THE VOICE OF ADVANCED COMMUNICATIONS

COMMS COUNCIL UK
THE VOICE OF ADVANCED COMMUNICATIONS

Home Affairs Select Committee – Fraud Inquiry

Evidence from Comms Council UK (Oct 2023)

Contact

For more information, please contact:

Comms Council UK
team@commscouncil.uk
020 3397 3312
@commscounciluk

Founded in 2004, Comms Council UK is a UK membership-led organisation that represents companies who provide or resell business and residential customers voice services over data networks (VoIP) as well as other "over the top" applications including instant messaging and video. The membership is a mixture of network operators, service providers, resellers, suppliers, and consultants involved in a sector that is diversifying rapidly from just voice services to other innovative IP applications.

Introduction

1. Our sector puts significant time and effort into tackling fraud and scams, and the issue is very important to CCUK members and their customers. We are pleased to submit evidence to this inquiry, to help guide next steps. CCUK representatives would also welcome the opportunity to expand on this submission in an oral evidence session.

The telecoms sector's role in tackling fraud

2. Given the complexity of tackling fraud, we ask that the Committee highlight the need for an **ongoing joined-up approach** between the industry, the Home Office, Ofcom, national security and law enforcement agencies, as well as international organisations and regulators. Given the range of threats that organisations in our industry deal with all the time – including IP PBX hacks[1], DDoS[2] and ransomware attacks as well as vishing[3] and smishing[4] scams – we have a huge amount of technical experience that can be drawn on to support the fight against these growing types of crime. Given the rapid pace at which threats and new fraud techniques develop, **improving and maintaining ongoing lines of communication with industry** will be key in keeping all relevant stakeholders up-to-speed and fast-tracking ways to resolve issues.

3. Members in our sector have found engaging with various Government, regulatory and law enforcement stakeholders on these issues to have been often mixed and disjointed at times in the past. There are a number of different streams of activity across different departments and industry groups, resulting in mixed communication, duplication of resources and slow action. Given the range of relevant people and bodies, we recommend that the Committee focus on ensuring that the ministers work to **reduce the siloed nature of government activity in this area**. We would recommend **one department (most likely the Home Office) have clear oversight** on the whole range of activity being undertaken in coordinating the Government, agency and industry response.

[1] IP PBX fraud is typically a financial fraud as expensive calls can be made whereby a revenue can be acquired from the telecoms carrier terminating calls to the likes of premium rate numbers or international destinations.

[2] DDoS (Denial of Service Attack) is similar to ransomware, whereby criminals aim to cripple a service provider by driving excessive traffic via its network, essentially disabling the service. They then demand some form of blackmail payment to the provider as means to stop perpetrating the attack.

[3] "Vishing" (voice phishing) is the obtaining of numbers and services to use in banking scam.s

[4] A CCUK information video (when formerly ITSPA) outlining some of these offences can be viewed here: https://www.youtube.com/watch?v=WgR-Y1DKf-A

4. The appointment of the Government Anti-Fraud Champion, for example, is welcome and we would urge this role to be **linked in with coordinating the existing activity and ensuring clear channels of communication** to escalate new fraudulent activity.

5. Greater resources and training is also required at the law enforcement level to understand the threats and help track down the criminals. This also needs greater coordination with international law enforcement bodies and regulators. **CCUK would be happy to support with training materials and webinars to assist in this matter.** Our members inform us that many of these offences are particularly persistent, organised and clever. Providers can stop most by watching for patterns, but without concerted attempts by law enforcement to track these people down, the fraud can grow exponentially. Currently there is minimal risk to the criminals – blocking attempted offences individually is important, but not a permanent solution – and therefore a limited deterrent.

Action Fraud and other developments

6. We support announcements around the replacement of Action Fraud (which we believe was well-intentioned, but too often ineffective when it comes to telecoms), but **much more detail is needed on these proposals**. Any replacement needs again to link in with the right channels of Government and industry, whilst having clear objectives and reporting KPIs.

7. More broadly, consideration around future changes must **ensure that they have a positive impact and that costs incurred by industry are not excessive**. A balance must be struck to ensure that the UK's vibrant and successful communications market – which enables the broader UK economy to do business – is not unduly hit by regulations that are well-meant but potentially ineffective.

8. When it comes to developing solutions, **success can only be seen by delivery and engagement on the ground by telecoms companies themselves, *supported* by effective regulation and institutions**. Regulations must not fail to take into account the importance of an open and flexible UK communication system, and **changes that are too heavy-handed can lead to just as many problems as regulations that are too light-touch** – e.g. the potential for over-blocking.

ENDS