Ping Identity

eBook

The New Rules of Fraud Prevention in the AI Era

How identity-first strategies prevent fraud without impacting CX

Table of Contents

The Reality Facing Leaders Today

AI has fundamentally reshaped fraud. Synthetic identities, deepfakes, and automated attacks are easier to execute, while social engineering is more convincing than ever. **Fragmented identity and fraud tools only widen the gaps** across channels and lines of business.

The rules of fraud prevention have fundamentally changed. Stopping fraud after the fact is no longer enough. Organizations need to break down silos and **move toward an identity-first fraud prevention strategy** that connects signals, policies, and orchestration, while also enabling trusted and low friction access. Legacy approaches cannot keep pace with modern threats or business expectations.

Throw out the old playbook on fraud.

It's time to adjust your fraud prevention mindset, and chart a new path towards trusted digital interactions.

87% of C-suite leaders experienced rising AI-related vulnerabilities last year. [1]

1. Fraud Prevention Starts with the Identity Layer

The Old Way

"Manage fraud with siloed tools and point solutions"

The New Rule

"Use a single identity to connect signals and decisions"

Organizations often focus their fraud prevention efforts at a single touch point, but this reactive approach fails to address the root causes of fraud. Tactics like phishing, credential theft, or new account fraud (NAF) driven by AI-created synthetic identities are often the beginning of a path that leads to financial or data losses down the road. These early-stage attacks allow fraudsters to exploit systems and accounts, setting the stage for significant downstream damage.

Stolen credentials remain a persistent threat, but modern attackers are increasingly exploiting "side doors" within fragmented systems to bypass traditional defenses. SMS OTPs and helpdesks often have weaker protection than the original identity verification check. Once the side door has been opened, fraudsters can cause significant damage. Fortunately, implementing **continuous re-verification from day zero across a unified landscape allows businesses to stop lateral threats before they escalate into a breach**. By adopting an identity-first strategy that treats every human and machine persona as a single, hardened perimeter, you can close those side doors.

Read the full blog post to learn more about how to prevent fraud early.

Case Study

A financial institution reduced fraudulent activity by **5X** using real-time identity verification during account creation. By addressing NAF, they saved over **$600,000** in direct losses within six months and significantly improved customer trust and operational efficiency.

5x
reduction in fraudulent activity

$600,000
saved in six months

According to TransUnion, synthetic businesses lost an estimated **$534 billion** in fraud last year.[2]

2. AI Alone Is Not the Answer

The Old Way

"AI is a 'silver bullet' that can detect and stop all types of fraud on its own"

The New Rule

"AI is only one piece of the digital identity security puzzle"

While AI should serve a key role in your fraud prevention efforts, it should also be part of a multi-layered approach that includes strong verification, authentication, orchestration, risk-aware controls, and adaptive access capabilities. Why? **Fraudsters often exploit human vulnerabilities, such as trust, rather than technical loopholes**. For example, social engineering attacks targeting helpdesks and phishing schemes capitalize on an individual's propensity to trust an email or link, leading to credential theft. These trust-based tactics require multiple capabilities, including, but not limited to, AI.

As fraudsters continue to utilize increasingly-sophisticated AI tools, the need for multi-layered defenses becomes even more evident. A hybrid approach that combines AI with identity verification tools, such as identity verification, adaptive authentication, and secure credentials, offers a more resilient solution that marries assurance and validation.

Read the full blog post for an in-depth look at what AI can and cannot do.

90% of data breaches now exploit the human trust side door to gain access.

The average cost of a social engineering attack is about **$130,000**, with total losses often reaching the **millions**.[3]

3. Friction Must Align with Real-Time Risk

The Old Way

"Apply the same controls to every user, every time"

The New Rule

"Dynamically adjust friction based on real-time risk"

Adding more security measures to the customer journey doesn't automatically lead to better protection. Overloading systems with excessive authentication steps often frustrates customers, makes vulnerabilities even more vulnerable, and complicates fraud detection. Fraudsters only need to exploit a single weak point to gain access, which means trust must be continuously evaluated throughout the customer journey. Adaptive authentication, which adjusts dynamically based on real-time risk signals, balances CX and robust protection.

No single control is effective across every journey, risk level, or interaction, which is why **fraud prevention requires a balanced combination of signals and protections**. By adding real-time threat protection and orchestration to your existing identity ecosystem, you leverage the right tools for the right risk and touchpoint in the customer journey.

Smarter security involves implementing context-aware signals and AI-driven insights that deliver tailored security responses based on risk.

Read the full blog post and discover how to balance risk, trust, and experience.

Over 75% of consumers say security and ease of use are important when interacting with brands online.

54% have stopped using an account or online service due to login frustrations.

Only the Capabilities You Need

You don't need to rip and replace. You need to solve challenges now.

Explore our fraud & identity services

4. Unite IAM & Fraud Teams

The Old Way

"Fraud tools try to solve identity in isolation"

The New Rule

"Pair fraud intelligence with IAM enforcement at the point of access"

Identity and access management (IAM) and fraud prevention are often treated as separate challenges, as evidenced by the fact that IAM and fraud teams are often separate functions in many organizations. This siloed approach creates gaps and fragmented defenses. Collaboration between identity and fraud teams is critical to closing these gaps and building a unified defense against modern threats and AI-powered attacks.

Cross-functional collaboration enhances visibility across the user journey, enabling real-time risk responses and a single view of your identities. By being proactive, you not only prevent financial losses, you build trust with customers by demonstrating a commitment to safeguarding their data.

Read the full blog post to discover how identity and fraud team synergies lead to better results.

Companies worldwide lost on average **7.7%** of their revenue to fraud over the past year, estimated to be about **$534 billion** in losses globally.[4]

48% of IT-decision makers say they are not effectively managing today's security and identity risks.

5. Fraud Protection & CX are One Decision

The Old Way

"Fraud prevention and CX are competing priorities"

The New Rule

"Build trust through consistent, risk-aware access"

No single control is effective across every journey, risk level, or interaction, which is why fraud prevention requires a balanced combination of signals and protections. However, strong protection does not have to come at the expense of your CX. Advanced identity services can quietly detect suspicious patterns and adjust the level of active security checks based on risk, reserving the bad experience for bad actors. **Modern fraud prevention strategies leverage real-time risk assessments and orchestration** to optimize customer journeys and personalization, keeping fraud at bay while maintaining satisfaction.

By integrating stronger assurance capabilities like "Keep Me Signed In" into your existing ecosystem, your business can achieve security that customers don't feel but is highly effective at stopping threats, minimizing frustration, and enhancing trust and loyalty.

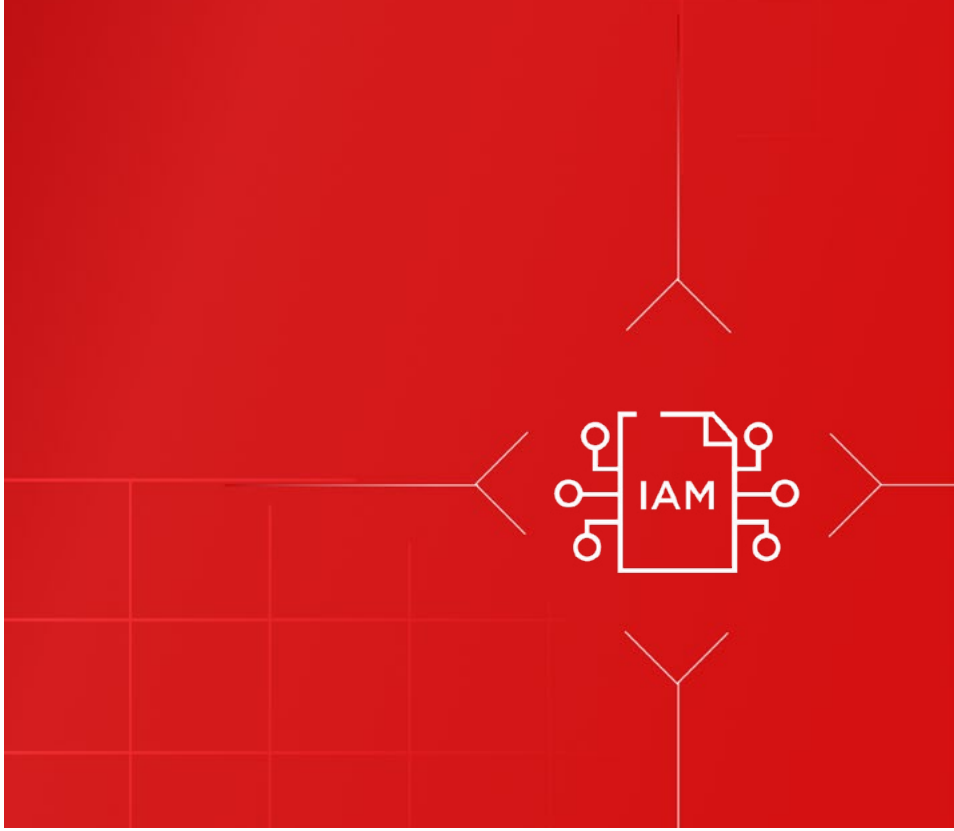
Read the full blog post to explore how identity security can actually enhance CX.

Case Study

A retailer saw a **$20 million** annual revenue uplift from reduced cart abandonment and saved **$5 million** in projected fraud costs by integrating advanced risk mitigation, orchestration, and single sign-on (SSO) across its customer journey.

$20M
uplift in annual revenue

$5M
saved in projected fraud costs



Turning Insights into Action

Here are practical starting points that support near-term wins while setting up long-term success. Rather than trying to overhaul everything at once, successful teams focus on the most impactful areas for their specific organization. Let's look at some of the questions keeping leaders up at night.

"How do we connect fraud signals across tools without replacing everything?"

Action step: Identify where risk, behavior, and authentication signals live today and establish a shared view of which signals should inform fraud decisions across channels.

"How should we actually use AI in fraud prevention today?"

Action step: Use AI to enhance decisioning for strong existing signals, rather than expecting it to compensate for disconnected tools, incomplete data.".

"How do we know when to trust a customer again?"

Action step: Map where customers get stuck in high-risk states today and define clear criteria for stepping trust back down based on behavior, not just time.

"How do we stop authorized fraud before customers approve bad actions?"

Action step: Focus on decision points before money or access changes hands, adding contextual risk evaluation and step-up only when behavior deviates from trusted patterns.

"How do we reduce fraud without adding friction for good customers?"

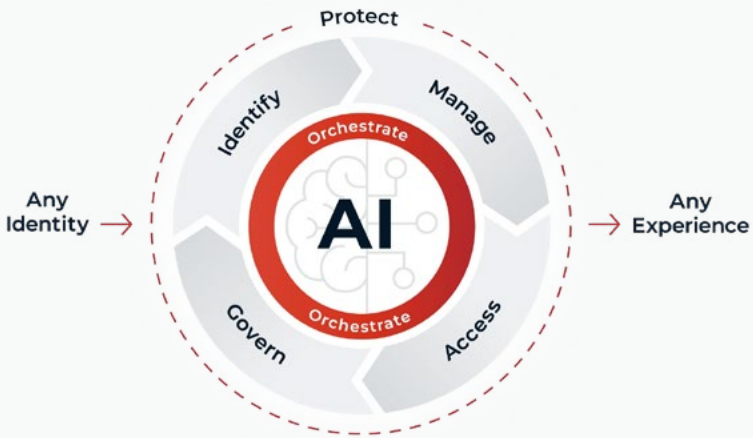
Action step: Review where blanket controls are applied and replace them with adaptive responses that scale friction up or down based on real-time risk.

The Playbook: Continuous Trust is Now Table Stakes

While the rules of fraud prevention are changing, one thing remains constant: identity is foundational to earning and maintaining trust in every digital interaction. Today, generative AI, automated bots, and increasingly sophisticated impersonation attacks are testing that trust, exploiting gaps that traditional, point-in-time identity controls were never designed to address.

To keep pace, organizations must rethink how identity supports fraud prevention. **A trust-focused, intelligence-driven security strategy binds each digital identity to a real person**, ensuring every interaction (from registration to recovery) is explicitly verified. It's critical to find an identity partner that can meet you where you are, whether that's adding capabilities to enhance your existing stack, or moving to an entirely new platform.

Regardless of the approach that fits your organization, **combining orchestration, advanced threat protection, and AI-powered identity services** enables businesses to stop fraud earlier, reduce exposure across the identity journey, and protect customers without adding friction.



Graphic 1: The Ping Identity Platform delivers seamless and secure user experiences without compromise.

Graphic 2: Ping's universal services work seamlessly with existing IdPs. Choose the capabilities your stack is missing, deploy without a rip-and-replace.

Real-World Case Studies

DigiKey Goes Passwordless, Saves Millions

Truckstop Puts The Brakes on Freight Fraud

Security Bank Levels Up Security & CX

More Ping Customer Case Studies

Real Challenges, Real Results

Discover how leading organizations are fighting fraud

Get the eBook

[1] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[2] https://financialit.net/news/cybersecurity/fraud-costs-businesses-nearly-8-their-equivalent-revenues-globally-transunion

[3] https://zerothreat.ai/blog/social-engineering-attack-statistics

[4] https://newsroom.transunion.com/h2-2025-global-fraud-report/

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. We let enterprises remove passwords, prevent fraud, support Zero Trust, and more. That's why more than half of the Fortune 100 choose Ping Identity. Learn more at pingidentity.com.

#4107-A | 02.26 | v04