Telecommunications Fraud Sector Charter

Opening statement

Telecommunications providers recognise the significant risk of fraud and scams against UK customers and providers. This is giving rise to substantial consumer harm and is affecting businesses. Faced by an increasing threat of industrial-scale fraud, telecommunications providers and Government will work in a coordinated manner with other industries and stakeholders to reduce its impact.

Actions under this Sector Charter, including solutions implemented by telecommunications providers to reduce fraud and scams, will accord with providers' legal and regulatory obligations, including in relation to data protection.

Specific fraud risks in the telecommunications sector

Fraud risks directly affecting telecommunications customers

Scam Calls

Criminals call to obtain personal information, socially engineer and/or defraud the victim. Scam calls are made more realistic by number "spoofing", which makes the call appear to be from a trusted number.

Smishing

Criminals use SMS/text messages to obtain personal information, socially engineer and/or defraud the victim.

Fraud risks resulting in wider customer financial fraud

Identity Theft/ Subscription Fraud

Criminals use personal data, which may be illegally obtained, to apply for mobile devices and other credit services in the victim's name. Customers suffer identity theft and telecommunications providers subscription fraud.

SIM Swap/ Network Divert Fraud

Criminals take over a customer's account by applying for a new SIM or network divert in their name. Criminals use personal data, which may be illegally obtained, and other credentials to pass security checks to access the victim's accounts.

Mobile Number Porting Fraud

Similar to SIM Swap, a criminal transfers a victim's number to another network to intercept communications intended for the victim to access the victim's accounts.

Actions to tackle fraud risks directly affecting telecommunications customers.

Action (1) – Work to identify and prevent scam calls		
Objective: Reduce the impact of scam calls on customers.	**Action:** Telecommunications providers will work to identify and implement techniques to block scam calls. This action will be supported by Ofcom through the Strategic Industry Working Group. Data on sources of scam calls will be shared within the industry. Data sharing to combat fraud and scams, will be supported by specific case studies which will be provided to the Information Commissioner's Office (ICO) for potential inclusion in its data sharing hub. Providers will extend data sharing to law enforcement and banking.	**Outcome:** Enhance call blocking solutions to protect customers and reduce fraud. **Agree approach 3-6 months. Implement 1-2 years.**

Actions to tackle fraud risks directly affecting telecommunications customers continued.

Action (2) – A co-ordinated approach to tackle smishing		
Objective: A coordinated attack on smishing from telecommunications, law enforcement, NCSC and banking.	**Action:**Telecommunications providers will work to identify and implement additional techniques to block smishing. This action will be supported by Ofcom and Mobile UK through the Mobile Scams Group. A co-ordinated effort to review the use of the 7726 spam reporting service will be initiated, involving telecommunications providers, law enforcement and banking to explore how the 7726 database can be used more effectively against smishing. Providers will consider messaging provided to customers using 7726 to encourage adoption. Providers will share reported URLs and phone numbers suspected to be linked with smishing with the National Cyber Security Centre (NCSC) and National Fraud Intelligence Bureau (NFIB). Providers will seek to restrict access to URLs confirmed by the NCSC as used for smishing in accordance with legal and regulatory obligations.	**Outcome:** Improve knowledge, and reduce volume and impact, of smishing. **Agree approach 3-6 months. Implement 1-2 years.**

Actions to tackle fraud risks resulting in wider customer financial fraud.

Action (3) – Use of Dynamic Direct Debit to tackle identity theft affecting customers and subscription fraud affecting providers		
Objective: Introduce a banking authorisation step into the Direct Debit initiation for new telecommunications contracts.	**Action:** The telecommunications industry will be supported by the banking industry in developing a pilot Dynamic Direct Debit system to facilitate three-way authentication and authorisation at the point of sale between a customer, their bank and the telecommunications provider. The pilot will consider usage by different customer demographics. The telecommunications industry will consider Open Banking to achieve this.	**Outcome:** Reduce risk of identity theft/subscription fraud. **Pilot approach 3-6 months. Implement 1-2 years.**

Action (4) – Use of real-time checking to tackle SIM swap and Mobile Number Porting fraud		
Objective: Enable fraud to be reduced by a co-ordinated telecommunications /banking industry effort.	**Action:** The telecommunications industry will continue to support the banking industry by supplying a consistent real time check of whether or not a mobile phone has recently been subject to a SIM-swap or MNP using GSMA's Mobile Connect Account Takeover Protection standard supported by all providers. Telecommunications providers will work with UK Finance to ensure the banking sector is fully aware of the SIM-Swap/MNP data available and to explore other information/services which providers may be able to supply to further reduce this fraud.	**Outcome:** Reduce risk of SIM-swap and MNP fraud. **Implement 3 months – 1 year.**

Action (5) – Sector information sharing		
Objective: Improve industry cohesion in detecting and responding to fraud.	**Action:** Telecommunications providers will share information within the industry to detect and reduce fraud against customers and providers. This action will be supported by a specific case study which will be provided to the ICO for potential inclusion in its data sharing hub. Providers will extend data sharing to law enforcement and banking.	**Outcome:** Rapid & regular sharing of information on sources and nature of fraud attacks. **Agree approach 6 months. Implement 6-18 months.**

Action (6) – Systematic sector analysis of shared fraud information and other intelligence		
Objective: Analysis of information to identify participants in significant/ repeated fraud against customers and providers.	**Action:** Telecommunications providers will analyse shared information (and information from other sources) to identify sources and participants in significant/repeated fraud against customers and providers to an agreed threshold. This action will be supported by a specific case study which will be provided to the ICO for potential inclusion in its data sharing hub. Information will be developed into actionable evidence to be shared with law enforcement.	**Outcome:** Identification of participants in significant/ repeated fraud against customers and providers made available to law enforcement. **Agree approach 3 months. Implement 3 months – 1 year.**

Actions to tackle fraud risks resulting in wider customer financial fraud continued.

Action (7) – Engagement by law enforcement to investigate significant / repeated fraud against customers and providers		
Objective: Create a more effective reporting route for significant / repeated telecommunications fraud.	**Action:**Telecommunications fraud reports will be submitted to Action Fraud by industry for recording on the national crime database. City of London Police (CoLP), National Economic Crime Centre (NECC), and NCSC will each appoint a telecommunications fraud point of contact for the providers to discuss significant/repeated telecommunication fraud. Providers will join the NECC Threat Group, through which they will share information where significant/repeated fraud has been identified that is impacting customers or companies. Where information is presented at the NECC Threat Group, the NECC will consider the optimum approach which may include creation of a pop-up fusion cell to tackle the issue, subject to internal prioritisation.	**Outcome:**Enhance collaboration to enable a more agile approach to tackling fraud. Enable action in cases of significant/ repeated fraud. **Agree approach 3 months. Implement 3 months – 1 year**

Action to support victims of telecommunications fraud.

Action (8) – Improve support given to victims of telecommunications fraud		
Objective: Improve fraud victim experience.	**Action:** Telecommunications providers will work with groups providing support to fraud victims to understand current concerns with telecommunications fraud victim handling and to identify best practice that could be adopted by industry. Telecommunications providers will work with these groups to respond to reports of poor victim handling. These groups will support providers with consistent signposting to victims on the support available should they require it.	**Outcome:**Improve treatment of fraud victims by industry. Improve current processes for support of victims. Increase customer awareness of courses of action following fraud. **Initial meeting with victim support groups within 3 months.** **Agree approach 6 months.** **Implement 6-18 months.**

Action to increase awareness of telecommunications fraud.

Action (9) – Increase fraud awareness		
Objective: Implement fraud awareness measures to reduce customer vulnerability.	**Action:** Telecommunications providers will support law enforcement and government by delivering communications sector fraud awareness messages. Providers will participate in a public and private sector strategic communication steering group, which will review the effectiveness of existing awareness measures and consider using more consistent cross-sector messaging to the public	**Outcome:** Increased fraud awareness; changed customer behaviour and reduced fraud risk. **Agree approach 6 months. Implement 6-18 months.**

Telecommunications providers will report to HMG and other stakeholders on their activities in support of this charter after 6 months, 1 year and 2 years.

Signatories

This voluntary charter is supported by:

- BT
- EE
- Sky
- TalkTalk
- Three
- Tesco Mobile
- Virgin Media & O2
- Vodafone