Tackling fraud in the contact centre.

Telcos

Telco fraud is lucrative - with customer accounts enabling access to payment details and bank accounts, as well as the means to make high cost calls and purchases.

To prevent it, organisations typically secure their digital channels, but in our experience contact centres, with their human element, remain vulnerable.

So, we proved the business case for tackling fraud at a UK telco contact centre...

Just how bad is it?

Telecommunications fraud saw a shocking rise in the UK in 2024, with Cifas reporting 108% increase in account takeover filings to the national fraud database (NFD) and a 91% increase in identity fraud in the first six months of the year.

Telcos tackling this face an unprecedented challenge to secure their customers without compromising efficiency.

Telco: what we know

Recent work with one of the UK's largest telcos enabled Smartnumbers to explore the scale of fraud in their contact centre in more detail. We're pleased to share the insight from this project.

The project involved using the Smartnumbers platform to analyse and flag inbound call details for the following four fraud risk factors:

01

Denylist numbers

02

Withheld numbers

03

Unusual call patterns

e.g. repeated calls in quick succession

04

Outside intel

Numbers and profiles flagged by other organisations using the platform e.g. large retail banks, insurance companies and telcos.

In one month

We reviewed calls flagged with one or more of the fraud indicators over one month:

100+
new fraudster profiles

We also see these individuals or organised crime groups targeting banking clients, using the same phone numbers and tactics.

58%
fraud calls from withheld numbers

This confirms the high risk nature of these calls and the value of flagging them.

x8
average number of calls per ATO

Before taking over a customer account an average eight calls is made to gather more data and make account changes.

Eight opportunities to stop them before a transaction takes place.

7.5 mins
length of average fraud call

During this time a fraudster may be attempting to gather further customer details or make account changes, such as adding an address.

Top five fraudsters

During the test period:

x219
fraud-related calls made

x78
targeted attacks on customer accounts

What fraudsters want

They called to attempt the following:

Acquire and validate stolen customer details

Get more access to other accounts

Change email and address details

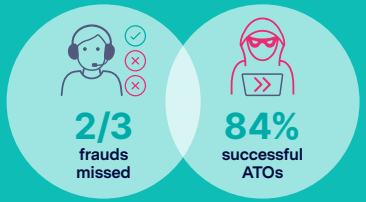
Initiate SIM swaps

smartnumbers.com

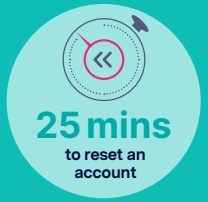
Deep dive findings

Wider analysis of the calls received outside the test period for the 78 accounts being targeted led to the discovery of four additional fraudster profiles and 17 new fraud related numbers.

Based on this study, the telco believes an estimated two thirds of fraudulent activity in their contact centres is currently being missed, especially the early-stage data gathering calls. And it is due to the success of these initial calls that the team had been seeing an estimated 84% success rate in account takeover attempts.



In addition to the inevitable monetary value of these fraud losses, the team also noted the operational cost of resolution, which included an average call time of 25 minutes spent resetting a customer's compromised account.



Find out more

Sign up today

Get exclusive access to a wealth of more great fraudster intelligence by signing up for our newsletter.

Get The Solution

Download

Find out more about the ingenious technology and processes we use to tackle fraud for the telco sector.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers