Tracking fraudsters. Securing calls.

The travel and hospitality sector is an attractive target for fraudsters, due to the typically remote sales environment and the high value, cross border nature of transactions, which often involve multiple providers.

In addition, customer accounts with travel companies provide a source of personal and financial data, and access to valuable loyalty points.

Travel and Hospitality

Just how bad is it?

As 80% of travel merchants surveyed in Ravelin's Global Fraud Trends 2024 predict an increase in the cost of fraud in the coming year, fighting fraud and abuse is clearly a top priority for the sector. Those who find ways to combat it could collectively prevent £billions in losses, relieve the administrative burden of dealing with fraud and secure their reputations.

Typical types of travel and hospitality fraud

Booking fraud

Fraudsters make flight or hotel bookings through the contact centre using stolen credit cards. This results in fraud losses through chargebacks when the real cardholder notices.

Loyalty fraud

Fraudsters target loyalty schemes because points have real-world monetary value as they can be redeemed for flights, hotel stays, upgrades, and gifts. They often bypass the security checks associated with traditional payments.

Fake travel agencies

Fraudsters pose as travel agents, selling overpriced or unusable tickets or hotel bookings to unsuspecting consumers, causing distress to the victim and putting the genuine travel company's reputation at risk.

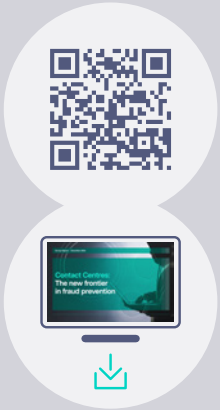
We've done our research

As digital channels become more secure, contact centres are a critical entry point for fraudsters, with data-gathering forming the early stages of fraud attacks across the business.

Our recent research validates this, with high numbers of travel industry respondents reporting fraudulent activity in contact centres both in the interactive voice response (IVR) system (66%) and with call agents (55%).

Survey respondents say fraudsters are targeting both:

Agents IVR



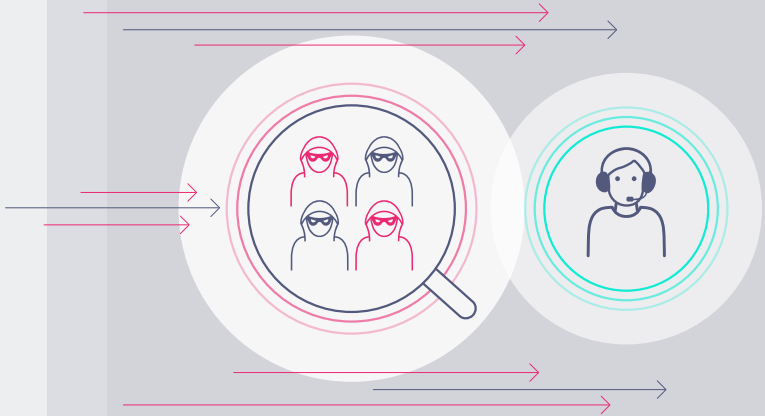
Download the survey report

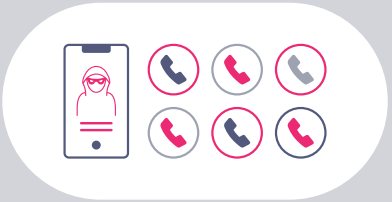
Spotting a fraudster

Contact centres are vulnerable because they are typically still reliant on knowledge-based security checks, which fraudsters can easily pass using stolen data.

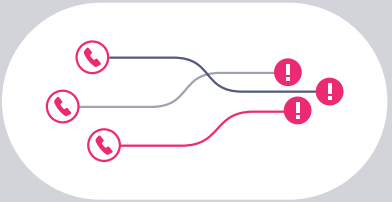
Once inside, fraudsters operate undetected, systematically targeting the IVR to steal more customer data or using their social engineering skills to manipulate contact centre agents into making account changes or initiating transactions.

But there are certain traits associated with these types of fraudulent calls that make it possible to spot them, when you know what you are looking for:

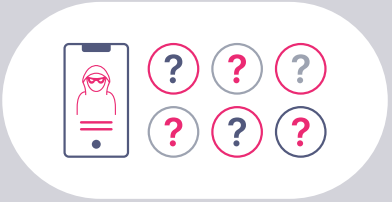




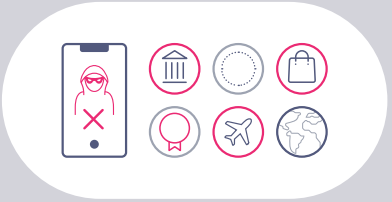
Calls from the same number are calling about multiple customer accounts



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



Callers attempting to avoid detection by withholding phone number



The number used is on your denylist or has been flagged as fraud-related by another company

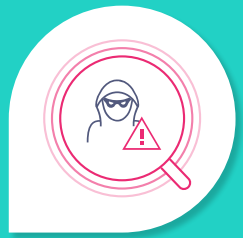
Our successful deployments with organisations across a range of sectors have revealed that with the right technology in place, it is possible to spot and flag suspicious callers in the contact centre and gain insight that can disrupt fraudulent activity.

How Smartnumbers can help

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

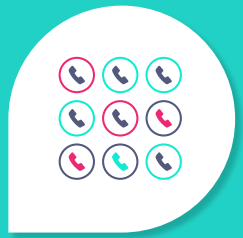
Smartnumbers' unique cloud-based technology checks each incoming call for suspicious numbers or behaviour and assigns a risk score. The risk score enables contact centres to decide how they want to handle the call and investigate further.

We focus on the following to identify potential fraudsters:



Call signalling

Data from the phone network helps us flag calls from denylist numbers, even if the caller has withheld their number to avoid detection – something fraudsters typically do.



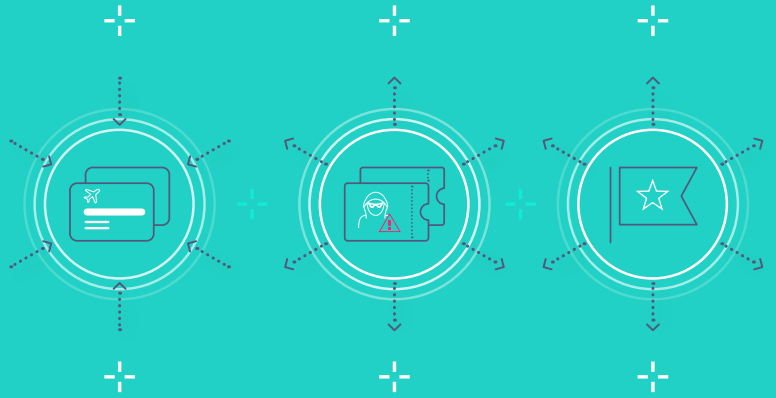
Caller behaviour

Unusual behaviour, such as multiple calls in a short period of time in the IVR, 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 check in real-time for calls from denylist numbers that have been flagged by our entire customer base.

Stop travel sector fraud in its tracks:



Prevent loyalty point theft

Detect fraudulent attempts to access customer accounts to transfer, or redeem loyalty points.

Flag suspicious bookings

Block unauthorised bookings or booking changes, and reduce losses and chargebacks through early intervention

Enhance trust and loyalty

Reduce operational time spent investigating and resolving fraud; protect brand reputation and improve customer experience.

smartnumbers.com

Smartnumbers Consortium

Collaboration is the best way to fight fraud, so we enable organisations from different sectors to share details on known fraudsters and communicate within the platform. This unique ability to securely share intelligence creates a powerful tool that can disrupt fraud in its early stages.

Smartnumbers customers 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.

Telephone: +44 20 3379 9000

Email: info@smartnumbers.com

Online: smartnumbers.com

smartnumbers