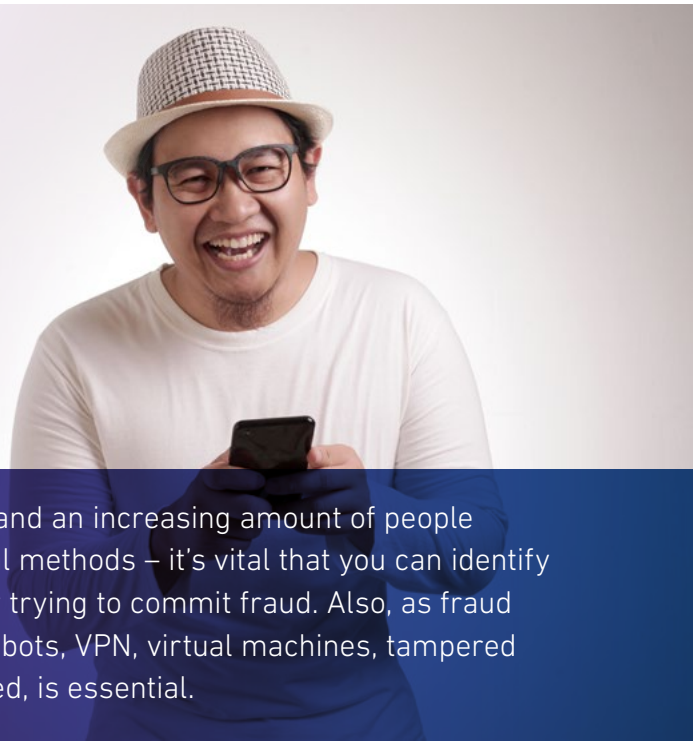
Product sheet

Behavioural Biometrics and Device Intelligence

Analyse every touchpoint to confidently recognise your customers and the devices they use to interact with you.



With internet use, via multiple devices, at its highest level and an increasing amount of people deciding to stick to online transacting than more traditional methods – it's vital that you can identify the difference between an actual customer and somebody trying to commit fraud. Also, as fraud attacks online become more sophisticated with the use of bots, VPN, virtual machines, tampered apps and more, understanding the device, and how it's used, is essential.

Behavioural biometrics and device intelligence can be used throughout the customer journey – from account opening and customer login to payments and ongoing account monitoring – to spot any activity or changes which indicate suspicious activity.

Our new behavioural biometrics and device intelligence solution is available through CrossCore as part of your fraud prevention process. The service continuously monitors hundreds of signals to predict the likelihood of fraud, identity theft or scams in progress. This can support businesses in a number of ways:

- **Onboarding:** Spotting potential ID theft.
- **Identify returning devices:** Both of good customers, but also those previously to be seen involved in fraud.
- **Account management:** Changing customer data, credentials, password resets or transferring funds.

Leveraging bespoke rules-based risking and supervised machine learning models, the service is designed to optimise fraud catch whilst minimising false positives.

This continuous and passive monitoring approach has zero impact on user experience as it does not involve any additional form fills. Moreover, monitoring begins from the first moment a user starts interacting with a website. This is especially effective at identifying fraud attacks that are otherwise difficult to detect, for example, we can see how the user navigates the page; bots are highly efficient and perform actions quickly, good customers are slower and tend to scroll and click around the webpage far more.

Why do devices and customer interactions need monitoring?

Know Your Customer (KYC) and standard fraud tools focus on assessing the individual and their standard personally identifiable information (PII) attributes, if there are fraud consortium matches (Experian Fraud Exchange, CIFAS) and whether there's a change of address.

Device and behavioural biometric data adds additional attributes, providing further insight into the user, the device and their location which has proved crucial in the fight against fraud.

Behavioural Biometrics

- Typing and mouse movement
- Scrolling and swiping
- Hesitation and distraction
- Device orientation
- Context switching
- Copy and paste
- Autofill
- Clipboard

Device Intelligence

- Device fingerprinting
- Geolocation
- RAT detection
- Bot detection
- VPN/Proxy detection – true IP
- True OS detection
- Tampered app detection
- Virtual machine detection
- Device consortia
- Active call detection

How does behavioural biometrics and device intelligence work?

User navigates to client site via browser OR opens an app

Experian starts capturing device and behavioural data

User clicks to action their online activity

CrossCore™

Case action updated and fed back into device and behavioural intelligence strategy and CrossCore™

Investigators access graphic user interface (GUI) to work referrals

API

CrossCore sends data and decision to client

What this means for you

- **Prioritisation:** By focusing on high-risk cases first, you can allocate resources more effectively and address the most significant risks
- **Proactive risk management:** Device and behaviour intelligence enables you to take a proactive approach to risk management by identifying potential security threats before they are exploited by attackers.
- **Compliance:** Can help support demonstrating compliance with regulatory requirements.
- **Improved decision-making:** By understanding the risks associated with each device and customer interaction, you can make more informed decisions about security investments, policies, and resource allocation.
- **Single customer view:** You can get a holistic view across all devices and every session.
- **Efficiency:** You can streamline the risk assessment process by automating the collection and analysis of device and behaviour related data. This reduces the time and effort required to assess risks manually.
- **Reduce false positives:** The precise and non-intrusive solution supports more accurate customer recognition, improving the experience and reducing false positives.
- **Improved customer experience:** Genuine customers can access their accounts quickly and easily whereas fraudsters can be stopped even in cases where they may have login credentials.
- **Protect good customers:** Spot scams and social engineering, protecting good customers who are being manipulated by fraudsters.

To find out more more about how Experian can transform your identity and verification process.

0844 481 9920
businessuk@experian.com
experian.co.uk/business

Registered office address:
The Sir John Peace Building
Experian Way
NG2 Business Park
Nottingham
NG80 1ZZ