experian

2027

DATA BREACH INDUSTRY FORECAST:

Consumers at Risk

14TH EDITION

Introduction

The cybersecurity industry has spent years preparing for bigger breaches, faster attacks and more sophisticated threat actors. Yet the signals emerging from 2026 suggest that the nature of the challenge is beginning to change.

Data breaches continue to occur at a record pace. The Identity Theft Resource Center (ITRC) recorded 1,803 data compromises in the first half of 2026 alone, impacting more than 471 million victim notices.[1] If current trends continue, 2027 is expected to become another record-setting year for data compromises. Equally concerning is the rise in consumer fraud losses. According to the Federal Trade Commission, consumer fraud losses reached nearly $16 billion in 2025, up sharply from $12.5 billion in 2024 and nearly three times the level reported in 2021.

At the same time, cybercriminals are increasingly leveraging artificial intelligence (AI), organizations are becoming more dependent on third parties and consumers are showing growing signs of breach fatigue and declining trust.

Taken together, these factors are creating a perfect storm and driving a new era of cybersecurity challenges. The next evolution of cybercrime is not just about preventing data breaches. It's about managing the consequences of decades of stolen information already circulating online and determining who's real and who isn't.

We predicted this shift last year in our industry forecast with "More Real Than Real: The Hacker's New Standard," which foreshadowed a future in which hackers could perform unprecedented data harvesting and stitch together enriched identity profiles. We believe this trend may accelerate significantly in 2027. Already, synthetic identity fraud increased eightfold globally in 2025 compared with 2024,[2] according to an industry report. It was the fastest-growing type of fraud tracked in the study.

In our **14th Annual Data Breach Industry Forecast: Consumers at Risk**, we focus on the long-tail consumer impact of security incidents and the growing effects of AI-powered threats. We believe we may be headed toward an information dystopia, where misinformation, disinformation, deepfakes and manipulation make trust increasingly difficult to establish. As the line between what's legitimate and what's fake continues to blur, businesses and consumers alike will face growing uncertainty and anxiety.

As a result of the vast amount of exposed personal information now available, consumers may realistically find themselves confronting a digital twin created in their likeness. Yet we also envision a rebellion of sorts, with consumers fighting back by weaponizing information to confuse and disrupt cybercriminals. The evolving tactics of both the hunter and the hunted could spark a new wave of identity verification methods and technologies, creating a booming market for services designed to prove authenticity and restore trust.

This year's predictions come from Experian's long history of helping companies navigate data breaches over the past 24 years. The following predictions represent what we see on the horizon in the world of data security incidents in 2027 and beyond.

The Data Breach Industry Forecast is Experian's attempt at looking into our crystal ball and providing cybersecurity predictions for what may lie ahead. The predictions aren't guaranteed, shouldn't be relied on as formal advice and are intended for educational purposes only.

01 Proof of being human becomes the hottest new market

The rapid growth of AI is creating a new challenge for organizations. As synthetic content becomes easier to produce and increasingly difficult to distinguish from authentic content, the ability to verify identities, communications and transactions will become more important.

Several converging trends are driving demand for verification. AI can now generate realistic text, images, audio and video at scale. Cybercriminals are using AI to improve social engineering attacks, while organizations are deploying AI across customer service, operations and business processes. As both legitimate and malicious uses of AI increase, distinguishing between authentic and synthetic interactions becomes more difficult.

In the coming years, we predict a majority share of cybersecurity and fraud-prevention investments may shift toward validating whether information, individuals and interactions are genuine. In fact, Juniper Research projects the digital identity verification market will expand from $18.8 billion in 2026 to $29 billion by 2030, a 54.6% increase in just four years.[3]

These may include digital identity systems, passkeys, cryptographic verification tools, liveness detection, behavioral analytics and content provenance technologies. The goal will be not only to prevent fraud but also to establish confidence that identities, communications and transactions are legitimate.

Customer experience, regulatory compliance, fraud prevention and brand reputation will increasingly depend on an organization's ability to prove authenticity. However, consumers may start to become frustrated with new or multiple verification protocols, so this shift has implications beyond cybersecurity. Increased friction may discourage consumers, potentially leading to abandoned applications, enrollments and online purchases.

Organizations that develop strong verification capabilities may gain a competitive advantage as trust becomes a differentiator. Those that can't may find it increasingly difficult to maintain confidence among customers, partners and regulators. But will trust outweigh ease? We predict a bumpy road for the next few years as businesses test new verification methods or increase steps and abandon them when consumer friction arises until an acceptable threshold is found.

TAKEAWAY:

The mantra moving forward is trust no one, verify everyone. Verification will emerge as one of the fastest-growing areas of investment. As synthetic content and AI-enabled impersonation increase, organizations will place greater value on proving authenticity than simply collecting information. The key question will be how much consumer pushback and potential financial fallout organizations are willing to endure in pursuit of greater trust and security.

"AI can create almost anything, so the ability to prove what is real and what is not may become the most valuable form of security. Organizations that can verify authenticity at scale will have a competitive advantage in a world where seeing is no longer believing. This shift is also likely to reshape cyber insurance underwriting standards, placing greater emphasis on controls that establish and verify authenticity."

— **John Farley**
Insurance Broker, Gallagher

02 The rise of the digital doppelgänger

Identity theft is evolving beyond isolated acts of fraud. Cybercriminals now have access to decades of breached information, powerful AI tools and increasingly sophisticated methods for organizing stolen data. As a result, identity crime is becoming more persistent, interconnected and difficult to detect.

Historically, identity theft often involved a discrete event, such as opening a fraudulent credit account, conducting an account takeover or filing a false tax return. Increasingly, however, threat actors are combining multiple data sources and multiple forms of fraud into a continuous process that may persist for years.

The amount of information available to cybercriminals continues to expand. This year, researchers at Cybernews identified a database containing approximately 24 billion records, much of it composed of information previously exposed in other incidents.[4] At the same time, large-scale breaches continued to expose millions of individuals to risk. These developments demonstrate that stolen information is increasingly being aggregated, enriched, repackaged and reused rather than discarded after an initial compromise.

Identity crimes are also becoming more layered and complex. According to the ITRC, more than 1 in 4 victims are now managing multiple identity incidents simultaneously. The report also found that unauthorized device access led to account takeover 87% of the time, while data breach victims experienced new account fraud in 62% of cases where misuse occurred.[5] Rather than isolated events, identity crimes are increasingly evolving into connected chains of compromise that can affect multiple accounts, institutions and aspects of a victim's life.

1 in 4

victims are now managing multiple identity incidents simultaneously.[5]

AI may dramatically accelerate this trend. Criminal organizations can use AI to organize stolen data, identify connections across records and build detailed victim profiles. These profiles may incorporate personal information, financial records, account credentials, behavioral patterns, location history, social media activity and other publicly available information.

As these capabilities mature, cybercriminals may begin maintaining continuously updated digital replicas of individuals. Unlike traditional stolen records that become less valuable over time, these digital twins could be continuously enriched with new information from future breaches, public sources and criminal marketplaces. In effect, criminals may shift from stealing identities to maintaining them.

The doppelgängers could power account takeovers, new account fraud, synthetic identity creation and highly targeted social engineering campaigns. They may also enable threat actors to better impersonate legitimate consumers across multiple channels, creating personalized attacks that are informed by years of data about a victim's habits, relationships, preferences and behaviors. Instead of using stolen information for a single transaction, criminal organizations will be able to leverage it repeatedly across multiple fraud schemes and throughout a victim's lifetime.

The implications for consumers could extend beyond financial fraud. As digital twins become more detailed, they may be capable of generating convincing communications, responding to challenges with accurate personal information and adapting tactics based on previous interactions. Consumers may increasingly face attacks that resemble legitimate interactions from businesses, financial institutions, colleagues, friends and even family members.

Organizations should expect authentication challenges to increase as cybercriminals become more effective at simulating legitimate users. Traditional knowledge-based verification methods may become increasingly unreliable as decades of compromised personal information remain available to threat actors. In some cases, consumers may find themselves competing with highly detailed digital replicas that possess enough information to appear authentic to automated systems.

TAKEAWAY:

Identity theft is evolving into identity coexistence. Years of data breaches have created a growing reservoir of personal information that cybercriminals can use to build increasingly detailed profiles of their victims. As these AI-powered digital twins become more sophisticated, consumers may face a future in which recovering from identity theft is no longer a one-time event but an ongoing battle to prove they're the authentic versions of themselves.

"We are increasingly seeing cyber criminals use AI tools to analyze stolen data and extract more value from it. AI allows them to more quickly identify the most sensitive documents, prioritize the information most likely to create leverage, and intensify pressure on victims in extortion campaigns. It also helps them organize and monetize stolen datasets more efficiently on the dark web and other criminal marketplaces. As a result, AI is making cybercrime not only faster, but also more targeted and more harmful."

— **Adam Soloman**
Partner, Hutton Andrews Kurth LLP

03 Consumers fighting fire with fire

Organizations have encouraged consumers to share more personal information in exchange for convenience, personalization and access to digital services. However, as data breaches continue to expose records at unprecedented levels, some consumers are beginning to question whether protecting their information is enough.

Many consumers already assume some of their personal information has been compromised. This shift may drive a new form of privacy behavior. Rather than simply restricting access to their information, consumers may begin taking deliberate steps to sabotage their data and reduce the value of the data organizations collect about them.

Consumers are already increasingly using privacy-enhancing tools and services. These include alternative email addresses, temporary phone numbers, credit freezes, identity monitoring services and data removal solutions. Looking ahead, however, we expect some consumers to move beyond data minimization and toward intentional data distortion.

This shift could take several forms. Consumers may maintain multiple online personas, provide incomplete or intentionally limited personal information, or use privacy tools that obscure behavioral and demographic characteristics. We've already seen this with services such as Apple's Hide My Email and Proton Mail aliases, which generate unique email addresses for different websites. While these aliases are legitimate, they intentionally obscure a person's primary identity and can make it harder for cybercriminals to correlate activity across sites.

The goal isn't anonymity. It's to reduce the effectiveness of exposed data. As a result, hackers may increasingly collect inaccurate or intentionally misleading information that's of little value for identity theft, account compromise or other forms of fraud.

This creates a potential conflict for organizations. If consumers increasingly provide incomplete, outdated or intentionally distorted information, organizations may face growing challenges related to data quality. Customer analytics, personalization efforts, fraud detection systems and AI models all depend on reliable information.

The long-term implications could be significant. Organizations may discover that collecting large quantities of information is less valuable if the quality and accuracy of that information continue to decline. For consumers, it may be a powerful way to fight fire with fire to thwart hackers and protect themselves.

TAKEAWAY:

Consumers may begin creating synthetic versions of themselves for daily online activity, reserving their real identities for a limited number of trusted interactions. They'll pollute data with disposable email addresses, fake social media profiles, inaccurate demographic information and multiple digital phone numbers, among other data points. Privacy will increasingly become an exercise in controlling, obscuring or limiting true personal information rather than simply protecting it.

04 Breach notifications need a reset

For years, organizations worried about unauthorized access to systems and data. In 2027, the larger challenge may be convincing consumers that a communication is legitimate.

We believe this growing trust crisis will force regulators to rethink how data breach notifications are delivered. Most breach notification laws were created for a world where consumers generally trusted communications from businesses and institutions. That assumption is rapidly disappearing.

Cybersecurity awareness programs have spent decades teaching people to be suspicious. Don't click on unknown links. Don't trust unsolicited callers. Verify requests before acting. Those lessons have been necessary and effective.

The problem is that suspicion may evolve into paralysis. AI is making it increasingly difficult to distinguish legitimate from fraudulent communications.

Consumers already live in a world where phishing emails impersonate trusted organizations, text messages mimic financial institutions and fraudsters spoof phone numbers. Now they also include AI-generated voice clones, personalized video messages, synthetic customer service agents and highly customized outreach built from years of breached data.

The result is a dangerous paradox: Real fraud alerts may appear illegitimate, while fake alerts may appear authentic. This environment is creating what we call trust fatigue. Consumers are receiving so many alerts, warnings, breach notices and security-related messages coupled with the propensity of other types of communications being fake that many are becoming not only desensitized but distrustful.

Consumer confidence in digital communications is already showing signs of erosion. Experian's 2026 U.S. Identity & Fraud Report found that 56% of consumers are very or extremely concerned about AI-enabled scams, while 60% are aware of AI-generated fake media and 53% are aware of AI-generated phishing attacks. As AI impersonation becomes commonplace, consumers may increasingly distrust even legitimate security alerts and breach notifications.

56% of consumers are very or extremely concerned about AI-enabled scams.

As skepticism grows, breach notifications, fraud alerts, password resets and customer-service outreach may increasingly struggle to break through the noise. Organizations will increasingly need to prove authenticity before asking consumers to act.

"In an age of AI-generated deception, the effectiveness of a breach notification letter will depend less on whether it is sent and more on whether it can be trusted. When any message can be faked, consumer trust becomes the first casualty and authenticity becomes the product. Organizations that meet this challenge will not only preserve stakeholder confidence during a crisis, but also demonstrate the resilience that cyber insurers increasingly seek to reward."

— **John Farley**
Insurance Broker, Gallagher

As part of the evolving landscape, we predict that federal and state regulators will be pressured to modernize breach notification requirements. The basic notification model has remained largely unchanged for more than two decades, yet today's threat environment is fundamentally different. Future requirements may emphasize clearer explanations, more actionable guidance and stronger mechanisms for validating authenticity. In an era defined by AI-generated deception, the effectiveness of a breach notification and other warnings may depend less on whether it's sent and more on whether consumers trust it enough to act.

TAKEAWAY:

The most damaging breach of 2027 may be the breach of consumer confidence itself. As consumers become increasingly skeptical of digital communications and overwhelmed by growing volumes of data breach notifications, trust in the existing notification model will continue to decline. This erosion of confidence will place increasing pressure on organizations and regulators to rethink how breach events are communicated, creating momentum for more modern, transparent, actionable and consumer-focused disclosure practices.

"Many breach notification laws in the U.S. are antiquated and have not kept pace with how people actually receive and process information today. The intention behind prescriptive notice requirements was to protect consumers, but in practice, breach notices are often too long, too dense, too technical, and too easy to ignore. They may be opened too late, discarded with routine mail, or read without the recipient understanding the key takeaway and actions to take. Shorter, clearer, and more direct notifications would better equip consumers to respond and protect themselves."

— **Adam Soloman**
Partner, Hutton Andrews Kurth LLP

Experian® Data Breach Resolution

2026 breach landscape by the numbers[6]

* Data reflects H1 2026 industry reporting and trends through July 2026.

- 1,803 data compromises
- 471.2 million victim notices
- ~3,600 projected compromises if current pace continues through year-end

The return of mega-breaches[7]

- 275 million victim notices generated from a single compromise involving the Canvas education platform.
- 58% of all victim notices reported during H1 2026 came from this one event.

Number of compromises by industry*

- Financial services: 387
- Healthcare: 281
- Professional services: significant activity
- Manufacturing: rapid growth
- Education: mega-breach driven

*ITRC highlighted education and manufacturing as sectors experiencing unusually high impact in 2026. Financial services remained the most frequently compromised sector and healthcare remained second.[7]

Emerging risk signals

Manufacturing

- 74 million victim notices and 32 insider threats generated from manufacturing-related incidents in H1 2026.[7]
- 21 malicious insider events tracked, reflecting a sharp increase year over year.[8]

Only 24% of breach notices included information about attack vectors, the lowest rate recorded by the ITRC.[6]

WHAT THIS MEANS FOR ORGANIZATIONS

The first half of 2026 suggests another record-setting year for data compromises. Mega-breaches, insider threats and high-volume notification events continue to expand organizational exposure, increasing the importance of rapid response, customer communication and identity protection services.

Better outcomes unmatched value

Count on Experian Data Breach Resolution for the partnership, solutions and performance to create the best possible outcome. Gain control and confidence with the value that only Experian Partner Solutions can provide.

Let connect about how these insights can help you.

1-866-751-1323

Experian.com/databreach

Breachresponse@experian.com

[1] Identity Theft Resource Center (ITRC), 2026 H1 Data Breach Report, July 2026.
[2] LexisNexis® Risk Solutions' Cybercrime Report
[3] https://www.juniperresearch.com/research/fintech-payments/identity/digital-identity-verification-research-report/
[4] https://cybernews.com/security/24-billion-credentials-data-leak/
[5] Identity Theft Resource Center 2026 Trends in Identity Report (June 2026)
[6] https://www.idtheftcenter.org/podcast/weekly-breach-breakdown-itrc-h1-2026-data-breach-report/
[7] https://www.idtheftcenter.org/post/mega-breaches-malicious-insiders-h1-2026-data-breach-report/
[8] https://www.prnewswire.com/news-releases/itrc-malicious-insiders-surge-as-h1-2026-data-compromises-set-pace-for-record-year-302825633.html