TruValidate

IDENTITY PROOFING

Device Risk

Help prevent digital fraud in real time

Stop fraud, not good customers

Distinguish fraudsters from real customers based on device recognition, context and behaviour.

Build trusted connections

Leverage device history with device-to-device and device-to-account associations based on confirmed fraud reports from our global network. Access over 6,000 analysts, over 10 billion known devices and over 100 million known detailed fraud reports.

Focus on your risks

Apply device intelligence to your unique fraud challenges with custom, configurable business rules.

TruValidate Device Risk provides insightful multi-device recognition technology and a unique device intelligence approach to disrupt fraudsters, without compromising the customer experience. Our device intelligence approach is based on an established and diverse real-time global network.

Insightful technology, diverse capabilities

By recognising internet-connected devices without requiring personal identifiable information (PII), TruValidate Device Risk adds an independent layer of digital identity separate from personal data which may have been compromised.

- → **Accurately recognise all device types**
  We analyse thousands of permutations of device attributes to precisely identify a device while minimising false positives.

- → **Uncover and track hidden fraud patterns**
  Advanced analytics, searching and reporting capabilities can help you spot suspicious transactions and device patterns — which can be quickly tracked using our flexible business rules editor.

- → **Reveal device and account links**
  Discover hidden connections between devices and accounts to help uncover fraud rings — even across subscribers and industries.

- → **Evasion detection**
  Stop fraudsters hiding behind proxy servers, TOR networks, VPNs and other anonymising technology while detecting high-risk activity, such as time zone mismatches.

Visit: **transunion.co.uk/truvalidate**

TransUnion

TruValidate™

How Device Risk works

Device Risk tracks relationships between devices and accounts by leveraging device history and confirmed fraud reports from our global network of fraud analysts.

Device Risk can be easily integrated into any native app (iOS, Android, Windows, Mac OS) or web application. Apply to customer touchpoints where fraud risk is a concern, such as account creation or modification, purchase or transfer.

Common use cases for Device Risk

- **Uncover coordinated fraud rings**
  Disrupt coordinated malicious activity using our privacy-by-design approach which links together devices or accounts associated with fraud, without relying on personally disclosed information.

- **Streamline applications with robust device recognition**
  We analyse hundreds of attributes to accurately recognise a device while minimising false positives.

  Leverage shared evidence from our global network to identify devices with previous connections to fraud without adding unnecessary friction for trustworthy customers.

- **Tailor your fraud prevention strategy**
  Whether you're fighting account takeover, synthetic identities, payment fraud or promotion abuse, our system tracks over 50 different types of fraud.

  Our actionable Approve/Review/Deny response includes detailed reasons why a transaction was denied, helping you detect and stop fraudsters who move from business to business before they damage yours.

- **Review fraudulent behaviour patterns**
  Device Risk can be integrated with Behavioural Analytics, powered by NeuroID, under one solution, delivering wider understanding into how applicants interact with your application forms.

Want to know more about how device data and insights can be used to help strengthen your fraud strategy and build trust with customers?

Get in touch by calling **0113 868 2600** or visit: **transunion.co.uk/truvalidate**

TruValidate™