UK FINANCE

Consultation: Tackling scam calls – expecting providers to block more calls with spoofed numbers

Date: 28 03 2024

Address:
Scams consultations
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

Sent to: scamsconsultations@ofcom.org.uk

Executive Summary

UK Finance is the collective voice for the banking and finance industry. Representing more than 300 firms across the industry, we act to enhance competitiveness, support customers and facilitate innovation.

The financial services (FS) industry welcomes Ofcom's proposals on the approach to expecting providers to block more calls with spoofed numbers. All member firms are supportive of the improvements to the general conditions, however given the harms experienced by victims, businesses and to other sectors as a result of CLI spoofing we would urge that the implementation timeline for the 'small change' proposed is significantly accelerated.

We are pleased to see horizon scanning for the migration of attacks to +447 is already under consideration, our experience is that criminals are incredibly aggressive and are able to adapt to controls rapidly and thus consider this obvious gap needing to be closed at pace.

Finally, we are disappointed to see a complete move away from CLI authentication, and we firmly believe that this cannot be discarded without a more robust and layered approach to the controls being required to protect the public from call spoofing harm. As such the following areas should be included in parallel to the horizon scanning activity:

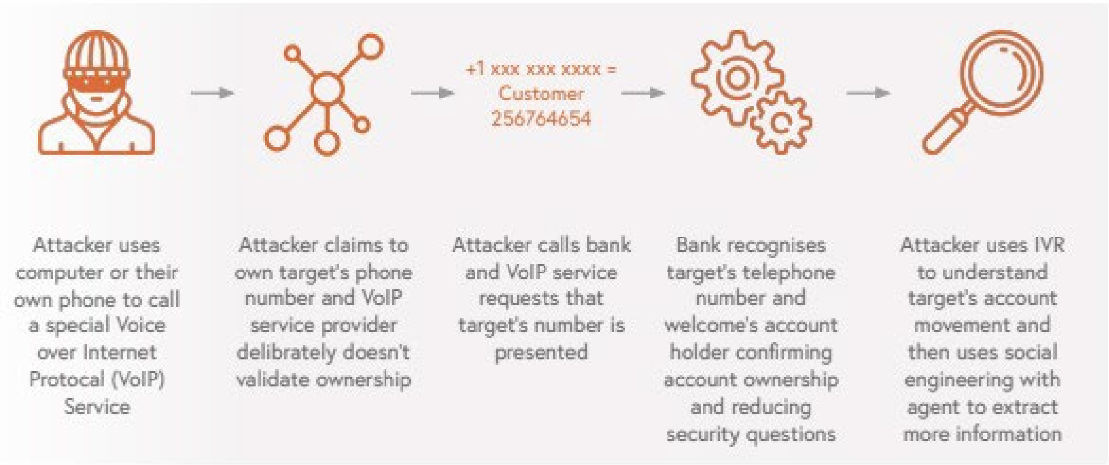
- The successful voluntary Do Not Originate (DNO) initiative we are in support of needs to become mandatory. There is a need for proactive onboarding of companies that are prolifically impersonated and further overlay services onboarded to close the technical gaps with DNO.
- Due to the volume of spoofing into the contact centres of financial services, telecoms and other business types, there is a need to increase accessibility of call tracing to assist with criminal disruption.
- Where criminals are unable to leverage vulnerabilities, they will migrate to acquiring or taking over existing legitimate services. We would therefore also urge Ofcom to reconsider our previous recommendations in response to the consultation on 'Good practice guide to help prevent misuse of sub-allocated and assigned numbers'.

Consultation question 1: Do you have any views on the potential impact of the proposed change?

On a customer level, it is viewed that this will have a beneficial impact on the Bank's customers and prevent potential spoofing where the Presentation CLI is also spoofed e.g., to a Bank Number which is not currently on DNO list, or where the number is a 'near' number. This is a positive change that will further mitigate scams.

However, on the current understanding this will not prevent a narrow range of spoofing/fraudster attacks that have been seen by the Bank, which are targeting a bank itself and where the Fraudster is presenting a customer CLI, and the calls originate abroad (see below). This is relevant to specific examples where (in conjunction with Telco Partners and Fraud Prevention partners) the Bank is able to establish both the Network and Presentation CLI have been spoofed, and where other information indicates the call is being injected into foreign telco networks and pretending to be a UK Mobile (without registering as a mobile on the local mobile network).

Figure 4: How Fraudsters Spoof ANI/CLI



Attacker uses computer or their own phone to call a special Voice over Internet Protocal (VoIP) Service

Attacker claims to own target's phone number and VoIP service provider delibrately doesn't validate ownership

Attacker calls bank and VoIP service requests that target's number is presented

Bank recognises target's telephone number and welcome's account holder confirming account ownership and reducing security questions

Attacker uses IVR to understand target's account movement and then uses social engineering with agent to extract more information

Case studies – Disruption of criminals via call tracing.

An enhanced capability from Telco's is required to help support institutions such as Banks investigate fraud attacks to disrupt criminals. This could include with the capability, in conjunction with Ofcom, to be able to bring a 'fraud investigation' ticket to the supplying Telco. Then for them to be required to investigate this and any upstream Telco's to be compelled as part of their license to investigate and supply data back down to enable an organisation to understanding/investigate where attacks are originating.

Example 1
As explained above our Members are seeing fraud attacks where fraudsters are spoofing customer numbers (target victim) and calling in to the bank. A single institution has quoted that several of these spoofed customer calls occur per week, which result in successful fraud. Across the wider industry this may result in thousands of fraud cases, impacting thousands of victims.

Example 2
Another member has experienced withheld numbers being used by criminals that impersonated the bank to defraud 50 businesses, in just two months.. https://www.msn.com/en-gb/news/newsbirmingham/santander-issues-warning-to-account-holdershttps://www.msn.com/en-gb/news/newsbirmingham/santander-issues-warning-to-account-holders-over-problem-that-is-rampant/ar-BB1jRYDfover-problem-that-is-rampant/ar-BB1jRYDf

There has been no traction with telco partners to trace or investigate some of these instances, despite those seeking the trace being regulated entities. Whilst privacy is incredibly important and there are restrictions around electronic communications, the threshold for law enforcement is too high, and despite confirmed fraud by a regulated entity these investigations cannot be progressed. A requirement for law enforcement involvement to commence any tracing allows criminals to continue to steal funds, these funds are often used commit further economic crime .

Ideally, there would need to be the ability to harvest data attached to the calls to show the VOIP provider and the source of the call itself e.g., IP address

DNO – enhancements
We have seen and continue to see significant impact from DNO, and believe this should now be made mandatory and enhanced further:

- Higher-risk numbers linked to impersonation scams (e.g., regulators, county courts, business accounts) should be proactively onboarded, below is an excerpt from an FCA examples
- Further overlay services should be utilised to limited calls that slip through gaps due to the technical limitations across some areas of the infrastructure.

Case study - high risk numbers outside of banking

The UK's financial regulator has warned of an increasing number of scammers pretending to be the watchdog.
The Financial Conduct Authority (FCA) said its impersonators aim to get people to hand over money or sensitive information, such as bank account PINs and passwords.
The public reported more than 7,700 instances of this type of scam to the FCA's contact centre so far this year. Reports of this type of scam have more than doubled since 2021, the FCA said.
https://www.bbc.co.uk/news/business-66650783

We urge Ofcom to reconsider our previous recommendations in response to the consultation on ‘Good practice guide to help prevent misuse of sub-allocated and assigned numbers’. A need for stronger Telco controls around validation of numbers, particularly when calls are being routed in from abroad, and controls around any number claim scenario. This could potentially extend to stating the types of controls institutions such as Banks would want the carriers/Telcos to be required to implement as part of their license

Also, the spoofing of brands on SMS continues to impact businesses not onboarded to the Mobile ecosystem Forum (MEF) SenderID Registry, resulting in additional victims and money flowing to criminals. The SenderID Registry needs to be mandated for all SMS suppliers. Also companies at a high-risk of impersonation need to be onboarded, in order to proactively protect the public.

Finally, we see there is a need to for further incentivisation on telecoms (reputational or financial) to encourage further behaviour change as well as increased transparency. 17 per cent of Scam cases originate from telecommunications, these are usually higher value cases such as impersonation scams and so account for 45 per cent of losses. There is a fundamental need for a more equitable approach to collaborative mitigation, where solutions have been sought by the financial services telecoms, have put paywalls in place.

https://www.ukfinance.org.uk/system/files/2023-10/Half%20year%20fraud%20update%202023.pdf
Consultation question 2: Do you agree with our proposed change to Paragraph 4.19 of the CLI Guidance? If not, please explain why.
The view is that this restriction potentially could be extended further. In regard to the mobile exclusion, the Bank would like to see further requirements around this section

- *UK mobile users roaming overseas making calls back to UK numbers, i.e. calls with a CLI from the +447 range;*

Within this step, it would be beneficial (where technically possible) to require ingress carriers to confirm (if not done already) with UK Mobile Operators that the mobile number is indeed registered with the operator as being out of the UK.

Calls that are routed into the UK from aboard, and cannot be verified are truly registered as roaming should be either:

- Blocked
- Have the Network CLI amended to a specific Ofcom range to allow consuming parties to make risk scored decisions (e.g., in line with partner Telco services) whether to accept the call, or place into a higher risk category.

It is acknowledged that this would be problematic without appropriate verification services offered by UK Mobile Operators, or the underlying network operator.

The guidance around CLI should also include changes to allow end users/telco partners to request and receive appropriate support from within the upstream UK Telco/Carrier providers when investigating spoofing issues related to fraud or scams. The current position does not support provision of investigation e.g., an agreement on a set of depersonalised information that can be provided to a requesting carrier to allow end parties e.g., Banks, Financial Institutions to tie together fraud attacks which involve spoofing. This change would allow an agreed set of parameters to be exchanged between Telco Partner's and made available to the requesting consumer (for the specific purpose of fraud detection e.g., under Ofcom Agreement with the end party). Examples would be the egress/ingress carriers, country of origin – but no personal data – to allow linkages with other data points and establish patterns that can be provided to the appropriate legal bodies.

Consultation question 3: Do you agree with proposed implementation date of six months after the publication of the Statement? If not, please explain why.

The implementation should be 3 months rather than six months, to mitigate the harm to potential victims. Ofcom has stated this is a simple amendment, and a final statement will also take time for Ofcom to produce. Below are two pieces of analysis we believe can aid demonstrating this is a proportionate ask.

UK Finance industry stats – Scale of confirmed fraud for impersonation scams.

In H1 2023 the impersonation related scams accounted for 17,046 cases. Telecommunications is the dominant enabler for the impersonation scam type, taking a conservative estimate that 50% of these scams/cases are enabled this way, would result in 4,250 cases in the additional 3 months https://www.ukfinance.org.uk/system/files/2023-10/Half%20year%20fraud%20update%202023.pdf

Case Study – Scale of harms from attempted spoofed calls

In November 2022, the UK's biggest ever fraud operation brought down a criminal group running an online service – iSpoof – that enabled number spoofing calls to be made. Criminals used the service to attempt to steal personal information, impersonating trusted organisations such as banks. The service had additional features like Interactive Voice Response (IVR) call handling with custom hold music and call centre background noise. Victims contacted would be instructed to share six-digit banking passcodes with the scammers, allowing them to access their bank accounts. The service facilitated around 3.5 million spoofed calls between June 2021 and July 2022 in the UK, with 350,000 calls lasting more than one minute.

The iSpoof case demonstrated the scale that the criminals are operating at using phone calls. With this type of technology available to criminals, they are able to engage with consumers impersonating legitimate financial services as part of an initial contact. This allows the criminals to socially engineer victims into expecting further calls with multiple ruses, to build confidence and then later ask the victim to make an investment once trust has been built up.

https://www.actionfraud.police.uk/news/more-than-100-arrests-in-uks-biggest-ever-fraudhttps://www.actionfraud.police.uk/news/more-than-100-arrests-in-uks-biggest-ever-fraud-operationoperation

This demonstrates that ***on average in just 3 months 807.7k call attempts were made and 80,769 calls that successfully lasted over 1 minute***. This shows that criminals can be incredibly aggressive and the pace of implementation for iterative controls needs to be timelier.

Finally, the regulatory process to achieve the changes proposed by Ofcom is extensive and onerous. The work prior to the consultation release, the consultation cycle and implementation timeline mean this entire process for what is a simple change will have taken circa a year. There is a need for a nimbler process to achieve changes such as this.

Consultation question 4: Do you agree with our assessment of the potential impact on specific groups of persons?

We agree.

Consultation question 5: Do you agree with our assessment of the potential impact of our proposal on the Welsh language?

No comments

If you have any questions relating to this response, please contact ✂ **Principal, Remote Payment Channels** ✂

✂
Principal, Remote Payment Channels