



How Experian helped a leading telecoms provider deliver a 26% increase in fraud savings

Case study

The customer opportunity and why it mattered.

A leading telecommunications provider was facing a growing fraud challenge across its digital sales channels, particularly within handset upgrades, new customer applications, and SIM-only journeys.

Fraudsters were successfully bypassing traditional fraud controls, including credit checks and Know Your Customer (KYC) processes, by using genuine identities and stolen personal information.

The impact extended beyond financial losses. Customers who became victims of these scams often suffered account compromise, damaged credit records, financial harm, and significant distress. Fraud levels had become so severe that the organisation was considering restricting its online sales channels and removing certain high-value handsets from sale altogether.

The business needed a way to identify and stop fraudulent activity before orders were fulfilled, rather than detecting it after losses had already occurred.



The Experian offering: how we partnered to deliver better customer outcomes.

In May 2025, the provider implemented the behavioural biometrics and device intelligence solution, delivered through Experian's fraud prevention capabilities.

The solution was deployed across all digital customer journeys, including new business, upgrades, and SIM-only applications.

Unlike traditional fraud controls that rely heavily on identity verification, credit data, and KYC checks, the solution introduced an additional layer of intelligence by analysing:

- **Device characteristics and trust signals**
- **Behavioural biometrics**
- **Location and IP intelligence**
- **Indicators of automation and bot activity**
- **Device compromise and virtualisation signals**
- **User interaction patterns, such as unusual autofill or copy-and-paste behaviour**

This approach enabled the business to identify suspicious activity even when fraudsters were using legitimate identities and passing standard verification checks. The solution also provided fraud teams with no-code rules and controls, allowing them to respond quickly to emerging threats without lengthy development cycles.

“

Richard Harris, Strategic Account Director for Experian, explained:

“Fraudsters are constantly evolving their tactics, which means organisations need controls that can adapt just as quickly. By deploying behavioural biometrics and device intelligence, we helped the client dramatically reduce fraud, improve operational efficiency, and create a safer experience for genuine customers.”



The impact: targeting an industry-wide challenge.

By introducing behavioural and device intelligence before fulfilment, the organisation shifted from a reactive fraud management model to a proactive prevention strategy.

Suspicious transactions could be identified and reviewed before devices were dispatched, significantly reducing fraud losses while maintaining a smooth experience for genuine customers.

The results were immediate and substantial:

- ✓ **53% of the fraud identified before delivery was flagged**
- ✓ **Fraud savings increased by 26%**
- ✓ **Increased operational efficiency through faster fraud response and rule management**
- ✓ **Fraud losses reduced by 19%**
- ✓ **Significant reduction in high-value handset fraud**



The wider impact was equally important. By making the organisation a far less attractive target for organised fraud groups, the solution protected online revenue streams and enabled continued growth through digital channels. As fraudsters were no longer able to operate successfully against this provider, attacks increasingly shifted towards other operators.

“

As the client's Senior Risk Manager noted:

“We are impressed with the new Device & Biometrics product. This strategic partnership is a great fit and it's made a significant dent in fraud volumes in our digital channel.”

What this means for organisations facing similar challenges.

This case demonstrates that modern fraud prevention requires more than traditional identity and credit-based controls. Organisations facing sophisticated fraud attacks can benefit from a layered approach that combines behavioural biometrics, device intelligence, and real-time risk assessment to identify threats earlier in the customer journey.

Key lessons include:

- Prevention is more effective than detection after the event.
- Behavioural and device signals can reveal fraud that traditional checks miss.
- Fraud controls must be adaptable to keep pace with rapidly evolving attack methods.
- Strong fraud prevention can protect revenue while maintaining a positive customer experience.
- Successfully reducing fraud can deter organised criminal groups from targeting the business altogether.

For organisations experiencing fraud that continues to pass conventional verification processes, adding behavioural biometrics and device intelligence can help reduce losses, improve operational agility, and restore confidence in digital channels.



Arrange a consultation

Email



Find out more



Registered office address:

The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk

© Experian 2026.

Experian Ltd is authorised and regulated by the Financial Conduct Authority. Experian Ltd is registered in England and Wales under company registration number 653331.

The word "EXPERIAN" and the graphical device are trade marks of Experian and/or its associated companies and may be registered in the EU, USA and other countries. The graphical device is a registered Community design in the EU.

All rights reserved.