Protecting contact centres with fraud prevention.

The UK financial industry lost £768 million in 2016 to fraud according to the Financial Fraud Association UK. While cyber security is constantly improving, contact centres are increasingly seen as the weak link in the fight against fraud, so telephone fraud is a growing challenge. The ability for your contact centre agents to identify suspicious callers before speaking with them reduces the risk of phone fraud and reduces average hold time. This improves customer experience and improves contact centre productivity by serving customers quicker.

Accurate fraud risk of callers

The smartnumbers fraud prevention service is able to accurately measure the fraud risk of callers by analysing information in the call signalling that is only available for network operators. This is possible as smartnumbers is directly integrated with the core telephone network at SS7 level (the international standard providing carrier connectivity across the globe), and examines attributes of the call that identifies fraudulent callers, such as:

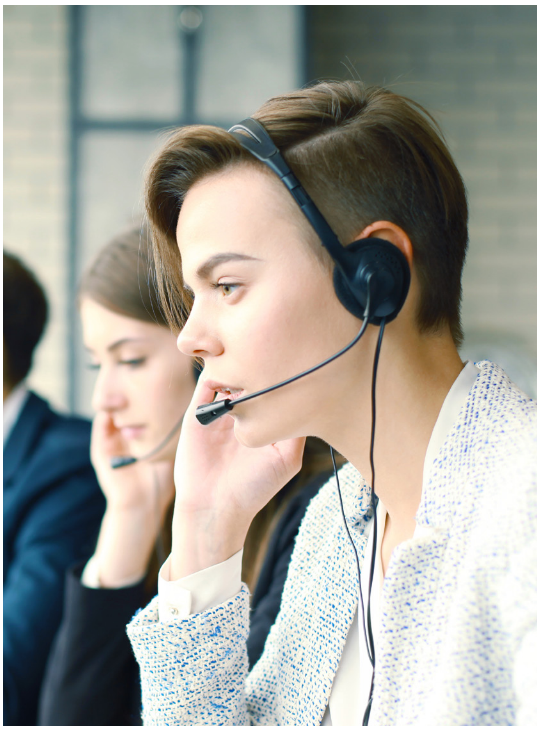
- If the caller has spoofed or masked their identity.
- The caller's ID if they are attempting to hide their CLI (Calling line identity).
- If the call has been diverted across multiple networks.
- Suspicious behaviour, such as repeated attempts while withholding the CLI.
- If they are calling from a high-risk operator or network.

Improving customer experience

The smartnumbers service analyses every incoming call while it is in the network. This means that suspicious calls are detected before the call is answered and actioned appropriately while genuine callers are served quicker to reduce average hold times.

Simple implementation

The smartnumbers service is network agnostic and is cloud-based so works with your existing telecoms infrastructure and telecoms provider.



Key benefits

- **Reduce direct/indirect financial loss:** Protect your brand reputation and avoid account takeovers by accurately identifying suspicious callers.
- **Improve customer experience:** Reduce customer frustration by eliminating 'false positive' flags, connecting them more quickly with agents.
- **Improve call centre productivity:** Reduce the time taken to authenticate genuine callers, reducing average hold times and agent call duration.

Features in-depth

Multi-factor analysis

- Restricted call signalling data that is only available to telecom operators such as withheld CLIs.
- Incorrect or missing signalling information that can be indicative that calls have travelled through a 'grey route'.
- Suspicious call routing, such as a call that has been diverted through multiple networks.
- The type of phone service the caller is using. For example, fraudsters use VoIP phone services to appear to be in a different country.
- If the caller has spoofed their identity via a rogue operator or VoIP service.
- The caller's verified CLI, where unverified CLIs are indicative of fraudulent callers.

Features on the roadmap

Machine learning to refine the fraud score by using additional data sources, including:

- Identifying mobile caller's location when roaming abroad.
- Integrates with publicly shared databases to identify known individual offenders and operators e.g. Telecommunications UK Fraud Forum (TUFF) and the Cifas databases and telecom numbering databases
- Call behaviour and pattern analysis to detect anomalies. Learning is shared across all customers.
- Enable supervised machine learning by integrating with phone systems so call centre agents can send feedback about fraudulent calls.
- Management information and caller patterns for analysis by the bank's fraud and security experts.