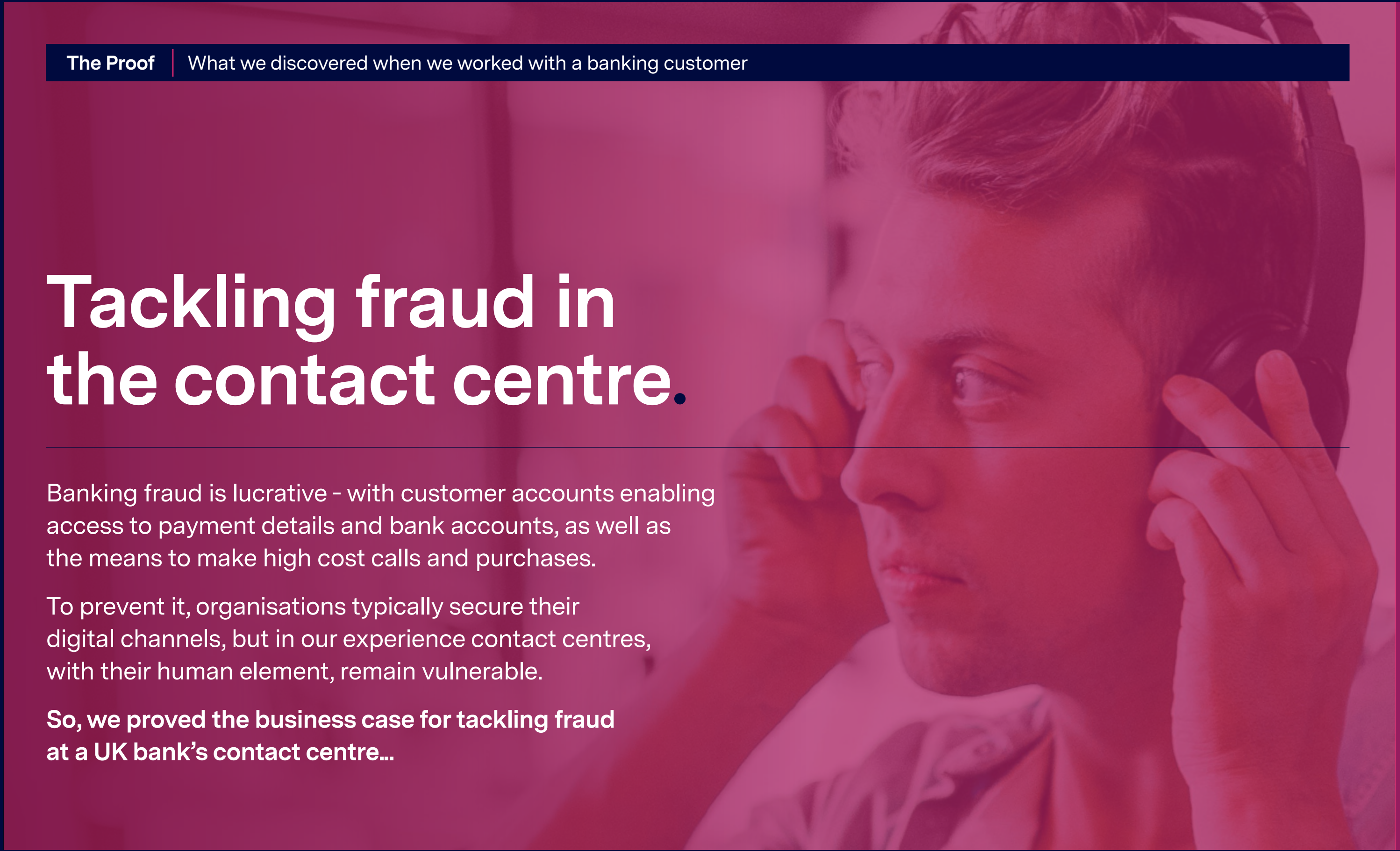


Tackling fraud in the contact centre.

Banking 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 bank's contact centre...

Banking

The challenge

This leading retail bank is at the forefront of the fight against financial crime, motivated to prevent fraud losses and protect its customers. It knew fraudulent activities were taking place across all customer channels, and the bank was sure the contact centre was playing a key role. It just needed proof.

The bank believed fraudsters were exploiting vulnerabilities in the telephony channel to conduct fraud-related activities at various stages of the fraud lifecycle, including harvesting personal data, monitoring account transactions, and making account changes.

In order to explore this further, the bank established a project team with the following remit:

01

Oversee all calls

To monitor its 45,000+ daily contact centre calls for fraudulent behaviour.

02

Discover the real scale

To understand the true extent of fraud in the contact centre and the full range of fraudster methods.

03

Spot fraud earlier

To discover ways to identify and prevent fraud earlier in the fraud cycle, which typically spans 90 days.

The solution

To help achieve these goals, the bank implemented Smartnumbers' AI-based fraud prevention platform for contact centres: Smartnumbers Protect.

The solution checks each incoming call for suspicious numbers or behaviour and assigns a risk score. The risk score enables contact centres to decide how they want to handle the call.

The platform focuses on the three areas shown on the right to identify potential fraudsters.

When fraud is flagged, fraud investigators can build fraudster profiles - including phone numbers and tactics used - within the platform and securely exchange intelligence with the wider business, other financial institutions and crime prevention bodies.

01

Call signalling data

Data from the phone network enables calls from withheld and denylist numbers to be flagged.

Withheld numbers are a big concern for contact centres, as fraudsters often hide their numbers to avoid detection.

02

Caller behaviour

Unusual call patterns, such as multiple calls in a short period of time, can indicate fraudulent activity.

Using AI and machine learning, the system can recognise and flag unusual caller patterns and call histories.

03

Consortium data

Fraudsters repeatedly attack multiple organisations and multiple sectors, so we maintain a list of known fraudsters discovered by our customer base.

We check and update this data in real time.

The outcomes

Securing contact centres to prevent downstream fraud

The bank's hypothesis was that, in most cases, the fraudster touches the contact centre at some point, even if the final transaction takes place elsewhere. So, they decided to close this area of vulnerability and help prevent fraud downstream.

Deploying Smartnumbers enabled the bank's customer ops and fraud teams to work together to log, share and receive fraud intelligence about known fraudsters from other financial institutions and organisations from other sectors within the platform.

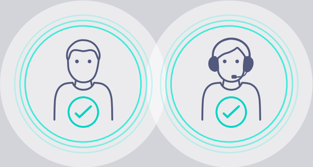
The ability to collaborate between organisations provided the bank with access to a broader dataset of confirmed fraudsters, further enhancing the bank's ability to detect and prevent fraud.

Fraud prevention success

Over a period of 17 months, the use of Smartnumbers' technology made it much more difficult for fraudsters to target the IVR or manipulate call agents.

In numbers, this equates to:

- Over 12,000 suspicious calls flagged
- A 30% reduction in unauthorised fraud via telephone banking.
- Hundreds of thousands of pounds saved per month in fraud losses and enhanced overall financial stability.



Improved customer and employee experience

The initiative has also positively impacted customer experience by reducing the manual effort required to evaluate callers and identify fraudulent activities.

There has also been a marked improvement in the team's employee experience. Contact centre teams are more confident in dealing with their customers and fraud teams have access to more reliable information.

The insights

At the contact centre

After further analysis of the suspicious calls captured by the platform, the bank discovered the following types of fraudulent behaviour in the contact centre:

- ! High call volumes from different mobile numbers belonging to the same bad actor
- ! Fraudsters repeatedly targeting multiple organisations using compromised data harvested via text messages and emails from fake government institutions
- ! Reconnaissance calls carried out by known fraudsters to check if fraudulent banking applications were accepted.
- ! Reconnaissance calls for information about banking transactions to enable fraudsters to carry out targeted attacks
- ! Existence of fraudster ‘clusters’ following similar patterns

Beyond the bank

In addition, using the platform’s fraudster profile and intelligence sharing features, the bank was able to:

- ✓ Identify and confirm over 100 fraudsters that are operating across multiple banks.
- ✓ Access additional insight about known fraudsters provided by other banks using the platform
- ✓ Spot fraud in real time using data on denylisted numbers from other Smartnumbers customers
- ✓ Collaborate on complex investigations for presentation of cases to law enforcement - within the platform and in person

Fraudster behaviour

The bank has been able to gain deep insight into the methods of prolific fraudsters. The fraud team has been able to identify information that it has never had access to before, such as:

- How many different phone numbers a fraudster uses.
- Techniques such as whether they use different voices or accents to disguise themselves.
- Whether a fraudster operates alone or in a group.
- Fraudster patterns across other banks and organisations, identifying which customers, how often and the methods

smartnumbers.com

Industry collaboration

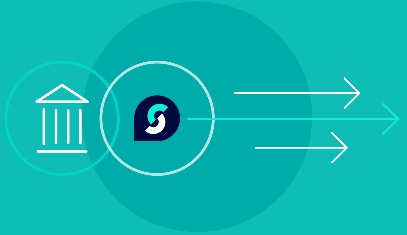
The key to combating fraud overall is collaboration and this is a key part of this success story. The ability to share intelligence through the platform enabled the bank to:

- Exchange information with other organisations in a quick, easy, secure way.
- Confirm suspected fraudsters based on insight from other banks.
- Provide law enforcement with valuable evidence to help fight organised crime.

What’s next?

The initiative is ongoing and continues to enable the bank to protect customers and their accounts. The bank is able to understand how fraud is evolving, and align strategy and technology across the organisation.

They can now also leverage fraud intelligence from the contact centre to help prevent fraud in other channels.



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 banking sector.

☎ **Telephone: +44 20 3379 9000**

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers