General

Ofcom call for input: options to address mobile spoofing

BT Group Response

BT Group

23 September 2024

Executive Summary

Please note, sections we consider confidential are marked in blue confidential

- As part of BT's drive to 'Connect for Good', we are committed to working with our partners to help protect users of communications services from scams and fraud.
- Ofcom is correct to consider what technical solutions are available to prevent spoofing of UK mobile CLI. We note that the diversity of UK and global network architecture requires deployment of a range of solutions to enhance the protections offered to end users from suspicious traffic.
- BT believes a solution incorporating home routing is likely to offer the best protection to UK citizens and consumers in the medium term. With this in mind, we note the following points in relation to Ofcom's call for inputs:
    1. Ultimately, rollout of VoLTE-based home routing is likely to provide a global solution to allow roaming checks to take place. ✂.
    2. BT favours CAMEL-based (Group 2) solutions which allow home routing as the most effective interim solutions before VoLTE roaming agreements are ubiquitous across the world. ✂.
    3. 'Group 1' solutions set out in the document - which we understand to be those requiring establishment of checks at the international gateway - would likely be effective in reducing the impact of mobile spoofing, but would be disproportionate and have unintended consequences – it would take several years to introduce due to technical complexity, there would be potential impact on network performance (and associated consumer detriment), and would carry significant implementation costs (for limited incremental benefit given points 1 and 2 above). A similar effect could be achieved via removal of CLI seen by the end user, but we believe further consumer-focused research would be needed to assess the behavioural impact of this policy.
    4. In any solution introduced in the UK, some consideration will be required to address scenarios where a definitive "roaming/not roaming decision" is unavailable (i.e. – there are likely to be some scenarios where a "not roaming" marker is incorrect). We therefore have some concerns about mandatory blocking of all these calls (due to end user harm caused by legitimate calls not being connected).
    5. Firewall solutions (such as Hiya) being deployed across networks in the UK and abroad are likely to reduce the impact of spoofed CLI, although their recent deployment on our network means we have limited data available on their impact;
- As we have noted in previous Ofcom consultations on call blocking, the interconnected nature of UK communications networks requires ***all*** market participants to implement agreed solutions, with clear consequences (such as regulatory investigations) for those who continue to send bad traffic onto other networks.

- Ofcom should consider setting out a roadmap of its future work in prevention of voice and messaging scams. This could include:
    - a timeline for expected delivery of 'industry traceback';
    - closer alignment with existing Ofcom policy work on legacy retirement given that new technologies are not vulnerable to scams in the same way as legacy services;
    - detail on other interventions Ofcom would like industry to take to prevent scams;
    - any detail which can be shared on timelines for enforcement activity;
    - further information on how this would interact with Ofcom's future approach to enforcement of Online Harms obligations.

  This would ensure a common understanding across industry of Ofcom's expectations.

Contents

Page

1 BT/EE continues to drive forward plans to protect end users from scams

We have had notable successes in our work to protect end users…

1.1 BT Group has worked hard to protect our customers from scams/fraud in recent years as part of our wider programme to ensure that we 'Connect for Good'.

1.2 Fraudsters who leverage communications networks are highly organised and sophisticated, with anecdotal evidence suggesting many are linked to international criminal organisations. The openness of communications networks means it will be very challenging to stop all suspicious traffic reaching consumers. Nonetheless, working alongside our industry partners, BT has had some notable successes in this area:

- We have long advocated the mandatory blocking of international calls with UK Calling Line Identification (CLI) data outside exceptions permitted by NICC standard ND1447, and were early adopters of such measures for both network and presentation numbers. We welcome Ofcom's decision to require all communications providers (CPs) to do this;
- Our new 'Scamguard' product underpinned by Hiya, which was made available to our retail users starting in the summer of 2024, has given end users the option of new functionality to screen calls which might be fraudulent. While it is too early provide granular data on the impact of this intervention, early anecdotal evidence suggests it has been successful;
- Our work with industry and cross-sectoral partners, third sector organisations, regulators, government, and law enforcement agencies has facilitated the creation of national frameworks to tackle the scourge of fraud and scams – with all interested parties represented around the table. For example, we have long advocated for new data sharing initiatives in line with priorities set out by the UK Government.

..while we agree a challenge remains, it is increasingly difficult to quantify

1.3 We recognise that there is more to be done by all parties – including communications companies - with an interest in protecting end users from scams and fraud, not only because our business requires people to continue to place trust in communications services but also because it is the right thing to do.

1.4 We agree Ofcom is correct to consider what technical measures can be taken to close the lacuna in UK CLI spoofing focused on mobile numbers. We note, however, that it is increasingly difficult for telecommunications providers to quantify the scale and scope of the problem – and its

relative impact compared with other types of fraud, as we do not ultimately know the content of calls which pass through our network.

1.5 It is therefore challenging for us to answer questions Ofcom raises in its call for inputs regarding the scale and scope of the problem, and the proportion of suspicious traffic which can be attributed to 'traditional' voice telephony[1]. ✂.

1.6 Any information we can use to infer that a call might be suspicious is most usefully framed alongside wider anecdotal evidence which is already available, including panel- based and sampling data which reflect the experiences of the wider population on scams. We note Ofcom already conducts a substantive programme of work in this area, as well as gathering industry-wide information on suspicious call volumes, and believe this most accurately captures end user experience of voice calling compared with any available alternative.

1.7 Moreover, we do not hold any data on the relative volume of fraud in channels outside 'traditional' telecommunications services. For example, we do not have any information on the extent to which 'over the top' style services[2] are used to commit fraud/facilitate scams as we do not hold any data on the content of these interactions.

[1] For the purposes of this response, we use 'traditional voice telephony' to denote voice traffic delivered over Number Based Interpersonal Communications Service as per section 32 of the Communications Act

[2] This might include Number Independent Interpersonal Communications Services or End User-to-End User services

2 We support Group 2 options as most likely to have the greatest positive impact

The problem is likely to diminish over time with rollout of new technologies

2.1 As Ofcom correctly identifies, the rollout of Voice over Long-Term Evolution (VoLTE) roaming will provide substantive protection against mobile spoofing, as it will allow for home routing of calls where a user is roaming internationally. The home network can then take appropriate action should a call appear to be from a spoofed mobile CLI.

2.2 ✂. While it is not yet clear when 2G/3G networks will be retired globally, it is likely that new technologies will be the primary solution to the problem of mobile spoofing.

2.3 Moreover, BT/EE has also made new firewalls available to all digital voice and mobile users which – while primarily intended to provide protections for users of internet protocol (IP) or VoLTE services – are likely to provide a layer of protections to customers who use them in particular if a given UK CLI has already been deemed suspicious (✂).

2.4 This has three important consequences for any new Ofcom intervention in voice markets:

a. firstly, it means that any intervention proposed by Ofcom is likely to be on an interim basis until VoLTE roaming is ubiquitous;

b. second, it means that there is no single intervention available to stop all spoofing of mobile CLI until that time (because there will be a range of call routing scenarios depending on whether VoLTE roaming agreements are in place), and;

c. finally, any cost/benefit analysis of proposed interim solution(s) should only consider the incremental difference in protection available today compared with quasi-universal VoLTE roaming rollout – noting that the 'gap' between now and then is likely to diminish over time.

We believe Group 2 interventions offer the most timely/cost effective opportunity for blocking, although they will not be ubiquitous

2.5 The most effective interventions therefore – when considered in terms of likely impact relative to cost – are likely to be based around Group 2-style solutions which incorporate home routing. BT/EE's business current policy is to seek CAMEL routing agreements with roaming partners wherever feasible and currently ✂.

2.6 ✂.

We see substantial challenges with proposed Group 1 interventions

2.7 There are substantial limitations with proposed 'Group 1' interventions, which we understand to mean those interventions where International Gateway Providers performs a 'look-up' against a database at the point of receiving a call.

2.8 In BT's view, none of these will be either quick or easy to implement – and are likely to involve high costs and technically complex (and novel) interventions. International gateway providers – including BT - have used a variety of technologies in the design of their networks, and we do not believe that these could be easily augmented to perform these types of functions. All would require changes to the call model, and either modified call routing, signalling interfaces or application programme interfaces (APIs) – at the time of writing, it is not clear to us the extent to which solutions to these challenges exist in the market or would require bespoke development.

- More broadly, such changes are likely to have impacts on capacity and performance, end-to-end service monitoring, security and integration challenges. This would apply not only to the International Gateways, but also the Mobile Network Operators supporting the roaming checks. All of these aspects would have to be carefully considered, particularly when dealing with platform components that are also underpinning UK Critical National Infrastructure (such as emergency calls).

2.9 Group 1 proposals are – therefore – likely to involve substantial costs to international gateway providers and, ultimately, their wholesale customers as well as Mobile Network Operators. Different Operators are likely to have different timelines to develop a Group 1 solution due to the capability of their current platform solutions, but we would make an initial estimation of a timeline for industry in general of several years.

2.10 We note that a similar solution has been proposed in Ireland with the Irish regulator, ComReg, suggesting a 6-month implementation phase is likely to be appropriate. However, we do not believe this is directly applicable in the UK for the following reasons:

- ComReg maintains databases for numbering in the Republic of Ireland to facilitate queries regarding the home network of a given user. There is no such database in place in the UK;
- We understand ComReg had been liaising with providers for a prolonged period prior to its April 2024 determination, meaning that there has been a longer period for providers to introduce a scheme into their work plans;
- ComReg has specifically excluded providers with a revenue of less than €50m. While we understand the reasons for this, as noted above, the UK voice ecosystem is premised on multiple networks which interconnect at a range of different points. Any lacuna for a specific group of providers is likely to fundamentally undermine the effectiveness (and therefore the benefits) of any such system in the UK – we would expect bad actors would seek to exploit these loopholes should they be left open (for example, by spoofing numbers allocated to 'non-compliant' providers).

2.11 We note that Ofcom would likely be required to determine what constitutes an "international gateway" in any consultation/statement given the range of interpretations – both from a network architecture perspective (i.e. at what point in a given provider's architecture is international traffic deemed to have 'entered' the UK) and from a communication provider perspective (i.e. whether a provider considers itself to be an international gateway – in particular if it is receiving traffic with a UK CLI).

CLI data modification might offer an interim solution for those legitimate roaming calls which do not benefit from home routing

2.12 We agree with Ofcom that removal of CLI for end users would offer some form of protection for end users receiving international calls with from UK numbers, as they would be more likely to screen these calls. However, we note that this might lead to consumer harm as large numbers of legitimate calls from roamers would not be answered. Moreover, this functionality would only have an impact if the end user device had CLI display facilities (which are not available on all handsets). We believe Ofcom should consider research into consumer behaviour in this area to understand better the potential impact of this intervention as the impact of this change will ultimately depend on the end user approach to removed CLI.

2.13 We generally do not believe blocking calls which are marked as 'not roaming' is appropriate because this response is not definitive, meaning there is a risk of legitimate calls (including urgent ones) being blocked. This scenario would require consideration prior to any new solution being introduced.

3 Any solution requires an industry wide approach and consideration as part of a wider programme of work

The UK's voice architecture means a common approach is required

3.1 'Traditional' voice telephony[3] in the UK is characterised by a high volume of different providers – each with unique business models and approaches – interconnecting networks and services at multiple points under commercial terms facilitated by common industry standards. This model is underpinned by Ofcom's regulatory regime which has, in historical terms, tended to place a high importance on competition and choice – compared with alternative systems (such as those operated by providers of number-independent interpersonal communications services) which have tended to favour proprietary ecosystems.

3.2 While the 'traditional' voice telephony model has substantive benefits for end users, including ensuring that they have a choice of communications providers while benefitting from network effects, it has limitations from a blocking perspective. No single provider is able to guarantee the veracity of all traffic terminated on their network.

3.3 This has important implications for how any blocking of suspected bad traffic can work. Primarily – as Ofcom correctly identifies - it requires all providers in the ecosystem to take measures to prevent suspicious calls to ensure that end users can be protected. Otherwise, malicious traffic can enter a terminating providers network from a UK telecommunications provider irrespective of checks put in place at the point of ingress of traffic into the UK network. At the same time, however, it requires development of *common standards* to ensure that measures are applied uniformly to ensure that no end user is disadvantaged and can still benefit from 'legitimate' calls.

3.4 Development of common standards, however, is generally more complex and time consuming than imposition of a unilateral approach given the range of stakeholders, network architectures, and timeframes for implementation. We note that this is not explicitly listed in the Ofcom factors in the section 'Framework for evaluating options' but believe it warrants explicit consideration in any impact assessment of the different options should Ofcom decide to consult on policy changes.

3.5 Moreover, any policy change (made either via the General Conditions or associated Guidance) is likely to require Ofcom to continue and update its enforcement programme into compliance with General Conditions relating to phone and text scams to ensure that all CPs are complying with new rules. Communications providers only have limited leverage to impact bad actors who continue to send bad traffic across their networks, not least because interconnect is in most cases a regulatory requirement.

[3] For the purposes of this document, traditional voice telephony is used to denote voice communications delivered via number-based interpersonal communications services as defined by Section 32/32A of the Communications Act 2003

This should be grounded in a wider programme of work that is clearly signalled for all industry participants

3.6 Given the complexities involved in any industry-wide application of new rules, Ofcom should consider encouraging this process through – for example – setting out a timeline regarding its expectations and likely interventions in the voice market in the medium term (i.e. over the next 18-24 months). This could include:

- When it expects to begin its first investigations following launch of its enforcement programme in February 2024;
- Preferred interventions (if any) around 'industry traceback', which would establish a formal process for the identification of malicious voice traffic being passed between UK networks, and how it expects industry to introduce these;
- The extent to which it expects legacy network closures to impact its work on scams and the associated benefits to citizens/consumers;
- Any other interventions that Ofcom is considering or expects to consider over the medium term, including those relevant to providers covered by the Online Services Act given their increasing prominence in this space;
- A clear statement of future work is likely to be helpful in ensuring all market participants are aware of the expected interventions/progress of Ofcom's work in preventing malicious voice scams and plan their workstacks accordingly.

A clear timeline will make clear to all market participants Ofcom's expectations of them on scams prevention and will also ensure that these can be clearly established in respective programmes of work.

Date

Find out more at bt.com

Offices worldwide

Registered office: 1 Braham Street, London E1 8EE

Registered in England No. 1800000

BT Group