CCSG Response to Ofcom CFI: Reducing mobile messaging scams: Evidence and options for addressing consumer harm

Introduction

Ofcom notes in its initial paragraph that: *“Scams lead to significant financial and emotional harm and can reduce confidence in telecoms services more broadly”*[1]. Communications Crime Strategy Group (CCSG) members agree with this fundamental assessment. Our customers **and** services are vulnerable to *“industrial”* fraud and we underline our commitment to addressing such scams. This is an industry priority as much as a regulatory one. We require no further incentives to engage with these threats.

Services from major UK communications providers have been subject to pro-active self-regulatory and regulatory action to counter fraud as part of the **Fraud sector charter: telecommunications** which was negotiated in 2021 and brought into effect during the period from October 2021 – December 2023[2]. This included:

- Action (1) – Work to identify and prevent scam calls ;
- Action (2) – A co-ordinated approach to tackle smishing; and
- Action (4) – Use of real-time checking to tackle SIM swap and Mobile Number Porting fraud.

From nine areas for Action agreed between members of the CCSG and the Home Office / DSIT. Ofcom’s Call For Information (CFI) *“Reducing mobile messaging scams”* overlaps industry work on Action (2) A co-ordinated approach to tackle smishing, notably national deployment by mobile companies of SMS filters.

In its CFI Ofcom clarifies that its focus on “*mobile messaging scams”* reflects the UK’s regulatory framework, structure and Ofcom’s powers rather than current consumer harms and/or existing responses from communications and internet platform providers to scams and fraud risks. Ofcom’s CFI includes Short Message Services (SMS) and Rich Communications Services (RCS) in its treatment of mobile messaging. CCSG members have considerable experience of dealing with scam SMS (termed Smishing under the 2021 Sector Charter) and this is reflected in our comments on the CFI both collectively and individually.

Despite Ofcom’s confidence that RCS falls under its communications regulatory powers based on legal and technical analysis, CCSG members have much less experience of RCS and RCS scams. These services are provided to UK-based customers from internet platform(s) operated by Google and are subject to end-to-end encryption. As a consequence, communications providers’ visibility of traffic on RCS, including of scams, is limited and indirect.

The customer relationship for P2P RCS also varies with some users contracting with a host mobile provider for these services and others directly with Google. In either case providers do not have direct visibility of such messages as these are carried by OTT messaging channels.

The capability of UK communications providers to comment with confidence and / or to take steps manage scams on RCS is analogous to their situation in respect to What’s App provided by Meta or iMessage services provided by Apple and scams which arise in these, than with SMS.

[1] Reducing mobile messaging scams – Paragraph 1.1.

[2] CFI paragraph 2.4.

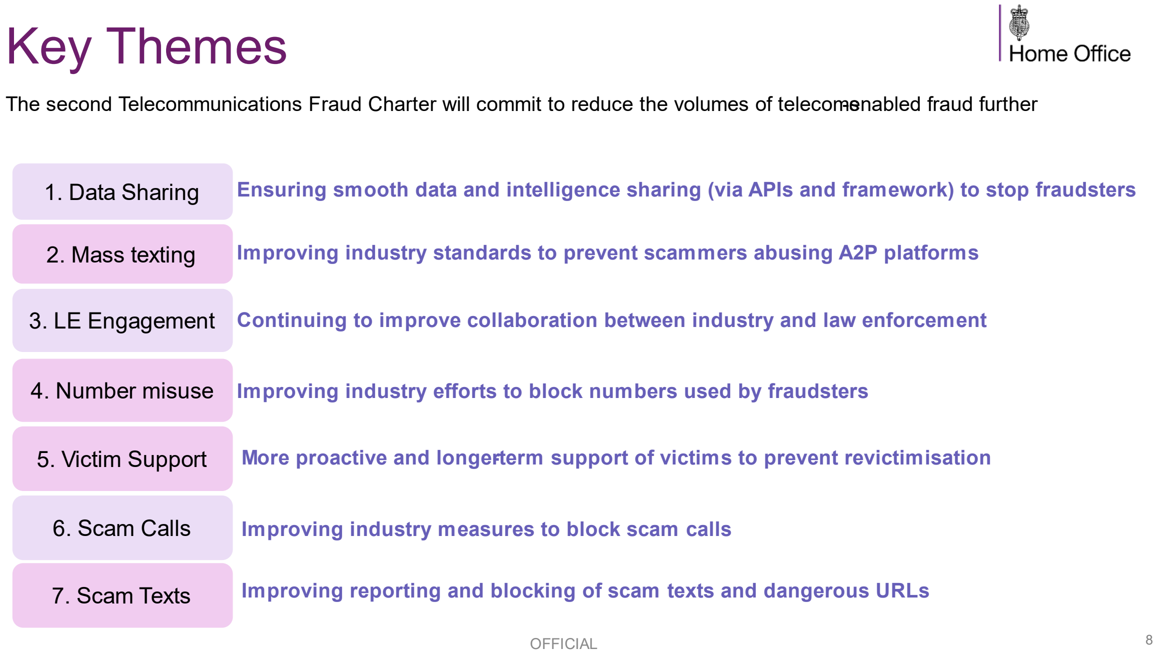
CCSG members would also comment that RCS use appears nascent in the UK in comparison with What's App and iMessage services. Ofcom's own market research will, no doubt, illuminate this point and also provide evidence of the relative occurrence of scams and fraudulent messaging on each of SMS, What's App, iMessage and RCS. For Ofcom to go forward and apply further measures on the UK consumer experience of RCS would seem to require substantial input from, and agreement with, Google who is the relevant internet platform provider.

There is a final, broader point about Ofcom's discussion of intervention to make the UK communications market more resistant to scams and fraud – as we commented above it is *"traditional"* in scope. It is also traditional in the sense that it uses a regulatory a model of identifying an issue, bringing out a CFI/CD, retiring to consider responses within Ofcom, before publishing a statement etc. This model may not be as effective to a threat characterized (as Ofcom recognizes[3]) by continual, at times rapid, evolution as is the case with SMS scams.

Ofcom, by virtue of its role, is able to gather information on demand and to override regulatory concerns on the part of market participants– such as sharing of SMS volume limits and other approaches to addressing scams – which may cross over into competitive areas. Under Mobile UK providers operate a Messaging Scams Group (MSG) which Ofcom attends and which we believe should be expanded to create a consultative forum, similar to the Strategic Working Group role. An ongoing dialogue of scam practice and response, moderated by Ofcom and supported as required by regulatory direction, would be more flexible, responsive and, ultimately, more effective in addressing these threats.

Towards a consistent strategic approach to tackling messaging scams

The earlier **Fraud sector charter: telecommunications** contained 9 areas for Action agreed CCSG members and the Home Office / DSIT. In recent (pre-election) discussions some 8 areas for action were identified by the Home Office as possible priorities for a second Sector Charter.



Key Themes

Home Office

The second Telecommunications Fraud Charter will commit to reduce the volumes of telecom-enabled fraud further

1. Data Sharing	Ensuring smooth data and intelligence sharing (via APIs and framework) to stop fraudsters
2. Mass texting	Improving industry standards to prevent scammers abusing A2P platforms
3. LE Engagement	Continuing to improve collaboration between industry and law enforcement
4. Number misuse	Improving industry efforts to block numbers used by fraudsters
5. Victim Support	More proactive and longer-term support of victims to prevent revictimisation
6. Scam Calls	Improving industry measures to block scam calls
7. Scam Texts	Improving reporting and blocking of scam texts and dangerous URLs

OFFICIAL

8

Source: Home Office Charter Roundtable – 23 May 2024

[3] CFI paragraph 2.4.

Ofcom's mobile messaging CFI invites comments on further work to address:

- Action 2: mass texting / fraudulent SMS which originate from aggregator / A2P channels; and
- Action 7: Scam / fraudulent texts.

CCSG members agree that dealing with fraud requires communications providers to focus where they have responsibility and can act effectively. For UK communications providers this includes commitment to action to suppress fraud which uses voice and SMS services as a route to the victim of fraud.

It is important that decisions taken by Ofcom to suppress fraud are not driven by regulatory architecture rather than consideration of consumer harm and how this should most effectively be addressed. CCSG members believe that a consistent, programme of actions by messaging providers and, where necessary, the regulator, will create a consistent and effective route forward in terms of suppressing fraud using communications and on-line messaging services.

In addition to the present CFI on message scams, Ofcom has also separately issued a CFI in respect of voice call scams. This separate CFI focusses on Scam / fraudulent calls which spoof UK mobile numbers.

CCSG members believe It is correct to treat responses to messaging and voice scams as distinct. While there may be common approaches with respect to measures such as consumer awareness, there are critical differences in targeting approach used by fraudsters and in technical options to defend customers in respect of these scam types.

A strategic response to these threats is illustrated below:

	National origination	**International origination**
SMS	➢ Message filtering ➢ Prevent misrepresentation ➢ Act against UK-based bulk originators: volume limits, service cut off, liaison with law enforcement to target originators; ➢ Customer awareness.	➢ Message filtering ➢ Prevent misrepresentation ➢ Establish secure national network boundary against ingress of bulk SMS; ➢ Customer awareness.
Voice	➢ Prevent misrepresentation; ➢ Act against bulk originators; ➢ Support investigation of major UK-based frauds by law enforcement; ➢ Customer awareness.	➢ Prevent misrepresentation; ➢ Act against bulk originators and transit routes which support bulk origination; ➢ Customer awareness.

Messaging scams, including SMS scams, can be made subject to analysis of content by a provider with relevant access and capability before delivery to a customer. In contrast, voice calls (at least when real-time[4]) cannot currently be subject to the same scrutiny of content for a combination of technical and legal reasons.

[4] Voice notes may straddle this distinction.

Nevertheless, it is possible to examine the activities of communications and platform providers to consider what broad types of protection may be applied to protect customers from fraud using messaging services.

From experience of SMS scams and of e-mail including from internet platform providers, CCSG members would identify a number of measures which, in aggregate, should act to suppress messaging fraud and scams.

These should include the following broad types of activity:

1. Preventing / restricting fraudsters' ability to misrepresent themselves as other originators, whether in terms of organization, brand or location of message origination;
2. Messages should be subject to analysis of content, origination and other aspects by a provider to identify likely fraudulent messages;
3. Likely fraudulent messages should be filtered or blocked by the provider or should be routed to a separate spam or scam message folder, identified to the customer;
4. The customer who receives a message they consider fraudulent should be able to report (or confirm) this to their communications or internet platform provider;
5. Data from filtering/blocking and customer reporting should be used by providers to inform their analysis and improve filtering/blocking of likely fraudulent messages including the identification of new forms of fraud, new targets and new content;
6. Where providers support third party commercial access to customers – aggregator channels in the case of SMS - there should be arrangements in place to ensure that fraudulent messages are also suppressed whether these are the same arrangement as for person-to-person messaging or dedicated commercial access arrangements which are able to achieve a similar or better degree of protection;
7. Development of new forms of fraud, new targets and new content should be reflected in provider customer-facing activity including fraud awareness and fraud response.

Following this logic Ofcom's role in seeking to limit the impact of messaging scams and fraud, and subject to appropriate powers covering different messaging platforms, should be to:

1. Ensure that providers have in place capabilities which provide the necessary broad types of protective measures, while reflecting the operation of specific messaging services;
2. Consider whether or not provider capabilities are effective in suppressing/limiting messaging scams on relevant services; and
3. Encouraging or, where relevant, requiring action by providers to UK consumers where provider capabilities are insufficient or ineffective in suppressing/limiting fraudulent messaging.

Other issues

Ofcom sets out a summary of its **general duties** in section 2.6 of the CFI. These include a duty to have regard to *"the desirability of preventing crime and disorder".* These duties date back some years and do not identify fraud as a crime Ofcom should have particular regard for.

This formulation pre-dates the action of competition and regulation on availability and pricing of communications services which, together with technological change in IT capabilities and communications infrastructure, has opened the door to the *"industrialization"* of fraud against customers and providers. This is correctly described by Ofcom as *"mass scale"* in the CFI[5].

We do not think that government need alter Ofcom's duties to specifically add *"fraud"* to Ofcom's general duty to prevent *"crime and disorder".* However, Ofcom should consider whether a fraud impact review should be a formal element of its regulatory decision making. This would be consistent with the approach taken by UK communications providers in the development of new services. In Ofcom's case publishing this analysis would ensure regulatory transparency with respect to future regulatory measures.

Ofcom devotes a small number of paragraphs in the CFI to the question of verification of the identity of the (UK) pre-pay mobile communications user at point of sale. **Customer identify verification** has been discussed in the UK in the past as a mechanism to respond to all crime types. This has not been supported reflecting the impact on mobile service access of a point-of-sale mechanism, the likely emergence of *"mobile muling"* as an adjunct to *"money muling"* and providers' ability to support law enforcement with other approaches.

In terms of the CFI focus on limiting scams we believe that approaches such as limiting SMS volumes where customers are not identified will be effective. This was also the conclusion of the recent joint industry / law enforcement fusion cell, chaired by the NECC, into measures to suppress bulk SMS and call origination.

One CCSG member has commented that there seems to be clear evidence that substantial improvements made by the providers will successfully address scam SMS origination from UK networks. It has seen scam SMS origination fall from over 1m / day to low thousands / day. This has been achieved by: introducing SMS limits on new SIMs, more sophisticated and faster detection and barring of SIMs originating suspect traffic and 24/7 blocking of scam SMS using Spam Shield.

Ofcom raises the role of **information sharing** to combat fraud. Within the SMS market scams reported by customers to 7726 are shared across mobile providers so that all providers can see national level data on 7726 reports. This now includes data from handset reports from Android and iOS handsets. This data is used by providers to inform their effectiveness in combatting fraudulent SMS. We believe that this form of data sharing between providers works effectively even at relatively low volumes of customer reports.

A disappointing outcome of the initial Sector Charter was CCSG members' inability to share data from 7726 as requested by certain third parties. Looking forward we believe that it would be feasible for data available within providers' SMS filters to be considered for sharing between providers and with third parties, to inform the effectiveness of action against SMS scams.

[5] CFI paragraph 3.21.

Ofcom highlights the existence of **SIM farms** as a technical mechanism to host a large number of SIMs for outbound SMS transmission. It is correct that SIM farms have this capability, but providers believe that other technical means exist which can also generate large messaging volumes from connected SIM cards. On this basis it may be more accurate to discuss technical means of bulk outbound messaging scams rather than highlight SIM farms as Ofcom does in the CFI. This is the approach which providers have used in their recent cooperation with the NCA on action to suppress bulk outbound messaging scams.

Communication providers make extensive use of **volume and other origination limits** to manage bulk origination of fraudulent SMS. Whether these should be lower than current dynamic limits and whether limits should be consistently applied by all providers, given different markets/market segments is not straightforward. Rather than intervene on a 1-off, or periodic, basis we suggest Ofcom and providers discuss fraud countermeasures in a moderated forum in order to develop a dynamic best practice approach given the continuing evolution of fraudsters' practice.

CCSG members would welcome periodic updates in respect of Ofcom's **use of its enforcement** powers under sections 128 to 130 to act where there has been "persistent misuse of an electronic network or service" which has contributed to fraud against consumers or providers.

Government should move forward to **enact relevant Ofcom code**s so that its powers are effective across the range of messaging services used by UK consumers and businesses. Whether these are identified as communications or on-line in the UK regulatory regime should not be the primary distinguishing characteristic in respect of regulatory action.

CCSG – 07/10/24

About the Communications Crime Strategy Group

The Communications Crime Security Group (CCSG) is a forum for crime and security leaders from UK communication providers. Its role is to:

- Set the communications industry's strategic direction on crime reduction and security;
- Influence the national crime-reduction and security agenda; and
- Ensure appropriate resources are directed to priority areas.

The CCSG aims to be the *"crime and security"* voice for the telecommunications sector, sharing information and ideas that reduce crime, improve security and build customer trust. CCSG Members are: BT EE, Sky Mobile, TalkTalk, Tesco Mobile, Three UK, Virgin Media O2 and Vodafone UK.

It addresses shared priorities by establishing sub-groups of Members' staff with management responsibility for relevant issues and by acting in partnership with active third-party organizations.

Sub-groups are empowered by the CCSG to share Member information and ideas to reduce the impact of criminal activity, improve Member security and protect customers. Information sharing takes place in a manner consistent with UK Data Privacy and Competition Law and regulation.

CCSG Members' priority areas for 2022/23 are:

- **Fraud**: continuing technical measures to reduce harm to communications customers from scam calls, SMS and other frauds combined with work to improve intelligence sharing, victim support and fraud awareness under the Telecommunications Sector Fraud Charter agreed with the Home Office / DCMS;
- **Intelligence sharing**: collection, management and dissemination of intelligence on fraud, physical network vandalism and theft, and other crime risks faced by CCSG Members;

Where sub-groups or third-party organizations identify a requirement for external lobbying of communications industry stakeholders the CCSG facilitates this by:

- Allocating resources to develop appropriate collateral; and
- Ensuring participation of senior-level executives in the delivery of industry's message.

CCSG Member companies are: BT EE; Sky Mobile, TalkTalk, Tesco Mobile, Three UK, Virgin Media O2 and Vodafone UK.