Spoofed numbers

UK Finance response to the Ofcom consultation on Calling Line Identification (CLI) authentication: a potential approach to detecting and blocking spoofed numbers.

Executive Summary

UK Finance is the collective voice for the banking and finance industry in the UK. Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers, and facilitate innovation. This includes helping lead the industry's collective fight against economic crime in the UK, including combatting fraud and cybercrime.

The financial services (FS) industry welcomes Ofcom's proposals on an approach to detect and block spoofed numbers. All member firms are supportive, however given the harms experienced by victims, businesses and to other sectors as a result of CLI spoofing we would urge that the consultation and implementation processes proposed are significantly accelerated.

In addition to our response, we would welcome further discussion with Ofcom on the operational impact and consumer harms caused by spoofed calls.

If you have any questions relating to this response, please contact: Dianne.Doodnath@ukfinance.org.uk

Question 3.1: Do you agree with our analysis of the ways in which number spoofing is used, and the extent and types of harm associated with its use? If you have any further evidence which demonstrates the extent and types of harm involved, please provide this.

The scale and level of attack associated to the ways CLI spoofing drives home the onslaught of criminal approaches to consumers across the communications infrastructure. Harms not captured in the consultation document are outlined below:

1. Not all spoofed calls results in a loss. Those that do not may include damaging the user experience, brand reputation and trust in phone numbers. There is reputational brand damage to those impersonated via spoofing or just by vishing calls where the criminals have sufficient personal information to manipulate the customer into thinking they are speaking the legitimate business.[1]
2. In the iSpoof example, 70,000 victims stayed on the line for over one minute with the criminals, yet 3.5 million calls were attempted to over 350,000 potential victims. This onslaught of unwanted contacts is normalising the expectations of consumers — a quarter ignore withheld numbers as per your research findings — and this in itself is making it harder for legitimate entities to reach out to the consumers that have been socially engineered.
3. The level of near number spoofing (a digit is changed) is not captured, albeit it is discussed in the iSpoof case study. It is not clear if international or technical gaps would mean these are mistaken as legitimate numbers, as the database would house them as some near numbers inactive but owned by some members. One member alone observed 6 cases of near number spoofing with a total victim loss in excess of £1 million.
   In each of these cases, when that number is called back it appear to be from decommissioned numbers that are not in use. We believe it would be reasonable for OFCOM to work with call providers to block these high-risk numbers, where it can be evidenced, they are being used in a fraud attack.
4. There is a significant operational impact of spoofing on our members in terms of the volumes of contacts within their contact centres and the handling of the customer reports. These operational resources could remain focused on mitigating other economic crime threats and customer care, rather than managing the spoofing claims which are due to lack of controls within another sector. When a major attack/ large lost occurs, our members will undertake an incident management process which includes but is not limited to the following:
   1) Operational calls influx triggering the need for incident management and a full root cause analysis.
   2) Evaluating the customer reports to determining if the calls are indeed fraudulent.

[1] https://www.which.co.uk/news/article/amazon-issues-warning-to-customers-amid-growing-threat-of-impersonation-scams-aArUA1p4DWQU

3) Carrying out investigations to determine how the calls are coming through.
4) Carrying out investigations to determine level of fraud being reported or if data is being harvested.
5) Assessment of the control framework, determine where there are gaps.
6) Determine the incident risk control/s to close any identified gaps.
7) Industry engagement via trade associations (TAs) to determine if other members are experiencing the same, have additional intelligence or potential controls.
8) Customer remediation.
9) Applying new transaction and profiling rules.
10) Issuing replacement cards/ account details.

Question 4.1: Do you agree with our assessment that while Ofcom rules and industry measures are likely to help to reduce scam calls, more needs to be done to tackle number spoofing? Provide reasons for your answer and include any suggested measures that could have a material impact on reducing the incidence of scam calls involving number spoofing.

1) Yes, there are significant gaps within the existing interim measures and initiatives that criminals are exploiting these aggressively. In the case of iSpoof, 3.5 million spoofed calls were made by criminal subscribers to UK victims in one year alone. The existing solutions do not mitigate against a repeat of organised criminals misusing CLI.
2) There are significant technical constraints with the existing initiatives, as some call providers (CP) are not able to protect their customers to the same extent. And one call provider has already expressed that the more numbers onboarded for Do Not Originate (DNO), the less effective it is mitigating with existing capabilities.
3) The criminals have widened their approaches to impersonate high priority companies not on the DNO list. The parties being impersonated are unable to onboard to the DNO list as they would have to change their call display policies which can require technical changes which are disproportionate, and/or the criminal impersonation attacks are intermittent making it hard to justify these changes.
4) The most recent publication of our stats in May 2023 shows that c.44 per cent[2] of the value of scams are lost via telecoms enablers (spoofed calls and SMS), as such additional measures to comprehensively mitigate call spoofing would be most welcome to help protect victims from criminal approaches at source.

Question 5.1: Is the approach to CLI authentication we have outlined feasible and workable?

The proposals are logical providing there is sufficient automation, governance and enforcement that drives the right behaviours. The existing processes in other regions for their variant of implementation would be a good sense check on potential standard practices for The Administrator.

There are already equivalent oversight systems to The Administrator in the FS two payment rails, for Cards and Faster Payments, that maintain the integrity of data, enforcement and drive positive incentives for stakeholders. These may prove a valuable comparator for the frameworks required to support a central function.

The onboarding of rogues as legitimate entities, and manipulation of the meta data or technical faults for the calls are the core areas of vulnerabilities to this type of framework.

Question 5.2: To what extent could adopting this approach to CLI authentication have a material impact on reducing scams and other unwanted calls? If you consider an alternative approach would be better, please outline this and your reasons why.

The estimated losses from Ofcom's analysis are circa £100 million given there is under reporting. Currently the main analysis of this has been on consumers losing funds as a victim of scams and unauthorised fraud. There will be examples where businesses are defrauded, including impersonation of suppliers, company executives and family members in virtual kidnappings.[3]

A process that eliminates the ability to impersonate trusted phone numbers is important, as artificial intelligence (AI) develops and advances into mainstream usage. Criminals' ability to impersonate relatives to amplify scams will intensify.

2) https://www.ukfinance.org.uk/news-and-insight/press-release/over-ps12-billion-stolen-through-fraud-in-2022-nearly-80-cent-app
3) https://abc7chicago.com/virtual-kidnapping-scam-ransom-fbi-phone/11517180/

There remains an education piece required to ensure the consumers can understand the new system is in place, as well as allowing them and businesses to centrally report spoofed calls. A comms campaign would be required to socialise the importance of the changes and reporting.

Question 5.3: Are there additional measures that could be adopted to further strengthen the suggested approach and/or minimise the identified exemptions?

The Administrator should have an added function of sharing of intelligence where there is a threat actor accessing the network system. The infringement types listed within the consultation do not factor and cater to criminal testing of infrastructure. The listed types 'inadvertent and irregular or persistent' could leave a gap where a single call is attempted to ensure a route is clear for illicit calls.

Question 6.1: Do you agree with the approach outlined for the monitoring and enforcement of the rules with regard to CLI authentication? Are there any alternative approaches that we should consider?

This is not within our sectors expertise, however equivalent models adopted within the USA/ Canada/ France as well as payment scheme governance models could be evaluated by 'The Administrator'. There is a need to take lessons learned about criminal behaviours and their aggressive approach to circumventing controls.

The multi-agency policing unit, the Dedicated Card and Payment Crime Unit (DCPCU), that UK Finance sponsors actively takes smishing intelligence and cases forwards in partnership with many call providers. This opportunity is not leveraged within the spoofed calls environment due to the tracing constraints. The additional capability to trace calls will lead to more prosecutions which will deter the criminals. The administrator and Ofcom should seek to actively engage the DCPCU and other law enforcement agencies as appropriate.

Question 7.1: What are your views on the timescales for the potential implementation of CLI authentication, including the interdependencies with legacy network retirement?

While the legacy network retirement is a material element there is a need to move forward at pace. A consultation output from Ofcom in 2024 that is tied to PSTN switch over by the end of 2025 is not in step with the criminal onslaught against potential victims. It has already taken several years to create the globally agreed protocol STIR/SHAKEN, and while the last consultation in 2019 identified core challenges with overseas calls it yielded no movement on the numbering database to mitigate MNP and assist law enforcement with criminal disruption in the interim.

Based on the Impersonation victim volumes of 2022[4], the projected impact across the next three years (2023-2025), would be 135,000, which is 123 victims per day.

Question 7.2: Do you agree with our assessment of the administrative steps required to implement CLI authentication and how these should be achieved?

These should be achieved in parallel, leveraging the insights of how these have been achieved in different regions and across payment systems to accelerate the process. These cannot be left until the full PSTN switch over is complete, as some parties that are more advanced in their deployment of VOIP could begin testing the infrastructure to inform new policy/rule considerations.

Question 7.3: Should a common numbering database be implemented to support the CLI authentication approach? Please provide any comments on the steps needed to implement a common numbering database, including on the feasibility of the industry leading on (a) the specification; and (b) the implementation?

In our 2019 response to the Ofcom Trust in Phone numbers consultation, we put forward that a numbering database would be welcome to mitigate a number of issues (e.g. MNP and traceability) in addition to spoofing. This is still our position however we would like to amplify that the inability to trace calls has allowed the criminals to avoid prosecution and has only led to the issue growing exponentially. The consultation itself highlights that the UK is the worse region in Europe for spoofed calls, according to HIYA analysis. If, despite the growing harms and the imminence of the PSTN switch off, this CLI consultation fails to progress, the central database should still be created.

4) https://www.ukfinance.org.uk/system/files/2023-05/Annual%20Fraud%20Report%202023_0.pdf

Question 8.1: Do you agree with the proposed framework for impact assessment and the potential categories of costs and benefits? Please identify any other factors that we should take into account in our assessment.

Adding a number to the DNO list does not guarantee that all call attempts will be blocked. While the majority of onboarded numbers will be protected, technical constraints may mean that a good proportion of calls are still connected. These constraints relate to the technology available on the networks involved, the route the call takes across networks and whether the providers of the networks are able to make use of the full DNO list. Measuring the additional/ delta in protection having implemented this Vs DNO gap reduction should show additional benefits to protecting these high-risk numbers.

The benefits gained from traceability should also be captured, such as the number of additional law enforcement operations and additional lines of enquiry to commence investigations. Also, the number of years of incarceration should be captured.