

E-Book

Fraud without friction: Are you stopping fraud, or stopping customers?

How consumer brands stop fraud without losing
legitimate buyers at checkout



Table of Contents

1	Summary
3	Setting the stage: The AI fraud surge and the CAPTCHA war
5	The silent revenue killer: Where consumer funnels bleed
7	Protecting revenue with background threat intelligence
9	The defense stack: How modern identity tools stop fraud without slowing growth
13	Bringing this back to your team

These materials are intended for general informational purposes only and are not intended to be legal, privacy, security, compliance, or business advice. You are responsible for obtaining security, privacy, compliance, or business advice from your own professional advisors.



Summary

For consumer companies, every digital touchpoint serves two roles: attracting shoppers and exposing API endpoints to potential attacks. Adding new channels, mobile apps, or loyalty features opens up fresh opportunities for sales, but it also creates targets for automated fraud.

When security concerns escalate, organizations often respond by adding heavy verification steps. These rigid barriers may block some fraud, but they also turn away genuine buyers and reduce overall sales.

Security metric category	Primary focus	Financial and customer impact
Tracked costs	Fraud chargebacks, direct theft, chargeback processing fees	Appears as an explicit line item on financial reports, leading teams to add more security friction
Hidden losses	False declines, registration drop-offs, abandoned password resets	Over <u>\$231 billion</u> lost annually to <u>false declines</u> ; 42% of shoppers abandon purchases over forced password resets

The common approach to digital security (relying on blanket friction, static login barriers, rigid password rules, and intrusive bot challenges) creates a massive barrier to sales. While AI-driven automation allows bad actors to bypass static controls with ease, these same hurdles actively penalize legitimate customers.

Globally, false declines and authentication drop-offs cost businesses hundreds of billions annually. Up to 40% of legitimate consumers who encounter an unexpected security barrier never return to that brand, quietly destroying customer lifetime value long before a fraudulent chargeback ever occurs.

Instead of viewing security and user experience as competing priorities, modern Customer Identity and Access Management (CIAM) evaluates risk continuously in the background. By checking context signals automatically during token issuance, companies can block fraud in real time while keeping sign-up and checkout fast for real shoppers.

Setting the stage: The AI fraud surge and the CAPTCHA war

To understand why traditional security controls fail, we need to examine how bad actors use artificial intelligence. Basic CAPTCHAs, static IP rate limits, and fixed password rules were designed for an era when attacks were manual or driven by simple scripts.

Today, automated credential-stuffing botnets and generative AI tools allow bad actors to launch sophisticated attacks at scale.



The CAPTCHA problem:

Blocking real fans while bots buy out inventory

A clear example of this issue happens during high-demand event drops, ticket sales, and limited-edition product releases. To combat scalper bots, ticketing platforms and retail brands frequently increase CAPTCHA difficulty, forcing users to complete multiple rounds of distorted image recognition and puzzle solving.

In practice, this approach backfires. Modern computer vision AI models (such as YOLO and vision transformers) can solve complex image puzzles in less than 200 milliseconds, allowing automated bots to bypass security and buy up inventory. Meanwhile, real human buyers struggle with distorted image tests, encounter repeated validation errors, get frustrated, and abandon the platform. Static hurdles do not stop automated abuse; they simply penalize real shoppers while bad actors adapt.

The financial impact of false declines and friction

When security tools operate without real-time identity context, they reject valid buyers by mistake. Core industry metrics highlight the scale of this problem:

The \$231 billion false decline problem

False declines happen when valid e-commerce purchases are flagged as fraudulent. Research from [Signifyd and Datas Insights](#) shows average false decline rates at 1.51% of total sales, with projected merchant losses exceeding \$231 billion annually. Without real-time behavioral and device intelligence, security systems treat unfamiliar human buyers as threats.

Registration funnel bleed

[65% of online consumers](#) **abandon a site** when forced to complete a complex account creation process.

Checkout password reset drop-off

[42% of shoppers walk away](#) from a purchase if forced to reset a password during checkout.

Permanent brand churn

[55% of consumers stop using a brand entirely](#) after experiencing repeated account access issues or unexpected security lockouts.

The silent revenue killer: Where consumer funnels bleed

Most executive teams operate with a significant blindspot. Finance and risk management teams track chargeback rates and direct fraud losses closely because they appear as explicit costs on financial statements. However, marketing, digital product, and customer experience leaders often remain unaware of the far larger losses occurring silently during sign-up, sign-in, and checkout.

When marketing teams spend heavily to attract qualified traffic to a platform, introducing a forced password reset or mandatory registration form at checkout causes up to 42% of those high-intent buyers to leave.

Industry-specific friction points

Authentication friction impacts key consumer sectors in distinct ways:



Streaming and media: Aggressive account-sharing checks, short token expiration windows, and strict device-linking limits trigger immediate subscriber churn, particularly on smart TVs and mobile companion apps where typing complex passwords is difficult.



Gaming and iGaming: Account takeover attempts surge during live events, esports tournaments, and in-game item drops. Enforcing heavy identity verification during registration causes player drop-off, driving users to competing platforms.



Consumer fintech: Complex Know Your Customer forms and repetitive multi-factor authentication prompts during low-value peer-to-peer transfers create frustration, pushing users toward simpler apps.



Retail and e-commerce: High-intent shoppers regularly abandon carts when triggered for extra verification on low-risk repeat purchases or when forced to create an account before buying.



Travel, hospitality, and loyalty: Stolen airline miles, drained gift card balances, and compromised VIP points damage brand reputation. Credential stuffing against legacy API endpoints allows bad actors to hijack accounts. Yet, requiring travelers to pass static security hurdles every time they check a flight status degrades the guest experience.

Industry sector	Primary security threat	Typical blunt response	Commercial impact
Retail & e-commerce	Credential stuffing and bot attacks	Mandatory account creation and static CAPTCHAs	High cart abandonment and over \$231 billion in global false declines
Streaming & media	Account sharing and takeover attempts	Frequent device re-authentication prompts	Subscriber churn, especially on smart TV apps
Consumer fintech	Account takeover and identity fraud	Mandatory multi-factor authentication on every transaction	User drop-off during rapid peer-to-peer transfers
Travel & hospitality	Loyalty points theft and account takeover	Front-loaded identity verification forms	54% abandonment rate during loyalty program onboarding
Gaming & iGaming	Botting, multi-accounting, and takeover	Slow, multi-step registration hurdles	Loss of high-value players during live event drops

Protecting revenue with background threat intelligence

Security strategies built on higher walls no longer work. Adding more form fields, forcing frequent password changes, or showing security challenges to every user blocks legitimate buyers while automated bots bypass the barriers.

Identity-based security shifts protection to the background. Instead of asking every user to prove who they are through manual challenges, a modern identity engine evaluates context signals automatically behind the scenes every time a user interacts with a platform.

Contextual risk intelligence architecture

During the authentication handshake, the identity platform ingests and correlates multiple real-time telemetry streams in under 50 milliseconds:

1.

Device posture and fingerprinting

Evaluating TLS fingerprinting (such as JA3/JA4 hashes), HTTP header ordering, browser environment entropy, and canvas rendering signatures to confirm whether the request originates from a legitimate browser or a headless bot runner.

2.

IP reputation and network data

Checking incoming requests against threat databases to identify residential proxy networks, data-center bot ranges, TOR exit nodes, and suspicious VPN configurations.

3.

Behavioral velocity and impossible travel

Calculating physical velocity limits between successive authentication requests (for example, detecting a login initiated in Chicago followed 10 minutes later by an API call from Frankfurt).

4.

Breached credential feeds

Using k-Anonymity cryptographic lookups to evaluate submitted username and password pairs against billions of leaked records from known third-party data breaches.

When these background signals confirm that a session is low risk (which applies to over 90% of legitimate traffic), the user encounters no security prompts. The system issues secure OpenID Connect tokens and JSON Web Tokens (JWTs) instantly, allowing the user to complete their purchase or access their loyalty rewards with zero added friction. Friction is reserved strictly for genuine anomalies.

The defense stack: How modern identity tools stop fraud without slowing growth

To implement background security, enterprise organizations rely on a purpose-built identity platform that orchestrates threat intelligence across four defensive layers:

Defense stack layer	Technical capability	Practical outcome
1. Perimeter defense	Bot detection, IP reputation filtering, sliding-window rate limiting	Filters out malicious automated traffic before it reaches your login box or APIs
2. Credential security	Breached password detection using k-Anonymity hash lookups	Prompts targeted resets when submitted passwords match known data breaches
3. Frictionless authentication	Biometric Passkeys, WebAuthn/FIDO2, Touch ID, Face ID, social login	Replaces passwords with phishing-resistant keys, eliminating password reset drop-offs
4. Contextual verification	Adaptive Multi-Factor Authentication (AMFA) triggered by risk score	Keeps low-risk sessions unprompted, challenging only high-risk anomalies

1.

Blocking automated abuse before the login gateway

The most efficient way to stop fraud is to filter out malicious traffic at the perimeter before it ever reaches your login box, registration form, or transaction APIs.

Auth0 Attack Protection uses machine-learning models trained on billions of monthly login transactions. By evaluating IP reputation, request velocity, and historical threat data, the platform identifies automated bot scripts and credential-stuffing attacks at the edge.

During the first half of 2023 alone, 9.3% of retail registration attempts and 51.3% of password-based retail logins on the Auth0 platform were identified as scripted attacks and managed automatically.

In practice, enabling automated bot detection reduces malicious traffic by over 40% on average, with large enterprises seeing bot traffic drop by nearly 90%. When attackers encounter modern perimeter defenses, they abandon the target in search of softer, legacy systems.

2.

Stopping account takeovers and password friction

Credential stuffing (where attackers test millions of stolen username and password combinations across consumer sites) remains one of the primary drivers of account takeover.

Modern identity platforms neutralize this threat through two proactive mechanisms:

1. Breached password detection

Auth0 checks submitted credentials against a real-time database of leaked passwords using k-Anonymity, ensuring raw passwords are never exposed. If a user attempts to log in using a compromised password, the system prompts an immediate, targeted password reset, protecting the account before a takeover occurs.

2. Transitioning to biometric Passkeys

Passkeys replace passwords with public/private cryptographic key pairs bound to the customer's device (via WebAuthn and FIDO2 standards). Private keys remain stored inside device Secure Enclaves, while the identity server verifies signed challenges using the public key. Because Passkeys are bound to origin domains, they natively resist phishing, credential stuffing, and man-in-the-middle attacks. They eliminate forgotten password loops entirely, boosting login success rates while elevating security.

3.

Protecting the journey with adaptive verification

Broad, mandatory verification prompts frustrate legitimate customers. Adaptive Multi-Factor Authentication evaluates contextual risk dynamically at request time.

If a customer logs in from a recognized mobile device on their home Wi-Fi network, extra verification is bypassed completely. If that same user attempts to transfer funds, redeem high-value loyalty points, or change their shipping address from an unrecognized IP address in a different country, Auth0 triggers targeted verification (such as a WebAuthn prompt, TOTP code, or push notification). Extra security steps in only when actual risk dictates it, keeping the path clear for standard buyers.

4.

Securing automated AI transactions

As consumers deploy AI assistants to shop, compare prices, and manage bookings on their behalf, security systems need to distinguish between **malicious automated bots** and **legitimate customer AI agents**.

Legacy anti-bot tools block all automated traffic indiscriminately, shutting down valid AI-driven sales. Modern identity platforms solve this using delegated token vaults and fine-grained authorization (FGA based on Relationship-Based Access Control, or ReBAC). Human users authenticate strongly via Passkeys and issue short-lived, permission-scoped tokens (using OAuth 2.0 Token Exchange, RFC 8693) to their AI agents. This allows the agent to execute specific API transactions (such as checking availability or placing an order under a set dollar limit) while blocking unauthorized or high-risk actions automatically.

Bringing this back to your team

Evaluating security tools requires looking at both risk reduction and checkout conversion. Before launching your next digital experience or tightening security rules, bring marketing, digital product, and security leaders together to review where your revenue funnel may be losing shoppers.

Consider these three starting points for your next leadership meeting:

1.

Track registration and checkout drop-off

Review conversion data across sign-up, login, and checkout screens with your product team. Calculate the revenue lost to forgotten password resets, long forms, and unnecessary verification prompts.

2.

Compare false declines against chargebacks

Review your current false decline percentage with your risk management team. Compare the direct cost of chargebacks against the estimated lifetime value of legitimate customers turned away by overly aggressive fraud rules.

3.

Shift to background verification

Plan a roadmap to replace mandatory account creation and password friction with continuous risk signals, biometric Passkeys, and perimeter bot protection.

Take the next step

You do not have to compromise customer conversion to keep your platforms secure. By shifting security evaluation to the background, you can protect your top-line growth while stopping automated fraud in real time.

Download the checklist

Get [The Fraud Without Friction Audit Checklist](#) to evaluate your security controls, identify false declines, and eliminate checkout friction.

Explore industry solutions

Learn how identity infrastructure protects high-volume platforms with [Auth0 for Retail](#) and manages automated interactions with [Auth0 for AI Agents](#).

Talk to an Auth0 architect

[Schedule a technical scoping session](#) with our engineering team to review your current security setup and streamline your checkout journey.

