

The fraud without friction audit checklist

Are your security controls protecting revenue or stopping customers?

Getting customers to your storefront is hard enough. Blocking legitimate buyers at checkout with intrusive CAPTCHAs, false declines, and unexpected login hurdles is frustrating and expensive.

Most executive teams track chargeback costs closely, but few measure the silent revenue leaking from false declines and conversion-killing security friction.

Use this checklist to walk through your current fraud and identity setup. It will help you identify where rigid security barriers are getting in the way of sales and where simple, modern threat intelligence can block fraud silently in the background.

Instructions: Check each box that matches your current setup. If you are not sure or know you rely on a static, blanket rule, leave it unchecked and treat it as an open gap.

1. Bot defense and perimeter security

- ☐ Do you filter out automated bot traffic and credential-stuffing scripts at the perimeter before they reach your login box or APIs?
- ☐ Can real customers complete checkout without being interrupted by intrusive image or puzzle CAPTCHAs?
- ☐ Do you use edge rate-limiting and IP reputation filtering to stop brute-force attacks automatically?
- ☐ Is your anti-bot protection smart enough to block malicious scripts without slowing down legitimate human shoppers during high-demand sales drops?

2. Credential security and ATO prevention

- ☐ Do you automatically check submitted passwords against real-time breached credential databases to block compromised logins?
- ☐ Do you offer biometric Passkeys (Touch ID, Face ID, Windows Hello) to eliminate password vulnerability entirely?
- ☐ Can users securely reset compromised accounts without getting stuck in slow, friction-heavy email reset loops at checkout?
- ☐ Do you use cryptographic hash lookups (such as k-Anonymity) so sensitive user credentials are never exposed during breach checks?

3. Background risk telemetry

- ☐ Does your system evaluate background signals (such as device fingerprinting, browser posture, and IP reputation) in under 50 milliseconds?
- ☐ Can you detect impossible travel anomalies, such as a login in Chicago followed minutes later by an API request from Frankfurt?
- ☐ Do more than 90% of your legitimate, low-risk users pass through login and checkout with zero security prompts or challenges?
- ☐ Are session tokens issued silently in the background once contextual risk is confirmed as low?

4. Adaptive verification and step-up security

- ☐ Do extra security checks (like Multi-Factor Authentication) trigger strictly when a session's risk score actually spikes?
- ☐ Are low-risk repeat purchases on recognized devices allowed to proceed without forcing extra verification steps?
- ☐ Do you reserve step-up authentication for high-risk actions, such as updating shipping addresses or redeeming high-value loyalty points?
- ☐ Do you provide seamless push-notification or biometric verification options rather than relying solely on delayed SMS one-time passcodes?

5. False declines and revenue governance

- ☐ Do your leadership and risk teams actively measure false decline rates alongside traditional fraud chargeback metrics?
- ☐ Is your false decline rate tracked and kept below the industry benchmark average of 1.5%?
- ☐ Are returning, verified customers automatically exempted from aggressive payment fraud checks based on identity history?
- ☐ Does your identity system pass real-time user context and risk telemetry directly to downstream payment and fraud engines?

6. Vertical-specific friction management

- ☐ **Retail and E-commerce:** Can high-intent buyers check out smoothly without being forced into mandatory account creation forms or repetitive verification?
- ☐ **Streaming and Media:** Can users stay logged in across Smart TVs and mobile devices without encountering frequent re-authentication prompts?
- ☐ **Fintech and iGaming:** Can users complete instant registrations or low-value transfers without being stalled by heavy front-loaded verification?
- ☐ **Travel and Loyalty:** Are customer loyalty points, gift cards, and VIP miles protected from credential stuffing without degrading the daily guest experience?

7. AI agent and automated transaction readiness

- ☐ Can your security architecture distinguish between malicious scraping bots and legitimate customer AI shopping delegates?
- ☐ Can your system issue short-lived, permission-scoped tokens (using OAuth 2.0 Token Exchange) to AI assistants without exposing user credentials?
- ☐ Do you enforce fine-grained spend limits and action boundaries on automated AI transactions?
- ☐ Can customers easily view, manage, or revoke permissions granted to their personal AI shopping assistants?

Calculate your score

Add up your checked boxes to see where your customer and security setup stands:

24–28 boxes checked

Optimized

Your setup blocks fraud silently in the background while keeping checkout completely open for legitimate buyers.

16–23 boxes checked

Solid, but Leaking Revenue

Your core defenses work, but static security hurdles and false declines are likely costing you sales.

Under 16 boxes checked

High Conversion Risk

Outdated security controls and blanket friction are driving shoppers to competitors and penalizing real customers.

Ready to eliminate checkout friction without raising risk?

Evaluating your fraud controls is just the starting point. Resolving false declines and login drop-offs does not require ripping out your technology stack or compromising on security standards. By evaluating contextual risk quietly in the background, you can shut down automated fraud in real time while keeping checkout fast and open for genuine buyers.

[Book a 30-minute scoping session](#) with an Auth0 solution architect to walk through your checklist findings, evaluate your current security setup, and build a tailored plan to eliminate false declines and protect top-line revenue.