Consultation response - Promoting trust in telephone numbers

Date: 06 06 2019

Address:
Adrian Ball
Ofcom
Riverside House
2A Southwark Bridge Road
London SE1 9HA

Sent to: [consult.numbermanagement@ofcom.org.uk]

Introduction

1. UK Finance is the collective voice for the banking and finance industry. Representing more than 250 firms across the industry, we seek to enhance competitiveness, support customers and facilitate innovation. This includes ensuring that the UK is the safest and most transparent financial centre in the world, working with members, law enforcement, government agencies and industry to create a hostile environment for criminals.

2. Ofcom's consultation on promoting trust in telephone numbers 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.

Response

3. 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 proposed introduction of a common numbering database ahead of the implementation of the STIR standard in the UK. This is critical to the preservation of trust in telephone numbers. Without it, consumers will remain at heightened risk of harm through fraud. As 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]

4. Indeed, the UK is seeing unprecedented levels of fraud, which the Office for National Statistics cited as fraud is now the most commonly experience offence.[2] Scam calls (criminals purporting to be banks, the police, utility companies and the like) are a significant enabler of fraud and

[1] https://www.thepaypers.com/expert-opinion/the-changing-nature-of-fraud-in-telecommunications-industry/773807.
[2] https://www.ons.gov.uk/peoplepopulationandcommunity/crimeandjustice/bulletins/crimeinenglandandwales/yearendingsept2016

have become a widespread problem. They are commonly used in impersonation scams, of which there were 10,924 cases amounting to £92.7 million in losses in 2018.[3] And this is just a subset of the fraud types and losses associated with nuisance calls as social engineering/duping customers over the phone is a prolific attack vector where spoofing is an unmeasured enabler; more information on this can be found in our report *Fraud the Facts 2019*.[4]

5. We acknowledge that there will be a delay in the effectiveness of STIR due to telecommunication industry decisions regarding PSTN switch-off being undertaken by different companies, at different times and in different locations depending on their plans. As such, the common numbering database will deliver industry benefits and help scam prevention years earlier and should be delivered as soon as viable. Without factoring in new initiatives such as Confirmation of Payee or any other mitigating activities, and based on a linear projection of current trends, the forecast growth of scams losses between 2019 and the proposed introduction of the common numbering database in 2022 could total c.£500m, arising from around 60,000 cases. By the time STIR has been implemented in 2025, the same forecast could increase to c. £1bn from around 120,000 cases should fraudsters adapt their MOs to overcome new barriers. Therefore trust and confidence in using voice services will be diminished if this issue continues to escalate unchecked.

6. The issue is compounded by the lack of general public awareness around number spoofing. Many victims wrongly assume the legitimacy of a phone number displayed, and all businesses and government bodies are at risk of having their numbers spoofed. The inability of consumers to verify who is calling them and the lack of mechanism for companies to protect the use of their numbers has forced telecoms providers, banks, government, law enforcement and Ofcom into the unenviable position of instructing customers not to trust the number they have been called from.

7. Currently the mechanisms available to trace ownership of numbers is severely limited, and this is preventing potential disruption efforts. The common numbering database will support enforcement activity by telecoms providers themselves as well as assist law enforcement with their lines of enquiry.

8. While the common numbering database will allow telecoms providers to progressively implement technical measures to verify that CLIs are valid and authentic and subsequently enable the provision of suitable indicators of 'trustworthiness' to anyone receiving a call, we believe that a wider set of measures and initiatives will further contribute to reducing the incidence of nuisance calls, including those from non-UK phone numbers. These include:

    - stronger and mandatory intelligence sharing between telecoms providers;

    - network-led best-practice guidance. Sharing scam/fraud typologies needs to become a requirement to support the sector and help stakeholders deal with new and growing threats to the telecoms industry;

    - a single set of definitions for mandatory reporting, etc. to ensure consistency of data and enable typology analysis to be undertaken;

[3] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019.
[4] https://www.ukfinance.org.uk/policy-and-guidance/reports-publications/fraud-facts-2019.

- a central body aggregating and promulgating typology data from other sectors (inc. banking and finance) in order protect consumers;

- Further public awareness initiatives to encourage reporting into 7726.

- Ofcom members to also explore trusted routes for telecoms providers to share vulnerability and typology data with financial-services firms' such as the National Economic Crime Centre; and

- the development of industry standards such as a service-level agreement to close down "bad" numbers.

9. If you have any questions relating to this response, please contact [Dianne Doodnath], [Manager, Economic Crime – Remote Payment Channels] at [Dianne.Doodnath@ukfinance.org.uk].