Stop Scams UK's Submission to Ofcom's work on combatting scam calls and number spoofing

About Stop Scams UK

Stop Scams UK is an industry led collaboration made up of responsible businesses from across the banking, technology and telecoms sectors who have come together to help stop scams at source. Stop Scams UK currently has 17 members. These are: Barclays, BT, the Co-operative Bank, Gamma, Google, HSBC, KCOM, Lloyds Banking Group, Meta, Microsoft, Nationwide, NatWest, Santander, Starling, TalkTalk, Three, and TSB.

Stop Scams UK exists to facilitate cross-sector collaboration. We know that for scams to be successful, they will touch on at least two, if not each of the banking, technology and telecoms sectors. We believe that it will only be through enabling, leading and delivering collaboration across these sectors that systemic solutions to scams will be realised. We provide the resource, leadership and trusted space for our members to share problems, identity opportunities, overcome blockers and drive projects forward to the benefit of consumers and business.

In September last year, Stop Scams UK launched 159 an easily memorable short code phone service that connects the customers of many of the UK's retail banks directly, safely and securely with their bank, should they receive an unexpected or suspicious call on a financial matter. Over 80,000 calls have now been made to 159 and the service was recently expanded to accommodate an even larger number of banks, including the Co-operative Bank, the Nationwide Building Society, and TSB.

In addition to 159, Stop Scams UK is a programme of work to enable and pilot improved data sharing between our members. Both policy makers and industry stakeholders have recognised that better data sharing will be critical to helping stop scams. Our data sharing work is one of a number of R&D projects, which include work on Information Gathering Accounts and spam call tracing, that are currently being taken forward by Stop Scams UK and its members.

Stop Scams UK welcomes the opportunity to contribute to Ofcom's work. This response complements those submitted by our members and should be read in conjunction with those responses.

Context

As Ofcom has recognised, scams and fraud are a significant and systemic problem. Not only do they cause real harm and distress to consumers but they undermine trust in businesses and economic activity. Worryingly, scams are growing at an exponential rate.

According to figures published by UK Finance, in the first six months of 2021 reported Authorised Push Payment Fraud – a type of scam where victims are manipulated by criminals, often through social engineering, into making payments to scammers – was 60% above the equivalent level for 2020, with the losses incurred by consumers and businesses 71% higher.[1]

[1] Stats from UK Finance Half Year Fraud Update.

In the first six months of 2021 alone, criminal gangs stole over £355m from individuals and small businesses by pretending to be a bank or other service provider and encouraging them to make a payment or transfer money.[2] Although these numbers are alarming, they do not tell the complete story: we know that the distress caused to scam victims can be enormous.

Scammers are making use of increasingly sophisticated means to try and defraud people, combining websites, text messages and phone calls, as also complex and nefarious 'social engineering' scripts. The only way to effectively tackle this harm is for businesses across each of these sectors to work together on the development of technical solutions to scams and for that action to be backed by appropriate and proportionate regulation.

Ofcom's proposed measures

Stop Scams UK supports each of the three programmes of work that Ofcom has proposed to take forward in relation to scams and number spoofing. Detailed responses are attached to this submission in relation to: 1) Calling Line Identification and 2) changes to its good practice guide to help prevent the misuse of sub-allocated and assigned numbers.

Our members and particularly our banking members have raised concerns about the use of spoof numbers to perpetrate fraud and scams. Ofcom's measures are therefore to be welcomed, particularly the modification of General Condition (GC) C6) to require providers, where technically feasible, to identify and block calls with CLI data which is invalid, non-dialable, or which does not uniquely identify the caller.

We also welcome the changes Ofcom is proposing to make to its guidance for providers on what Ofcom expects them to do to comply with the rules in GC C6. 2 including:

- Clarifying that the format of a CLI should be a 10- or 11-digit number;
- Making use of information that identifies numbers which should not be used as CLI, such as Ofcom's numbering allocation information and the Do Not Originate (DNO) list;
- Identifying calls originating abroad that do not have valid CLI and blocking them; and
- Identifying and blocking calls from abroad spoofing UK CLI.

We believe that the measures proposed will help mean that calls with the most obviously spoofed CLI data will not reach the intended recipient. This should help reduce the number of scam calls and the incidence of people who are scammed. We also welcome Ofcom's proposed changes to its good practice guide to help prevent the misuse of sub-allocated and assigned numbers, and its publication of the Do Not originate list which will also help strengthen the efficacy of its modification of the General Conditions.

We note that while these measures are welcome and necessary, they will not in themselves end the use of spoofed numbers. It is an unfortunate fact that scammers have proved ingenuous and will always find new means of contacting people and business. Stopping the use of spoofed numbers will require ongoing innovation. Stop Scams UK looks forward to engaging further with Ofcom on this important work.

[2] Stats from UK Finance Half Year Fraud Update.