WHITE PAPER

Holiday readiness starts at checkout:

Where revenue is captured and loyalty is won or lost

Holiday readiness starts at checkout: Where revenue is captured and loyalty is won or lost

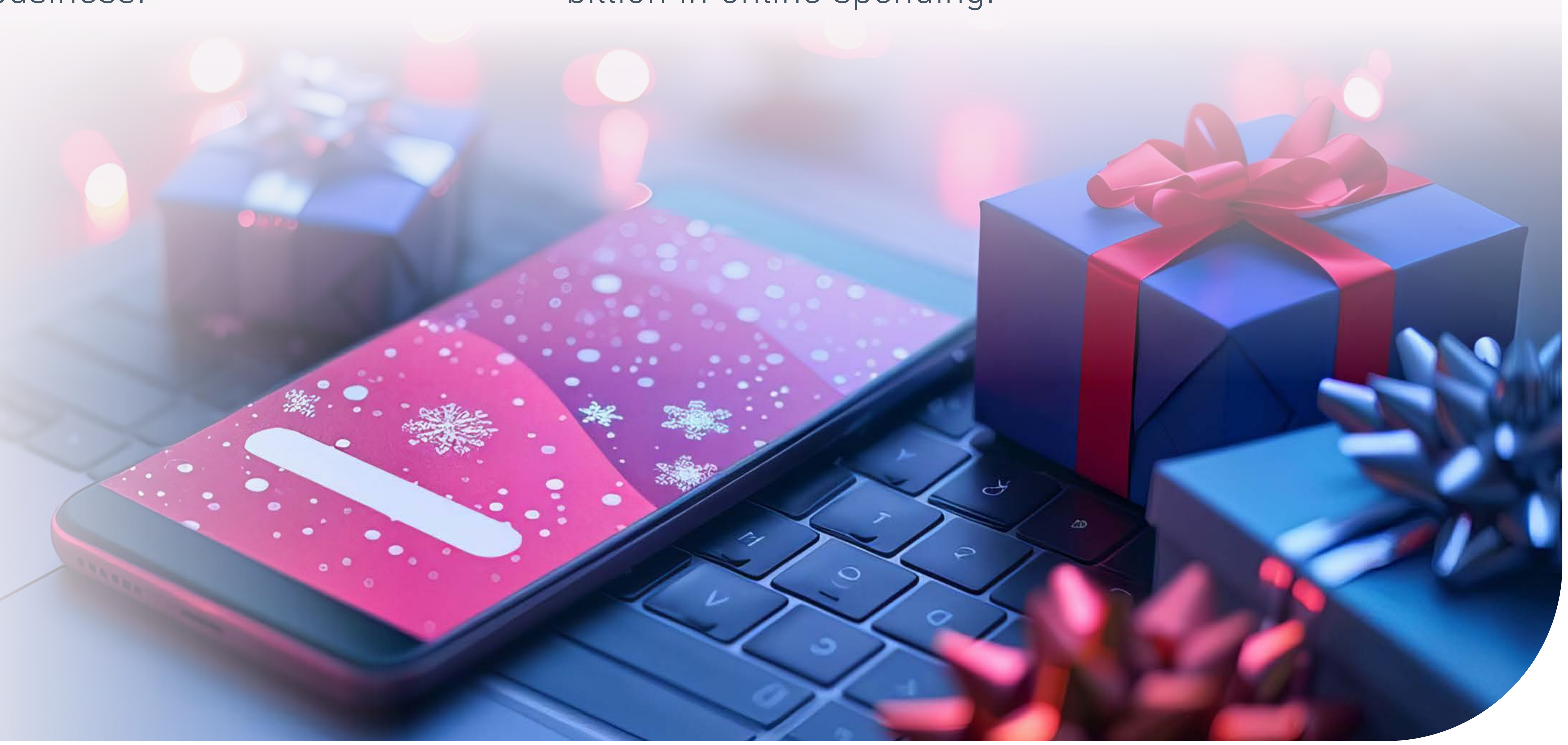
Every holiday season, retailers invest millions of dollars to attract shoppers, drive traffic, and capture demand during the year's most important revenue period. By late summer, merchandising teams are finalizing promotions, marketing campaigns are ramping up, and operation teams are stress-testing systems in anticipation of weeks of elevated transaction volume. But every one of those investments ultimately converges at a single moment: **checkout**.

Consumers haven't stopped spending, but they have become more selective about where they spend. Experian's 2025 Holiday Spending Trends report found shoppers prioritized value, convenience and relevance, while **66% of marketers expected holiday marketing spend to increase**, despite only 22% of consumers expecting to spend more during the season.

For fraud and payments teams, that **raises the stakes of every checkout decision**. Every legitimate shopper who reaches checkout represents a marketing investment, customer acquisition cost, and revenue opportunity. A false decline no longer impacts only fraud metrics – it impacts the business.

Holiday shoppers don't stick to one calendar. Nearly **45% of consumers begin shopping before November**, while 62% continue purchasing throughout December, resulting in sustained transaction volume for weeks. That shift was reflected in the 2025 holiday season, which **generated a record $257.8 billion in online sales**, including 25 individual days surpassing $4 billion in online spending.[1]

The retailers that win this holiday season will **make smarter checkout decisions - maximizing approvals for legitimate shoppers** while intelligently identifying the small percentage of transactions that truly warrant additional scrutiny.



THE STAKES

Revenue protection: The new fraud KPI

For fraud and payments leaders, holiday readiness means preparing to make better decisions under higher transaction volumes. Every approval, decline, and step-up authentication influences revenue, customer experience and long-term loyalty. That's because checkout has become one of retail's most important revenue moments, determining whether marketing investment and purchase intent become revenue or disappear.

Historically, fraud teams were measured primarily by how much fraud they prevented. Today, success is measured much more broadly. Approval rates, false declines, customer friction, chargebacks, and conversion all influence business performance. Every checkout decision now balances two equally costly outcomes: approving a fraudulent transaction or declining a legitimate customer. During the holiday season, when retailers have invested heavily to acquire shoppers and transaction volumes are at their peak, both mistakes become significantly more expensive.

Every approval is a revenue opportunity realized. Every false decline is a revenue opportunity lost.

The trust advantage of invisible security

Consumers expect retailers to protect them from fraud, but they don't want that protection to come at the expense of convenience. The challenge for fraud and payments leaders is balancing both. Experian's 2025 Identity and Fraud Report highlights a significant trust gap. While **52% of consumers hold retailers** responsible for their online security, **only 19%** actually trust them to deliver it.[2] By contrast, payment providers enjoy a positive trust gap – consumers trust them more than they even expect to.

Over the past decade, payment providers have invested heavily in authentication experiences that are fast, passive, and largely invisible to legitimate customers. Consumers rarely stop to think about the security because it works quietly in the background. Authentication happens seamlessly, creating confidence without disrupting the buying journey.

Retailers don't need to become payment providers, but they can adopt the same design principle: make security intelligent enough to fade into the background. Leading retailers are shifting toward layered identity strategies that confidently recognize legitimate shoppers behind the scenes and reserve step-up authentication for the small percentage of transactions that truly present risk.

Consumers trust payment providers because security feels seamless - not because it's absent.

As holiday transaction volumes increase, the brands that earn trust won't necessarily be those with the strongest security controls. They'll be the ones whose controls are the least disruptive to legitimate customers. Retailers that make security feel effortless will be better positioned to build trust, reduce abandonment, and maximize approvals without increasing fraud.

$257.8 billion

Record U.S. online spend during 2025 holiday season is **up 6.8% year-over-year**

$20 billion

BNPL volume during the 2025 season is up 9.8%. Each BNPL transaction is a checkout where the payment layer built trust that the retailer didn't.

Adobe Analytics, January 2026

~33%

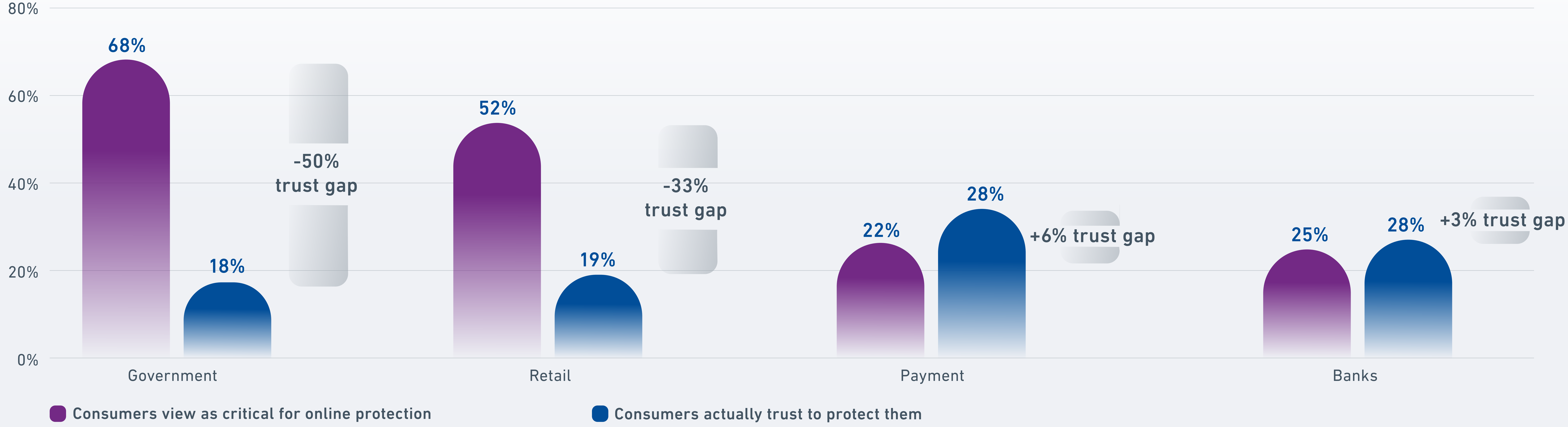
Retail trust gap: 52% of consumers expect retailers to protect them online; only 19% actually trust them to do it.

+6%

Payment providers trust gap — positive, not negative.

Experian 2025 Identity & Fraud Report / MRC

Consumers' relationship to trusted entities



Source: Experian 2025 Identity & Fraud Report, Presented at MRC, October 2025

THE SHIFT

Four forces are rewriting what consumers expect at checkout — and what they'll abandon when they don't get it

Invisible security is now the expectation

65% of consumers say invisible security methods are extremely or very important to them.[2]

86% of U.S. consumers expect companies to address their security and privacy concerns — this is table stakes, not a differentiator.

Guest checkout has become the preferred experience

43% of consumers prefer guest checkout.

72% use guest checkout even when they have an account.[2]

The unnecessary friction problem is measurable

25% of consumers who encountered onboarding friction followed through with abandoning, choosing a competitor instead. Among high-income households the rate is 50%; among 25–39 year olds, 45%.[2]

16% of all attempted online transactions experience friction flagged for suspected fraud risk; **70%** of that friction is unnecessary.[3]

AI-generated phishing is now businesses' **top AI-enabled fraud risk at 53%**, followed by AI-assisted first-party fraud (51%) and document forgery (45%) — the same AI driving record retail traffic is accelerating fraud tooling.

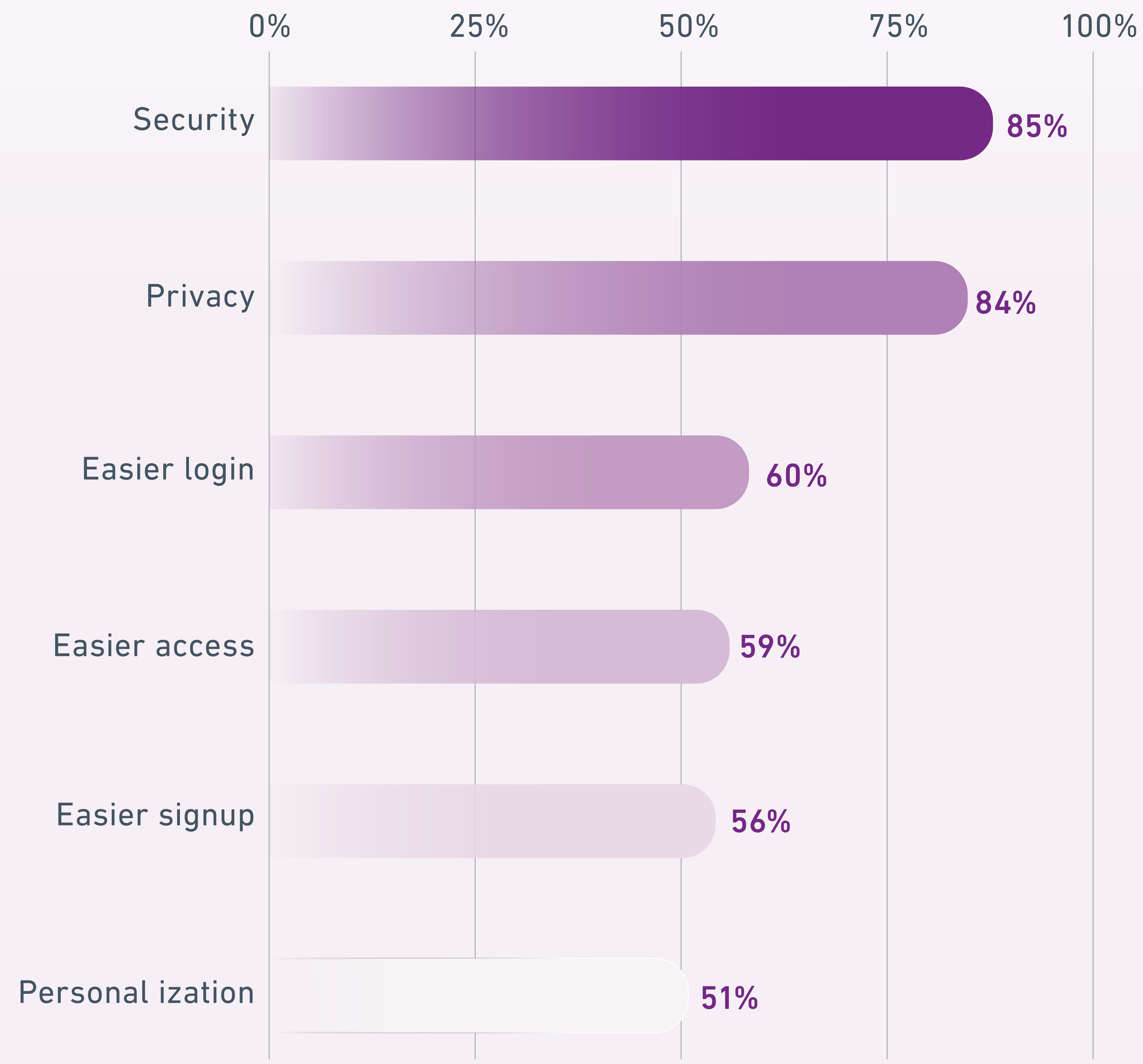
Gen Zers are the most active and least protected consumers

14% of 18–24 year olds report no awareness of scams and are 3x more likely to say they have no fraud concerns than older generations.[4]

Yet **Gen Z is twice as likely as boomers to experience digital security breaches**; nearly 1 in 3 reported having a social media account hacked in the past year.[4]

What builds consumer trust in the online experience – overall importance by dimension

Security and privacy lead by a wide margin. Convenience and personalization matter, but they are downstream of the trust foundation. Building the wrong thing first is why the retail trust gap persists.



Source: Experian 2025 Identity & Fraud Report, MRC October 2025

THE IMPERATIVE

Protect the sale, not just the season

Holiday traffic magnifies every checkout decision. Even small increases in false declines or unnecessary friction can translate into significant lost revenue during peak season. The objective isn't simply stopping more fraud. It's protecting every legitimate sale while minimizing exposure to bad actors.

BEFORE PEAK SEASON

Stress-test before volume hits

- Test authentication and fraud tools against peak-level transaction volume in September
- Review guest checkout performance. As the dominant path (72% usage),[2] any added friction could impact high-intent customers who already chose your store
- Benchmark approval rates and false declines before traffic surges
- Evaluate whether identity signals can confidently recognize trusted customers before introducing step-up authentication

DURING PEAK SEASON

Tune for approval rate

- Approval rate and conversion rate are two sides of the same coin
- Tightening checkout too aggressively against fraud will suppress legitimate sales
- Watch customer friction and abandonment
- Track approval rate weekly from October through January. If approval rate dips materially during peak days, fraud rules are overtightened

CASE STUDY

Smarter Identity Intelligence for Better Outcomes

Experian account ownership verification at a large U.S. retailer

CHALLENGE

A large U.S. retailer sought to improve the online experience, increase conversions and lower operating expenses.

The core question: *How do you approve good customers faster without increasing fraud exposure?*

SOLUTION

Account Ownership Verification's positive identity-match signals were deployed as the basis for an improved auto-approve strategy.

Pilot: A 3-month offline data test was followed by a 1-month live test to calibrate internal models.[5]

THE RESULTS?

$8+ million captured additional monthly revenue from otherwise declined transactions.

10% enhanced online auto approval strategies.

Reduced operating expenses by simplifying backend orchestration.

Reduced consumer friction without increasing risk.

CLOSING THE CAPABILITY GAP

Conversion and fraud protection run on the same infrastructure

The same identity-matching signal that confirms a legitimate customer owns the card they presented is what stops card testing, synthetic identity and bot-driven fraud before they reach the order confirmation screen.

16%

of all attempted online transactions experience friction for suspected fraud risk — 70% of which is unnecessary.

Experian Fraud Management

53%

of businesses cite AI-generated phishing as their leading AI-enabled fraud risk, ahead of AI-assisted first-party fraud (51%), document forgery (45%), bot attacks (40%) and deepfake voice/video (37%/35%).

Experian 2026 Fraud & Identity Report

85%

of consumers are concerned about identity theft when doing business online; 80% are concerned about credit card information being stolen.

Experian 2025 U.S. Identity & Fraud Report

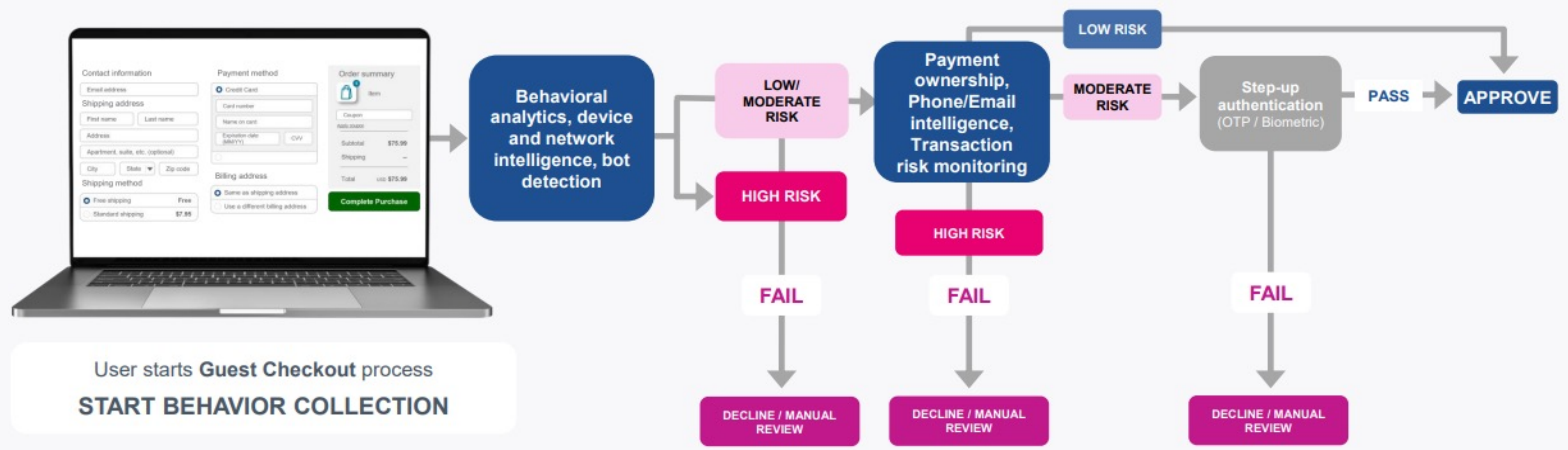
35%

of merchants plan double-digit fraud budget increases; 37% already use behavioral analytics.

Experian 2025 Identity & Fraud Report / MRC

Security without friction — the layered checkout workflow

An example of an effective approach includes running three verification layers sequentially, escalating only when needed. Most legitimate transactions clear at Layer 1 or 2 — never experiencing step-up friction. Fraud gets routed to decline or manual review without adding latency for good customers.



Source: Experian, "Security without friction in the Checkout Workflow," MRC October 2025

The biometrics adoption gap: merchant vs. consumer

76% of consumers trust physical biometrics and 83% trust behavioral biometrics — yet only 29% of merchants prioritize physical biometrics and 37% use behavioral analytics.[2] Consumer readiness for invisible authentication is ahead of merchant deployment. The gap suggests an implementation lag that translates directly into unnecessary step-up friction and false declines.

THE PATH FORWARD

Prioritize by revenue protection and trust-gap closure.

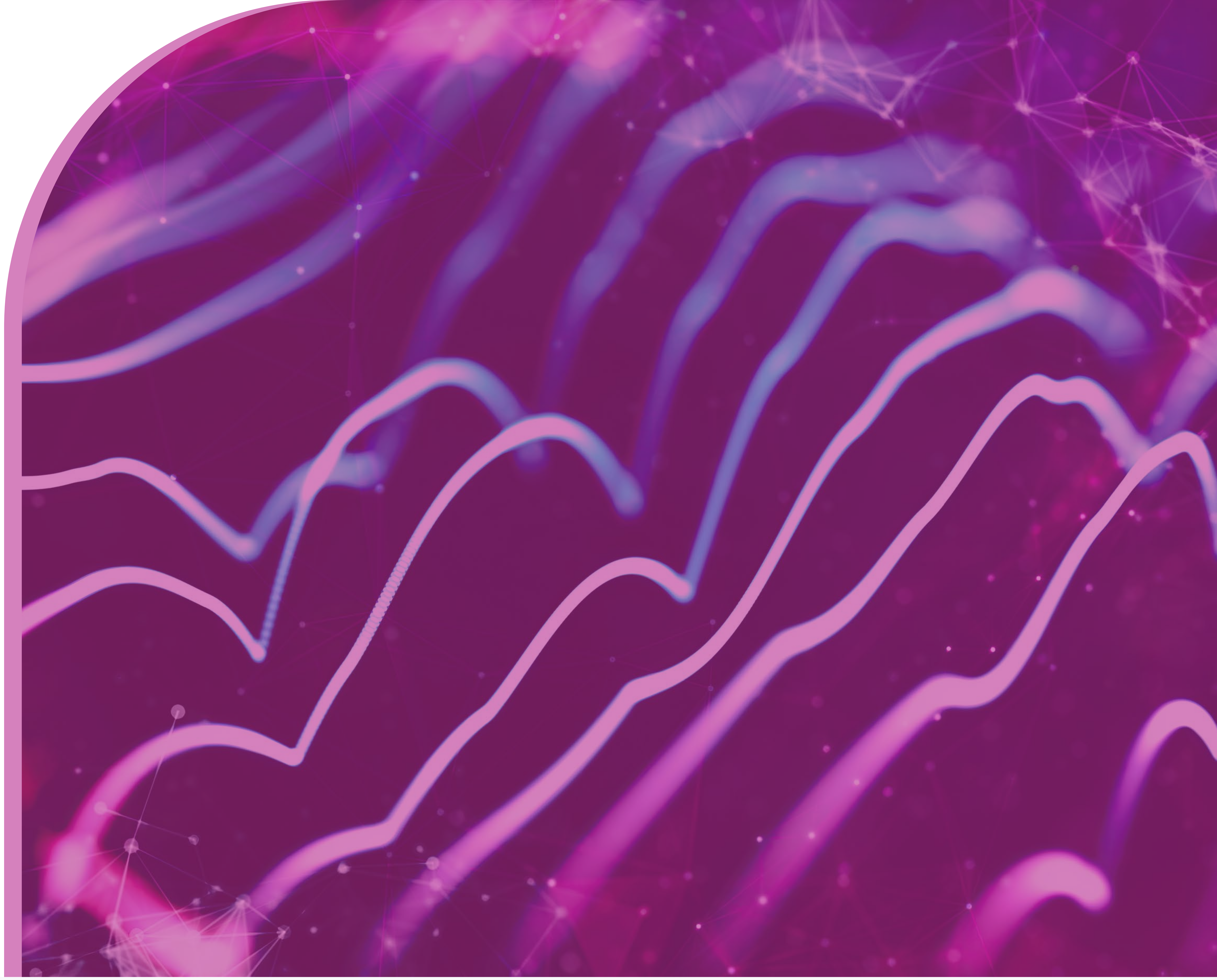
The trust gap is closed through a layered approach that makes security invisible to the consumer. Below are some sample strategies to consider ahead of holiday shopping season.

Initiative	Revenue / trust impact	
Preseason guest checkout and fraud stack stress test	HIGH	This helps prevent false-decline revenue loss at the dominant checkout path.
Card-testing and bot detection tuning	HIGH	This protects inventory and checkout flow from automated fraud that spikes at peak.
Identity verification layer at checkout (Account Ownership Verification or equivalent)	HIGH	This helps reduce false declines and fraud losses.
Behavioral analytics and biometrics deployment	MEDIUM-HIGH	83% of consumers trust this, but it's currently under-deployed (only 37% of merchants); yet it closes the invisible security gap consumers explicitly want.

Let’s talk strategy

The teams that move on this in the next 60 days will be positioned to win wallet share during the highest-spend window of the year. We’d welcome a working session to pressure-test this framework against your specific portfolio data.

Contact us to schedule a strategy conversation



Sources

[1] Adobe Analytics, "Holiday Shopping Season Drove a Record $257.8 Billion Online with Consumers Embracing Generative AI Tools," January 7, 2026

[2] Experian, "2025 Identity and Fraud Trends for Retailers: Payments, Biometrics and Consumer Trust," presented at MRC, October 1, 2025. Includes data from Experian 2025 Identity & Fraud Report (n=2,000+ consumers; 200+ businesses)

[3] Experian Fraud Management, false-decline and transaction friction benchmarks

[4] Deloitte, "2024 Connected Consumer" — Gen Z digital security data

[5] Experian, "Friction-free Festivities: Strategies to Improve Conversion & Reduce False Declines," webinar, September 18, 2024. Includes Experian retailer case study data.

[6] Experian, "U.S. Identity and Fraud Report"

[7] Experian, "2026 U.S. Fraud and Identity Report," April 2026

[8] Experian. Security without friction in the Checkout Workflow," MRC October 2025