Fingerprint

State of AI Fraud & Privacy Report

AI & privacy regulations are rewriting the fraud playbook: How leading organizations are adapting

SEPTEMBER 2025

Executive Summary

Artificial intelligence has fundamentally transformed the fraud landscape, creating threats that operate at unprecedented scale and sophistication.

At the same time, consumers are becoming more privacy aware, and governments are enacting increasingly stringent privacy regulations, making it more difficult for enterprise organizations to confidently differentiate legitimate users from potential bad actors with high accuracy.

Our comprehensive survey of fraud prevention professionals across payment platforms and banking, fintech, and B2B SaaS sectors reveals that organizations across all industries are grappling with a seismic shift in the threat environment that demands equally transformative defensive strategies.

This report is based on survey data collected by Censuswide on behalf of Fingerprint between August 29 and September 4, 2025. The research surveyed 300+ fraud and risk managers, CTOs, CIOs, CISOs, and product leaders across fintech, financial services, payment platforms, and B2B SaaS organizations in the United States.

Censuswide is a member of ESOMAR, the global association and voice of the data, research, and insights industry, and complies with the MRS code of conduct based on ESOMAR principles. The company specializes in robust, high-quality market research and maintains an extensive network across 65 global markets.

KEY FINDINGS

The research exposes significant variations in preparedness across different types of organizations.

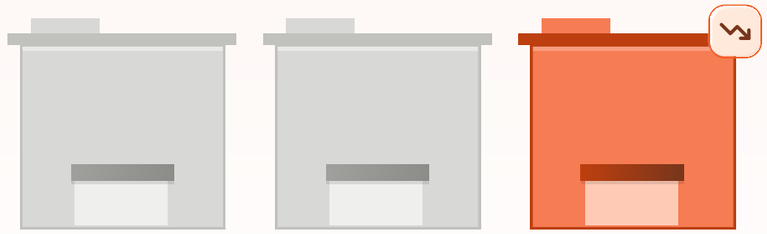
- 41% of fraud attacks targeting organizations are now AI-powered
- Over one-third (34%) of respondents say their organization sees up to $1 million in annual fraud losses from AI-powered attacks
- 93%[1] of fraud teams report noticeable operational impacts from AI-driven threats
- 62% of B2B SaaS respondents indicate their fraud teams spend significantly more time on manual processes due to AI-powered attacks
- Looking ahead, 90%[2] of respondents say their organization is likely to adopt more persistent, privacy-compliant visitor identification methods in the next 12 months

The scale of AI fraud

A threat that transcends industries

ChatGPT. Claude. Gemini. DALL-E.

AI tools are becoming increasingly popular, and easy access to them has created an AI arms race between bad actors — who use the technology to commit fraud at scale — and enterprises finding ways to use the technology for fraud prevention.



41% of attacks targeting organizations are **AI-driven**, and over one-third of organizations reported annual losses of nearly **$1 million.**

Our survey found that this arms race affects all organizations, regardless of size, sector, or geographic location. **The data reveals the stark reality: an average of 41% of attacks targeting surveyed organizations are now AI-driven.**

Additionally, 21% of respondents say they face even higher numbers of AI-driven fraud attempts, suggesting that some sectors or organization types may be disproportionately targeted by these advanced threats.

The financial impact across industries

The financial consequences of this AI-powered fraud epidemic are staggering and universal — 99%[3] of organizations surveyed have experienced measurable fraud losses linked to AI-powered attacks in the past 12 months, **with over one-third of organizations reporting losses up to $1 million.**

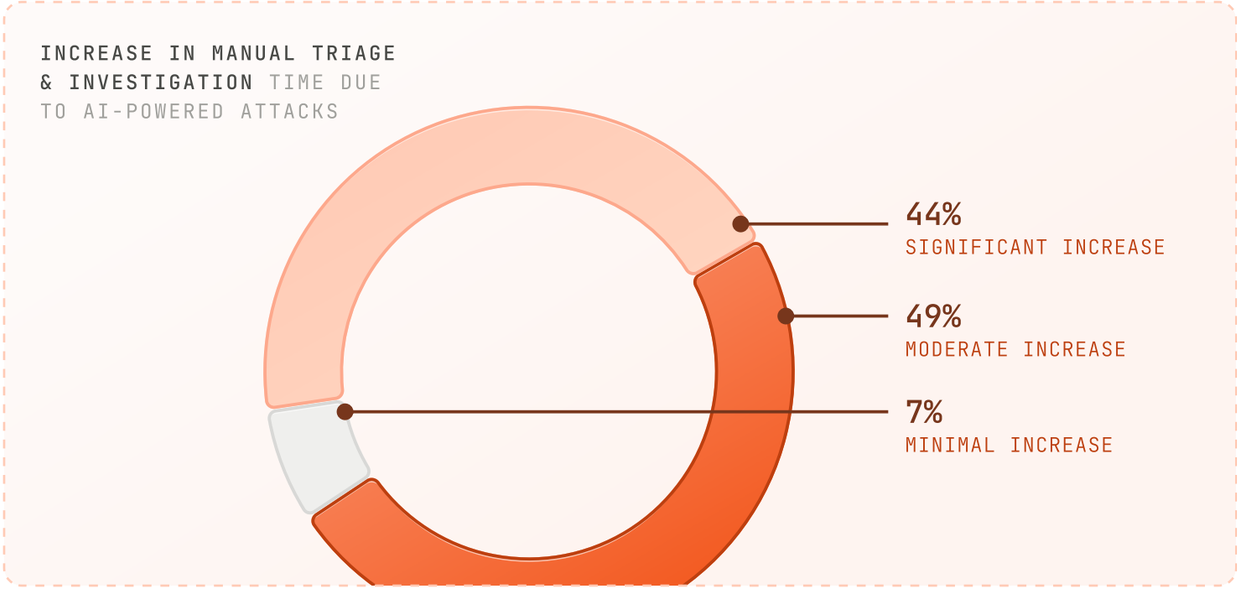
The distribution of losses reveals the broad impact of AI-driven fraud:

- Average loss is $414,000 per organization
- Nearly half (48%) report losses between $100,000-$500,000 annually
- Only 17% report losses under $100,000

Operational strain: The hidden cost

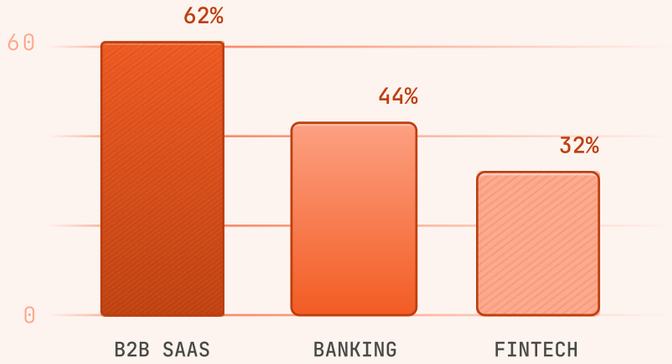
Beyond direct financial losses, AI-powered attacks are forcing fraud teams to spend significantly more time on manual investigation and triage.

Over 44% of respondents report that their teams now spend significantly more time on manual triage and investigation due to AI-powered attacks, while nearly half (49%) describe a moderate increase in investigation time. Only 7% report minimal impact on team workload, indicating that virtually all organizations are feeling operational pressure from this new threat landscape.

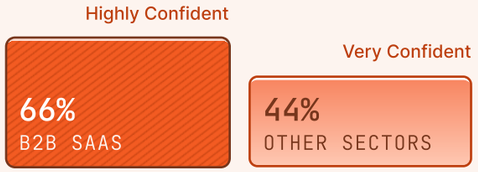


The impact on manual investigations varies by sector, with B2B SaaS organizations reporting the highest operational burden: **62% of B2B SaaS respondents indicate their fraud teams spend significantly more time on manual processes due to AI-powered attacks**, suggesting that software-as-a-service models may be particularly vulnerable to AI-driven fraud schemes.

Percentage of respondents in specific sectors that spend significantly more time on manual processes due to AI-powered attacks



Confidence level in current fraud prevention tools' ability to detect AI-powered attacks across sectors



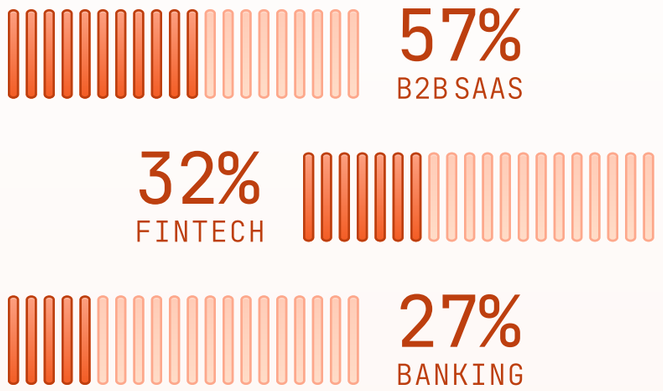
The double-edged sword of privacy technology

As consumers become increasingly privacy-conscious, and as regulations like GDPR and CCPA continue to be updated to provide more protections for consumers, organizations face a fundamental challenge: **How can they maintain effective fraud prevention while respecting user privacy and complying with evolving regulations?**

The research reveals the depth of this challenge. **Over one-quarter (27%) of respondents report that privacy-first technologies severely impact their fraud detection capabilities, while nearly half (49%) describe moderate impacts.** Privacy-focused browsers, VPNs, consumer privacy preferences, and regulatory requirements are collectively creating blind spots that sophisticated fraudsters are learning to exploit.

The impact on user identification is even more pronounced: **40% of respondents indicate that privacy-first technologies are significantly reducing their ability to accurately identify users, while over half (51%) report moderate impacts on identification accuracy.**

SECTORS EXPERIENCING SIGNIFICANT REDUCTION IN DEVICE/BROWSER IDENTIFICATION ACCURACY DUE TO PRIVACY-FIRST TECHNOLOGIES



Sector-specific privacy impacts

The privacy challenge affects different types of organizations in varying ways. B2B SaaS organizations report the most severe impact, with **57% indicating that privacy-first technologies are significantly reducing their identification accuracy**. This suggests that software companies, which often serve privacy-conscious enterprise customers, may be facing the most acute version of this challenge.

Traditional sectors show different patterns of impact, with fintech companies slightly more likely than banking organizations to report significant privacy-related detection limitations (32% vs. 27%). This may reflect differences in legacy system capabilities and regulatory interpretation between established financial institutions and newer technology companies.

Industry variations: Leaders & laggards in the fraud prevention race

Financial services: A tale of two approaches

The survey reveals significant differences between traditional banking institutions and fintech companies that extend beyond simple technology adoption to fundamental strategic approaches.

A higher percentage of respondents (54%) at traditional banks report higher average rates of AI-powered attacks (vs. 47% for fintech organizations), yet they lag significantly in adopting modern detection and prevention technologies.

Only 33% of banking respondents are evaluating AI-powered fraud detection tools, compared to 52% of their fintech counterparts — highlighting greater agility at fintech organizations when it comes to their fraud prevention strategies.

Additionally, fintechs are more likely to rate their fraud prevention as significantly ahead of competitors (38% vs. 25% for traditional banks) and show higher adoption rates of advanced identification technologies.

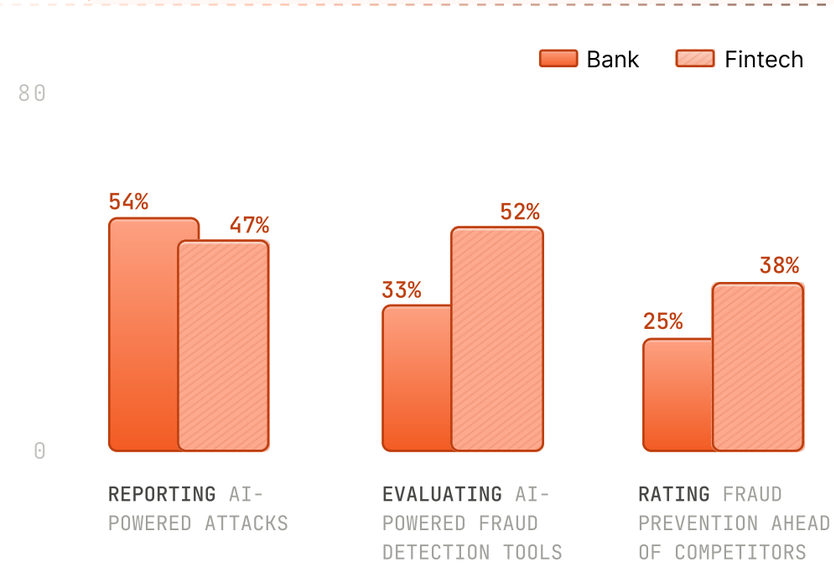
Payment platforms occupy a unique position in the financial services fraud prevention ecosystem, serving as critical infrastructure that must balance innovation, user experience, and account security. The survey reveals that these organizations are taking comprehensive approaches to fraud prevention, with **51% evaluating AI-powered fraud detection tools and an equal percentage hiring specialized fraud prevention talent.** Payment platforms also show strong adoption of device-based identification methods, **with 47% using device intelligence and fingerprinting techniques.**

B2B SaaS: High stakes, high performance

B2B SaaS organizations report the highest operational impact from AI-powered attacks, but also demonstrate some of the most advanced capabilities in fraud detection and prevention.

Two-thirds (66%) of B2B SaaS respondents express high confidence in their current fraud prevention tools' ability to detect AI-powered attacks, compared to the overall average of 44%, who are very confident. They also demonstrate superior device recognition capabilities, with an average recognition rate of 67% compared to 55% across all sectors.

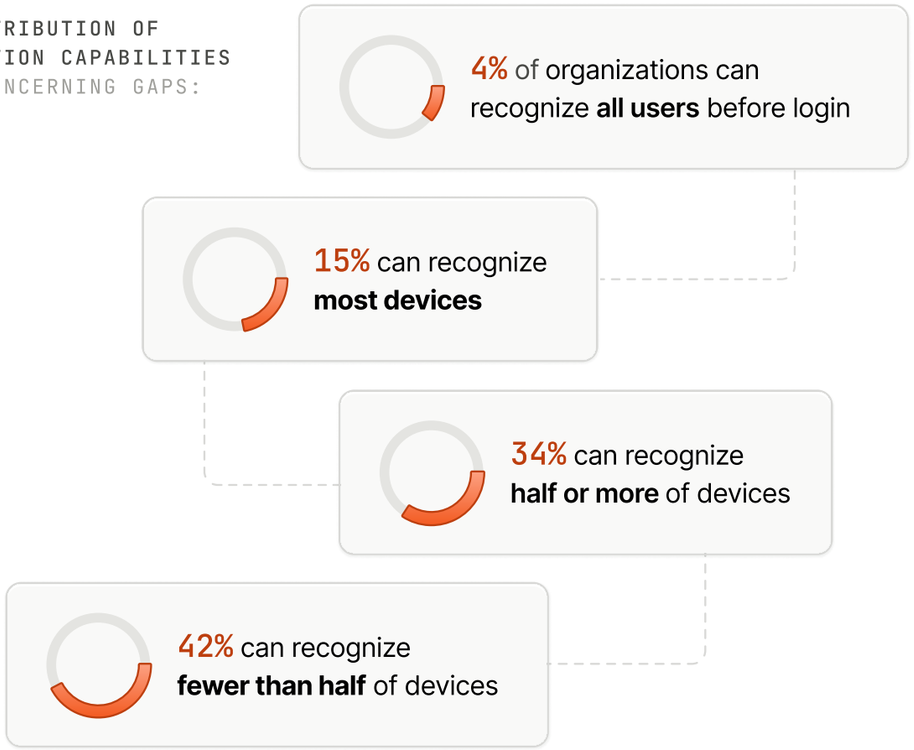
This pattern suggests that B2B SaaS organizations, despite facing significant challenges from both AI-powered attacks and privacy restrictions, are investing heavily in advanced fraud prevention capabilities and achieving measurable results.



The critical role of device intelligence in modern fraud prevention

The survey reveals significant room for improvement in device intelligence capabilities across all industries. On average, organizations can reliably recognize only 55% of unique devices and browsers before login or account creation. This means that nearly half of all user interactions occur with limited visibility into device history and risk factors.

THE **DISTRIBUTION OF RECOGNITION CAPABILITIES** SHOWS CONCERNING GAPS:



The variation across sectors is noteworthy and reflects different levels of investment in device intelligence capabilities. B2B SaaS organizations surveyed demonstrate the highest device/browser recognition rates at 67%, while payment platforms achieve 53%, fintech companies reach 51%, and traditional banking organizations lag at 47%.

The survey also reveals that organizations already recognize device fingerprinting as one of the most important signals for detecting suspicious behavior, ranking it as the top priority alongside geolocation, because it addresses several critical challenges organizations face, including:

Persistence across privacy changes.

Advanced device intelligence providers can persistently identify browsers and devices with high accuracy, even as privacy technologies and regulations evolve.

AI attack resilience.

While AI-powered attacks can increasingly mimic human behavior patterns and manipulate traditional fraud signals, device-level characteristics are more difficult to manipulate convincingly and manipulation often leaves telltale traces.

Pre-authentication protection.

Device intelligence enables organizations to assess risk by recognizing trusted devices before users provide login credentials. This capability is crucial for helping prevent account takeover attempts, credential stuffing attacks, and other types of fraud that exploit credential verification.

Key takeaways: Adapting to AI-powered fraud

Unlike previous threat evolutions that affected specific industries or use cases, AI-powered fraud threatens every organization with an online presence.

The survey data reveals that while awareness of the problem is high, organizational responses have been uneven and often inadequate. The gap between the sophistication of AI-powered attacks and the capabilities of traditional fraud prevention approaches continues to widen.

Device intelligence provides a layer of real-time signals that all organizations can use to proactively fight AI-powered fraud at scale. And as privacy regulations continue to evolve and traditional identification methods become less reliable, device intelligence provides the persistent, privacy-compliant foundation necessary for effective fraud prevention.

As the survey responses show, the cost of inaction extends beyond immediate financial losses to include operational inefficiency, customer friction, and competitive disadvantage. Organizations that recognize the threat of AI-driven fraud and act decisively to modernize their fraud prevention capabilities will be best positioned to protect their assets, serve their customers, and maintain their competitive position.

[1] Combines “Significantly more time spent on manual triage and investigation” and “Moderate increase in investigation time” responses.
[2] Combines “Very likely - actively planning implementation” and “Somewhat likely - under consideration” responses.
[3] Combines “Less than $100k,” “$100K–$500k,” “$501k–$1M,” and “$1.1M+, please specify in millions” responses.

Learn more about how device intelligence can strengthen your fraud prevention strategy against AI-powered threats.