TruValidate®

DIGITAL INSIGHTS

Device Risk

OVERVIEW

In today's rapidly evolving digital landscape, fraud has become increasingly sophisticated and pervasive, posing challenges for organizations. From account takeover attacks and synthetic identity fraud to device spoofing and multi-device fraud, digital fraud threats are present and constantly evolving, which can result in financial and reputational damages for organizations.

TruValidate® Device Risk helps reduce digital fraud in real time

TruValidate Device Risk is designed to address these challenges proactively, providing advanced detection and prevention capabilities to your organization. By leveraging sophisticated analytics and machine learning (ML) combined with advanced evasion and anomaly detection, TruValidate Device Risk promotes a better customer experience.

TRUVALIDATE DEVICE RISK HELPS ORGANIZATIONS TO:

Leverage trusted connections

Leverage extensive device history with device-to-device and device-to-account associations based on reported fraud from a global device risk consortium. Access to risk insights and detailed fraud reports to enhance your Device Risk processes.

Focus on your risks

Apply device intelligence to address your unique fraud challenges with configurable business rules. Tailor the solution to help assist your specific needs, helping support protection, fraud capture and efficiency.

Reduce fraud

Help distinguish fraudsters from real customers using advanced device recognition, contextual analysis and behavioral insights.

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 low impact on the consumer experience, flagging risky individuals early in the customer journey to increase pass-through rates for legitimate users.

Gain actionable insights

Utilize reporting from the device risk portal to make informed, data-driven decisions to support continuous improvement to your fraud control objectives.

HOW IT WORKS

TruValidate Device Risk assesses the relationships between devices and accounts in real time by leveraging device history and confirmed fraud reports. It can be easily integrated into any native app or web application.

Apply to any customer touchpoint where fraud risk is a concern, such as account creation, application, login, change of details, payment and check out.

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.

Help detect virtual environments and bots

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

Risky device and account linkages

Discover connections between devices and accounts to help uncover fraud rings and devices — across subscribers and industries.

Help support the needs of your organization

Features a flexible rules engine with configurable rule sets that can be chosen for your organization's unique fraud strategy. Reporting capabilities to flag suspicious transactions and device patterns.

Harness advanced evasion and detection capabilities

Guard against fraudsters hiding behind proxy servers, TOR networks, VPNs and other anonymizing technology while helping to detect high-risk activity, such as time zone mismatches, language, screen resolution and IP address data anomalies.

Recognize device types

Device Risk analyzes thousands of permutations of device attributes to help to identify a device while reducing false positives.

Fraud patterns

Advanced analytics combined with machine learning models and granular reporting capabilities can help to spot suspicious transactions and device patterns — via our flexible business rules editor.

Analyze complex patterns with predictive and proactive machine learning models

Use predictive and dynamic machine learning models with configurable rules to help detect fraudulent activities. This frees up data scientist expertise to focus on fraud capture rather than managing static rules.

Innovative technology, diverse capabilities

Device Risk helps to detect unusual device behaviour.

COMMON USE CASES FOR DEVICE RISK

Account takeover (ATO) prevention

- **Challenge:** Fraudsters use stolen credentials to gain unauthorized access to user accounts.
- **Solution:** Device Risk can help to detect unusual device behavior and flag potential ATO attempts, helping prevent unauthorized access and protecting customer accounts.

Synthetic identity fraud

- **Challenge:** Fraudsters create fake identities using a mix of real and fabricated information.
- **Solution:** By analyzing device patterns and behaviors, Device Risk can help identify inconsistencies that may indicate potential synthetic identities, allowing institutions to take action before fraud may occur.

Payment fraud

- **Challenge:** High volumes of fraudulent transactions, leading to financial losses and chargebacks.
- **Solution:** Device Risk can flag suspicious device behaviors and high-risk transactions, reducing fraud and chargebacks.

Promotion abuse

- **Challenge:** Fraudsters exploit promotional offers and discounts.
- **Solution:** Device Risk can help to detect device patterns that may indicate promotion abuse, helping support use of promotional offers by genuine customers.

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.ca/Solution/device-risk