CCSG Response to Ofcom CFI: Reducing scam calls from abroad which spoof UK mobile numbers

Introduction

Ofcom notes in the initial paragraph of its recent Statement Tackling scam calls that: *"Scam calls can result insignificant financial and emotional harm to victims. They can also lead to a reduction in trust in telephone calls"*[1]. Communications Crime Strategy Group (CCSG) members agree with this fundamental assessment. Communications customers **and** services are vulnerable to the emergence of *"industrial scale"* 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) *"scam calls from abroad which spoof UK mobile numbers"* follows Action (1) Work to identify and prevent scam calls, notably work done by industry and Ofcom on the treatment of Calling Line Identity (CLI) in the Strategic Working Group.

In its CFI Ofcom clarifies that its focus on "*scam calls from abroad which spoof UK mobile numbers"* reflects the development of the UK's CLI framework and its treatment of calls from abroad. Ofcom's CFI does not address the use of UK based spoofing of UK mobile numbers.

Two issues seem fundamental in considering the timing of how industry and regulator should respond to the need for action:

1/ whether there is a significant current concern about the use of spoofed CLI of UK mobile numbers to defraud UK communications customers?

2/ If not, how quickly, might this concern reasonably be expected to arise?

As Ofcom points out there is limited current evidence that UK mobile numbers are being spoofed in volume whether from the UK or from abroad. Also there is no current agreement internationally across industry as to how this risk should be addressed technically.

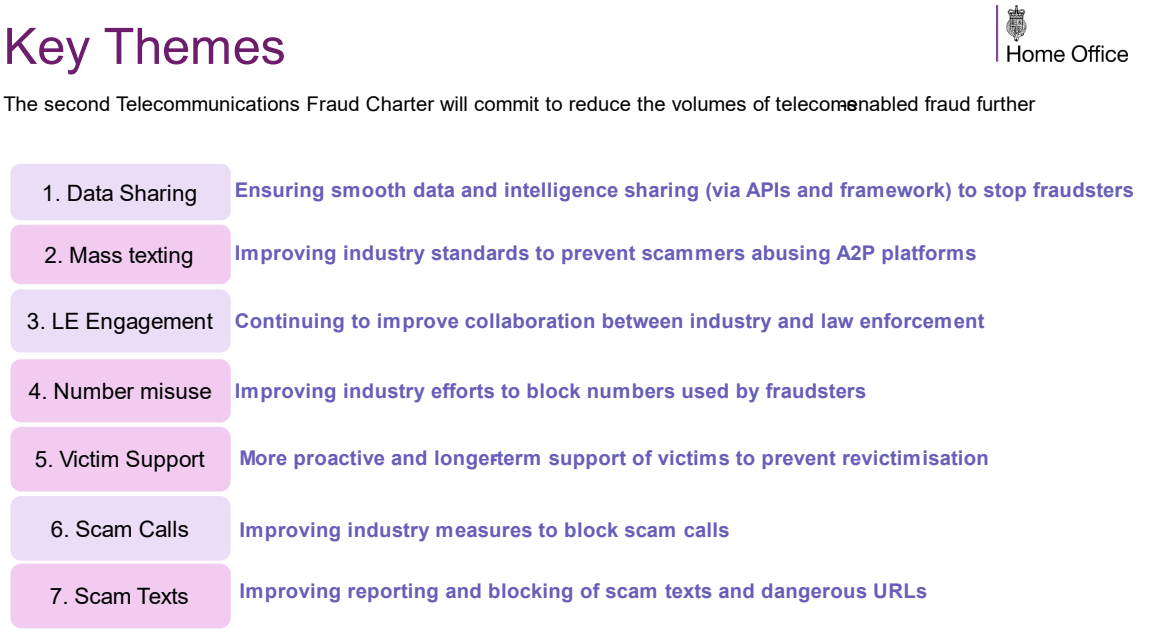
✂

[1] Ofcom Statement Tackling scam calls – 29 July 2024 – paragraph 1.1. Repeated in CFI paragraph 2.7.
[2] CFI paragraph 2.4.

For this reason CCSG Members agree that action against the spoofing of UK mobile numbers is justified, including, in the specific case of a call from abroad which spoofs a UK mobile number. To take this forward industry and Ofcom will, however, have to agree on **how** this will be done. Otherwise, there is a risk intervention will be ineffective and investment at risk of mis-direction.

Towards a consistent strategic approach to tackling voice 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.



Source: Home Office Charter Roundtable – 23 May 2024

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

- Action 6: Improving industry measures to block scam calls.

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 call providers and, where necessary, the regulator, will create a consistent and effective route forward in terms of suppressing fraud using voice communications services.

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 remain critical differences in targeting approach used by fraudsters and in current technical options to defend customers from these scam types.

A strategic response to these threats is illustrated overleaf:

	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[3]) cannot currently be subject to the same scrutiny of content for a combination of technical and legal reasons.

When considering the preferred industry approach to the reduction of scams and fraud on voice calls Ofcom should also consider what the strategic *"end-game"* for UK customers will be. In particular, what should be the target for how customers will be advised to consider voice calls with UK CLI (of different types), international CLI and CLI withheld / unavailable. Arguably, this is already visible in outline from Ofcom's policy supported by market research, however, identifying a viable strategic end-game will support Ofcom's tactical proposals such as in the case of calls from abroad which spoof UK mobile numbers.

Other issues

Ofcom sets out a summary of its **general duties** in section 2.21 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[4].

[3] Voice notes may straddle this distinction.
[4] CFI paragraph 3.21.

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.

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"* contributing to fraud against consumers or providers from the spoofing of CLI or otherwise.

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 - 23/09/24

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.