Ofcom Consultation - Good Practice Guide on sub-allocated assigned numbers

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.

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

Ofcom's consultation on Good Practice for sub- allocated assigned numbers helps to address important issues facing society. This response only addresses aspects of direct interest to the banking and finance industry, foremost among which is economic crime.

Response

- Ofcom has already pushed forward several welcomed initiatives to mitigate the harm caused to consumers by spam, including the ICO-Ofcom Joint Action Plan, Ofcom's Do Not Originate and the allocated numbering list. We welcome the additional proposal of guidance which will ensure the approach to number allocation is consistent. Clear guidance is critical to the preservation of trust in telephone numbers, and without it, consumers will remain at heightened risk of harm through fraud. We welcome Ofcom's effort to raise and level the standard of expected due diligence and activity following misuse for sub allocated numbers.
- 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.
- 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

1. https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807
2. https://www.ispreview.co.uk/index.php/2022/01/vodafone-uks-new-sms-firewall-dramatically-cuts-scam-texts.html
3. https://www.mobileuk.org/news/guest-blog-were-investing-millions-with-ee-and-bt-to-protect-our-customers-from-scams

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 are now personalised to include the victims' involvement in the scam rather than an unauthorised or unknown activity. Prevention is a critical factor where all enabling sectors play an important part in prevention of victim harm.
- In addition to this there are increased takeovers of genuine trusted account within other sectors to circumvent controls, this has been seen with the SMS aggregators, where trusted messaging routes have been taken over. Security controls to avoid misuse of legitimate services need to be a default requirement due to the harm to victims.
- 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 appalling impact on a victim's confidence.
- There is a need to bring Over The-Top players, call centres services/providers into regulation as they can all impact CLI and signalling, this is to ensure a common standard with the use of numbers to ensure trust in CLI can be restore; criminals will aggressively misuse all gaps in standards to manipulate victims. Whilst these services/providers remain unbound by RIPA/PECA/General Conditions this will continue to leave a significant and scalable gap for criminals to exploit. Also, the CLI behaviours need to be consistent and include the handling of out of use numbers such as quarantining prior to reuse.

Section 3. Due diligence checks before sub-allocating or assigning numbers

The numbers being supplied can be used to cause significant harm to consumers both financially and emotionally as described earlier in the evolution of criminal typologies. The highest standards to protect end consumers should be adopted when providing numbers, and whilst the list of reference points suggested are a positive step, the due diligence approach used within the financial sector below illustrates how a regulated gatekeeper sector is required to manage risks to the legitimate economy. Other sectors bringing risk of economic crime into the system should become required to take their own equivalent measures to equally tighten the level of controls and barriers to help mitigate the scourge of criminals targeting potential victims. In addition, the learnings from the financial sector around systematic vulnerabilities of reference sources should be well understood to avoid criminals circumventing of these controls within the guidance document Ofcom produces.

In the financial sector there are a range of due diligence checks performed (see the current-guidance for industry), which includes but not limited to the list below. This standard set for due diligence is a condition of license to avoid the misuse of licensed facilities.

The type of information referenced should include the nearest equivalents of:

- details of the customer's business or employment
- the source and origin of the consumer data they will be leveraging during the relationship
- details of the relationships between signatories and any underlying beneficial owners
- the expected level and type of activity that will take place during the relationship
- Systems and controls to avoid account/call services takeover

1. https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807
2. https://www.ispreview.co.uk/index.php/2022/01/vodafone-uks-new-sms-firewall-dramatically-cuts-scam-texts.html
3. https://www.mobileuk.org/news/guest-blog-were-investing-millions-with-ee-and-bt-to-protect-our-customers-from-scams

In some situations, it is necessary to carry out 'enhanced due diligence', these situations include:

- when the customer is not physically present when carrying out identification checks
- when entering a business relationship with a person that has been denoted on the FCA website or CIFAS database as well as their family members and known close associates
- when entering a business relationship with a 'politically exposed person' - typically, a non-UK or domestic member of parliament, head of state or government, or government minister and their family members and known close associates.

- when you enter into a transaction with a person from a high risk third country identified by the EU
- any other situation where there's a higher risk of fraudulent activity.
    - Typology information shared within the sector can help to identify high-risk activity.

The enhanced due diligence measures for customers who are not physically present and other higher risk situations include:

- obtaining further information to establish the customer's and business owner's identity
- applying extra measures to check documents supplied by a credit or financial institution
- making sure that the first payment is made from an account that was opened with a credit institution in the customer's name
- finding out where funds have come from and what the purpose of the call service will be.

The enhanced due diligence measures when dealing with a politically exposed (*or equivalent may be a person denoted by the FCA or CIFAS*) must include:

- making sure senior management gives approval for a new business relationship
- taking adequate measures to establish where the person's wealth and funds involved in the business relationship come from
- carrying out stricter ongoing monitoring of the business relationship - this should include the monitoring of intelligence sources to understand if there are complaints logged in relation to scams and fraud.
    - Sources of complaint records should include reporting to Call Providers, 7726, Action Fraud, Financial Sector and Ofcom as a minimum.

Companies House

The National Crime Agency, UK Finance and anti-corruption agencies have all repeatedly point out systematic vulnerabilities with company's house data. The dataset is a passive library of data with no verification of data submitted. Research and company house own search tools are showing systematic misuse involved in major Money Laundering schemes include BBLs and Russian laundromat. Anti-Money Laundering regulations explicitly prohibit firms from using Company house data as sole reference as it is not verified data.

Section 4: Ensuring continued compliance and reassessing risk after transfer of numbers

- Changes of circumstance should include not only a big change in the level or type of business activity as per the consultation documents, but also change in the ownership structure of a business.
- The same checks that are undertaken during the sub-allocation of numbers should be performed as part of the ongoing due diligence checks, to ensure all previous details are still valid. Ongoing due diligence should have a standard timeframe, this should be revised or informed based on intelligence and the typologies seen within the sector.

1. https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807
2. https://www.ispreview.co.uk/index.php/2022/01/vodafone-uks-new-sms-firewall-dramatically-cuts-scam-texts.html
3. https://www.mobileuk.org/news/guest-blog-were-investing-millions-with-ee-and-bt-to-protect-our-customers-from-scams

Section 5: Responding to incidents of misuse

- There should be obligatory reporting of misuse to the regulator to allow analysis of misuse typologies to determine the common gaps. For example, if it is found to be commonplace that lower tier services have a greater volume of misuse due to disparity in the deployment of due diligence controls, the regulator could make these controls a condition of licence as is the case within the financial sector for Anti Money Laundering.

- There is a need for the intelligence gathering from confirmed instances of misuse, this information should be communicated across the sector to prevent recurrence. The victim compromise point is often not sighted to the banking sector until the customer have become a victim. As part of potential victim care, the financial sector needs to be informed to support efforts to protect consumers from becoming victims.

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.

Intelligence Sharing

The sharing of real time intelligence and new typologies are critical to attacks being replicated across the sector, below are some approaches Ofcom should encourage to limit repeat attacks and reduce the number of potential victims. Below are some suggestions which replicate the approach taken in the financial sector.

1. https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807
2. https://www.ispreview.co.uk/index.php/2022/01/vodafone-uks-new-sms-firewall-dramatically-cuts-scam-texts.html
3. https://www.mobileuk.org/news/guest-blog-were-investing-millions-with-ee-and-bt-to-protect-our-customers-from-scams

- **Formal typology publications**: Whilst blocking abroad welcome, it is unfortunate some use cases will remain, criminals are ingenious and often exploit any gaps in their evolving techniques, we would recommend the guidance document reference expectations that providers keep abreast of new industry typologies. We would suggest Ofcom could publish a summary of new typologies to licensed carriers on a periodic basis; to ensure the guidance and expectations do not become dated as the criminals evolve their tactics.

- **Within industry:** The SMS Firewalls are helping the Mobile Network Operators to block not only SMS but also block phone numbers[2,3], this could be used as a source of intelligence for those that are assigned those numbers or law enforcement lines of enquiry. Operators could be made to collate and share the data for these SIMs and where they were located, to determine if there are any pattern/correlation that could be used by Law Enforcement to disrupt the root cause.

- **Cross sector intelligence**: The financial sector hold routine weekly intelligence sharing calls on behalf of our industry, which often surface the latest techniques the criminals are deploying in their attacks on consumers and those that fall victim. The Financial Services sector shares typologies during bilateral meetings with Ofcom, to inform the Telcom sector of criminal approaches to circumventing controls. This intelligence should be combined with Law enforcement and the insights of the call blocking overlay service; and shared back with the Telcom industry on a weekly basis. Also, any good practices could be shared to enhance the mitigation of service/number misuse. This will allow call providers to have an sight of the ongoing criminal methodology to and adapt processes in a timelier fashion; limiting the need for refreshed guidance as criminals adopt new techniques.

1. https://thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807
2. https://www.ispreview.co.uk/index.php/2022/01/vodafone-uks-new-sms-firewall-dramatically-cuts-scam-texts.html
3. https://www.mobileuk.org/news/guest-blog-were-investing-millions-with-ee-and-bt-to-protect-our-customers-from-scams