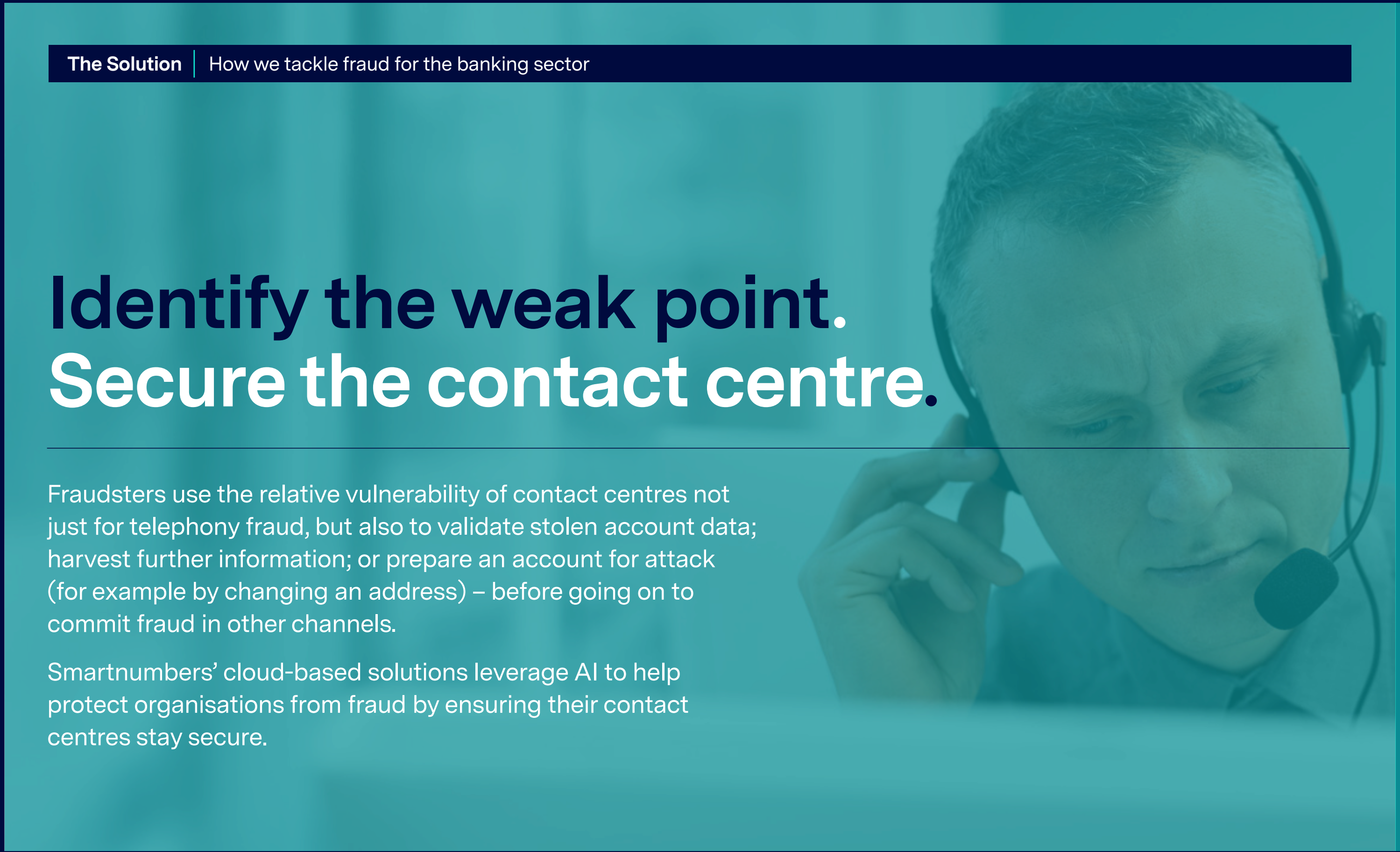


Identify the weak point. Secure the contact centre.

Banking

Fraudsters use the relative vulnerability of contact centres not just for telephony fraud, but also to validate stolen account data; harvest further information; or prepare an account for attack (for example by changing an address) – before going on to commit fraud in other channels.

Smartnumbers’ cloud-based solutions leverage AI to help protect organisations from fraud by ensuring their contact centres stay secure.

smartnumbers.com

Just how bad is it?

Fraud represents 40% of all crime in England and Wales, presenting significant risks to businesses and consumers.

UK Finance's 2024 fraud report found that a staggering £1.17 billion was stolen from consumers in 2023 through both authorised and unauthorised payments.

The scale of the issue is well known.

Typical types of banking fraud

By exploiting weaknesses in IVR systems or manipulating contact centre agents to divulge information, fraudsters carry out a number of different activities in the contact centre depending on the stage of their attack, including the examples on the right.

These activities are not isolated incidents - these attacks are typically carried out by organised crime groups. Teams of professional fraudsters continuously and systematically target multiple accounts, across multiple organisations and sectors, over and again.

Doing the reconnaissance

Validating and enriching the stolen information they have, for use in consumer scams or to carry out transactions at a later stage

Setting up the fraud

Making amendments to accounts for future fraudulent activity, adding an email or changing an address for example

Taking cash out

Creating fraudulent loan applications in order to gain access to funds.

Laundering money

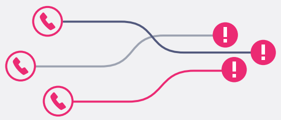
Checking when stolen funds have cleared before transferring them elsewhere.

Find out more about these types of fraud.
Download our Fraud Lifecycle guide.

Spotting a fraudster

Signs of this kind of banking fraud can be tricky to spot using standard contact centre checks, especially if the ‘customer’ appears to have all the correct information. But there are certain caller traits that can help identify them:

Calls from the same number are calling about multiple customer accounts



Multiple frequent calls from the same number to the contact centre IVR

Calls from withheld phone numbers in an attempt to avoid detection

Numbers used may have been denylisted by contact centres from other sectors, such as banks or insurance companies

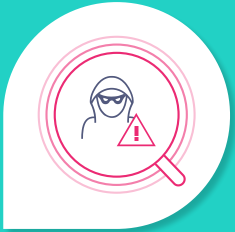
Our successful deployments with several leading UK retail banks prove that with the right technology in place, it is possible to flag these calls in the contact centre and stop fraud in its tracks.

How Smartnumbers can help

The Smartnumbers Protect platform offers banks an additional layer of protection to help spot suspicious calls into the contact centre.

Smartnumbers' unique cloud-based technology 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.

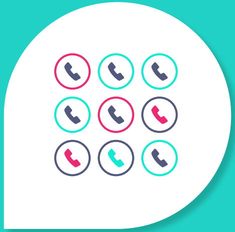
We focus on the following areas to identify potential fraudsters:



Call signalling

Data from the phone network helps us flag calls from withheld and denylist numbers.

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



Caller behaviour

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

We can recognise and flag unusual caller patterns and call histories using machine learning

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.

Smartnumbers benefits:

Stop banking fraud in its tracks

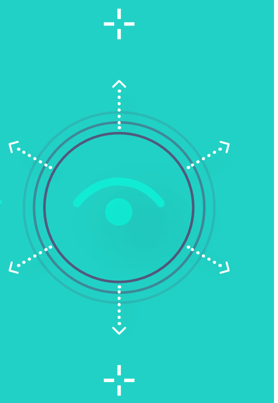
Spot fraudsters targeting your contact centre and stop them before they gain access to your customers' accounts.

Gain a complete picture of fraud in your organisation.

Maximise contact centre efficiency

Spot fraud in real time and prioritise high risk cases.

Reduce fraud losses and deliver a better, faster caller experience for legitimate customers.



Fraud intelligence sharing

Gain greater insight into organised crime activity.

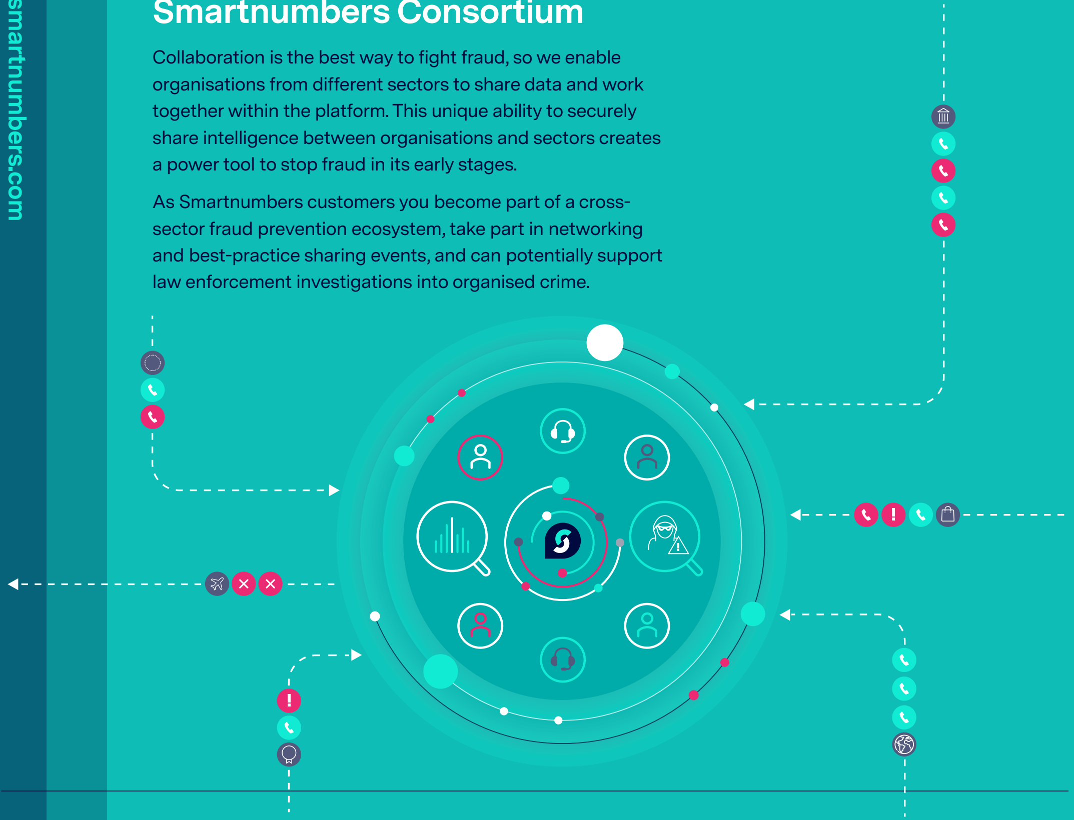
Create and share fraudster profiles with other organisations, including phone numbers and tactics.

smartnumbers.com

Smartnumbers Consortium

Collaboration is the best way to fight fraud, so we enable organisations from different sectors to share data and work together within the platform. This unique ability to securely share intelligence between organisations and sectors creates a power tool to stop fraud in its early stages.

As Smartnumbers customers you become part of a cross-sector fraud prevention ecosystem, take part in networking and best-practice sharing events, and can potentially support law enforcement investigations into organised crime.



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 Proof

Download

Find out how we proved the business case for tackling fraud at a UK bank's contact centre in this download.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers