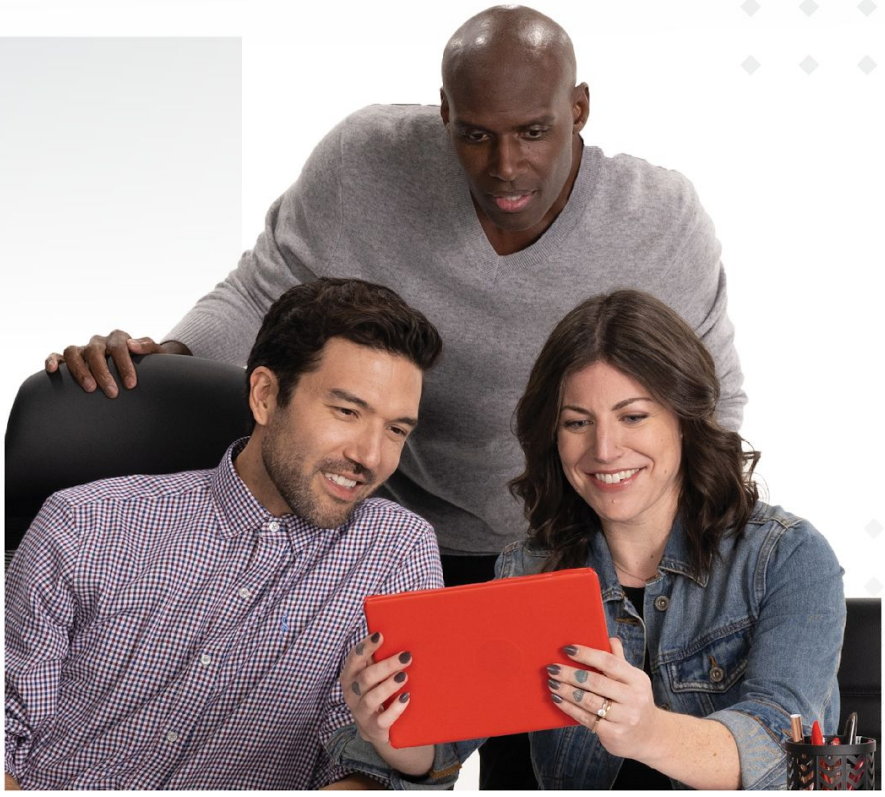
The Ultimate Guide to Online Fraud Prevention

How to Choose a Customer Identity and Access Management Solution that Supports Your Most Critical Business Objectives



GUIDE

Table of Contents

Introduction

The COVID-19 pandemic has accelerated the shift to online across industries, and criminals are taking advantage of this shift to attack vulnerable individuals and businesses. Account takeover attacks are up 131%[1], and even with prevention measures in place, the typical organization loses 5%[2] of its revenue to fraud every year. Because fraud losses can rapidly get out of hand, fraud prevention is a critical part of any organization's business strategy. However, increased security measures often result in poor customer experiences that lead to high session abandonment rates and lost revenue. This can lead to conflict between fraud teams and other parts of the business, resulting in unsatisfying trade-offs between security and experience.

Fortunately, it doesn't have to be this way. In an ideal scenario, fraud prevention is invisible, adding no friction to the vast majority of user sessions while still effectively protecting the organization from fraudsters and only using friction commensurate to the threat level. To do this, fraud prevention must be integrated fully into the broader customer journey. Fraud tools can work together with identity tools to effectively determine whether users are real, or criminals, and take targeted action.

How do you get fraud prevention right?
Read on to gain a deeper understanding of:

- The changing fraud landscape and its impact on your counter-fraud strategy
- The multi-step fraud prevention process and the various tools available for your counter-fraud toolbox
- The relationship between fraud prevention and the customer experience
- The path to a dynamic counter-fraud strategy

1. https://resources.sift.com/ebook/q3-2022-digital-trust-safety-index-account-takeover-data-trends-and-insights/he%20median%20loss.
2. https://legacy.acfe.com/report-to-the-nations/2022/

How Do Fraudsters Commit Fraud?

Cybercriminals are not a homogenous group. The word “fraudster” brings to mind the image of a shadowy figure in a hoodie hunched menacingly over a screen, but that may not necessarily be the case. Fraudsters vary widely in age and live in every country. Many work alone, but many others work in “fraud rings” and for large, well-funded criminal organizations. Some of these criminals choose to work entirely online, while others are charismatic con-artists who charm information out of victims by posing as legitimate service providers, then use that information to access accounts. And of course, plenty of these bad actors make use of technology to greatly increase the scope and reach of their attacks.

Fraudster Tactics

Account Takeover
Account takeover is a form of online identity theft in which a cybercriminal illegally gains unauthorized access to an account belonging to someone else. Once the fraudster has used the stolen credentials to log into an account, they may do one of several things. The most straightforward and obvious option is to use the payment method on file to make a purchase. However, there are several other actions the fraudster might take, all of which ultimately lead to a financial loss for the account holder, the business, and/or even an unrelated third party.

A cybercriminal may begin by changing notifications and/or shipping information. The criminal might then use the card on file to make a purchase, or they may simply log into an account in good standing to make a purchase via other stolen payment credentials. In some cases, a purchase may not be involved at all – account takeover may be a path to stealing reward points or even personal and/or payment information from the account, which they can then use to perpetrate fraud elsewhere.

New Account Fraud
New account fraud may be perpetrated by a human fraudster, but it is more likely to include using bots to automate the creation of fraudulent user accounts. Sometimes, these new accounts will use synthetic identities instead of stolen, legitimate identities. These new accounts are sometimes used for checkout fraud with stolen credentials but also to:

- generate spam
- spread misinformation or malware
- abuse signup bonuses
- influence the results of reviews and voting processes

Social Engineering
Social engineering scams may not originate on an e-commerce website directly, but they can still lead to significant fraud losses. Social engineering refers to the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The scammer may convince a legitimate user to complete transactions that are actually against their best interests.

One of the biggest challenges in stopping social engineering lies in the fact that **these scams lead legitimate users to take actions that will lead to financial losses**. When a user falls prey to a phishing scam, identifying fraudulent activity becomes very difficult until long after the transaction is complete.

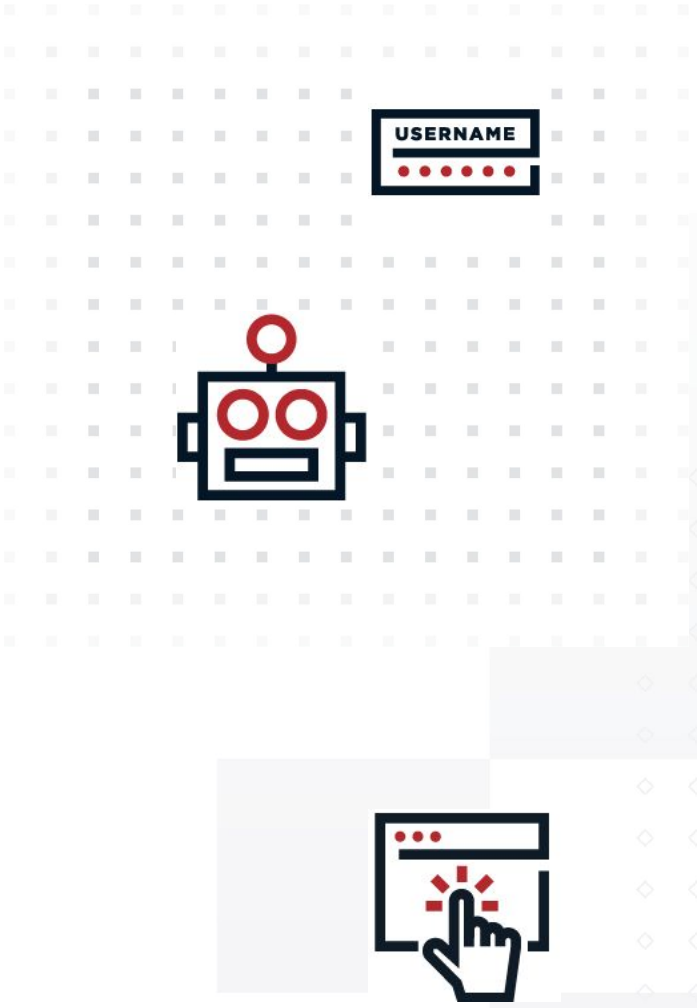
Fraudster Tools

BOTs and Emulators
Bots may be involved in any of the attack vectors outlined above, but they are especially handy for tedious attack vectors like testing stolen credentials or committing brute force password attacks, which are attempts to discover a password by systematically trying every possible combination of letters, numbers, and symbols until chancing upon one that works. Bots are also efficient at perpetrating new account fraud at scale. A bot attack is the use of automated web requests to manipulate, defraud, or disrupt a website, an application, an API, or end-users. Bot attacks started out as simple spamming operations and have branched into complex, multinational criminal enterprises with their own economies and infrastructures.

Bots are particularly insidious because they are so easy to program and deploy. Even someone who isn't overly technical can watch an online tutorial or download a file to create and modify their own bot. It shouldn't be surprising, then, that **bad bots make up over 30%[3] of internet traffic**.

Bot attacks are often carried out using emulators, which are programs that disguise a device to resemble another device. For example, after acquiring a user's device ID and bank account information, a fraudster can use an emulator to make their desktop appear to be the user's mobile phone. The fraudster can then intercept the MFA verification sent to the user's phone to access the user's account and transfer money to the fraudster's bank drop.

Malware and Ransomware
In certain cases of social engineering, an unwitting user may be tricked into activating some form of malware (short for "malicious software"), which is a file or code, typically delivered over a network from a phishing scam that infects, explores, steals, or conducts virtually any behavior an attacker wants. This may include ransomware, which is a form of malware designed to encrypt files on a device, rendering files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.



3. https://securitytoday.com/articles/2023/05/17/report-47-percent-of-internet-traffic-is-from-bots.aspx#:~:text=Imperva%20Inc.,increase%20over%20the%20previous%20year.

The Cost of Fraud

Why is fraud such an expensive line item? The problem lies in the fact that fraud resolution is time-consuming and costly, especially in cases where a fraudulent transaction is discovered after the fact. In 2023, global cybercrime damage costs will exceed $8 trillion dollars[4].

How to Prevent Fraud

Fraud prevention is a complex, multi-step process involving a variety of tactics and tools. Fraud teams build tailored counter-fraud strategies that broadly aim to do several things: detect fraudulent activity across the digital estate, automate decisioning to respond to the signals coming out of detection tools, initiate remediation measures, and collect information about fraudulent activity in order to improve their defensive posture.

Fraud Detection

Fraud detection is the signal phase in which digital interactions are evaluated for fraud risk. Traditional detection methods focus on the transaction, but modern fraud detection tools can begin scanning sessions much earlier. The information gathered in the fraud detection phase forms the foundation for an effective counter-fraud response. There are many kinds of fraud and risk signals that an organization may collect, and most organizations opt for a layered approach to detection to ensure that fewer fraudulent sessions slip through the cracks. This means deploying multiple detection tools simultaneously to measure different things at different points throughout the session.

Use Case: Large-scale U.S. Wireless Carrier and Retailer

A company offering wireless services and internet for customers, businesses, and government agencies came to Ping looking for a solution that would improve security and make it easier for their authorized resellers and employees to conduct business.

Client Challenges:

- ✘ No control over the types of devices and networks that resellers use
- ✘ MFA fatigue was beginning to compromise both security and experience
- ✘ Loss of productivity and sales due to repeated MFA prompts
- ✘ Increased e-commerce fraud, especially around the busy holiday season

Ping Solution:

- Fraud Detection: PingOne Protect
- Deployed fraud solution to learn our traffic patterns and behaviors, then implemented risk-based authentication to prompt MFA only in high-risk situations
- Fine-tuned PingOne Protect risk policies to step up MFA on anonymous networks
- Expanded threat insights by integrating logs with security tools, like Splunk

Final Results:

- Implementation took 3 months and covered 30 PingFederate policies, 200+ connections; the success rate was high with only 2 applications failing
- Reduced MFA prompts from multiple times per day to one time per week
- Decreased fraud activity without creating extra friction for trusted connections/internal employees
- Prompted additional security measures for anonymous and suspicious networks

4. https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

Decisioning

Decision-making or decisioning tools are used to aggregate the signals from the detection phase and consolidate them down to a decision based on the perceived risk of the session and/or activity. These decisions are based on fraud thresholds and logic defined by internal fraud teams and enforced by authorization tools.

Historically, many fraud teams have developed and built decisioning tools internally based on their specific requirements, but these homegrown tools are often difficult to keep up to date as new fraud detection methods come on board. The decisioning phase becomes more complex as organizations must scan for fraud throughout the user journey and may choose to initiate mitigation at different points throughout the session – for example, not only at the point of transaction but also when viewing saved personal information, changing profile information, and changing user settings.

In order to set up automated, effective decisioning, fraud teams must define the logic that determines the risk levels that will trigger mitigation. This logic is housed in the decisioning tool, which should be set up to collect and analyze all sources of risk signals.

Use Case: Retail & Commercial Bank

A European bank came to Ping Identity hoping to improve their counter-fraud measures aimed at stopping social engineering scams.

Client Challenges:

- ✘ End customers vulnerable to scams and social engineering
- ✘ Legitimate customers passed biometric checks but authorized transactions under coercion
- ✘ Fraud team deluged by cases and challenged to mitigate threats in a timely manner
- ✘ Customers losing trust and loyalty after falling victim to scams

Ping Solution:

- Decisioning: PingOne Authorize
- Risk assessment based on multiple detection tools feeding into dynamic authorization decisions
- Mitigation: Customers pushed down different paths based on risk level

Final Results:

- Identified where users were vulnerable to scams and adjusted the user experience to minimize risk
- Caught and prevented a £10k scam within 12 hours of go-live
- Greatly reduced the number of fraud cases that require manual review

Mitigation

Fraud mitigation can come in several forms. Ultimately, any action undertaken to hinder a potentially fraudulent outcome can be considered mitigation. Mitigation may include killing a session, identity verification, or simply stepping up MFA to gain more assurance about a user's identity.

Unfortunately, mitigation measures run the risk of impacting the user experience. Deploying too many counter-fraud tools may make legitimate users perceive that they are being treated like criminals. That is why numerous signals (detection), brought together with unifying fraud logic (decisioning) that then leads to one of many actions to stop fraud (mitigation), creates the best balance between fraud prevention and the user experience.

In order to lessen the impact of fraud mitigation on the user experience, fraud prevention tools need to be integrated with other tools that also shape the user journey: authentication and access management tools as well as identity proofing and affirmation tools.

Use Case: U.S. National Bank

A major financial institution came to Ping with a major fraudulent account creation problem. They had no available mechanism to verify user identity or detect bots.

Client Challenges:

- ✘ Bots and fraudsters were successfully creating "ghost accounts"
- ✘ The registration experience was insecure and undesirable
- ✘ Manual verification calls were driving up operational costs and were not scalable
- ✘ The company's true cost of fraud was $4 per $1 of every fraudulent activity

Ping Solution:

- Bot detection: PingOne Protect; Identity verification: PingOne Verify; Orchestration: PingOne DaVinci
- Implemented risk evaluation for non-human and anomalous activity
- Orchestrated verification checks for large-balance personal loans

Final Results:

- In one month, Ping checked >$775,000 in loan value, preventing $400,000 in fraudulent loads, saving the business $1.6 million.
- Extrapolated to one year, that's saving $19.2 million in fraud costs.
- Prior to implementing identity verification, the call center was making on average over 300+ outbound verification calls a month to validate member wire transfer requests. After verification, outbound call volume was reduced by 100%, saving the call center ~37 hours/month.
- Future savings from implementing similar measures for more use cases.

Counter-Fraud Tools

As fraudsters advance their methods and fine-tune their approaches, fraud teams are racing to keep up. Manual review isn't enough anymore, so digital fraud management tools proliferate. These tools generally fall into one of several categories, broadly aligning to one or more of the steps of the fraud prevention process outlined above.

Payment Fraud Protection

Company losses from payment fraud are expected to increase even further as shopping continues to shift to the online environment. Automated payment fraud protection tools can help improve fraud detection accuracy and decrease the need for workers to address issues manually. Features such as address verification service (AVS) help companies detect suspicious payment activity when the billing address entered does not match the billing address the bank has on file for the card. AVS is often used in conjunction with other tools, such as CVV codes. Payment fraud protection tools incorporate features such as risk rules, risk scoring, real-time monitoring, and velocity checking to detect and block fraudulent purchasing activity.

Behavioral Biometrics

As fraudsters become increasingly sophisticated, traditional security measures such as PINs are less effective. Behavioral biometrics are an increasingly popular tool to differentiate between humans and bots or between authorized and unauthorized human users. Whereas physical biometrics capture unchanging human features such as fingerprints, behavioral biometrics measure interactive human gestures. For example, the way we hold our phones, our scroll patterns, and our keystroke pressure and speed are micro-gestures that are unique to each of us. Digital tools are starting to use these biometric data to flag fraudulent activity when a specific customer's behavior does not match their previous behavior on a website or their behavior resembles that of a bot.

BOT Detection & Management

Many bots are designed to cause harm, but not all bots are bad. For example, Google uses good bots to index and rank webpages on Google search results. Bot detection and management tools aim to distinguish between good and bad bots and to determine which ones can access a website. This capability is critical: As important as it is to block bad bots, it is also important to allow good bots in order to ensure a website's visibility and relevance. Bot detection and management tools distinguish between human, good bot, and bad bot visitors and use machine learning and threat intelligence to detect fraudulent activity. These tools are effective in preventing bad bots from activities such as credit card fraud, inventory hoarding, and credential stuffing.

Device ID

Device identification focuses on devices rather than users. Information such as a device's type, IP address, local time zone, and browser language forms a "fingerprint" for the device and can help companies detect fraud. For example, if one specific device is linked to five different accounts attempting to make purchases on a website, device ID tools register potential fraudulent activity. Some advantages of using device ID tools are that they do not require personal user data, and they can block returning fraudsters based on a device they tried to use previously.

Identity Proofing and Affirmation Tools

In the past, online identity was confirmed with usernames, email addresses, and passwords. Now, these measures are insufficient. Depending on the nature of their business, companies today must use different identity proofing tools to ensure that a user's claimed identity matches their actual identity. One component of identity proofing tools is the rapid scanning of a user's historical transaction data gathered from public and private sources. This is known as knowledge-based authentication (KBA) and is often seen as an antiquated method that adds too much friction. More modern methods include evaluation of a user's physical features. Some companies use manual checks, such as having a user present a passport or driver's license over their computer camera. Other companies use facial biometric tools, taking a picture of a user's face over their computer camera to verify their identity.

Payment Orchestration Tools

Companies use payment orchestration tools for routing and validating transactions and securing the payment process with multiple payment providers. By orchestrating a complex transaction process in one hub, these tools help prevent digital threats from penetrating different parts of the transaction process. Payment orchestration platforms collect and share data that can help companies add points of friction for potential fraudsters while offering a smooth transaction process for authorized users. Payment orchestration tools are particularly helpful for preventing chargeback or transaction fraud.

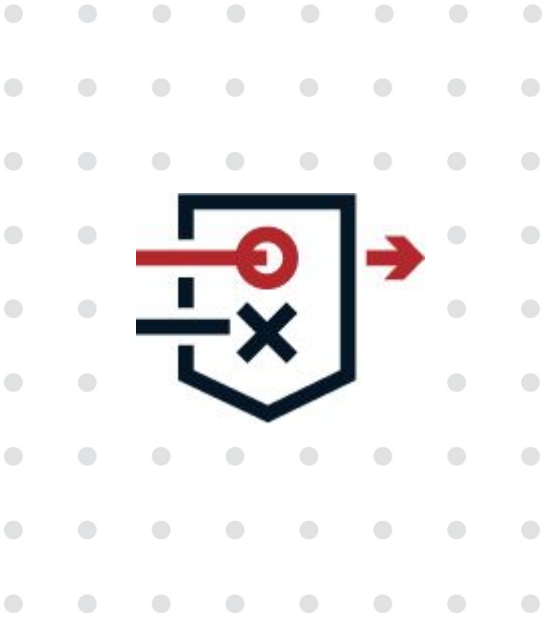
Authorization Tools

After a company authenticates users, it then gives users different levels of access within its website. Authorization tools grant or deny users permission using settings and parameters set by security teams and using access tokens. Some tools focus only on authorization, while others combine authentication and authorization features. By using authorization tools, companies establish an infrastructure that determines the access and permissions of both outside users and internal company members.

Dynamic authorization tools – also known as attributed-based access control (ABAC) or externalized authorization management (EAM) – go well beyond traditional authorization tools by giving businesses the ability to evaluate any data set and enforce policy-based decisions on which actions are allowed based on that data.

Fraud & Financial Crime Hubs

Fraud and financial crime hubs – sometimes called decisioning hubs – are used to simplify and automate the decisioning process. These are often authorization tools with some orchestration capabilities. The goal of these tools is to simplify fraud management by centralizing fraud logic and decisioning. The greatest benefit of these tools is their promise to greatly reduce the need for manual review.



The Role of Fraud & Risk Teams

With the increase in e-commerce and the accompanying increase in online fraud, it is harder for most companies to monitor and prevent fraud manually without the help of automated tools. However, some companies rely exclusively on human teams for fraud detection and prevention. This decision is often based on the idea that human workers can more accurately identify fraud and decrease the rate of false detection by examining each case individually. These workers use their company-specific knowledge to tailor the company's fraud-prevention approach to the unique company context. Nonetheless, there are downsides to employing a team specifically for fraud prevention: It is costly for businesses; the demands posed on these teams may vary significantly between sales-peak and sales-dip periods; and humans may take longer than automated tools to detect and prevent fraud, thus frustrating customers.

Most organizations tend to take an approach of partial automation, with fraud and risk teams performing some manual reviews but also focusing on broader fraud-prevention strategies based on data from automated tools.

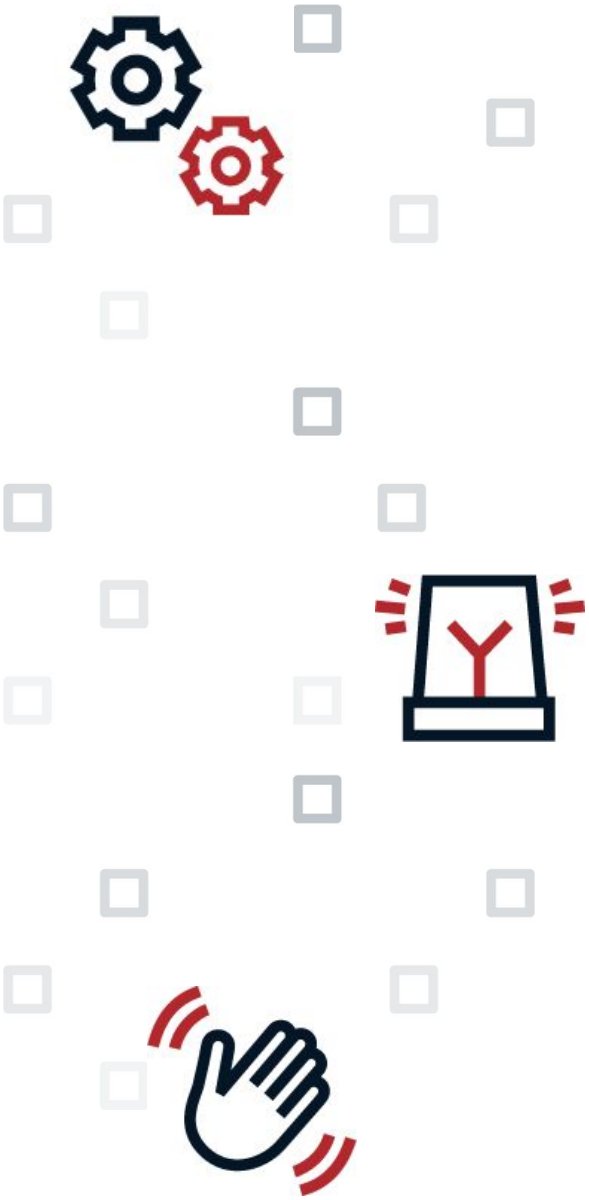
A Note on Identity Teams

While fraud teams often operated in a silo in the past, this is beginning to change. With the advent of new technologies in fraud detection, identity proofing, and access management, identity teams can now work together with fraud teams to the benefit of the broader organization. As the focus of fraud prevention shifts from protecting the transaction to protecting the end-to-end user journey, integrating identity and fraud tools into seamless and secure user flows can help both teams meet their metrics.

The Additive Nature of Fraud Prevention

Because methods for fraud are so sophisticated and rapidly evolving, counter-fraud measures must constantly adapt. This can be frustrating for companies that devote substantial effort to deciding on, developing, and implementing a counter-fraud strategy. Instead of emphasizing the use of specific tools and technologies, a counter-fraud strategy should focus on general principles for counter-fraud measures, such as determining the financial and human resources to devote to counter-fraud. Additionally, companies should adopt new counter-fraud technologies to enhance – not replace – previous ones. Taking an additive approach to counter-fraud can both improve the effectiveness of these measures and optimize companies' resource investment in cybersecurity.

Building a Case for Integration: Fraud Prevention and the Broader Customer Journey



The Cost of Poor Customer Experience

Fraud teams aren't traditionally responsible for customer experience metrics, and yet they must think about the impact of their efforts on the customer experience nonetheless. Why?

The customer experience is the main competitive differentiator in industries such as e-commerce, and even in financial services and banking, where customers expect to encounter higher levels of security and friction, **a poor user experience can lead your customers to seek out competitors who make online interactions easier**.

In fact, many fraud teams find their requests to implement additional fraud prevention tools blocked by executives who fear that the negative impacts of additional security checks will increase session abandonment and ultimately drive customers away.

The State Of Customer Experience

Your customers want a better experience than they're getting today.

55% of people say a company sharing their personal data without permission is more likely than any other scenario (even a data breach) to deter them from using that brand's products.[1]

Only 1 in 10 customers strongly agree that most brands meet expectations for **a good experience.**[2]

One in three consumers (32%) say they will walk away from a brand they love after just **one bad experience.**[3]

63% of customers often abandon a brand for another when the online experience is poor.[5]

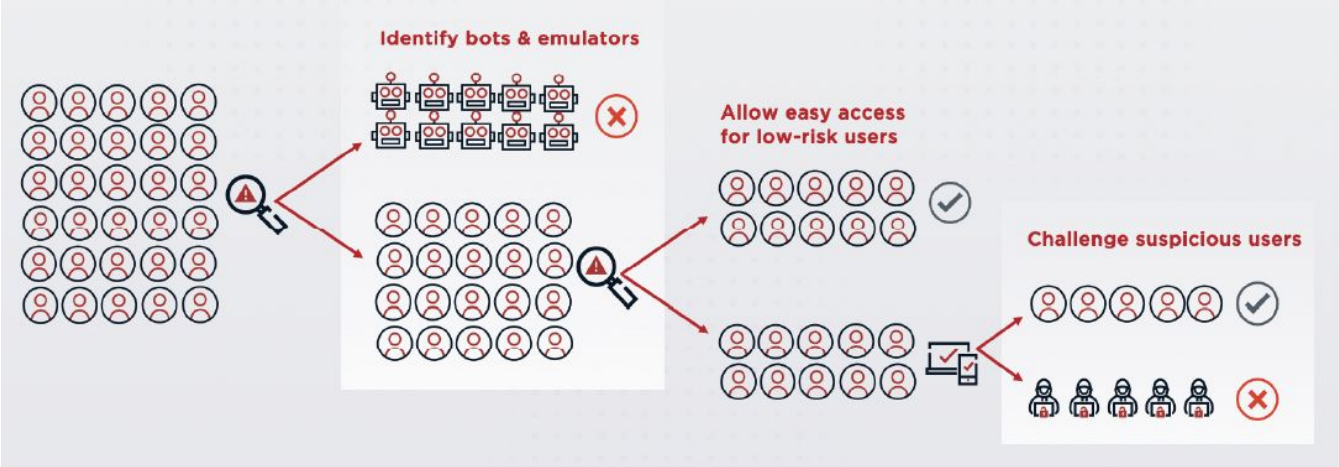
93% of consumers agree it's important that every interaction they have with a brand is excellent.[6]

68% of customers feel their experience with brands online needs to be made easier.[4]

1 2019 Consumer Survey: Trust and Accountability in the Era of Data Misuse, Ping Identity.
2 Deliver the CX They Expect: Customer Experience Trends Report, Acquia.
3 Experience is everything: Here's how to get it right, PwC.
4 Deliver the CX They Expect: Customer Experience Trends Report, Acquia.
5 2019 Consumer Pulse Survey, Accenture.
6 Ibid.

Security vs. Seamlessness: Finding a Balance

Customers value security, convenience, and privacy. There is no perfect formula that will work for every organization, but taking an integrated approach to fraud prevention and customer identity can help strike the right balance. The trick is to evaluate user sessions for fraud continuously and introduce friction by initiating mitigation only when it's needed.

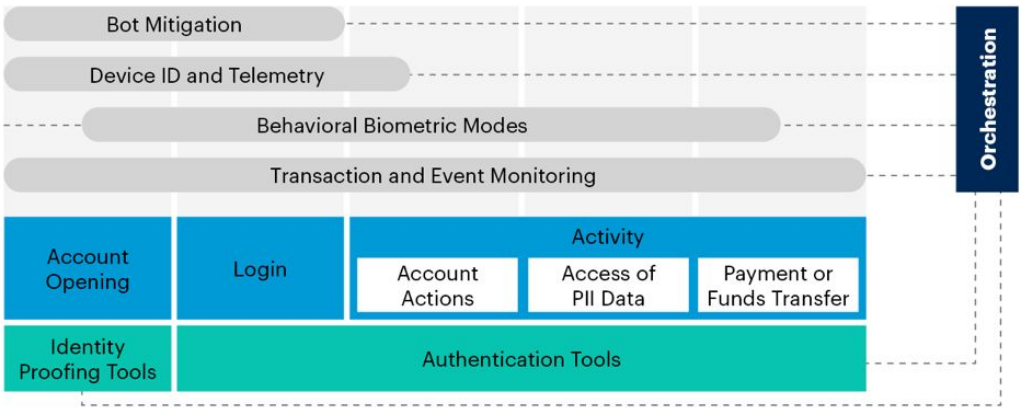


Bringing the Right Tools Together

The customer journey is at the center of everything your organization does, and fraud prevention plays an important part. Standalone fraud detection tools are not effective if the information they collect isn't being incorporated into the broader user journey. Fraud and identity teams can and should work together to orchestrate customer journeys centered around trust. As per a Gartner® report:

> The lines are blurring between online fraud detection, identity proofing and user authentication use cases. The boundaries between protecting events such as as registration, login or payment are disappearing, as instead, vendors increasingly focus on preventing fraud across the digital customer journey.
>
> – Gartner, Market Guide for Online Fraud Detection, Akif Khan & Dan Ayoub, 12/12/2022

Span of OFD Capabilities Across a Typical Digital Customer Journey



The Constant Evolution of the Counter-Fraud Strategy

Of course, even the model outlined above cannot remain static. Fraudsters are motivated, technically savvy, and endlessly inventive. New attack types emerge constantly, and fraud teams are usually left reacting to the changes in the fraud landscape. The whole landscape is so fast-moving that by the time an organization has defined, agreed on, and implemented its strategy, new threats may have emerged that make the strategy irrelevant.

An effective counter-fraud strategy must focus on higher-level principles rather than implementation details, helping the business make smarter decisions about the best approach to detecting, preventing, and managing fraud. Rather than committing to a specific set of tools and techniques, a well-defined counter-fraud strategy can outline the general principles for adopting, maintaining, and reinforcing counter-fraud measures through technology. A key point here is that this is an arms race; as fraudsters come up with new exploits, researchers and software companies develop new countermeasures. A pragmatic counter-fraud strategy will emphasize the need to stay up to date through continuous investment in both new technologies and people with the skills to apply them.

Fraudsters aren't sitting still, so fraud teams can't afford to rest on their laurels, either. Your fraud prevention strategy will require constant review and regular updates to ensure you and your customers remain protected. However, with the right tools in your toolbox, you'll have the agility to keep up with the fast-moving fraud landscape.

Ready to take the next step?

Explore CIAM fraud prevention must-haves
Download the Checklist

At Ping Identity, we believe in making digital experiences both secure and seamless for all users, without compromise. That's digital freedom. Ping enables enterprises to combine our best-in-class identity solutions with third-party services they already use to remove passwords, prevent fraud, enable Zero Trust, or anything in between. And they can do it all with a simple drag-and-drop canvas. That's why more than half of the Fortune 100 choose Ping Identity to protect every single digital interaction from their users, while making experiences frictionless. Learn more at www.pingidentity.com.

#3624 | 12.24 | v07