The New Rules of Fraud Prevention: Keeping Out Fraudsters, Not Customers

How advanced technologies and digital identity are rewriting the book on fraud

EBOOK

Table of Contents

Introduction

Fraud has reached a new evolutionary stage, and if organizations don't adapt, they could be facing extinction. Artificial intelligence (AI) has provided bad actors with a variety of new tools, like synthetic identities and deepfakes, to employ in their schemes, emboldening fraudsters to increase their attacks on businesses and consumers.

To meet these growing and evolving threats, organizations must first understand that the rules of fraud prevention have changed and pivot their strategy in a new direction. The old ways of thinking aren't enough to safeguard enterprises and build customer loyalty in today's digital environment.

It's time to throw out the old playbook on fraud, and focus on the new rules governing the game. Let's explore the antiquated adages that are putting your organization at risk, adjust our fraud prevention mindset, and chart a new path forward towards secure digital interactions and strong customer trust.

The average account takeover (ATO) attack rate increased by 24% YOY in 2024, following a massive 354% increase in 2023.[1]

Chapter 1: Fraud Begins with Identity Crime

The Old Way of Thinking:
"Fraud starts when money is stolen."

The New Rule: "Fraud ends with the transaction; it starts with identity crimes."

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

By targeting these identity crimes at the beginning—during account creation or login—businesses can disrupt fraud before it escalates, reducing financial losses, protecting consumer trust, and minimizing reputational and operational risks. For instance, stopping a fraudster from creating fake accounts with stolen identities ensures subsequent fraudulent activities are prevented altogether. Moreover, addressing identity crimes early improves operational efficiency, as it eliminates the need for costly remediation efforts. Early intervention also strengthens customer relationships, demonstrating a proactive commitment to security.

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

5X
reduction in fraudulent activity

$600,000
saved within six months

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.

According to TransUnion, synthetic identity fraud was up **184%** from 2019 to 2023, making it the fastest growing fraud type.[2]

Chapter 2: Seamless Fraud Prevention Exists

The Old Way of Thinking:
"More security always means added friction."

The New Rule: "You can enhance security without sacrificing CX."

Customers often associate security with cumbersome measures, such as CAPTCHA, repeated multi-factor authentication (MFA) prompts, or lengthy logins. This misconception can lead to hesitancy around implementing additional security layers, as businesses fear alienating customers. However, strong protection does not have to come at the expense of your customer experience (CX). An identity fraud solution 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, keeping fraud at bay while maintaining satisfaction.

By integrating these capabilities, businesses can achieve security that customers don't feel but is highly effective at stopping threats, minimizing frustration, and enhancing trust and loyalty.

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

$20M
uplift in annual revenue

$5M
saved in projected fraud costs

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.

81% of consumers say that ease of use is important when interacting with brands online.

Chapter 3: Smart Security is Adaptive & Balanced

The Old Way of Thinking:
"More is More" or "MFA is Enough"

The New Rule: "The 'right' amount of security measures always depends on the context."

Adding more security measures to the customer journey doesn't automatically lead to better protection. Overloading systems with excessive authentication steps often frustrates customers, increases vulnerabilities, and complicates fraud detection. Fraudsters only need to exploit a single weak point, no matter how many layers exist. Adaptive security, which adjusts dynamically based on real-time risk signals, balances CX and robust protection.

MFA is an essential component of modern security, but is not sufficient on its own. Social engineering, session hijacking, and other advanced fraud tactics can bypass MFA. By layering adaptive MFA with policy-based access control (PBAC), dynamic session behavior monitoring, and fine-grained access control, businesses can address these vulnerabilities more effectively and reduce their reliance on static security measures.

Smarter security involves implementing context-aware tools that deliver tailored security responses based on risk. These strategies ensure a seamless yet secure experience, blending simplicity and security.

Dive Deeper: Read the full blog post and discover how to achieve balance with adaptive, smarter security.

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.

Own Your Identity Strategy

Let's discuss your challenges and objectives.

Talk with an IAM expert today

Chapter 4: Identity & Fraud Teams Must Unite

The Old Way of Thinking:
"Identity and fraud are distinct."

The New Rule: "Identity and fraud are two sides of the same coin."

Identity management and fraud prevention are often treated as separate challenges, as evidenced by the fact that identity and access management (IAM) and fraud teams are often separate functions in many organizations. This siloed approach creates gaps that fraudsters exploit by leveraging stolen credentials, synthetic identities, and automated bots to bypass fragmented defenses. Collaboration between identity and fraud teams is critical to closing these gaps and building a unified defense against modern threats.

Unified platforms and cross-functional collaboration enhance visibility across the user journey, enabling real-time risk responses. This proactive approach not only prevents financial losses, but also builds trust with customers by demonstrating a commitment to safeguarding their data.

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

Fraud scams and bank fraud schemes resulted in over $485 billion in losses globally in 2023.[3]

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

Chapter 5: AI Alone Isn't the Answer

The Old Way of Thinking:
"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 puzzle."

While AI is a powerful tool in fraud prevention, it should be part of a layered approach that includes best practices and other proven fraud prevention tools. Fraudsters often exploit human vulnerabilities, such as trust, rather than technical loopholes. For example, phishing schemes capitalize on an individual's propensity to trust an email or link, leading to credential theft that no AI alone can prevent. Moreover, fraud tactics continuously evolve, requiring ongoing monitoring and updates to AI systems. Even with cutting-edge models, human error and social engineering tactics can bypass sophisticated algorithms.

As fraudsters employ AI for deepfakes and synthetic identities, the need for multi-layered defenses becomes evident. A hybrid approach that combines AI with traditional identity verification tools, such as behavioral biometrics, liveness detection, and dynamic workflows, offers a more resilient solution. AI is a key player in the fight against fraud but must be part of a broader, integrated defense framework to achieve comprehensive protection.

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

41% of IT-decision makers expect cybercriminals' use of AI to significantly increase identity threats over the next year.

AI could enable fraud losses to reach $40 billion by 2027.[4]

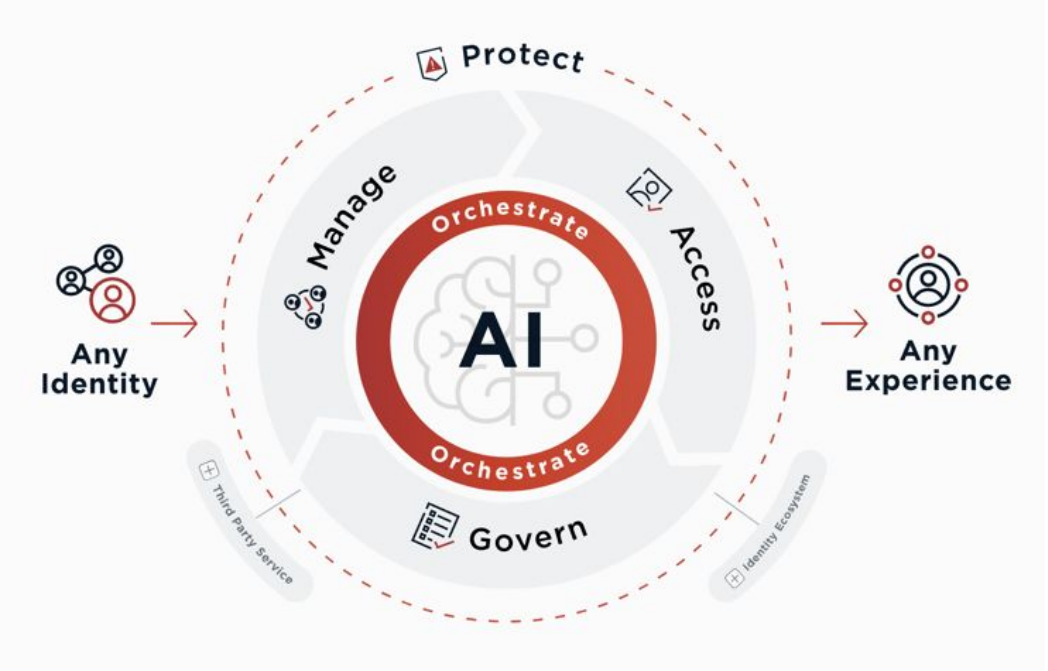
Chapter 6: Navigating the New Rules with Modern IAM

While fraud prevention has a new set of rules, one thing has remained the same: Identity plays a key role in helping your customers trust every digital moment with your brand.

However, new technologies like generative AI and automated bots threaten to undermine this trust, putting both businesses and consumers at risk. It's time to throw out the old ways of thinking and use these new rules of fraud prevention to inform your IAM strategy.

With a unified, intelligence-driven platform, you can foster confidence and equip yourself with the agility to counter ever-evolving and growing fraud threats. Capabilities like advanced threat protection, orchestration, and AI-powered identity services enable organizations to stop fraud early, regardless of its sophistication.

As cyber criminals find new ways to attack, identity acts as a critical defense, empowering businesses to protect customers while cultivating trust and loyalty in today's digital-first economy.



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

Chapter 7: Hear From the Experts

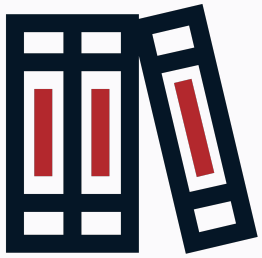
2024 Gartner® Magic Quadrant™ for Access Management

2025 Gartner® Critical Capabilities for Access Management

The Forrester Wave™: Customer Identity and Access Management Solutions, Q4 2024

2024 KuppingerCole Leadership Compass: Passwordless for Enterprise

2024 KuppingerCole Leadership Compass: CIAM



Level Up Your Identity Game

Discover how leading organizations are fighting fraud.

Get the eBook

#4107 | 02.25 | v02

1. https://sift.com/index-reports-account-takeover-fraud-q3-2024?aliId=eyJpIjoiU3OxV1BmVFZ5aXFKcjh2WSIsInQiOiJXRUxtbDFycXdjTVdndERJcVd3VndRPT0ifQ%25253D%25253D
2. https://www.transunionafrica.com/content/dam/transunion/roa/business/documents/fraud-trends/reports/Zambia-2024-Omnichannel-Fraud-Report.pdf
3. https://bankingjournal.aba.com/2024/01/nasdaq-finds-scams-ed-to-486-billion-in-losses-in-2023/
4. https://www2.deloitte.com/us/en/insights/industry/financial-services/financial-services-industry-predictions/2024/deepfake-banking-fraud-risk-on-the-rise.html