DSIT consultation: Proposed Statement of Strategic Priorities for telecoms, radio spectrum, and post

Comms Council UK (CCUK) response

Comms Council UK is a membership-led organisation that both represents and supports telecommunications companies that provide services to business and residential customers in the UK. We keep Britain talking in its various guises by providing or reselling 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. CCUK represents its members at a policy level, builds coalitions to collaborate on industry initiatives and provides a platform to help members prepare for change, learn about new trends and develop new business relationships.

CCUK welcomes the opportunity to respond to this Consultation. Our response is primarily covering Strategic Priority 3 of the Consultation: *Supporting growth through a transparent, competitive, and fair retail market.*

General Comments

CCUK fully supports the addition of a responsibility for Ofcom to continue to work on all aspects of fraud utilising UK telecoms services and infrastructure. However, we would urge DSIT to go further and suggest that Ofcom considers a more all-encompassing approach to fraud remedies. A long-term plan, the elements of which we detail in this response, is needed to ensure effective and efficient support for areas such as law enforcement, and prevent unnecessary additional costs for the telecommunications industry.

The harm created by the multitude of ways fraud is being perpetrated continues to grow, despite the recent measures implemented by Ofcom in their CLI Guidance[1]. Ofcom is primarily focussed on residential consumer harm, but should have greater consideration for the business community and its supply chain.

Ofcom's current approach fails to reflect the whole of the telco ecosystem. It is not holistic in its considerations of the various mitigation tools already in existence or being developed, and thus is enabling loopholes for perpetrators to continue to exploit, both now and in the future.

There are recent examples of effective regulation that are neither prohibitively costly or have long implementation timescales. In Ireland, ComReg took a more comprehensive approach in combatting scam calls and texts when consulting in 2023, and produced a package of interventions across the Telecoms ecosystem. In their recent announcement with respect to a SenderID registry ComReg[2] stated:

---

[1] Guidance on the provision of Calling Line Identification facilities and other related services (Ofcom, 2024)
[2] ComReg launches SMS Sender ID Registry to help prevent text scams (ComReg, 2025)

The overall net financial benefit of all the interventions is estimated at approximately €1.2 Billion by 2030, in addition to the huge benefits to society of reducing scam calls and text.

The UK must become more proactive in order to keep pace with the ever-changing fraud landscape and technologies, and needs a different approach in order to achieve this. However, these changes must be backed up with not only supporting regulation, but the enforcement of such regulation. Indeed, we have observed little action against telecom providers who ignore their existing regulatory obligations, in a way which is unfair on the rest.

Additionally, the telecoms sector requires solutions that will enable the identification of bad actors within the sector, prevent these parties from continuing to operate and support the sharing of information that will enable other organisations such as Law Enforcement to be proactive.

The UK could be much stronger in the area of Telephone Number management, relying on processes that were developed decades ago, with very little adaptation to the current telecoms ecosystem nor the ability to adapt for future technologies. Until the UK has an efficient and reliable way to manage telephone numbers and can accurately identify the users of the services utilising such numbers, then any short-term fraud prevention remedies are merely a sticking plaster.

Recognition of the complex supply chain

CCUK have consistently had challenges in encouraging Ofcom to recognise both business users and the complex supply chain involved in many business communications services.

As recognised in the Consultation, a thriving supply chain is necessary for resilience, innovation and competition. However, the providers within this supply chain can range in size from listed companies through to microbusinesses; effective regulation and the accompanying solutions must be scalable in both cost and ease of implementation for any sized organisation.

There are numerous cases, such as the recent One Touch Switch (OTS) implementation, that have been designed with large, vertically integrated providers in mind and, as such, smaller operators find it too costly and difficult to implement such programs. Smaller providers do not have the benefit of cost amortisation across millions of customers. The reality is that there are a large number of business providers whose customer base number is in the hundreds, or low five figures.

Clarification of the Consultation statement on criminal behaviour

We would also query the Consultation statement "*Ofcom should continue to work with telecoms operators to identify and address the vulnerabilities in telecoms networks that are exploited by criminals, and we expect further close collaboration with government over the coming years".* This statement is unclear as to whether it applies to network vulnerability to attack, e.g. DDOS, or if it covers the wider areas of fraud.

If it only applies to the former, then DSIT should consider expanding the statement to cover fraud and misuse across the telecoms infrastructure, primarily so that Ofcom can develop regulation to support the various fraud and misuse initiatives that are being developed with

Government and industry. Without a regulatory remit there is little hope that the telecoms industry, in its entirety, will voluntarily adopt anti-fraud measures.

That being said, any regulation must be light touch in order to compel providers to act, whilst being flexible to a fraud and misuse landscape that constantly adapts to preventative measures. We foresee the use of artificial intelligence (AI) as a perfect example of such adaptation.

Ofcom budget

Ofcom must allocate sufficient budget to ensure that enforcement of current and future obligations can be fully realised across the telecoms industry as a whole, and not just focused on Communications Providers (CPs) who are engaged and complying with the rules.

Additionally, Ofcom needs to dedicate the resource to carry out in-depth cost benefit analysis on solutions which will enable the industry to be flexible in its approach to implementing new fraud mitigation tools in order to keep pace with fraudsters.

While Ofcom is rightly engaged in addressing online harms, fraud itself is an online harm, and therefore directly an Ofcom responsibility due to the inherent use of telephone numbers throughout the fraud chain. This would benefit from greater attention, and thus we encourage DSIT to direct Ofcom to work more actively on identifying ways to reduce fraud.

It is understood that the current Administration Fee paid by CPs who have self-declared their relevant turnover has been reduced for the proportion relating to telecoms. We warn that reducing budget in this area could be problematic when Ofcom needs to carry out enforcement or investigate solutions which will future proof the UK against the continued attacks from bad actors.

Future of numbering

Ofcom have been promising a review of the numbering regime for a number of years but, to date, nothing has been forthcoming.

Based on legacy telecommunications services, the UK numbering regime is becoming outdated. There are no number ranges designated for Internet of Things (IoT) applications, despite the significant growth in the adoption of IoT-enabled devices. Similarly, the numbering ranges for mobile use fail to recognise the developments both in the UK and worldwide of mobile applications.

Virtual and Cloud Mobile services are significant growth markets within the business telecommunications sector, yet fail to be recognised or catered for by Ofcom. This lack of recognition and the difficulty in obtaining number ranges for these emerging technologies threatens both innovation and competition within the UK communications market.

Therefore, we would recommend that Ofcom develop an outcomes-based numbering strategy which has fraud prevention as a key pillar as a matter of high priority, or at least provide a detailed statement to industry as to its intentions in this area. Despite having many of the

necessary regulatory tools, its lack of sufficient action thus far has put the UK at risk of being caught out by technological advancement.

Effective number management

Whilst there are calls for a centralised number management system, there is no consensus in the industry on how this can be achieved, nor the appetite to incur significant cost in the development of such a solution; Ofcom also appears to have no interest in mandating such a solution.

The UK appears to be unique in its process of assigning large blocks of numbers to a CP. This approach does not reflect the true use of a single number nor does it aid understanding who is utilising a number or its **application** and, as with the aforementioned numbering plan, has its roots in decades-old legacy telephony which has changed very little from its inception.

Such a numbering system would also play a significant role in reducing consumer and business harm when there is a CP failure. Despite repeated requests, there is still no Ofcom mandated process for 'supplier of last resort' in the case of a voice network provider ceasing trading.

Whilst this was not a priority for legacy fixed line communications, the world has rapidly moved on with IP-based voice solutions designated to become the de-facto voice service for both residential and business end users within the next two years.

A centralised number management system would allow continuity of service routing for ported out numbers, and the ability to identify and transfer number ranges from failed businesses.

Number independent communications services

We are starting to see fraud originate outside of the traditional telecoms ecosystem, as fraudsters increasingly use Over-the-Top (OTT) messaging applications.

Ofcom has its hands tied with regards to Number Independent Interpersonal Communications Services (NIICS) as the requirements on NIICS were not transposed from the European Electronic Communications Code (EECC) into the Communications Act (2003).

Whilst tightened regulation on NIICS is expected within the EECC review later this year, Ofcom is helpless to follow suit. CCUK would strongly suggest a legislative review of the Communications Code and the inclusion of NIICS into the Act.

Do Not Originate list (DNO)

Currently, the Ofcom-managed DNO list has a few thousand numbers registered which are primarily financial services and government departments telephone numbers which should not be used to originate calls.

CCUK strongly recommends that the DNO list should be expanded to include all unallocated, unassigned and invalid numbers, as well as other numbers provided by both CPs and enterprises which should not be originating calls. For example, government departments such as HMRC and DWP support lines which only ever take inbound calls.

A more comprehensive DNO list would greatly reduce the volume of numbers which today pass through telecoms networks as legitimate traffic, therefore, reducing the overheads required by the networks both in capacity and additional functionality when inadvertently routing bad traffic. If the DNO were actively managed and interactive, it could also be one of the first ports of call for investigation by Law Enforcement, and for any traceback requests (checks on where the call originated from)[3].

Within this list of numbers, other criteria could be added for numbers which are out of service; for example, numbers previously used by law enforcement for special operations and which must never be re-assigned. CCUK estimates that less than 12% of numbers should be originating legitimate calls when unallocated, unassigned and invalid numbers are removed.

Traceback

Traceback functionality is used to identify the origination and call path of illegal or abusive calls, such as scams, spoofing and unlawful nuisance calls. By tracing calls hop-by-hop through provider networks, traceback can reveal the source of harmful traffic, identify non-compliant or high-risk providers and support mitigation and enforcement. It also promotes accountability by putting providers on notice when they are receiving unlawful traffic from upstream partners, in turn encouraging rapid mitigation and disruption of illegal calling activity. Traceback can also be particularly valuable in tracing and disrupting calls that originate outside the UK.

CCUK would encourage DSIT to make the implementation of traceback a priority to encourage CPs to 'Know Their Traffic' (KYT) and to support reporting other CPs who enable bad traffic to be onward routed.

Traceback needs to be supported by a register of CPs and contact details to aid an effective and efficient industry process as detailed in the section below.

Internationally, traceback is being considered as a deterrent by groups, such as the One Consortium[4] and CEPT[5] aimed at identifying both bad actors and countries which are facilitating bad behaviour. CCUK encourages DSIT to ensure Ofcom engagement with such initiatives to guarantee the UK can engage in tracing calls to their origination, as well as ensuring the UK is seen to be leading this deterrent at an international level, therefore, sending a message to bad actors/countries that the UK is considering all fraud mitigation tools.

Communications Provider mandatory registration

A CP register is required to enable accurate identification of CPs, and as the first step in the traceback process.

A registration regime would build confidence within the supply chain as to the legitimacy of CPs requesting and utilising telephone numbers, and provide granularity as to the identity of the true service provider. Additionally, the information obtained from any tracebacks will inform

[3] Therefore supporting the Home Office On-line Crime initiative.
[4] One Consortium, 2025
[5] ECC Work Programme Database (ECC, 2025)

the validity of the CP enabling calls and help to close down the ability for bad traffic to be routed by less scrupulous or engaged CPs. This would also have the added benefit of enabling better enforcement of the relevant regulations.

There are estimated to be circa 4,000 providers of business communications services, many of whom provide number-based services and will not be focused on the fraud discussions or engaged with Ofcom.

Any CP wishing to offer communications services must register with a central body. Whilst ideally this would be Ofcom, it is recognised that they may be resource constrained and may wish to contract this out to a third party.

Know your Customer (KYC) and other due diligence should be carried out in order to obtain registration.

The registration should not be a perpetual registration and a renewal timeframe should be defined.

Reporting

Registered CPs should provide regular reporting on the numbers they have allocated or sub-allocated. This should also include numbers that have been ported in.

Ofcom should issue reports on CPs that have had registration suspended or removed, this could primarily be related to traceback activity and enforcement.

Additionally, Ofcom should inform range holders when they have taken action against a registered CP utilising the range holders' number resource.

Sanctions

The regulator should have the ability to suspend or remove a CPs registration. This could be coupled with reporting on how many times a CP has to respond to traceback requests and whether this is an indication that this CP is not carrying out their required due diligence and are actively enabling bad traffic in their network.

Without being able to accurately identify bad actors in the supply chain, any measures that industry, the regulator or Government introduces will not be fully effective in fighting misuse. Bad actors in the supply chain will continue to operate and stay under the radar.

Whilst there appears to be consensus in the industry that a registration system would prove invaluable in fighting misuse, such a solution would have to be mandated either through legislation or regulation. A voluntary uptake will not work as bad actors will move to a supply chain that is not part of the registration regime.

Access

The registry should ultimately be a single data set with an API and portal access for registration, report submission and queries which allows real time updates to the data set. However, an interim solution could be facilitated using semi manual processes.

Conclusion

The above initiatives, if considered collectively as a five year plan, could be significantly effective in reducing fraud avenues, provide industry with cost effective solutions and offer an efficient path to implementation.

Further, if the approach to the aforementioned program of work stipulates future proofing as a prerequisite to enable the integration of additional developments, the cost inefficiencies and complexity of supporting disparate solutions can be avoided.