Report

Closing the trust gap

Identity and fraud insights for merchants in 2025

Table of **contents**

Closing the trust gap in e-commerce

This inaugural merchant-focused edition of our 2025 U.S. Identity and Fraud Report explores how merchants and retailers are navigating consumers' ongoing demands for trust and privacy. Drawing from the experiences of hundreds of businesses and thousands of consumers, this report focuses on four themes.

1

Payments are dominating in usage and trust

Payment providers continue to lead not just in consumer usage, but in trust — a trend that has held steady across the past four years of Experian's larger identity and fraud research. Peer-to-peer (P2P) payment apps and payment system providers are among the most used and most trusted digital platforms. With 83% of consumers reporting at least some usage, these tools are setting the standard for seamless, secure experiences. Notably, payments were the only category to receive more trust than consumers felt they were owed — a rare signal of overperformance in a skeptical market.

2

There's a trust gap for retailers and marketplaces

Retail apps rank high in consumer engagement and are second only to P2P apps in enhancing the online experience. Yet, when it comes to consumer trust and protection, branded retail sites and e-commerce marketplaces fall short. Consumers expect more from these platforms — especially when it comes to protecting their data and preventing fraud. They aren't confident those expectations are being met and are increasingly choosing guest checkout or abandonment.

3

Digital natives expect and need more protection

Despite being digital natives, 18—24 year olds[1] are the least aware of online scams and the most likely to say they have no concerns about fraud. They're also more likely to prefer guest checkout and less likely to trust traditional authentication methods. For merchants, this generation represents both a risk and an opportunity: businesses that can protect and gain the trust of future consumers without increasing their reliance on PII may see a huge payoff.

4

Consumers want invisible and visible protection

Consumers consistently perceive physical and behavioral biometrics tools as the most secure authentication methods, yet merchants are slow to adopt them.[2] While consumers' understanding of behavioral tools still seems limited, they deliver exactly what they want: invisible, intelligent security. For merchants, especially at guest checkout or during financing, biometrics and behavioral analytics represent a missed opportunity to build trust without adding more friction to the user experience.

[1] The youngest surveyed age was 18, which isn't a complete representation of Gen Z but 18—24 year olds will be used interchangeably with Gen Z in this report.

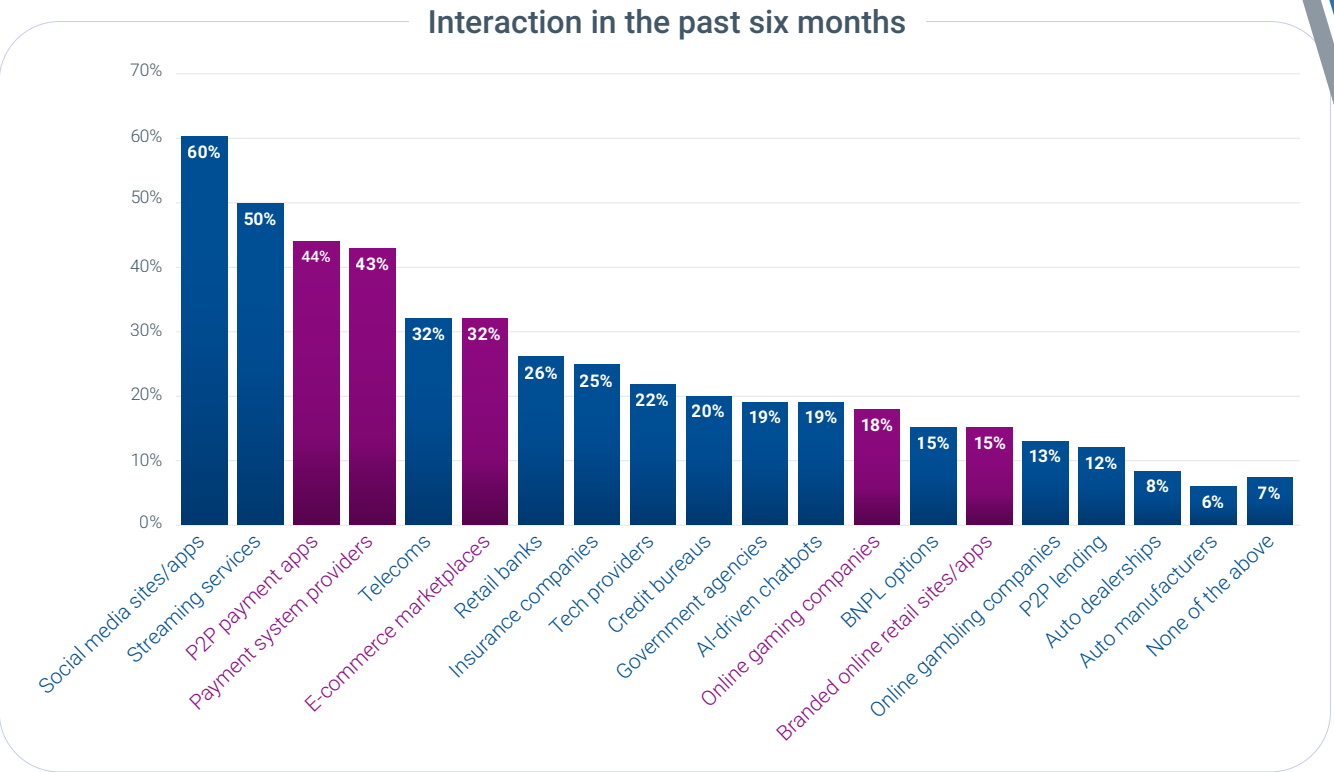
[2] Biometrics were defined for survey respondents as: Physical biometrics are distinctive, measurable characteristics that are used to identify; behavioral biometrics are distinctive, measurable characteristics that are used to identify.

Where are consumers spending their time?

The domination of payments

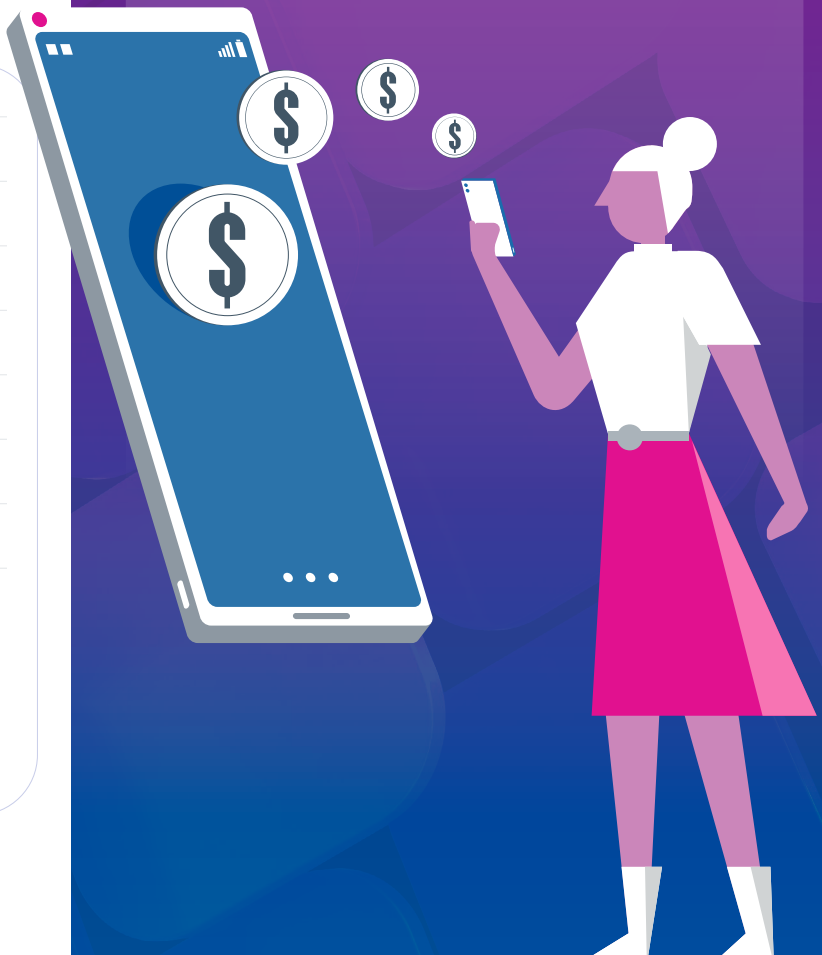
According to our latest consumer research, social media and streaming services continue to dominate online activity, but payments and e-commerce are close behind. While 60% of consumers report using social media in the past six months and 50% report using streaming services, P2P payment apps and payment system providers also rank among the most frequently used services. More than **80% of consumers report some lifetime usage of P2P payment apps and 43% report use in the past six months**.

Table 1: In the past six months, with which of the following types of organizations have you had any interaction online?



80%

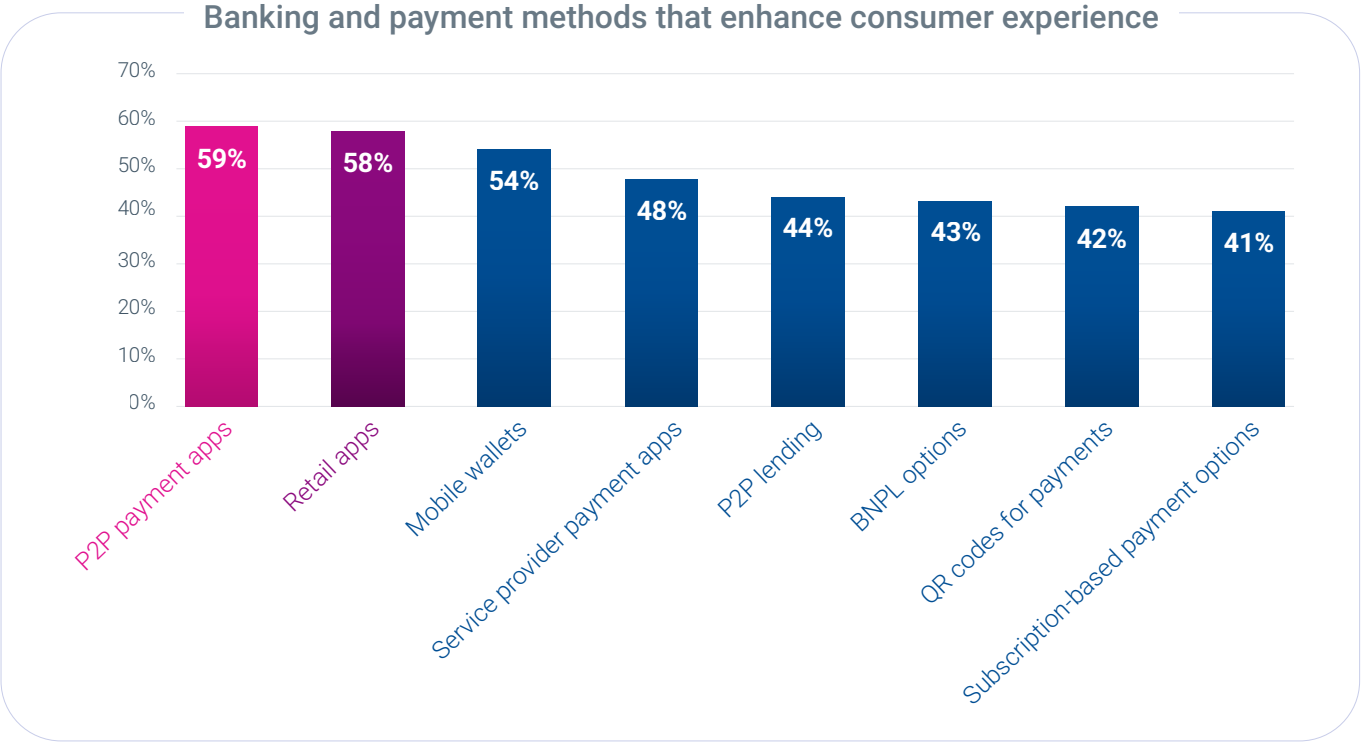
of consumers report some lifetime usage of P2P payment apps and 43% report use in the past six months.



When consumers were asked how important it was for different businesses to protect them online and how much they trusted them to actually do so, **payment providers were the only category to receive more consumer trust than expected in return**.

How did payment providers become as ubiquitous as streaming services? Speed, simplicity and satisfaction. **Consumers ranked P2P apps as the number one contributor to an enhanced online experience** — a signal that real-time payments and seamless interfaces are meeting the rising expectations. But there's more under the surface; it's also about the delicate balance of trust they're retaining. When consumers were asked how important it was for different businesses to protect them online and how much they trusted them to actually do so, payment providers were the only category to receive more consumer trust than expected in return. This is a rare vote of confidence in a landscape where skepticism is rising. In 2024, Experian reported an overall decrease in consumer trust — dropping 10%—20% for all industries (2024 Identity and Fraud Report). Although there was only a slight rebound this year, payment providers continue to remain among the most trusted businesses for the fourth year in a row.

Table 2: How do these banking and payment methods impact your overall experience, if at all?



This enduring trust positions payment platforms as anchors in an increasingly expanded ecosystem. Consumers are more likely to transact with unfamiliar merchants if they use a well-known payment provider — a behavior observed consistently since 2022 (2022 Identity and Fraud report). For merchants, this is a clear signal: payment platforms and payment fintechs have consumer trust and are a lead worth following.

The challenge and opportunity for retail apps

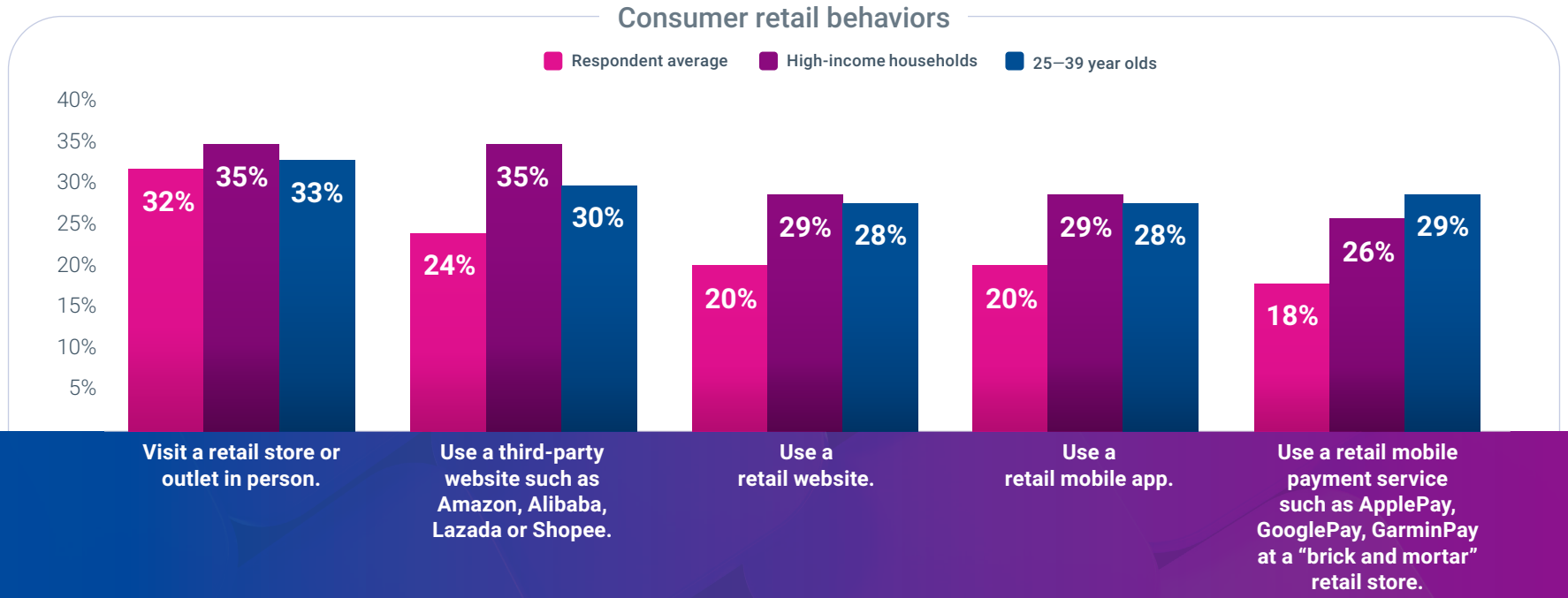
Retail's influence continues to extend beyond clicks. In-person shopping still tops the list of consumer retail activity, with 32% of respondents saying they visit physical stores most often. Yet, digital behaviors are accelerating, especially among high-income households and consumers aged 25—39, who are significantly more likely to use third-party sites, retail websites, mobile apps and mobile payment services.

77% of consumers said they've used a retail app before — second only to P2P payment apps — and ranked them as the **second-highest tool for enhancing the online experience**, cited by 58% of consumers (Table 2). This signals a growing expectation for retailers to deliver not just products, but the personalized, frictionless journeys apps offer.

However, the respondent data suggests retailers may not be meeting the mark. When asked about their recent usage, just 15% reported interacting with branded retail sites/apps — compared to 32% of consumers who reported using e-commerce marketplaces (Table 1). It goes further — e-commerce marketplaces have trained consumers to expect speed, simplicity and confidence. According to the Marketplace Shopping Behavior Report 2025, 63% of consumers prefer e-commerce marketplaces over brand websites. Consumers said they're easy to use (72%), and most consumers trust them to deliver quality (61%).

In a landscape where the same product is available across multiple platforms, merchants will have to invest more aggressively in the user experience that consumers want and are receiving from e-commerce platforms. And they'll need to do so without asking for more information, which consumers are reluctant to give.

Table 3: Which of these retail behaviors do you do regularly (always or the vast majority of the time)?

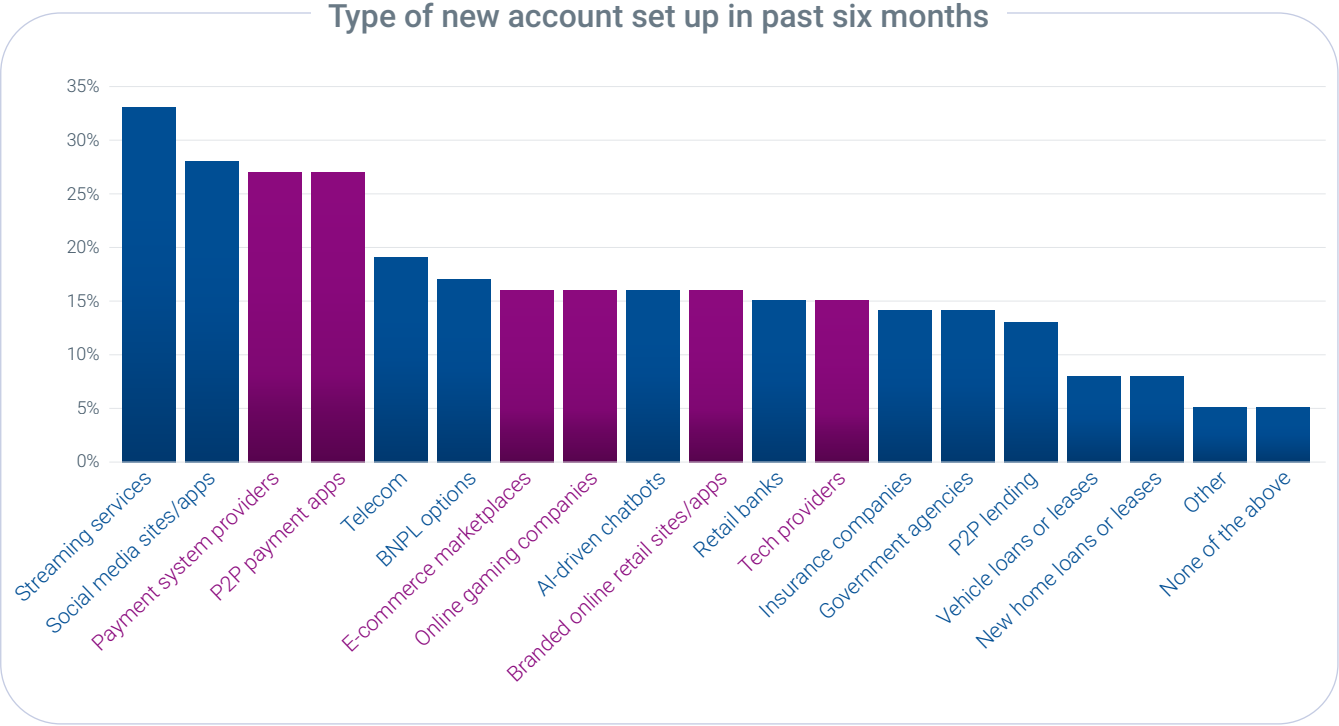


Could guest checkout be winning?

While 40% of consumers say they've opened a new account with a retailer in the past six months, the reality may be more nuanced. Among 18–24 year olds, **20% couldn't recall** whether they had or not — a sign that onboarding is either so seamless it's forgettable or so optional it's being bypassed altogether.

When asked where they had opened a new account, **payment system providers and P2P payment apps** ranked third and fourth respectively, just behind streaming services and social media, and significantly ahead of e-commerce marketplaces, online gaming platforms, branded retail sites, and even traditional institutions like banks, insurers, and government agencies.

Table 4: What type of new account have you set up in the past six months?



40%

of consumers say they've opened a new account with a retailer in the past six months. The reality may be more nuanced.

What about the 46% of respondents who said they hadn't opened an account in six months? While that number drops by age group, it's worth observing that consumers are increasingly choosing not to open accounts at all when possible. Our identity and fraud research has shown consistent abandonment rates during account creation, despite a dip from post-pandemic era expectation levels.

2023

51% considered abandoning; **37%** followed through.

2024

38% cited friction as a reason to abandon; **18%** followed through.

2025

Among high-income earners, **50%** considered abandoning, and among 25—39 year olds, **45%**.

So, what do consumers want? Survey data consistently shows consumers want businesses to recognize them online (65% of U.S. consumers say it's extremely or very important to them in 2025), and 40% say they're very or extremely trusting of businesses that do. While businesses may eagerly interpret this to mean more account openings, it's more likely that consumers just want to be recognized as being genuine and well-intentioned.

In a Capterra survey, **43% of shoppers said they prefer guest checkout**, and **72% of those still use it even when they already have an account**. The reasons are clear: speed, simplicity and privacy. **Shoppers expect checkout to take four minutes or less, and more than half say they'll abandon their cart if asked to reenter payment or shipping details**.

For merchants, this raises a critical question: How do you balance transaction conversion against fraud risks that arise when you know less about the buyer? The answer isn't to force account creation — it's to rethink guest checkout. Tools like accelerated checkout, passive identity verification and behavioral analytics now allow merchants to recognize and assess fraud and identity risks without requiring consumers' login credentials or even PII.

Interestingly, while passwords (82%) and account usernames (67%) were ranked highest overall for delivering a better customer experience, younger consumers disagreed. Gen Zers strongly preferred contact information, likely for its ease of recall. But when asked which methods made them feel most secure, the story flipped: Passwords dropped to 56%, usernames to 46%, and even contact information — favored for convenience — was trusted by just 50% of 18—24 year olds. In place of traditional authentication methods, Gen Zers trusted biometrics and behavior. Ranking highest for the fourth year in a row by the total surveyed group, 76% of consumers felt physical biometrics was the safest and 72% felt behavioral biometrics.

This reflects a broader trend: Trust in traditional methods like passwords, PINs and security questions is eroding, while confidence in biometric authentication continues to rise. For merchants, the message is clear: **consumers want fast, flexible and secure options — and they want to choose how they engage. This is where "optimized anonymity" comes in: giving consumers the privacy they want, while still enabling merchants** to make confident, low-friction decisions.

For merchants, this means:

- **Using biometrics and device intelligence to verify identity invisibly**
- **Leveraging behavioral signals to detect fraud in real time**
- **Offering post-purchase incentives to convert guests into loyal customers**

Guest checkout isn't a threat to building trust with customers — it's a test of your tech stack. And for merchants who get it right, it's a powerful way to win both conversion and confidence. When consumers are faced with the decision whether or not to create an account, it's worth considering that in a landscape where identity is both a security concern and a brand experience, the best onboarding may be the one that doesn't feel like onboarding at all.

What are the new rules of trust?

Consumers are more active online than ever and more concerned about the associated risks. In 2025, 57% of consumers reported a general concern about online activity. **Identity theft (68%) and stolen credit card information (61%) remain the top concerns, far outpacing newer threats like deepfakes or AI-generated fraud (31%)**. This underscores that consumers are struggling to trust online offerings when so many viable threats exist.

Among the most connected generation, Gen Z, awareness of threats remains critically low. Despite their fluency in digital platforms, this group was **3X more likely** to select "none of the above" when asked about online concerns, and **14% reported no awareness of scams at all**, significantly lower than other age groups.

Deloitte's 2024 Connected Consumer survey reinforces this concern, revealing that **Gen Zers are more than twice as likely as boomers** to experience digital security breaches — including hacked social media accounts, identity theft and falling for online scams. Nearly one-third of Gen Z respondents reported having a social media account hacked in the past year. While 85% of consumers overall are taking steps to protect themselves, 75% still feel they should be doing more, and many express a sense of powerlessness — unsure of what actions to take or believing that companies and hackers can access their data regardless.

This vulnerability has real consequences. In 2024, consumers lost over **$12.5 billion to fraud**, across offline and online activities, a record high according to the Federal Trade Commission. And the emotional toll is just as severe: The Identity Theft Resource Center reports that 95% of victims experience emotional distress, including anxiety, shame and depression.

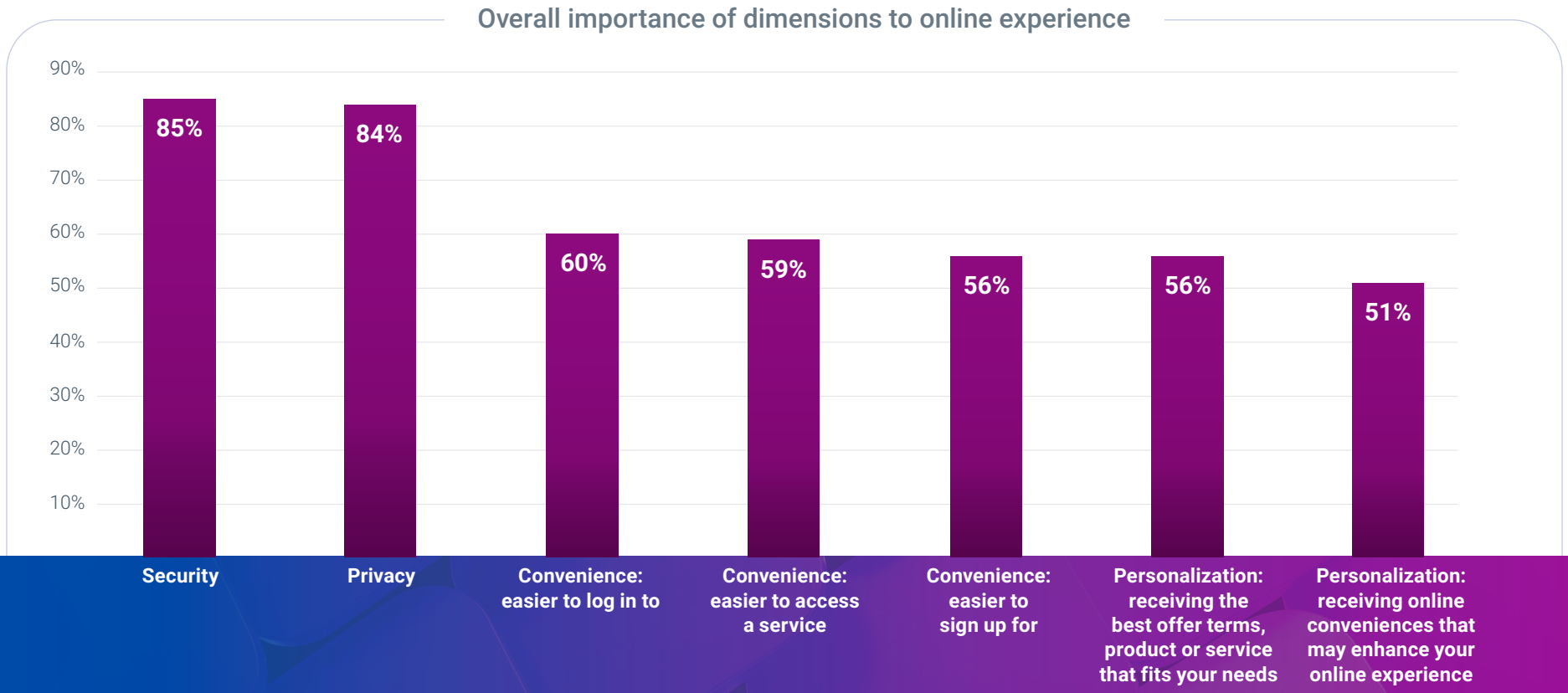
For merchants, this isn't just a technical challenge — it's a **brand imperative**. Fraud prevention must evolve from a backend safeguard to a **frontline promise**, especially for younger consumers who expect seamless experiences but lack the ability to spot threats. They represent the future, and there can't be an assumption that they'll just figure it out. The opportunity lies in proactive education, invisible protections and trust-building technologies that meet Gen Zers where they are: online, mobile and increasingly immersed in GenAI-powered environments. For the merchants that choose to do this work, they'll have tech stacks not only ready for this youngest generation, but the next ones as well.

The question may loom about where to begin. The answer is security and privacy. These two dimensions consistently outrank personalization and convenience as consumer priorities for online experiences. **85% of consumers prioritize security**, and **84% prioritize privacy** (Table 5) — the top answers four years in a row. For businesses, this seems like a catch-22 — how can you provide more security without asking for more information? Consumers provide some insight.

When asked what builds trust, consumers pointed to visible and invisible security measures, proactive fraud alerts, and clear communication about how their data is used. This aligns closely with the security they feel from invisible tools like behavior, which requires no recall or interaction from the user to seamlessly upgrade the security of new accounts and logins.

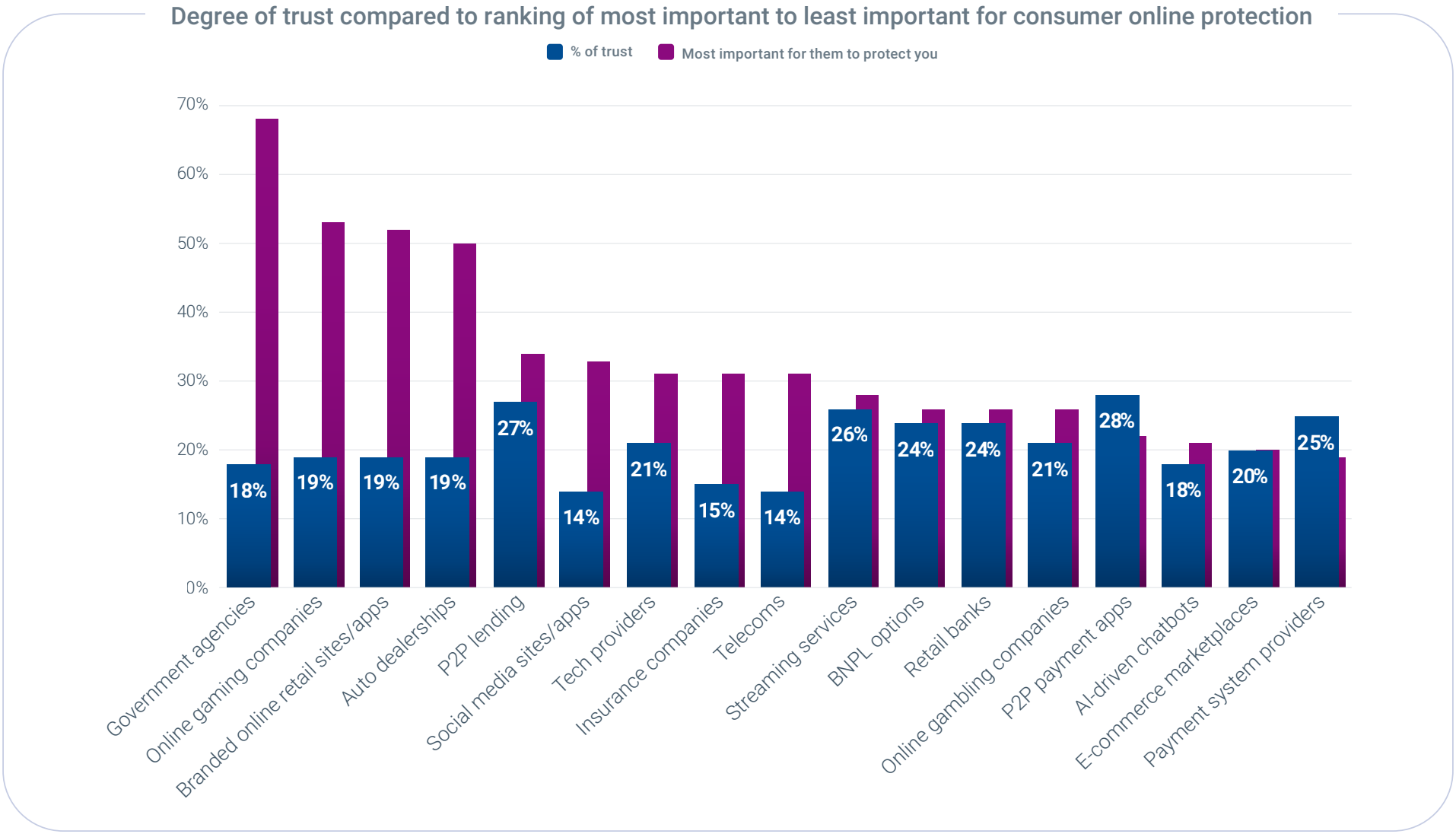
Consumers aren't just concerned — they're holding businesses accountable. **83% of U.S. consumers expect companies to address their security and privacy concerns**, a sentiment that has remained consistently high over the past four years (over 80%). This expectation spans industries and is especially strong among high-income households, who are more likely to reward brands that demonstrate visible and invisible security measures.

Table 5: Which dimensions are most important to your online experience?



But trust and expectations don't always align. When asked to rate their trust in specific businesses to address security and privacy concerns, **P2P payment apps, tied with credit bureaus, received the highest scores at 28%** — the highest among all categories. And while most levels of trust ranged between 18% and 28%, the expectation of protection remains much higher.

Table 6: How many consumers ranked this business as the first or second most important business to protect them online compared to how much consumers trust this industry to protect them online.



The opportunity is to close the gap — between what consumers expect and what they experience — by leading with transparency, control and consistency.

While 68% of consumers view government as either the most or second most critical for online protection, only 18% of consumers trust the government to actually protect them online. That results in a trust gap of 50% — the largest gap among all surveyed industries. How do the other industries stack up?

Payment apps and system providers were the only category to receive more trust than protection expected, boasting a 6% favorable gap. It's worth considering whether consumers use and value payment services because they exceed trust and protection expectations.

E-commerce marketplaces also met expectations square-on — holding at 20% in both categories, which is positive considering they were the fifth most engaged with business type in the past six months.

Meanwhile, **branded retailers and online gaming sites** have some of the widest gaps — over 30%. While businesses have similarly low expectations of protection (less than 20%), consumers ranked them second highest in importance of protection, after government agencies.

Consumers are watching closely, and they reward businesses that listen to their concerns about security and privacy, not just as a liability to be managed, but as an integral part of the relationship to be prioritized. The opportunity is to close the gap — between what consumers expect and what they experience — by leading with transparency, control and consistency.

That means:

- Explaining why data is collected and how it benefits the customer
- Offering user-directed privacy settings and opt-ins
- Demonstrating security through both visible and invisible protections

How are merchants responding?

Merchants are facing intensifying fraud threats, and they're beginning to respond with sharper focus and smarter tools. From account onboarding to post-purchase protection, the business survey data shows a sector under pressure but moving in the right direction.

Account takeover and transactional payment fraud are top concerns, with half of surveyed merchants reporting both as areas of increased stress and investment for 2025. These threats strike at the heart of consumer trust — especially when identity and payment credentials are compromised after an account is created. Merchants also report **the highest rates of new account fraud**, yet it ranks just 15th among their active investments for 2025.

This deprioritization reflects a broader tension explored earlier in the report: consumers want to be recognized, not necessarily registered. Many prefer guest checkout, and most expect speed and simplicity — not added steps. But while friction at sign-up may be unpopular, waiting until post-purchase to verify identity or assess risk can be too late. This is especially true when fraudsters exploit stored payment methods or financing options to bypass traditional safeguards. Protecting account creation is a critical investment — and it doesn't have to be friction-heavy. Invisible, intelligent tools can secure the journey without slowing it down.

Merchants are beginning to embrace this approach. When asked which tools in their fraud stacks they're emphasizing, **50% reported using secondary devices to verify identity** — more than any other vertical. And **35% are using behavior**, 10 percentage points higher than the average (25%). These tools offer frictionless security, helping retailers reduce fraud without compromising speed or simplicity.

Budget increases reflect this shift. All merchant respondents plan to increase their fraud budgets, with the majority targeting 8%–10% growth and **37% planning double-digit increases**. This aligns with their experience: **two-thirds say fraud losses have increased**, more than the overall average. The opportunity is to align more closely with consumer expectations — by investing in tools that protect identity and payment credentials early in the customer journey. Doing so helps reduce downstream impacts from account takeover and transaction fraud, while reinforcing the trust consumers place in businesses that recognize and protect them.

When asked which tools in their fraud stacks they're emphasizing, **50% reported using secondary devices to verify identity** — more than any other vertical. And **35% are using behavior**, 10 percentage points higher than the average (25%).

For report purposes, retailers included digital-only and click-and-mortar businesses that offer high-value products (e.g., TVs or smart appliances) or financing options for customers.

Closing the gap with Experian

Merchants are facing a rapidly evolving fraud landscape. Consumers are demanding more — more security, more transparency and more trust — especially in high-friction moments like guest checkout and financing. The good news? We offer solutions designed to meet these challenges head-on, especially consumers' top and second highest concerns.

Identity theft
68% say it's their top security concern

NeuroID, a part of Experian, provides behavioral analytics that provide a frictionless, invisible layer of protection by analyzing how users interact with digital forms — from typing speed and mouse movement to hesitation and copy/paste behavior. These signals help merchants distinguish between genuine users and fraudsters in real time, without collecting any PII.

By combining behavioral, device and network intelligence, NeuroID enables early detection of third-party fraud, synthetic identities, bots and scams — especially at guest checkout and account opening. Merchants using NeuroID have seen dramatic improvements in fraud detection accuracy, onboarding speed and customer experience — all while reducing manual reviews and identity verification costs.

Stolen credit cards
61% say it's their top security concern

Experian's payment card verification solution is a patented, passive identity verification solution that matches payment card numbers to consumer identity attributes — including name, address, phone and email — without requiring additional input from the user. It's especially powerful for merchants looking to reduce friction at checkout, improve auto-approval strategies and clean up card-on-file portfolios.

It enables merchants to verify whether a consumer truly owns the card they're presenting online — even in guest checkout flows. With real-time API or batch deployment options, it helps reduce false declines, increase conversions and prevent fraud — all while ensuring consumer privacy.

Together, these solutions offer merchants a powerful toolkit for building trust, reducing risk and delivering seamless digital experiences.

Learn more about our e-commerce fraud prevention solutions.