

## Insight Guide

# Expedite Customers to Checkout While Preventing E-Commerce Fraud.



**In the e-commerce industry, a friction-right customer experience is paramount.**

The customer experience is paramount to the e-commerce industry, where high standards exist for seamless, instant access to sites and mobile apps.

However, this heightened access and elevated experience needs to be balanced against the realities of organized fraud, as well as regulatory mandates for stronger customer authentication. TransUnion's global fraud and identity solutions provide e-commerce organizations with tools that satisfy the competing demands of catching fraud, authenticating good customers and providing a safe, secure and friction-right experience.







of customers report they have improved their customer experience by reducing friction with device-based reputation.

**TechValidate**  
by SurveyMonkey

## Our Experience

### Types of e-commerce merchants that use TransUnion:



Transactions protected by TransUnion from the past 12 months	E-commerce customers	All customers
 Number of transactions protected	3 billion	11.9 billion
 Number of risky transactions stopped	263 million	631 million
 Number of reputation reports submitted by analysts	5.9 million	20.8 million
 Percent of devices previously seen by TransUnion	63%	73%



# Create an Outstanding Experience and Shut Down Fraud

The e-commerce industry's meteoric rise — a 20% year-over-year increase and \$2.7 trillion in worldwide online revenue — has been unable to prevent an associated increase in fraud.<sup>1</sup>

**E-commerce fraud is up 5.5% year-over-year across all industries, but has risen significantly higher in several sub-segments.<sup>2</sup>**



**11.9%** Consumer electronics



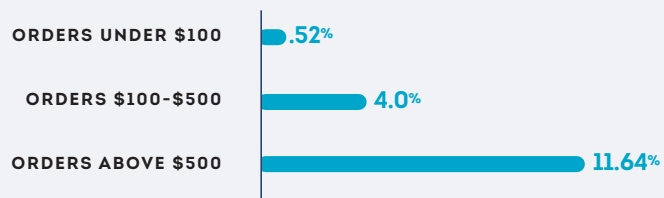
**36.7%** Jewelry



**172%** Cosmetics and perfumes

**Fraudsters show a strong preference for high-value targets.<sup>1</sup>**

**Fraud percentage increase by order amount:**



<sup>1</sup> Statista

<sup>2</sup> Global Fraud Index, Pymnts.com



Customers expect a consistent experience across all of their devices.

Skilled fraudsters will look for workarounds to every fraud-fighting technique you try. Combating this threat requires resources that will evolve with new trends and fraud vectors: smart tools, machine learning and crowd-sourced intelligence. Of course, it's critical to implement friction-right solutions for establishing identities, authenticating customers and preventing digital fraud in order to keep customers both happy and protected.

### Your Customers Expect a Friction-Right Experience

Today's online shoppers want an easy and secure experience, from login to checkout. Too much friction at any point paves the way for them to click over to a competitor offering a smoother path to purchase. Instead, give your customers secure protection while reducing friction and keeping fraudsters out.

### Your challenges:

- Promotion abuse is diluting the value of customer acquisition programs
- Improving the login experience without sacrificing security
- Authenticating shoppers while stopping account takeover (ATO)
- Fighting fraud and abuse across ever-changing vectors
- Enhancing usability, even as prices and margins decline



### The solution: Focus on your customer's device

Every purchase. Every engagement with your brand. Every attempt at fraud. They all rely on a web-enabled device, and TransUnion's powerful device recognition technology can confirm the reputation of over seven billion devices

## How TransUnion Prevents E-Commerce Fraud

TransUnion’s fraud prevention solutions use flexible business rules and advanced machine learning algorithms to detect devices with risky attributes and behavior. Our patented technology identifies and helps to quickly shut down coordinated fraud rings by recognizing connections between accounts and devices, regardless of business or industry.

This technology is further supported by our global network of fraud and security analysts, who submit millions of device reputation reports that detail the type of fraud or abuse a device is confirmed to have committed, such as:

- Gift card fraud
- Account takeover
- Shipping fraud
- Credit card fraud
- Promotions abuse
- Friendly fraud

Your Challenges	Our Solutions
<p><b>Friendly fraud is difficult to stem.</b> Whether it’s a customer disputing a charge, packages being lost in transit or even using and returning an item, friendly fraud can be challenging to shut down.</p>	<p>Our online fraud prevention solutions allow you to flag devices by specific types of past fraud or abuse. We’ll inform you if the device in use is associated with a history of friendly fraud, either with your business or with another merchant in our network.</p>
<p><b>Preventing promotion abuse.</b> Coupons, promotions and loyalty programs are all critical for acquiring and retraining customers, but unfortunately can also be targets for fraud and abuse.</p>	<p>We help identify good customers by their devices’ characteristics and past behavior. When we detect a device that has been involved in past promotion abuse or is showing unusual velocities, we alert you in real time.</p>
<p><b>Synthetic identities are hard to spot.</b> Fraudsters are outmaneuvering you, helped by techniques such as synthetic, forged, or hybrid identities, automated attacks, device spoofing and proxies.</p>	<p>With patented device recognition technology, we help you identify risk from device behavior and characteristics. We use advanced machine learning analytics, uncover false IP addresses and geolocations, and detect other techniques that fraudsters commonly use.</p>
<p><b>Your fraud solutions are adding customer friction.</b> You are constantly pressured by your sales and marketing departments to reduce user friction caused by your fraud prevention efforts, especially during sales promotions. But when you do, your fraud rates go up.</p>	<p>Through a combination of machine learning, device behavior, and device reputation, you can separate good customers from repeat abusers of your promotion programs. Now good users receive the best user experience while the fraudsters are stopped.</p>

## How to Provide Fast and Secure Access

The flood of breached credentials over the last decade has made it easier than ever for criminals to take over good customers' accounts. While merchants race to strengthen their authentication and identity proofing solutions, customers still expect the best possible online experience, beginning at login.

Common Challenges	Our Solutions
<p><b>ATO is rising.</b> Your customers trust you to secure the services you offer, but ATO can put them at risk of significant loss. Adding more layers of authentication decreases the risk of ATO, but can also negatively impact the user experience.</p>	<p>Prevent ATO fraud across the entire customer journey with a friction-right experience. If a customer is logging in from an authorized device for a low-risk activity, they'll be authenticated immediately as a trusted connection. For higher risk activities, step up to strong or multifactor authentication.</p>
<p><b>Credentials are everywhere.</b> Over 9 billion credentials, account details and passwords have been dumped on the dark web in the last decade, and traditional password-based authentication systems have been rendered obsolete.</p>	<p>You can no longer rely on single- or even two-factor solutions. Our comprehensive and real-time authorization solutions allow you to layer in multiple authentication options without adding friction.</p>
<p><b>Customers are treated like fraudsters.</b> If every visitor is subject to the same authentication prompts, you're either letting too much fraud in or creating too much friction for good customers.</p>	<p>Device-based authentication adds an essential dimension of context and risk to the authentication process, delivering insights on access requests, step-up authentication processes and device histories. Layer in solutions like One-Time Passcode (OTP) and Knowledge-Based Verification for technologically fluid authentication that is familiar to customers and reduces abandonment rates..</p>
<p><b>Your current tools miss risk signals.</b> Does your customer just want to view their account or see their order history? What if they want to repeat an order to the same address, or change their contact information? Each action represents a different level of risk, but most authentication solutions treat all actions the same.</p>	<p>Dynamic authentication combines interactive, mobile multifactor authentication with transparent, easy-to-use device recognition to ensure the appropriate friction-right method is being deployed at the right time.</p>
<p><b>Authorization is difficult to manage and track.</b> Regulatory standards such as the GDPR and PSD2 not only demand strong authentication, they also require authorization as an explicit and separate function. How do you go from, "Is this the right person?" to, "Is this person authorized for this request?"</p>	<p>Build authorization capabilities within your native app that allow your customers to authorize specific requests in real time, such as "Transfer \$50,000 to Acme Company?" or even, "Do you grant permission for this package to be delivered without a signature?" This allows you to automate authorization, improve validation and meet strong customer authentication and audit requirements.</p>



Personal Identity Solutions  
with TransUnion

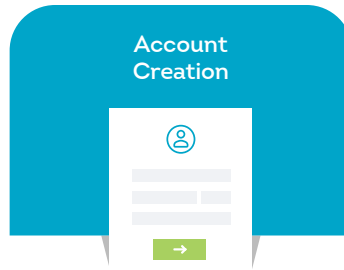
# Protect and Enhance the Entire Customer Journey



Digital  
Identity Solutions

1

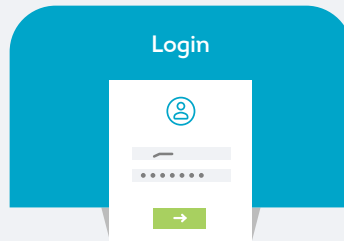
- Verified pre-fill to reduce abandonment
- Email and phone verification
- Address validation
- Prevent new account fraud



- Prevent promotions abuse
- Detect high velocities
- Uncover synthetic and stolen identities

2

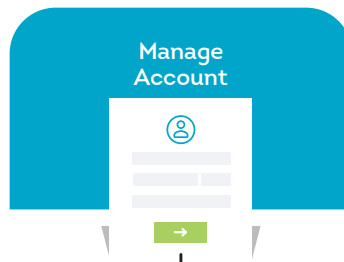
- Knowledge-based authentication
- One-time passcode (OTP)
- Account recovery and lockout support
- Call-center authentication support



- Stop account takeover
- Authenticate customers
- Reduce friction at login
- Authorize devices
- Provide multifactor authentication

3

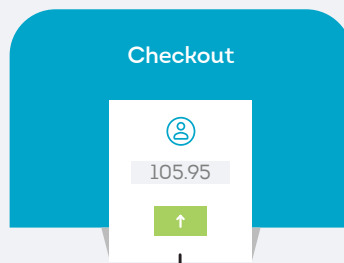
- Validate account changes to email
- Verify account changes to phone
- Validate account changes to identity elements



- Step-up authentication for account changes
- Stop account takeover
- Prevent call center fraud

4

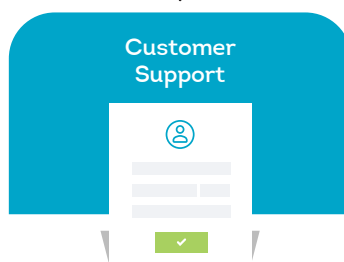
- Verify delivery and billing address
- IP matching
- BIN matching
- Detect re-shippers
- Reputational history



- Prevent payment fraud
- Stop promotion abuse
- Detect gift card fraud
- Prevent friendly fraud
- Reduce chargebacks
- IP and geolocation mismatches

5

- Reputational history
- Knowledge-based authentication
- Account recovery and lockout support
- Call-center authentication support



- Prevent returns fraud
- Stop social engineering with MFA
- Prevent call center fraud

<sup>1</sup>Not available in all regions

## Fraud Prevention and Authentication Solutions

---

To remain competitive, merchants must balance experience with security. That's what our products are built to do. Learn more about the solutions by visiting [iovation.com](https://www.iovation.com).



### Establish Identity

Establish identity with greater confidence by verifying against a broad set of personal and digital data.



### Authenticate Consumers

Secure each point of the customer journey with authentication methods tailored to the transaction risk level.



### Prevent Fraud

Proactively identify fraudulent transactions and behaviors of any given device in real time.

## Get in Touch

Find out more about our authentication and fraud prevention solutions. Contact us for a demo or visit [iovation.com](https://www.iovation.com)

### Portland Office

### United Kingdom