Ofcom Consultation - CLI Accuracy

UK Finance response

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

Date 20th April 2022

Sent to [scamsconsultations@ofcom.org.uk]

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

Ofcom's consultation on Calling Line Identification CLI Accuracy addresses important issues facing society. This response only addresses aspects of direct interest to the banking and finance industry, foremost among which is economic crime.

If you have any questions relating to this response, please contact:
[✂]

Response

- Ofcom has already moved forwards with several welcome initiatives to mitigate the harm caused to consumers from spam, including the ICO-Ofcom Joint Action Plan, Ofcom's Do Not Originate and the allocated numbering list. We welcome the changes to the granularity of the general conditions which is critical to supporting the preservation of trust in telephone numbers, without which, consumers will remain at heightened risk of harm associated with fraud and scams. We welcome Ofcom's efforts to raise and level the standard of expectations of carriers monitoring and agree with the proposed change to the general conditions.
- Public uncertainty over legitimate CLIs is an important driver of significant consumer harm through authorised push payment (APP) fraud, in particular impersonation scams. We accept that Ofcom can only enforce these measures on genuine firms and that 'bad actors' are unlikely to include these steps in their sales journeys. However, embedding more granular sub-categories on accuracy of CLI may identify bad actors due to the absence of previously observed controls.
- Criminals have exploited the Covid-19 pandemic to exploit individuals heightened financial insecurities. In 2021, this led to more than £214.8 million lost to impersonation type scams. Impersonations scams relating to banks or police increased 53% year on year and impersonation of others trusted entities increased 39%. These two scam types alone impacted over 55k people.

- The nature of this scam type means there are often life-changing sums involved in individual cases. For example, impersonation scams accounted for 28 percent of the total number of APP frauds in 2021 and accounted for 37 percent of the total value of all APP frauds.
- Additional analysis of the different scam types has shown impersonation scams are heavily enabled by an initial phone call, as the first point of outreach, which often results in the prospective victim being convinced to carry out transactions/make transfers of funds. The financial sector is at this stage unaware of the phone approach and does not receive any intelligence that a call resulted in the transaction and in many cases not until long after the funds have been transferred from their account. As the attack is outside the perimeter of the banking infrastructure, steps to prevent the criminals' approaches are a vital intervention point in the protection of potential victims from distress and loss of confidence as well as suffering losses.

Extracted from UK Finance Annual Fraud report 2022

	2020 - Impersonation Scams		2021 - Impersonation Scams	
	Banking	Other	Banking	Other
Cases (Complaints)	21177	19728	29,406	26,227
Payments	40497	33334	62,806	44626
Losses	£90.9mn	£55.8.mn	137.3mn	77.5mn

If the current trends continue without further interventions, by 2025 the number of impersonation scam victims would be 250k per year, the combined victims during the 4-year period 2022-2205 would be approximately 620k.

Evolution of criminal typologies

- In 2017 the president of the Communications Fraud Control Association acknowledged, following publication of its 2017 Global Fraud Loss Survey, *"many services now utilise the mobile phone as the contact point for verification, whether this is to receive a call to verify a transaction or a text message with a one-time passcode or authorisation code. The mobile account of a consumer has become fundamental as part of an authentication trail in many services such as banking. Fraudsters therefore target customers accounts in order not to defraud the telecoms company but actually target the consumer themselves in order to manipulate their financial or other services."*[1]. However, as criminals have evolved, the current modus operandi experienced is no longer focused solely on the circumvention of financial sector controls, but to influence the consumers into undertaking the processing of transactions by impersonating different trusted parties from banks, regulators, and law enforcement through to parcel delivery services.
- Industry research has demonstrated that the criminals behind impersonation scams are methodical, strategic and persistent. Research undertaken as part of a GSMA and UK Finance collaboration has revealed that the average scam call lasts over three quarters of an hour, and that on average a payment is made midway through the call. This could mean lifesavings are lost in less than half an hour, but the victim is held in dialogue post transaction to further ensure they believe the scenario presented by criminals.
- The fraud and scam attacks in the current climate are now personalised with the victim's involvement and no longer unauthorised or unknown activity. Prevention is a critical factor where all enabling sectors play an important part in mitigating the vulnerabilities the criminals exploit.

- In addition to this there are increased takeovers of genuine trusted accounts within other sectors in order to circumvent controls. This has been seen in the aggregator where trusted messaging routes have been taken over.
- Whilst we welcome Ofcom's proposed changes and increased granularity on CLI, we do believe the strength of the regulatory expectations should be more in line with the financial sectors regulator in relation to misuse of services. The trust in CLI is of paramount importance in today's fraud and scams landscape. The duty to protect consumers, the evolution of criminal attacks and the consumer harm, distress and loss in confidence is an important factor for tackling the scourge of fraud and scams. To preserve trust in CLI, there is a need to raise the expectations across the Telcom's services where the impact of lack of controls leads to ~~such~~ appalling impact on a victim's confidence.
- Spoofing statistics are not easily tracked, and the victim data UK Finance provides will not show the number of failed scams nor repeat attempts to contact potential victims. However, overlay services can inform the view on how many calls are bypassing the carriers filtering including Do Not Originate (DNO), and are being mitigated by the overlay services further downstream by services such as trueCall and HIYA.
    - Some services will be able to provide historical insights on the problem. From our own analysis hundreds of thousands of calls have been mitigated and therefore prevented tens of thousands of victims,
    - This analysis and our members feedback on the impact of protecting numbers shows that the DNO list is an important tool that goes beyond the carrier filtering for the fraud and scams being seen by victim reports to the financial sector.
- Independent sources of data should inform Ofcom's view of the problem landscape as there are gaps of insight where calls are occurring via the Over-The-Top Services and where the infrastructure cannot support DNO.

Implementation date

- The proposed 6-month implementation timeline along with firm dates for enforcement is welcome as this is an issue causing material harm today and delays result in numerous additional people being targeted. During the proposed 6 months implementation the number of victims of impersonation scams would be approximately 37,9k.

Do Not Originate (DNO)

- Given the harms and evolution of criminal tactics the DNO list implementation should become a minimum standard for any licenced carriers:

    - in the same way the banking sector has to report failures toits regulator, a failure in a carrier that stops DNO working should also be a reportable issue to Ofcom
    - given the level of material consumer harm, there should be a process to inform the owning business that there is a DNO failure, so they can be alerted to the potential that their customers are being targeted.
    - Ofcom should have the responsibility for ensuring that where DNO failure has occurred the carrier responsible identifies and resolves the underlying problem
    - this should become a priority area for Ofcom given the material harm to consumers and the risk in the loss of trust in CLI

The sharing of intelligence within the sector will support increased and focused mitigation of attacks with several learnings taken from the financial sector as below:

Case Study 1: NCA – post implementation, immediate migration

Multiple member banks that are participating have noted customer reports where they are called from a number that displayed the NCA contact number, under the instructions of the criminal the victim subsequently lost £1mn.

Case Study 2: FCA

A customer was called from a number that displayed the FCA contact number, under the instructions of the criminal the victim subsequently lost significant funds.

Case Study 3: FOS – Use of trusted arbitrator

A customer was called from a number that displayed the FOS contact number, under the instructions of the criminal the victim subsequently lost significant funds.

Case Study 4: CCJ – case study where the cases are published, and the courts are spoofed.

A number of customers were called from a number that displayed the courts contact number, under the instructions of the criminal the victim subsequently lose money trying to avoid the threat of additional fines.

From the case studies supplied over £1mn of losses occurred, it is imperative that a proactive onboarding approach of law enforcement, regulators, councils, and courts is undertaken to protect the public from this form of social engineering attack. These trusted organisations are all used as a ploy to encourage potential victims to move funds, whether it's to protect funds from risk, offering discounts for quick and early payments or threatening fines/arrest for lack of payment. These should all be prioritised for the list.

Over The Top services

- The Over-The-Top services need to have the equivalent obligations as other providers to avoid criminal misuse. The CLI behaviours need to be consistent across all parties such as the handling of out of use numbers including quarantining prior to number reuse. For all consumer protections relating to scams and fraud there is a need to ensure all gaps are closed, as criminals will exploit these aggressively.

Intelligence Sharing

- **Cross Sector Intelligence**: The Financial Sector hold routine weekly intelligence sharing calls on behalf of our industry, which often highlight the latest techniques the criminals are deploying in their attacks on consumers and those that fall for them. The sector shares typologies with Ofcom on a regular basis in order to enable the telecoms sector to have a better understanding of the current financial fraud threats and how criminals are circumventing controls. This intelligence should be combined with that of law enforcement and the insights of the call blocking overlay service and subsequently shared back with the Telcom industry on a weekly basis. Also, any good practices that can be shared to enhance the mitigation of service misuse, from sectors impacted. This will allow call providers to have an ongoing methodology to monitor trends and adapt processes in a timelier fashion; limiting the need for refreshed guidance as criminals adopt new techniques.

Within Industry: The SMS Firewalls are helping the MNOs block phone numbers that are detected within the SMS they have blocked; this could be used as a source of misuse intelligence for those that are assigned those numbers. The capability to identify this information is summarised in the following publications **Vodafone SMS Firewall** and **BT SMS Firewall.**

Business Guidance should be a mandatory obligation for call services

There is an opportunity for Ofcom to raise standards and protect victims and businesses becoming victims by setting expectations that best practice guidance is issued to businesses owners, such as the NCSC guides as below and the proposed telecoms security regulations and code of practice.

This would provide many new businesses a tool kit of essential best practices/standards to prevent and mitigate their businesses being misused by criminals. Too often unsuspecting businesses are targeted aggressively, and best practices are adopted after an attack has occurred. Prevention of today's challenges must become built into the sales processes.

- https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing Section 4 on telephone numbers.
- https://www.ncsc.gov.uk/guidance/business-communications-sms-and-telephone-best-practice

In addition, guidance sources should be supplemented with education material from appropriate sources such as:

- The Call Providers
- Ofcom
- Take Five

Alternately, the sector could create a Comms essential for businesses the equivalent of cyber essentials or leverage the approach within the proposed telecoms security regulations and code of practice.