a registered owner of the SIM can be determined from their phone number. This complication relating to national security, the Home Secretary's powers, the use of COMUGs as an alternative means of enabling international communications, and any plans to change laws relating to the use of COMUGs should be kept in mind when contemplating whether to introduce SIM registration requirements in the UK. **Suspension based on International Mobile Station Equipment Identity (IMEI)** UK providers are already mindful of IMEIs because they have a vested interest in preventing the resale of handsets stolen, whether they have been stolen from their business or stolen from consumers. There is no convincing evidence to suggest that a noticeable reduction in the number of scam messages would occur as a consequence of new obligations to suspend IMEIs.

Question	Your response
	Ofcom has already noted that sophisticated scammers are capable of altering a device's IMEI and changing the associations between SIM cards and IMEIs. Scammers who operate SIM farms that cycle through large numbers of SIM cards would more effectively be tackled by the provisions that were included in the Criminal Justice Bill. Please also see our comments below about other controls that would mitigate the risk of radio devices being used to generate large numbers of scam messages. **Measures to address scam SMS messages sent through aggregators** MEF has a particular interest in these measures as our membership includes the most important aggregators, with whom we work closely to reduce the number of scam and spam messages. MEF has already collaborated with its members to establish voluntary expectations that are codified in our Business SMS Code of Conduct[6], which was first published in 2018 and was then revised and enhanced in 2020. MEF is currently in the process of scrutinising the code and identifying potential new revisions to reflect changes in the market since 2020, and we believe the resulting version will continue to serve as a blueprint for the industry to follow. **Know Your Customer checks** Please note our observation above about KYC needing to be seen 'in the round' in order to effectively protect consumers. Consistent KYC requirements would ensure a level playing field for all, and should equally apply to aggregators as joint stakeholders within the ecosystem. MEF's Business SMS Code of Conduct already states expectations for KYC. We would be glad to participate in a process of harmonising KYC expectations across all the communications channels used to scam the public. We welcome the positive examples of MNOs and aggregators imposing KYC standards on upstream providers of messages. It is worth reiterating that these positive examples show what the industry is capable of delivering. However, the protection of consumers ultimately depends on consistency across the ecosystem, not the virtues of individual MNOs or aggregators when seen in isolation. Scammers are persistent in their methods and will seek to route traffic around the businesses which impose the highest KYC standards. The priority should be to raise the bar for all, without any exceptions, rather than asking more from businesses that already maintain the highest standards. We referred above to the potential for MEF to manage an informal conclave to regularly review how KYC checks are implemented in practice with a view to encouraging consistency in their application. We also believe such a conclave could be used to exchange intelligence about higher-risk businesses suspected of facilitating the distribution of scams if Ofcom was to participate and the terms of

[6] mobileecosystemforum.com/programmes/future-of-messaging/fraud-management/trust-in-enterprise-messaging/

Question	Your response
	reference clarify that such intelligence is being exchanged solely to prevent or detect criminal scams. **Dedicated connections** The MNOs which stipulate the use of specific connections for some of the best-known brands have made it more difficult for scammers to impersonate those brands. If other MNOs choose not to voluntarily follow their lead then it would be appropriate for Ofcom to seek to harmonise anti-scam practices by mandating all MNOs demand dedicated connections for messages involving those brands which are impersonated most often. **Intelligence sharing and reporting incentives** Many parties seek to portray a rosy picture of the extent to which anti-fraud intelligence is shared but we find the situation to be more nuanced in practice than is often admitted publicly. In particular: ● There are legitimate concerns that intelligence sharing can be counterproductive if bad actors also receive the intelligence. ● Those businesses which are most willing to share intelligence may not need to receive it so much, whilst businesses that place less emphasis on protecting the public may make little effort to gather intelligence, never mind sharing their intelligence or acting upon the intelligence they receive. ● The quality of intelligence shared by businesses tends to be heavily influenced by the disposition of employees working in key positions, and by the amount of time those employees can devote to sharing intelligence with their peers. ● The usefulness of intelligence is heavily influenced by the roles and responsibilities of the people who give and receive information because professionals in different businesses who have dissimilar roles and responsibilities may be little able to supply information which the other will find actionable. ● Some organisations that offer to serve as enablers of intelligence sharing appear to be more motivated by the opportunity to charge fees to participants than by delivering a measurable reduction in crime. ● Discrimination between reliable and unreliable businesses, and a focus on action are both vital to realising the benefits of intelligence sharing. The factors listed above make us circumspect about how much benefit can be gained by placing further emphasis on the benefits of sharing intelligence. There are examples of reputable businesses working together to tackle scams, and that should always be encouraged. However, it is not clear how much would be gained by simply holding more meetings, or implementing new mechanisms to exchange information, unless there is greater clarity in who is meant to contribute to these activities, what is the minimum expected of each participant, and the consequences if they choose not to contribute.

Question	Your response
	Some examples should help to illustrate the difficulties when seeking to demonstrably improve sharing of intelligence about potentially fraudulent activity. MEF is the industry leader within the UK when it comes to the active membership of message aggregators, so it would be natural to expect MEF would have the advantage in terms of facilitating the exchange of information about messaging scams between its members. MEF also plays a unique role in the UK industry as the intermediary that runs the SMS Sender ID registry, giving MEF the advantage in terms of coordinating information involving the impersonation of the big brands protected by the registry. Does this mean that other fora which would like to facilitate the exchange of anti-scam information should be directed to consolidate their efforts with MEF, as opposed to providing alternative channels for sharing information that may involve some but not all the same businesses? Sometimes pleas for more coordinated sharing of information has the contrary effect of encouraging division because professionals working for communications providers and adjacent businesses become confused about where is the best place to share their intelligence. It is understandable that Ofcom does not wish to be too prescriptive about the self-regulating activities of the private sector, but greater clarity about which existing fora have all the right participants to discuss specific kinds of intelligence would be an aid to consolidating the often ill-coordinated efforts of UK businesses. Further to the point above, associations like MEF tend to explain their reach by reference to the number of businesses who are members, but having a business as a member does not mean *the right people* within that business would be engaged in sharing information about fraud with their peers. It is often thought that anti-fraud professionals could simply sit together and discuss any and every fraud they may encounter. It is our experience that responsibility for tackling fraud is often separated between different roles within the same company or group of companies, and that the individuals in those roles may not have a manager in common other than the CEO. For example, some businesses unify responsibility for tackling messaging fraud and voice fraud, whilst others separate the responsibilities because different operating units are responsible for each communications channel. Other businesses separate fraud responsibilities between staff who serve the enterprise sector, including the big brands that are impersonated, and staff whose focus is on retail, such as using fake IDs to obtain handsets on credit. Having more specialised fora that focus on a narrower selection of frauds, such as the impersonation of big brands, might better suit those companies where the responsibilities are split, but it could also increase the burdens when the same staff have wider responsibilities, and so would be expected to participate in a multiplicity of intelligence-sharing programs. Intelligence-sharing programs with a narrower remit would also make it harder to spot patterns of fraudulent activity that cut across silos, such as a business being duplicitous when responding to KYC questions when seeking to purchase messaging services from one provider, and when seeking to purchase voice services from a different provider.

Question	Your response
	There are many anti-fraud professionals who work diligently to gather intelligence and share it with their peers, but their status does not always lend itself to this objective. For example, multiple staff within the same communications provider may be responsible for handling multiple different accounts with organisations that generate messages in bulk. There may not be any individual with a comprehensive overview of every messaging campaign so that they can identify warning signs of a messaging campaign that may have been co-opted by a bad actor, which may in turn be the customer of the communications provider's customer, as opposed to a business they directly deal with. The KYC guidance issued by MEF is being refined to better highlight how providers need to progressively develop policies to address issues like these. The common root of many of these difficulties is that there is no noteworthy training program for professionals who are tasked to mitigate fraud within the communications industry. Most staff paid to mitigate fraud have principally been trained on the job. This leads to a great deal of difference in how businesses arrange their anti-fraud efforts and what they expect from staff. What would be required to develop a common industry training program goes well beyond the scope of this particular call for input, but piecemeal initiatives to improve information sharing, or naive rallying cries to 'share more' are unlikely to yield significant gains if no effort is ever put into harmonising the job descriptions and qualifications of people tasked to investigate potential fraudulent activity and then share their findings. One way to make progress towards this harmonisation might begin with greater focus on common expectations, such as those described in MEF's Business SMS Code of Conduct, so that there are at least common definitions of the frauds that exist and how businesses should respond to various kinds of risk indicators. Ofcom could take the lead with this by choosing to regularise its own lexicon of fraud to encourage consistency in how everybody in the private sector and law enforcement describes and categorises fraud, and hence ultimately speaks to the public about the problem. An example of proliferation of different terms was touched upon above, in the observation that more professionals would recognise the term 'simbox' or GSM gateway than COMUG, and that not everybody is aware of all the different kinds of illegal activity that can be enabled by this same device. If there is no investment in the fundamentals of mitigating fraud, we expect that writing into contracts a new obligation to share information will yield negligible benefits in actual practice. This is because it would be near impossible for anyone to demonstrate non-compliance with the contract clause, however precisely it is worded. An improvement in the sharing of intelligence needs to stem from increasing the professionalism of staff with responsibility for fraud mitigation, and not solely from contractual clauses that will have least impact on the businesses that most need to improve. Better training of staff may not generate quick returns, but the lack of training has become an obstacle to improvement.

Question	Your response
	Measures to address SMS messages being sent through illegal equipment With respect, we do not believe that two recent arrests relating to the suspected misuse of SMS blasters is sufficient to demonstrate how well collaboration in this domain might work in practice. SMS blasters have been openly sold on the internet for years. Some vendors caveat that SMS blasters 'must not be used for illegal activities' but there are very few plausible uses of this technology that are also legal, begging the question of why these devices are being advertised for sale so widely and so publicly. There have only been two arrests in the UK for the misuse of equipment that is widely used in other countries and which has been available for sale for years. Further below we will point to evidence that this kind of equipment has also been advertised for use in the UK for years already. This rather suggests that an absence of intelligence about crime is being confused with an absence of crime. Note that a similar kind of radio equipment mentioned above, COMUGs, are not themselves illegal in the UK although the use of them might be, and there was considerable confusion about the legal status of these devices for many years. Note also that when French gendarmes searched a vehicle containing an SMS blaster that was used to disseminate a major phishing scam to inhabitants of Paris they were not able to identify the true nature of the equipment but fortuitously mistook it for a bomb[7]. Fortune was also evident in the detection of an SMS blaster driven around Oslo and Bergen that was used to disseminate a different phishing scam involving the impersonation of several banks. In the Norwegian case, the SMS blaster was detected by specialised anti-surveillance equipment used to protect Oslo's government district, initially leading to the erroneous suspicion that the SMS blaster was being used for espionage[8]. Although these arrests raised awareness of SMS blasters within Europe, we believe it is improbable that the combined efforts of law enforcement and the private sector within this region is close to the levels of sophistication attained by peers in East Asia, although East Asian countries keep detecting crimes involving SMS blasters with much greater frequency. We can provide examples of websites where these types of radio devices are openly sold, often with barely disguised explanations of how they can be used to disseminate scam messages. However, our experience suggests that any list we may provide would be far from complete. Put simply, there is no shortage of supply of equipment of this type, which suggests there is plenty of demand. And the type of customer that purchases this equipment is made apparent from the features advertised, such as the ability to avoid detection by simulating the behaviour of a normal human phone user. The oft-repeated belief that the relevant parties in the UK just need to work together to tackle the use of radio equipment to disseminate scams, but without

[7] commsrisk.com/suspected-paris-bomb-was-actually-an-imsi-catcher/

[8] commsrisk.com/oslo-imsi-catcher-arrest-suspected-malaysian-spy-now-investigated-for-fraud-with-international-ramifications/

Question	Your response
	any specificity about what those parties need to do, highlights how far behind the UK is compared to other countries which have implemented a wide range of specific and targeted controls. The controls found in other countries include targeted legislation, some of which is similar to the proposals that were in the Criminal Justice Bill, and the formation of dedicated law enforcement task forces. Additional measures to counter the risk posed by this kind of equipment are detailed in our answer to question 8. **Measures to address RCS scams** Google has been uniquely important in policing the use of RCS so far because communications providers have mostly chosen to rely on Google's Jibe platform to deliver RCS for their customers. That so many businesses have chosen to rely on Google for the backend of RCS is a major factor in determining how to tackle RCS scams. The common perception is that a lower ratio of scam messages are currently conveyed by RBM than by A2P SMS but the available data is too limited to confidently reach a conclusion. A lower incidence of unwanted messages by RBM may be due to it being a newer service that falls back to SMS if the recipient's phone is not capable of handling RCS messages. However, we believe the relatively low penetration of RBM by bad actors is likely influenced by Google's position in the marketplace. The extent to which MNOs have chosen to rely upon a single converged platform means Google is better able to quickly identify the abuse of policies and to deploy countermeasures that protect carriers and users than might be the case with a messaging service that relied upon a more distributed infrastructure. With Google selected as a common RCS technology partner by carriers, it can be argued that Google can effectively align policies and countermeasures, resulting in their consistent application to all RCS messaging services. The use of independent 'verification authorities' somewhat distributes responsibility for KYC; these authorities are meant to vouch for the identity of a business wanting to communicate with consumers via RBM. The introduction of independent verification authorities does not, of itself, explain how consistently high standards will be maintained for KYC. That various private sector entities may act as verification authorities explains *who* is meant to effect KYC controls but does not establish *which* controls they will impose, or whether those controls are consistently applied in practice. Our previous comments about seeing the need for KYC in the round should also be applied to this context of creating verification authorities for one communications channel. We anticipate that verification authorities for a channel like RBM will also want to extend their remit and provide additional services to the same customers by vetting them for outbound voice calls which display Rich Call Data (RCD). This makes it all the more important that the role of verification authorities be examined and governed at a general level, and not be

Question	Your response
	made specific by looking at one communications channel in isolation from others. **Traffic monitoring tools** Many businesses already engage in traffic monitoring on a voluntary basis. This actually leads to a complication in assessing the true scale of criminal activity, because many participants who operate at various stages in the conveyance of a message from its origin all claim to be filtering large numbers of scam messages already. If many parties are already filtering scam messages then this both demonstrates the voluntary commitment of the private sector to tackling scams, but also the imprecision of techniques that block some scam messages at one stage, but allows other scam messages to progress so they are then caught and blocked at a later stage. A wholly perfect filter would negate the possibility of ever identifying a scam message further downstream. The use of Mavenir's SpamShield by UK MNOs raises questions about the advantages and disadvantages of converging on one supplier of a particular anti-fraud technique. One obvious advantage is that it leads to a greater concentration of intelligence, which should result in more accurate decisions about when to block traffic. On the other hand, competitors will argue the concentration of intelligence may discourage innovation, not least because they will not have the same visibility of data to enable them to prototype and test alternative offerings. UK MNOs do not exist in isolation. Many are part of international telecoms groups, and some of those groups have an interest in handling traffic at a wholesale level. Meanwhile, other international communications businesses solely focus on wholesale traffic. Many of the international groups seek to execute anti-scam filters on the wholesale traffic they carry, not least because this can be considered more efficient than devolving responsibility for implementing filters at the level of the several MNOs owned by the same group. Communications providers who only compete at the wholesale level, and have no ownership stake in MNOs, are increasingly keen to advertise the anti-scam blocks they have implemented on behalf of their customers. This creates a kind of competitive parity in the motivation to block bad traffic at wholesale level, independently of any specific concerns raised by national operators or their regulators. We can infer that any traffic blocked by UK MNOs that comes into the country from abroad was not previously identified as harmful by filters applied to wholesale routes. This begs a question about whether filters implemented by communications providers that have the relationship with the intended end recipient will always be at a disadvantage due to the smaller amounts of traffic they see compared to upstream businesses, unless they engage the services of a business that can aggregate information across many MNOs or can separately obtain intelligence by scrutinising data from wholesale providers. Consideration should be given to seeking harmonisation of scam blocking expectations with the

Question	Your response
	UK's neighbouring countries as a way to increase the effectiveness of algorithms without necessarily encouraging the development of a natural monopoly for blocking services. In all these matters, it should always be emphasised that no algorithm for identifying scam messages will deliver perfect results. If expectations are raised too rapidly in advance of the development of technology that has been developed and tested using real-life data then it becomes inevitable that algorithms will incorrectly categorise some legitimate messages as harmful. Real-world evidence to calibrate the risk comes from the USA, where the groundwork necessary for the application of Rich Call Data to voice calls has resulted in numerous complaints that legitimate business calls have been mislabeled by algorithms as spam or potentially harmful[9]. It is also worth mentioning that the questions in this call for input have centred on tools to monitor the *content* of SMS messages. Much could also be gained by observing other patterns indicative of nuisance traffic, such as the frequency with which a particular originator sends messages. Light-touch regulation could encourage improvements or enforce greater consistency in the use of these other indicators of undesirable traffic. For example, one of the most effective indicators of harmful P2P traffic is an aberrant ratio between the number of messages sent from a SIM compared to the number of messages received by a SIM. Businesses that sell technology that empowers scammers often refer to the use of methods that simulate human behaviours in order to defeat anti-fraud controls. For example, they may advertise the ability to send messages between automated devices to make it appear as if they are real people because they are receiving messages from other real people. However, the lack of prescribed rules on how to effect such controls gives us reason to believe that a lot of progress could still be made by pooling intelligence about patterns of suspicious traffic, such as whether criminals are refining traffic patterns to evade detection, and by encouraging all businesses to make thorough use of traffic analysis of this type. There may be concerns about pooling intelligence of this type, especially if it is feared scammers will also obtain the intelligence, and thus obtain precise insights into how to avoid detection. To mitigate this, consideration could also be given to a series of anti-fraud products developed in recent years that involve federated machine learning[10]. The principle with federated machine learning is that the learning occurs across several organisations but no information is shared between them, leading to improvements in the ability of the technology to identify anomalous traffic patterns without overt communication of how patterns are recognised.

[9] www.fcc.gov/ecfs/document/108102252803712/1

[10] For example, see aida.inesctec.pt or www.pryvx.com/post/leveraging-federated-learning-to-bolster-fraud-detection-and-mitigate-fraud-crimes

Question	Your response
	RCS and traffic monitoring tools It follows from our comments above that more than can be done to pool intelligence in order to identify patterns indicative of the misuse of RCS. **Sender ID registries** MEF established the UK's SMS Sender ID registry in 2019 with the support of a cross-sector working group that also involved Mobile UK (representing MNOs), UK Finance (representing banks) and the National Cyber Security Centre (NCSC). NCSC observed that the new registry was immediately effective in reducing the impersonation of organisations that had registered, stating in their annual report for 2019[11]: *"The NCSC noted a dramatic fall in UK government smishing attacks using a SenderID in mid-2019, coinciding with the registry coming online. DVLA had a similar experience, noting long number MSISDN attacks becoming the norm from June 2019 onwards.* *The last (malicious) use of SenderID 'DVLA' was reported to the NCSC in May 2019 and has not been seen since, which will have clearly lowered the authenticity of many DVLA-based smishing campaigns. Seeing the positive effect this had on DVLA we invited the TV Licensing agency to participate in the MEF registry in late 2019."* Use of the registry is recommended in NCSC's guidance for business communications, most recently updated in October 2023[12]: *"Be careful when choosing a SenderID. Keep the number of SenderIDs to a minimum. Avoid special characters, and ensure the SenderID is added to the MEF Registry."* The success of the registry in the UK encouraged NCSC to assist MEF in promoting the development of similar registries in other countries[13]. *"Also, there has been global interest in the work we've been doing in this space, and we have supported MEF in discussions with governments and regulators wishing to understand more."* Private sector entities that have registered their SenderIDs also report significant reductions in fraud as a consequence. For example, a well-known financial services provider who registered during January 2023 advised that the number of smishing complaints from UK customers fell from 278 complaints in the first quarter of the year to 20 complaints by the fourth quarter. The effect of the registry is to have become the leading Know Your Traffic (KYT) control in the UK as compensation for the weakness of KYC controls that fail to

[11] www.ncsc.gov.uk/files/Active_Cyber_Defence_-_The_Third_Year.pdf

[12] www.ncsc.gov.uk/guidance/business-communications-sms-and-telephone-best-practice

[13] www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf

Question	Your response
	adequately discriminate against scammers when communications businesses onboard new customers. As a consequence of its success, the registry is prompting scammers to change their tactics, as already noted by NCSC in their 2020 annual report[14]: *"We have seen a continued shift in SenderIDs to the use of long numbers, which hopefully should be easier for targets to identify as suspicious."* This progress in tackling scams should be built upon by recycling the intelligence gained from blocked scam messages so there is scrutiny of those businesses with inadequate KYC controls and ultimately better investigation and identification of the front companies used by criminal syndicates for scamming. The voluntary registration program has worked well in the UK and in other countries where MEF has launched registries. However, mandatory registration of Sender IDs in the UK would be problematic. There is pertinent experience from other countries that chose to mandate registration by a deadline, then strictly enforced an allow-list so that any SMS not on the allow-list was automatically blocked. For example, India has been forced to repeatedly suspend blocks and postpone registration deadlines because too few organisations, including government departments, were aware of the need to register, despite extensive publicity campaigns. We believe the challenge of publicising a mandatory registration scheme with a strict deadline would be worse in the UK for two reasons: ● the UK is a large economy that is open to international businesses; and ● the UK's health service depends upon more than 6,000 separate general practices, many of which now routinely use SMS to communicate routine information to patients such as changes to surgery hours or notifications about prescriptions. A safer approach would involve the remaining public services, including health providers, setting an example by establishing their own deadlines for voluntarily registration. At the same time, soft pressure can be applied to businesses that are most likely to be impersonated, such as major banks, online retailers and delivery services. If key parts of the private sector continue to delay voluntary action then sector-specific deadlines may be imposed piecemeal, either because regulators in those sectors acknowledge a particular risk applies to organisations in their sector, or by Ofcom creating a priority list of the types of organisations that are most likely to be impersonated by scammers. This is less risky than a 'big bang' approach where everybody must register by the same deadline. In other words, if there are big retailers who are routinely impersonated but which remain unwilling to register on a voluntary basis then it would make sense to prioritise their registration than to set the same deadline for them and a small business that is unlikely to ever be impersonated.

[14] www.ncsc.gov.uk/files/Active-Cyber-Defence-ACD-The-Fourth-Year.pdf

Question	Your response
	As you note, the Sender ID registry that MEF maintains in the UK involves the following elements: ● a blocklist that MNOs use to proactively block unauthorised variants of Sender IDs or legitimate Sender IDs received by them via an unauthorised route; and ● the retrospective investigation of apparent scam messages that were not blocked. We believe it is unfair to only characterise this as a 'retrospective approach'. The investigation of apparent scam messages is a beneficial complement to the proactive blocking of large numbers of harmful messages; it is not the sole component. The registry cannot block the messages itself because messages are not routed via the registry, but if communications providers act on the advice of the registry then they can use their existing systems to filter large numbers of scam messages. This is a more efficient and cost-effective way to effect the consistent blocking of harmful messages than trying to implement a single national system through which all SMS traffic possessing alphanumeric Sender IDs would need to be routed or validated. You note several examples of registries from around the world, but there are others worth reviewing too. The Campaign Registry (TCR) runs a similar voluntary registry in the USA to that run by MEF in the UK, although TCR filters harmful A2P SMS messages that originate with 10-digit long codes (10DLCs) rather than alphanumeric Sender IDs. TCR is a member of MEF. Their 10DLC registry works in concert with the netnumber Services Registry (nnSR), another private sector registry which maintains information about the valid routing of messages, as run by netnumber, another MEF member. We believe the experience of managing voluntary registries in large economies should be weighed against the factors that influence the design and operation of registries that may be suitable for smaller countries. As already noted above, the Telecom Regulatory Authority of India's 'big bang' introduction of blocks on any A2P SMS message which was not on a national approve-list led to considerable tension with businesses and other organisations who felt they were given insufficient notice of the need to register. We believe the scale of the UK economy means the challenge involved in persuading organisations of the need to register is more commensurate with India and the USA than with some of the other examples that Ofcom has listed. In particular, it should be noted that blocking any A2P SMS message that is not on a national approve-list will not greatly change the burden for communications providers that already block large amounts of traffic, but it will create a new burden for many different organisations in the public and private sector. MEF also runs the voluntary SMS Sender ID registry in Spain, along the same lines to the registry in the UK. Our experience of managing multiple national registries tells us that multinational brands with the levels of brand recognition that make them most likely to be impersonated are wary of an evolving scenario where they acquire messaging connectivity from providers on a multinational basis but then

Question	Your response
	have to separately register their brand in each individual country where they have customers. It is MEF's intention to develop a global federation of registries so that multinational organisations will only need to register once to establish their identity and prevent impersonation in multiple jurisdictions. Being a nonprofit international association gives us an advantage with developing a federation of registries. National registries that do not seek a consistent approach with other national registries are at risk of creating an obstacle to business. This risk should be seen in the context that we expect registries for A2P SMS to become the prototype for more generalised registries that will mitigate the impersonation of brands across voice services and OCS as well as A2P SMS and RBM. Registries serve as an element of a strategy that weeds out imposters through the exercise of KYC checks. Any regulator seeking to tackle scams through mandatory registries will face the same difficult equation: the more users that need to be registered, the lower the cost needs to be to avoid creating an untoward burden on users, and this means fewer resources to perform KYC checks. The worst case scenario is that the industry adopts a 'mandatory' regime to reassure the public that they can trust the communications they receive, but this is fatally undermined by weak KYC which allows the regime to be infected by scammers. The registration approach adopted for A2P SMS in the UK so far has worked well because big organisations are motivated and are able to pay fees that cover the cost of stringent KYC checks. If smaller entities pay less for registration then this inevitably means fewer resources dedicated to KYC control of either those entities or for all entities, creating a vulnerability that scammers will seek to attack. The best example of the dangers of a universal system going awry comes from KYC controls meant to prevent scammers making robocalls in the USA. It was repeatedly asserted by the US Federal Communications Commission (FCC) that the origin of any call with a STIR/SHAKEN signature would be 'authenticated', a term which normally means that the apparent identity of the originator is known to be genuine. However, no specific and additional KYC checks were imposed as a consequence of implementing STIR/SHAKEN, and no additional fees were levied to cover the cost of additional KYC checks across the many millions of businesses and individuals who were suddenly 'authenticated' originators of phone calls. As a consequence, bad actors were especially motivated to get their calls 'authenticated'. The result was that the supposedly authenticated calls were soon found to be significantly more likely to be robocalls than calls which had no STIR/SHAKEN signature attached. STIR/SHAKEN provider TransNexus went into detail when they explained how the inadequacy of KYC checks was being exploited in practice[15]: *"The remarkable thing… is that almost 40% of calls signed B or C were robocalls. As we've reported in previous months, many of these calls were*

[15] transnexus.com/blog/2022/shaken-statistics-june/

Question	Your response
	signed by a downstream intermediate provider using their own SHAKEN certificate. *In this scenario, the upstream Originating Service Providers (OSPs) claim a SHAKEN implementation in their Robocall Mitigation Database (RMD) filings. However, they have not been approved to do SHAKEN by the STI Policy Administrator, so they really aren't doing SHAKEN. As Figure 1 illustrates, they aren't doing robocall mitigation either."* Other parties have since lobbied the FCC over the weakness of the KYC checks that are needed to underpin blocking or labelling of communications. One of these parties was Numeracle, a member of MEF that was so motivated to address the problem that in 2023 they voluntarily published their own standard for the KYC checks that communications providers should undertake[16] and circulated it to the FCC in order to encourage its adoption[17]. This has resulted in the wider acceptance of the standard within the USA after it became the basis of the new KYC guidance issued by the Cloud Communications Alliance, a US industry association[18]. However, the US example of rolling out improved voluntary KYC standards after educating the public about a mandatory scheme that was meant to make communications trustworthy might be considered an example of 'closing the stable door after the horse has bolted'. Reassuring the public that the communications they receive are trustworthy can backfire if insufficient KYC controls have been imposed in advance of informing the public about new technologies or processes that are supposed to guarantee the authenticity of the originator. Some segments of the US industry have played down the impression that there is a widespread problem with inadequate KYC, but concerns about the extent of KYC controls were brought into sharp relief earlier this year after prospective voters in New Hampshire received robocalls that misleadingly portrayed themselves as being official communications from the Democratic Party. The recipients of these calls would have seen the indicator of an A-grade STIR/SHAKEN signature displayed on their handsets. This signature was applied by Lingo Telecom. Such a signature would have given recipients increased confidence that the calls were made from a phone using the number of a high-ranking member of the Democratic Party in New Hampshire. Per the FCC order issued in August 2024 detailing the settlement reached with Lingo Telecom, the telco had not meaningfully determined who was making those calls in actual practice, creating a vulnerability exploited by fraudsters seeking to interfere in the election[19].

[16] www.numeracle.com/resources/know-your-customer

[17] www.fcc.gov/ecfs/search/search-filings/filing/1042778647719

[18] 24387091.fs1.hubspotusercontent-na1.net/hubfs/24387091/Know%20Your%20Customer/CCA%20KYC%20Policy%202024.pdf

[19] docs.fcc.gov/public/attachments/DA-24-790A1.pdf

Question	Your response
	"Lingo Telecom submitted evidence to the Bureau that Life Corporation had provided Lingo Telecom with a certification that Life Corporation would identify its customers and had verified that the telephone numbers used for all calls were associated with the customers. Lingo Telecom concluded that Life Corporation could legitimately use the telephone number that appeared as the calling party of the New Hampshire calls based on: (i) Life Corporation's certification to Lingo Telecom that Life Corporation would identify its customers and had verified that the telephone numbers used for all calls were associated with the customers; (ii) the past Know-Your-Customer research that Lingo Telecom had performed on Life Corporation; and (iii) the 16-year history of Life Corporation's traffic patterns as a customer of Lingo Telecom. Based on this conclusion, Lingo Telecom provided A-level attestations for the New Hampshire calls. Lingo Telecom took no additional steps beyond those recited above to independently ascertain whether the customers of Life Corporation could legitimately use the telephone number that appeared as the calling party for the New Hampshire presidential primary calls." Although the settlement with Lingo Telecom required them to pay USD1mn, the legal obligation to implement KYC checks within the USA remains sufficiently vague that Lingo Telecom continued to assert that the FCC had not identified any specific breach of the rules regarding the so-called authentication of calls[20]: *"The settlement announced on Wednesday contains no findings of any rule violations, and Lingo Telecom continues to believe that it complied with all FCC rules, including those pertaining to STIR/SHAKEN call attestations."* We provide this lengthy digression concerning KYC to highlight that whatever technology or process is followed to signal to recipients that a form of electronic communication is trustworthy, there is a risk of it being subverted if the obligations for KYC checks on the originators remain vague or are inconsistently applied in practice. This is the primary reason where we recommend caution with mandating follow-on controls, such as the blocking of A2P SMS messages that are not on a registry, until there is confidence that bad actors will not be able to take advantage of the supposed 'trustworthiness' of the newly-registered communications by exploiting weaknesses in the way KYC checks are performed. Seeking to present a high degree of confidence in the trustworthiness of communications without anyone funding a commensurate enhancement in KYC checks is risky. If fraudsters can subvert KYC checks then the subsequent markers that a communication is 'trustworthy' can be ruined in the minds of a public that has seen the markers are unreliable. MEF is currently in the process of revising its KYC guidance in cooperation with members. It is also understood that other industry associations are working on proposals for new codes of conduct to govern KYC. Whilst MEF cannot speak on

[20] www.prnewswire.com/news-releases/lingo-telecom-issues-statement-on-fcc-matter-302229138.html

Question	Your response
	behalf of others, there is an evident consensus for the need for enhanced KYC, but without any consistent position being widely adopted yet. We encourage Ofcom to monitor progress with the evolving KYC standards of MEF and other organisations and to factor them into deliberations over when it is appropriate to pursue other anti-scam controls that depend on the performance of KYC checks to weed out bad actors. Given that KYC decisions will always ultimately involve a degree of human judgement, we also reiterate MEF's willingness to work with Ofcom on monitoring and achieving the consistency of KYC decisions in practice. **MNO Sender ID policies** The answer above explains how we see MNO policies on blocking as an adjunct to maintaining common intelligence about which Sender IDs can be trusted. The position with respect to SMS Sender IDs is analogous to that when considering the benefits of a national Do Not Originate list for phone calls and numbers. We all want MNOs to block bad traffic; pooling resources through common block-lists and allow-lists will lead to a more consistent and efficient outcome than expecting each MNO to independently decide what to block or what to allow. **RCS verification** We again refer to our previous observations to explain why the work of RCS verification authorities need to be aligned and embedded within a holistic approach to managing intelligence that will determine which originators of communications can be trusted and which will be barred. **Supporting consumers to identify and report scam messages** There will be widespread support for programs to educate customers about risk, and MEF supports that goal too. However, we temper this support with a realistic appraisal of how much can be accomplished this way. Ofcom's own research suggests that customers who are aware of the risk of scams can become more complacent when handling a specific scam communication they have received. They may choose to 'investigate' for themselves, instead of simply discarding the scam communication. The onus must be on the communications ecosystem to reduce the number of scam messages received by consumers because investments made in raising consumer awareness inevitably lead to diminishing returns over time. **Identifying or filtering suspicious messages on the handset** In some respects, businesses within the communications ecosystem may prefer that consumers take responsibility for filtering harmful content. If a consumer chooses to purchase a spam-filtering app or block a number then nobody else is liable for the risk that legitimate communications may also be blocked. Users can set their own risk tolerance. Concerns about privacy are mitigated because the user has chosen to allow the content of their message to be scanned. However, this does not mean such methods are a panacea. If the onus is on the customer to implement their own methods and set their own risk tolerance then it begs

Question	Your response
	the question of how much reliance also needs to be placed on upstream methods of barring access to bad actors and filtering harmful content. Handset-based methods ultimately rely on the aggregation of intelligence, just like methods implemented by businesses involved in the handling of traffic, but the intelligence received at the handset is only collected *after* many other blocks and controls have been effected. The resulting algorithms used for flagging or filtering content on the handset cannot be based on as comprehensive an understanding of scammer activity as would be obtained if none of the upstream blocks or controls existed. This leads to the paradoxical outcome that more effective upstream controls lead to less effective anti-scam algorithms implemented on the handset, creating an irresolvable tension over the way resources are directed towards improving scam detection rates. There is also an inevitable tension between competitive offerings of on-handset technology because more popular solutions get visibility of more data, giving them an information advantage over less popular solutions, and discouraging the sharing of intelligence between providers of these solutions and with the rest of the industry. **Reporting suspicious messages** There is a community of self-described 'scambaiters' in the UK who voluntarily gather and report intelligence about scams. Informal spokespersons for that community argue that whilst it is helpful to have a conduit for the public to report the scams they come across, there is also a danger that too much reliance is being placed on the public and not all of the public's reports are being treated with the seriousness they deserve, as evidenced by them sometimes complaining that scams they have identified continue to persist long after they have been reported. This community also reports differences between communications providers in how rapidly they respond to the information they receive. Although it sits outside of the conventional methods that a regulator would use to gain input, Ofcom may consider it beneficial to engage in less formal dialogue with representatives of the scambaiter community rather than expecting them to reply to a consultation like this. It is the nature of the experience of scambaiters that they collect a lot of information which can be difficult to summarise. Consideration should be given to aggregating and freely sharing intelligence gained from the public so this can feed into the improvement of a variety of anti-scam controls.
Question 8: Are there other measures that we should include in our assessment of the	Confidential? – N There are other measures to address mobile messaging scams that should be considered. Before we list them here, it is worth noting that there is a strong division between measures that tend to be contemplated in highly developed

Question	Your response
measures that can address mobile messaging scams?	economies like the UK and measures which are currently being used, with some success, in developing economies. This reflects both an imbalance in the flow of information within the global communications sector and a biased assumption that all the most effective consumer protection work must be occurring in richer economies. This is detrimental to the cause of scam reduction. The global communications industry has not sufficiently drawn upon the vast pool of experience gained by communications providers in countries where the value of the amount lost by each victim may typically be lower, but the victim's capacity to bear those losses is also lower. Developing economies also tend to place far greater reliance on mobile messaging because there are fewer alternative methods of communication that are available, and messaging is closely associated with the use of mobile money services that have transformed the availability of financial services to the previously underbanked. It can also be argued that the impact of scams in such societies will be more keenly felt by victims, not least because cultural norms may prompt some to hide their suffering out of a profound sense of shame. **Honeypots** Many of the themes discussed in response to question 7 revolve around the ability to gather and act upon good information about the severity and frequency of scams. This includes asking customers to report on the scams they receive, where it is acknowledged that members of the public may not always accurately discriminate between legal and illegal communications. Honeypots use decoy devices to gather data from attackers who believe the decoys are genuine targets. A well-designed honeypot acquires superior information about the methods used by bad actors as well as providing a statistically robust measure of the number of attacks and of trends over time. The use of honeypots to gather intelligence is well established within the domain of cybersecurity, but rarely seems to be identified as a method that advanced economies might also deploy for gathering intelligence about scams communicated by electronic communications networks. This is especially peculiar given the frequency with which governments and regulators in developing economies mandate the use of honeypots to identify examples of communications fraud. A honeypot in this context would involve collections of actual or virtual phones, configured to receive and report upon unsolicited communications instead of generating any outbound traffic. There are a variety of ways in which a communications honeypot can be realised in practice. For example, the scam-filtering apps that consumers choose to run on their own handsets perform much the same role as honeypots; the user's phone passively receives communication and information about any scam or spam activity is then transmitted to the app provider to refine their algorithms. Another straightforward example would look much like the SIM farms referred to above, with the difference between that these dedicated SIMs and dedicated radio devices would only be programmed to passively receive communications.

Question	Your response
	There are many variations on this theme, each with their own relative advantages and disadvantages in terms of cost and capability, but the essential principle of a telecoms honeypot remains the same. India already mandates communications providers to implement honeypots with the intention of collating information about unsolicited commercial communication (UCC), i.e. spam. TRAI's latest consultation on consumer protection explicitly proposes an increase in the minimum number of honeypot devices in order to gain better intelligence about unwanted communications[21]. *Each Access Provider may be mandated to deploy one honeypot in a LSA [Licensed Service Area i.e. one of the 22 geographic regions used to subdivide the country] for every 200 complaints registered in previous calendar year subject to a minimum of 50 honeypots in each LSA or any such numbers as specified by the Authority from time to time, for recording the spam messages and voice calls.* *The spam message or call received on honeypots should be treated as definitive proof that the Sender was involved in sending the UCC [unsolicited commercial communication]... OAP [originating access provider] shall suspend the outgoing services of the Sender and shall initiate an investigation as provided for in regulation 25(6).* Most Sub-Saharan countries that implement telecoms honeypots use them as part of a strategy to mitigate tax losses due to frauds of the type described above when commenting on the use of COMUGs. However, expenditure on honeypots in these countries is often explained to the public as serving their interests by protecting them from consumer frauds, or assuring the accuracy of charging for communications services. Contracts for the running of national honeypots are typically awarded by the communications regulator or the relevant government department for a duration of 5 or 10 years, and usually paid for through a levy on communications providers or by awarding the supplier a fixed portion of the relevant taxes collected. The countries that run these honeypots include Ghana, Nigeria, Rwanda, Tanzania, Uganda and Zimbabwe. Bandwidth, a US communications provider, voluntarily implemented a honeypot consisting of 66,606 phone lines in collaboration with academics from North Carolina State University (NCSU) with the intention of gathering intelligence about spam and scam robocalls[22]. This honeypot received almost 1.5 million unsolicited calls over an 11-month period. Although their honeypot was only maintained for a fixed duration, the research won a prominent cybersecurity prize[23] and influenced the evolution of KYC guidance within the USA. The essential technology of telecoms honeypots is well known to the UK telecoms industry, though it tends to be associated with active testing of

[21] www.trai.gov.in/sites/default/files/CP_28082024.pdf

[22] www.usenix.org/system/files/sec20-prasad.pdf

[23] research.facebook.com/blog/2020/8/facebook-awards-200000-to-2020-internet-defense-prize-winners-at-usenix-security/

Question	Your response
	networks rather than passive collection of data about communications received. For example, many UK communications providers satisfy the requirements of the Ofcom Metering and Billing Direction using equipment that could equally well be used for honeypots. This prompted some concern during consultations surrounding the Criminal Justice Bill that legitimate deployments of test equipment could be banned as SIM farms unless there were explicit exemptions. The same consultation also highlighted commercial uses of the same kind of equipment, such as testing the experience of an overseas customer roaming inbound within the UK, or recreating the performance of a communications app to identify bugs and issues. Vendors of relevant test equipment anecdotally report that they receive unsolicited communications but the information is not retained because it does not relate to one of their customer's reasons for purchasing or renting the test equipment. Adapting equipment to collect information about messages and calls received should be relatively straightforward. Harnessing the spare capacity represented by existing test devices when they are idle could potentially be a very low-cost way of increasing our knowledge about scams. There is anecdotal evidence that suggests there is underreporting by the public of scams which target speakers of minority languages such as Mandarin Chinese. This may be because such groups are being targeted more often than the rest of society, or because foreign language communities are less likely to know about mechanisms to report scams. Staff working for communications providers may lack the language skills needed to identify or investigate some scams. A language-neutral honeypot has the considerable advantage that it would provide a clear picture of the extent to which scammers are targeting segments of society that are potentially more vulnerable. The analysis software developed by NCSU for the honeypot they implemented with Bandwidth was language-neutral, demonstrating the technical feasibility of gathering intelligence about scams in all languages. **Automated blocking of messages with URLs and automated removal of URLs from messages** Scammers often include URLs in messages that direct the unwary to phishing websites. Some countries have prohibited the inclusion of URLs in messages. For example, the Malaysian Communications and Multimedia Commission announced the prohibition of all URLs in SMS messages in April 2023[24]. There are communications providers in other countries that have voluntarily chosen to block messages containing URLs. For example, Globe, an MNO in the Philippines, voluntarily chose to block any P2P SMS containing a URL in September 2022[25].

[24] www.mcmc.gov.my/en/media/press-clippings/elak-scam-syarikat-telco-diarah-larang-pautan-url

[25] www.globe.com.ph/about-us/newsroom/corporate/globe-starts-blocking-sms-with-clickable-links

Question	Your response
	It is unfortunate that many otherwise responsible organisations consciously chose to include hyperlinks in their messages, increasing the risk of impersonation fraud. The public is less likely to fall victim to a scam phishing message if they never see a URL in a legitimate message. Some of these observations will have been in mind when Ofcom drafted its question about monitoring content. As always, decisions need to be made about how to balance freedom over what people can include in a private message with mitigating the risk of harm from deceptive communications. In the meantime, MEF is working to provide the senders of A2P SMS messages with a new facility so they can voluntarily register URLs they intend to include in the messages they send, so that any other URLs become signifiers of imposter fraud. **Registered and pre-approved message templates** The Indian approach to tackling scam and unwanted spam messages is worth mentioning because of the way it differs from approaches used elsewhere. They effectively have a national register, implemented using Distributed Ledger Technology, where bulk senders of messages register both themselves and templates for messages they intend to send. Messages are blocked if they do not comply to a registered template. The enforcement of these templates is strict in that a single spelling error could lead a message to be blocked, although templates are designed to permit some variables to be included. For example, the template for a notification about the departure time for a flight would include a variable so different times can be inserted whilst most of the rest of the wording of the message would be fixed. However, the use of variables, and the new development of pre-approving specific entries for variables, gives rise to some strictly controlled flexibility not available with some of the other anti-spam and anti-scam approaches used elsewhere. For example, forcing senders of messages to also register a limited number of URLs or phone numbers that can be inserted into the variables means consumers can receive messages with links to websites or callback numbers for customer services teams without blanket blocks of any content which fits that format, or the risk that scammers can mimic the template but lure victims to a phishing website or a fake helpline. MEF sees potential in providing registry users with the option to register templates if they desire. **Import controls and licensing of radio equipment commonly used by fraudsters** As noted above, customs officials in Thailand have proactively sought to detect and prevent the import of radio equipment commonly used by fraudsters, including COMUGs and SMS blasters. A recent press release from the Philippine government's official news agency referred to law enforcement agencies and a major communications provider collaborating on methods to stop the import of

Question	Your response
	SMS blasters[26]. The latter press release mentioned that criminals had resorted to shipping the equipment as components for assembly within the Philippines in order to defeat existing import controls. We believe it is inevitable that the UK will impose similar controls on the importation of radio equipment in future. This is because this equipment is becoming cheaper and smaller over time, making the equipment more attractive to criminals whilst easier to transport and conceal. Import controls would work in concert with a licensing regime consistent with managing the few SIM farm exemptions that were envisaged by the Criminal Justice Bill. Without import controls and licensing, the burden of detecting the illegal use of a growing number of radio devices will become a prohibitive burden. With respect to this kind of technology, it is important to recognise that the potential criminal uses include not just the dissemination of scams, but also invasions of privacy and threats to national security. Seeing these threats in the round justifies a holistic strategy for tackling the illegal use of radio communications devices that goes well beyond piecemeal rules previously crafted to address specific harmful uses of radio communications equipment. **Controls over advertising of radio equipment** Given the priority being placed on ISPs, online markets and social media networks to stop harmful advertising, and the risks relating to radio equipment mentioned above, we believe now is also an appropriate time to question if the advertising of radio equipment like COMUGs and SMS blasters should be curtailed on social media platforms. It has been argued that there are some legitimate uses for devices like SMS blasters, such as the sending of legal advertising messages to phones near the provider of a particular service, or the sending of warning messages to anyone in a zone affected by a natural disaster. These arguments strain credulity, though they may have influenced social media platforms and their policies on censoring harmful content. It would be in the interests of all parties if Ofcom played a positive role in determining when radio equipment is considered too potentially harmful to be advertised on social media. Several factors will be in mind when evaluating the potential harm caused by a device like an SMS blaster, relative to any potentially beneficial use. An SMS blaster forces nearby phones to disconnect from conventional networks, preventing that phone from being involved in any communication other than the receipt of the advertiser's SMS, including the making of outbound calls to emergency services. It is hard to believe that a respectable marketing business would use such a device, although marketing was the ostensible justification for the purchase of the SMS blasters used by the Paris SMS blaster smishing gang that was identified in late 2022 and early 2023. It also seems improbable that government agencies and NGOs that provide disaster relief would purchase

[26] www.pna.gov.ph/articles/1225396

Question	Your response
	highly specialised messaging equipment by searching social media for obscure vendors that are only contactable using online channels which are difficult to trace. A recent YouTube video advertised radio equipment that was depicted being secretly carried in an ordinary backpack through a shopping mall as the user connected to the phones of consumers around him. The YouTube video was published on 12 February 2024, two months before Bangkok police arrested scammers who repeatedly carried an SMS blaster in a backpack through the malls of a popular downtown shopping district[27]. The video[28] was recently removed by YouTube on the basis that it infringed their policies on harmful content. Google is a member of MEF and they assure us that they take great care to enforce their policies on harmful content. However, it does not take much effort to identify numerous other YouTube videos that continue to offer the sale of radio devices described as 'SMS blasters' and which match the technical specifications of the radio devices mentioned in this consultation. A YouTube search with the term "SMS blaster" led to a short video[29] published in 2019 which demonstrated the use of an SMS blaster and which provided the URL of a regularly updated Facebook page[30] which further explains how to use SMS blasters to send messages with a spoofed Sender ID. This Facebook page lists sales of equipment to customers all around the world. A different YouTube video[31] published in 2021 is labelled "4G LTE SMS Broadcaster/blasting in UK" and appears to have been filmed inside a Holiday Inn located within the UK. It depicts the user of the SMS blaster sending a large number of SMS texts where the Sender ID is "Voicemail" and the content reads "You have 1 new message". The owner of this YouTube account, 'Frank Chen', has posted 29 videos over the course of 7 years, most of which illustrate the use of SMS blasters and other radio equipment which could be used to cause harm. Searching for the same 'Frank Chen' user name on LinkedIn led to a post[32] with similar content promoting the functionality of SMS blasters. The LinkedIn post incorporated a video demonstration of an SMS blaster from the 'Frank Chen' YouTube account. A more recent YouTube video[33] from a different user depicts the installation of a 'high power IMSI catcher' in a car. The term 'IMSI catcher' is often used as a synonym for an SMS blaster. The device displayed inside this car is reminiscent of photographs of the SMS blaster found in a car used by the Paris smishing gang

[27] commsrisk.com/bangkok-police-arrest-hong-kong-smishing-scammers-carrying-an-imsi-catcher-backpack-through-shopping-malls
[28] www.youtube.com/watch?v=JX1HnvzQbqs
[29] www.youtube.com/watch?v=-vp_JrxWS5E
[30] www.facebook.com/mySMSking5796/
[31] www.youtube.com/watch?v=H6ZuDDY0Nyg
[32] www.linkedin.com/pulse/imsi-catcher4g-sms-broadcaster-frank-chen/?trackingId=v2HjDEC1Qem7qdLAI4in%2FQ%3D%3D
[33] www.youtube.com/watch?v=3SVikLI965I

Question	Your response
	and photographs of a different SMS blaster found in a car by New Zealand Police during a search they conducted in August 2024[34]. A search for SMS blasters being advertised on X (formerly known as Twitter) yielded a few relevant examples, but the information was minimal and any links pointed to webpages that have since been taken down. If adverts for radio communications equipment that can potentially be used to harm the public continue to appear on social media platforms then Ofcom may consider if there is a need to adjust guidance about harmful content that it issues per the Online Safety Act.
Question 9: Within the options set out, what should be the priority areas, if any, to further disrupt mobile messaging scams?	Confidential? – N We believe this question has been largely answered above. To summarise: ● A holistic approach is needed for KYC in order to consistently align the performance of KYC checks across all businesses which provide an entry point for scammers. Irrespective of the current legal differences, the alignment needs to cover voice and OCS as well as SMS and RCS. Delivery of this holistic approach begins with the conscious alignment of KYC standards and with the formation of industry groups that normalise the execution of KYC checks in practice. MEF is willing to lead these activities, having already established its Business Messaging Code of Conduct, which includes a KYC component, and by offering to host an industry conclave to align the performance of KYC checks in practice. ● Progressive encouragement should be given to public sector and private sector organisations to register with the existing SMS Sender ID registry, prioritising them by size and by the risk of being impersonated. This is preferable to the risks involved in adopting a 'big bang' transformation required by a mandatory registry with a fixed deadline for registration, especially if there are any doubts about the quality of KYC checks that will be performed for registrants. ● In addition to the above, more can be done to encourage organisations in the public sector and in other business sectors to voluntarily work with communications providers to protect the public from impersonation frauds. Communications providers often find themselves blamed for not tackling the bad practices that are ingrained in the way organisations work, such as the assumption that the recipients of a message should immediately respond although the sending organisation has done little to demonstrate the authenticity of the message. For example, if organisations continue to include URLs in the messages they send then they should be used sparingly, be written in full rather than shortened, and should be voluntarily registered per the new URL registration facility that we intend to add to the SMS Sender ID registry.

[34] www.police.govt.nz/news/release/op-orca-%E2%80%94-smishing-scam-smashed

Question	Your response
	● There is still much that can be done to improve the detection of anomalous patterns of traffic by refining the data analysis conducted by upstream and downstream communications providers. ● The successful reduction of scam messages for channels such as A2P SMS will drive criminals to adopt more expensive ways of communicating scams, including the use of radio equipment like COMUGs and SMS blasters. The rapid increase in the use of radio equipment should be anticipated by making an investment in specialist tools that law enforcement agencies will need to locate radio equipment and its users, and by introducing a licensing regime and import controls over relevant types of radio equipment. But finally, much of these improvements will be neutered if there is not a commensurate program to prosecute and hence deter the hardened organised criminals who are responsible for running the syndicates that generate the bulk of scam traffic, as demonstrated by the growing number of people forced to work in scam compounds in Southeast Asia and a growing number of other countries elsewhere. Blocking traffic and locating equipment used for crime can only be a palliative that increases the cost of running criminal enterprises that are so lucrative that the costs will be absorbed and the crime will continue unless it is tackled at source.

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