TruValidate™

DIGITAL INSIGHTS

Device Risk

OVERVIEW

Businesses are operating in a rapidly evolving landscape where digital fraud tactics are becoming increasingly sophisticated. From account takeovers and synthetic identities to device spoofing and multi-device attacks, these threats are diverse and constantly changing. Amid this environment, organisations are still expected to boost performance. That makes striking the right balance between driving growth and effective fraud mitigation more critical than ever.

TruValidate™ Device Risk helps prevent digital fraud in real time

TruValidate Device Risk is designed to address these challenges proactively, providing advanced detection and prevention capabilities to safeguard your organisation. By leveraging cutting-edge analytics and machine learning (ML) combined with advanced evasion and anomaly detection, TruValidate Device Risk empowers organisations to stay ahead of fraudsters — without impacting customer experiences.

TRUVALIDATE DEVICE RISK ENABLES ORGANISATIONS TO:

Combat fraud without impacting good customers

Distinguish fraudsters from real customers using advanced device recognition, contextual analysis and behavioural insights. Ensure legitimate users enjoy a seamless experience while keeping fraudsters at bay.

Build trusted connections

Leverage extensive device history with device-to-device and device-to-account associations based on confirmed fraud reports from a long-standing global device risk consortium. Access risk insights from more than 111 billion device reputation checks and over 185 million detailed fraud reports* to strengthen your security measures.

Focus on your risks

Apply device intelligence to address your unique fraud challenges with custom, configurable business rules. Tailor the solution to meet your specific needs, helping ensure maximum protection, fraud capture and efficiency.

*TransUnion internal analysis

TransUnion

Enhance operational efficiency

Streamline your fraud detection processes with automated risk assessments and real-time alerts. Reduce manual intervention and focus your resources on strategic initiatives.

Improve customer conversion

Assess the risk of digital transactions behind the scenes with minimal impact on the consumer experience, flagging any risky individuals earlier in the customer journey to increase pass-through rates for legitimate users.

Gain actionable insights

Utilise detailed analytics and reporting from the largest and long-established global device risk network to gain insights into evolving fraud trends and patterns. Make informed, data-driven decisions to continuously improve your fraud prevention strategies.

HOW IT WORKS

TruValidate Device Risk tracks relationships between devices and accounts by leveraging device history and confirmed fraud reports in real time from our extensive global network of fraud analysts. It can be easily integrated into any native app or web application.

Now you can protect your organisation across the entire customer journey. Apply to any customer touchpoint where fraud risk is a concern, such as account creation, application, login, change of details, payment and check out.

Innovative technology, diverse capabilities

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

Increase precision in fraud capture

Benefit from extended analyses of historical patterns and trends and increased data granularity to improve the accuracy and identification of sophisticated fraud schemes that evolve over time. Stay ahead of emerging threats with advanced detection capabilities.

Uncover risky device and account linkages

Discover hidden connections between devices and accounts to help uncover fraud rings and "guilty-by-association" devices — even across subscribers and industries.

Meet the unique needs of your organisation

Features a flexible rules engine with custom rule sets that can be tailored to your organisation's unique fraud strategy. Machine learning powered tracking, searching and reporting capabilities flag suspicious transactions and device patterns.

Harness advanced evasion detection capabilities

Better prevent fraudsters hiding behind proxy servers, TOR networks, VPNs and other anonymising technology while detecting high-risk activity, such as time zone mismatches, language, screen resolution and IP address data anomalies.

Accurately recognise all device types

Device Risk analyses thousands of permutations of device attributes to precisely identify a device while minimising false positives.

Track and uncover hidden fraud patterns

Advanced analytics combined with machine learning models and granular reporting capabilities can spot suspicious transactions and device patterns — which can be quickly tracked using our flexible business rules editor.

Detect virtual environments and bots

Identify virtual environments through browser data analysis, IP reputation signals and advanced anomaly and evasion detection techniques. Most automated attacks originate from virtual devices, allowing fraudsters to perform malicious activities at scale and erase traces.

Analyse complex patterns with predictive and proactive machine learning models

Use predictive and dynamic machine learning models with tailored rules and robust device signals to analyse complex patterns and proactively detect fraudulent activities with more precision. This frees up data scientist expertise to focus on fraud capture rather than managing static rules.

Increase the efficacy of your fraud strategy

Utilise TransUnion's data science expertise with the optional Risk Strategy Optimisation service. This data science managed service employs predictive ML models to detect fraud that may otherwise go unnoticed, minimising the reliance on expensive and limited data science resources.

COMMON USE CASES FOR DEVICE RISK

Account takeover (ATO) prevention

- **Challenge:** Online banking platforms face significant risks from account takeovers where fraudsters use stolen credentials to gain unauthorised access to user accounts.
- **Solution:** Device Risk can detect unusual device behaviour and flag potential ATO attempts, helping prevent unauthorised access and protecting customer accounts.

Promotion abuse prevention

- **Challenge:** Online retailers and service providers often deal with promotion abuse where fraudsters exploit promotional offers and discounts.
- **Solution**: Device Risk can monitor device behaviour and detect patterns indicative of promotion abuse, helping ensure promotional offers are used by genuine customers.

Synthetic identity fraud detection

- **Challenge:** Financial institutions struggle with synthetic identity fraud where fraudsters create fake identities using a mix of real and fabricated information.
- **Solution:** By analysing device patterns and behaviours, Device Risk can identify inconsistencies that may indicate potential synthetic identities, allowing institutions to take action before fraud occurs.

Payment fraud mitigation

- **Challenge:** Ecommerce businesses face high volumes of fraudulent transactions, leading to financial losses and chargebacks.
- **Solution:** Device Risk can identify suspicious device behaviours and flag high-risk transactions, reducing fraud and minimising chargebacks.

INDUSTRY-SPECIFIC USE CASES

Ecommerce fraud prevention

- **Challenge:** Online retailers face high volumes of fraudulent transactions, leading to financial losses and chargebacks.
- **Solution:** Device Risk can identify suspicious device behaviours and flag high-risk transactions, reducing fraud and minimising chargebacks.

Banking and financial services

- **Challenge:** Financial institutions struggle with synthetic identity fraud where fraudsters create fake identities using a mix of real and fabricated information.
- **Solution:** By analysing device patterns and behaviours, Device Risk can better detect and prevent unauthorised access, helping ensure the security of customer accounts.

Insurance fraud detection

- **Challenge:** Insurance companies need to identify fraudulent claims and recognise potential ghost brokers to prevent policy abuse.
- **Solution:** Device Risk can uncover hidden connections between devices and accounts, helping detect and prevent fraudulent claims.

Telecommunications

- **Challenge:** Telecom providers face risks from fraudulent account openings and device theft
- **Solution:** Device Risk can verify device authenticity and detect suspicious activities, helping prevent fraud and reducing losses.

Healthcare

- **Challenge:** Healthcare providers need to protect patient data and prevent unauthorised access to medical records.
- **Solution:** Device Risk can monitor device behaviour and detect anomalies, ensuring only authorised devices access sensitive information.

Travel and hospitality

- **Challenge:** Travel and hospitality businesses need to protect against booking fraud and unauthorised access to customer data.
- **Solution**: Device Risk can analyse device behaviour during booking processes, flagging suspicious activities and preventing fraud.

Gaming and online services

- **Challenge:** Online gaming platforms and services face risks from account takeovers and fraudulent activities, including promotion abuse.
- **Solution**: By leveraging device intelligence, Device Risk can identify and block fraudulent activities, better ensuring a secure and fair gaming environment.

For more details on how device data and insights can be used to help strengthen your fraud strategy and build trust with customers, visit: transunion.hk/device-risk