APITURE®
now part of CSI

Fraud Prevention Made Simple

4 Ways to Keep Account Holders Safe

Table of Contents

Introduction

Making Fraud Prevention a Top Priority

In today's digital-first world, fraud is evolving rapidly, threatening your financial institution and your account holders. As consumers and businesses increasingly rely on digital banking, cybercriminals are exploiting vulnerabilities to create false accounts or manipulate account records for monetary gain.

To keep pace with the growth of financial fraud, your institution must rethink how you approach fraud prevention. You require proactive, intelligence-driven strategies to detect and stop fraud in real time. This eBook explores how the fraud landscape is changing and what your institution can do to stay one step ahead.

The Rising Threat of Fraud in Digital Banking

45%

of Americans reported a security or privacy issue with their financial institution

Americans have widespread security concerns, with nearly half reporting a security or privacy issue with their financial institution, including:

Identity theft

Data breach

Phishing attempt

Source: The Harris Poll

At a Federal Reserve conference in July 2025, Sam Altman, CEO of OpenAI, warned that the world may be on the brink of a true "fraud crisis," driven by AI's growing ability to impersonate real people. He continued, "AI has fully defeated most of the ways that people authenticate currently, other than passwords."

The Federal Bureau of Investigation has also cautioned businesses and individuals about escalating use of AI in sophisticated phishing, social engineering, and voice and video cloning scams.

The numbers reinforce the urgency. Nearly one in three financial institutions suffered direct fraud losses exceeding $1 million in 2025, according to Alloy's State of Fraud Report, and 60% of institutions and fintechs reported an increase in fraud year over year.

> "AI has fully defeated most of the ways that people authenticate currently, other than passwords."
>
> Sam Altman | CEO | OpenAI

Why Proactive Fraud Prevention Matters

Traditional fraud detection tools are no longer enough to keep pace with today's rapidly evolving threats. In fact, 99% of financial organizations already use some form of machine learning or AI to fight fraud, according to Alloy.

With AI, financial institutions can spot advanced fraud patterns instantly, faster than any manual approach. And unlike legacy, rules-based systems that are limited in scope and slow to adapt, machine learning continuously learns from new data, becoming smarter and more effective over time.

By shifting to a proactive, AI-driven fraud strategy, financial institutions can:

- **Stop fraud in real time** by identifying suspicious activity as it happens.
- **Block fraudulent transactions before money leaves accounts,** reducing financial losses and the need for costly investigations and remediation.
- **Strengthen customer trust and loyalty** by demonstrating a commitment to protecting sensitive data and assets.
- **Improve operational efficiency** by reducing manual reviews and false positives, allowing teams to focus on true threats.
- **Gain a competitive advantage** with a stronger security posture that attracts security-minded users and partners.
- **Protect sensitive data, intellectual property, and confidential information** from unauthorized access and misuse.
- **Meet regulatory requirements with confidence,** lowering the risk of fines, penalties, and compliance failures.

Understanding Consumer Expectations

As digital banking becomes the norm, security is a deciding factor in where account holders choose to keep their money. For many consumers, that trust simply isn't there. In fact, 21% of those who chose not to bank with large national banks said that distrust drives their decision. Younger generations, in particular, are savvy about risk and have clear expectations for how institutions protect their funds. It is important to know how these security-conscious behaviors and expectations shape the way you think about fraud prevention. Here's what today's account holders expect from financial institutions:

- **Robust Security:** Consumers today are more security-conscious than ever. In fact, 60% of people say that robust security is a top factor when choosing a financial institution. Because security now drives account holder trust and loyalty, institutions that don't meet expectations risk losing customers before they even open an account.
- **Risk Mitigation:** Nearly 30% of Gen Z and millennials spread funds across multiple accounts to reduce exposure to risk. With this proactive approach to protecting their money, account holders are signaling that convenience alone isn't sufficient. Confidence in your security programs is just as important.
- **Strong Authentication:** Consumers now demand strong authentication. 83% of Gen Z and 86% of millennials expect multi-factor authentication for their accounts. Meeting this expectation not only prevents fraud but also reinforces the perception that your institution takes security seriously.

21%

of consumers chose a smaller financial institution because they **don't trust any large national banks**

The Price of Ineffective Security

Data Breaches Undermine Trust

Financial institutions spend years building trust with their account holders. However, one data breach can immediately erode this trust. According to an Accenture survey, 62% of customers lose confidence in their bank after a breach, and 43% choose to stop engaging altogether. Here are some real-life examples:

Flagstar Bank in 2021

- Affected 1.5 million customers
- Had to pay $3.5 million penalty to the SEC for misleading statements about the cyberattack

Capital One in 2019

- Affected almost 98 million customers
- Settled a $190 million class action lawsuit with affected customers

Fraud events can complicate customer retention, as disputes may result in negative experiences. As institutions pay more than $700 for each new customer acquisition, the cost to reacquire any lost customers can add up quickly. For example, if 200 customers leave due to a fraud concern, it equates to nearly $150K in new customer acquisition costs.

Additionally, the true cost of fraud goes beyond direct fraud losses. Research from LexisNexis shows that every dollar lost to fraud ultimately costs institutions $5.75 when factoring in extraneous costs. Once fraud occurs and financial institutions work to resolve the issue for end users, institutions take on additional expenses such as:

- Investigating the claim
- Paying legal and other fees
- Covering external recovery expenses

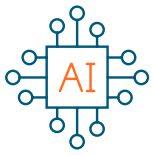
With the cost of fraud rising, and consumer expectations for risk and security soaring, your institution must invest in a proactive strategy to meet account holders' needs. Read on to learn four actions you can take immediately to boost your institution's fraud prevention efforts.

4 Pillars of a Proactive Fraud Strategy

1. Protect Payment Processes
2. Improve Identity Verification and Authentication
3. Enable a Proactive Fraud Protection Tool
4. Be Transparent About Security Policy

#1

Protect Payment Processes



Next-gen innovations such as AI- and machine learning-based technology

Positive pay tools for checks and ACH batches

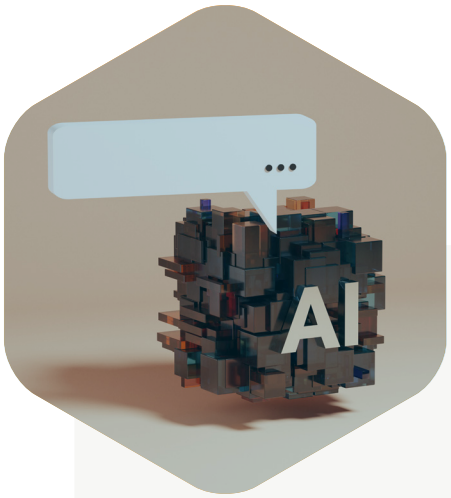
Fraud prevention measures within bill pay that block suspect activity in real time

Payments are one of the most targeted areas for fraud, which means embedding protection directly into every stage of the transaction lifecycle is critical. By using proactive fraud tools, your institution can identify suspicious activity early, reduce losses, and preserve account holder trust without disrupting the user experience. You ultimately want to ensure that threats are detected immediately and stopped before funds leave the account. Be familiar with, and use the following technology tools to protect payment processes:

- **AI and machine learning** innovations can play a central role in protecting payments. These technologies analyze large volumes of transaction data in real time to identify subtle patterns and anomalies that traditional rules-based systems often miss. AI and machine learning models continuously adapt to evolving threats, improving accuracy over time and strengthening defenses.
- **Positive pay tools for checks and ACH batches** provide another critical layer of defense. By matching presented items against approved transaction details—such as amount, payee, and date—positive pay helps you prevent altered, duplicate, or unauthorized payments from being processed. When discrepancies occur, these tools flag items for review before settlement, dramatically reducing check and ACH fraud exposure and giving businesses more control over outgoing payments.
- **Built-in fraud prevention measures within bill pay** further enhance real-time protection. These tools monitor payment behavior as it happens and automatically block or challenge suspicious activity, such as unusual payment amounts, new payees, or abnormal transaction timing. When you stop potentially fraudulent transactions in the moment, you not only prevent losses, you also reassure account holders that your financial institution is actively safeguarding their money.

#1

Protect Payment Processes



Using AI to Combat Fraud

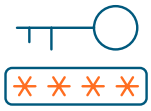
Artificial intelligence plays a critical role in predicting risk and delivering proactive alerts. Financial institutions that use AI and machine learning experience significantly fewer fraud losses than those that do not.

Key benefits include:

- **Pattern recognition:** AI analyzes massive datasets to detect anomalies and emerging fraud trends.
- **Real-time detection:** Transactions and behaviors are evaluated as they occur, allowing you to stop fraud before losses happen.
- **Fewer false positives:** AI improves accuracy, reducing unnecessary friction for legitimate users.
- **Automation:** Routine detection tasks are automated, freeing analysts to focus on high-risk, complex cases.
- **Data integration:** By unifying transaction, behavioral, and demographic data, AI delivers a more complete picture of user activity.

#2

Improve Identity Verification and Authentication



Encourage users to use passkeys instead of passwords

Incorporate multi-factor authentication within security controls

Identity verification and authentication are the foundation of an effective fraud prevention strategy. Today, 83% of Gen Z and 86% of millennials expect their bank to offer multi-factor authentication. These expectations indicate a broader demand for proactive security measures that protect accounts from the moment they are opened to other touchpoints within the customer lifecycle.

To meet this demand, your institution must strengthen identity verification and authentication with layered, modern controls. During account opening, identity verification and Know Your Customer (KYC) processes help ensure that only legitimate users gain access, using trusted solutions such as Alloy and Footprint. Your institution should combine multi-factor authentication with additional security layers to safeguard your systems and protect users' accounts and sensitive data.

#3

Enable a Proactive Fraud Protection Tool

Notifications that monitor for excessive or suspicious overrides, duplications, or cancellations

Existing event data—account logins or changes to email address and phone number—that provide real-time visibility into suspicious account activities

Intuitive dashboards that provide snapshots of digital banking activities

A proactive fraud strategy begins with embedding strong safeguards throughout systems and processes. However, to see real impact, your institution can pair these controls with intelligence-driven tools, allowing you to pivot from reacting to losses to preventing fraud in real time.

Real-time alerts, continuous monitoring, and intuitive dashboards provide immediate visibility into high-risk activity such as suspicious logins, account changes, or unusual transactions. When combining these efforts with data about how account holders are navigating and interacting with your platform, you can securely share insights with fraud-prevention partners via APIs — ultimately blocking threats before funds ever leave an account.

As proactive detection and AI-driven tools continue to mature, financial institutions can stay ahead of increasingly sophisticated attacks, strengthening security while reducing losses at scale.

#3

Enable a Proactive Fraud Protection Tool

Real Results From Using Proactive Measures with AI

AI is lending its processing power to positively change fraud prevention activities. According to Alloy, 99% of financial institutions are already using machine learning or AI to combat fraud, and 93% believe it will revolutionize their capabilities. Some positive results using this technology include:

Key benefits include:

- AI-driven fraud detection systems at JP Morgan Chase helped block threats before funds left accounts, contributing to $1.5B in prevented losses.
  Source: AI Expert Network
- Real-time, AI-driven tools have cut fraud losses up to 60% at many institutions.
  Source: Feedzai
- Machine learning delivers a 60% improvement in detection, 50% reduction in false positives, and 40% fewer undetected card-fraud cases.
  Source: Resolvepay
- AI-driven fraud detection has prevented an estimated $25.5 billion in global fraud losses in 2025, with 90–98% detection accuracy.
  Source: AllAboutAI

#4

Be Transparent About Security Policy

Communicate your security strategy and policies to account holders

Reinforce good security habits

Remind account holders about ongoing scams and give them tips to stay safe

Communicating openly about your institution's security practices is one of the fastest ways to strengthen trust with account holders. Yet, there is still a gap between expectations and reality. A recent Accenture survey found that while 85% of account holders view transparency in cybersecurity communication as essential, only 28% say their financial institution delivers it effectively.

The research also showed that only the top 10% of financial institutions truly meet account holders' needs for clarity and proactivity around cybersecurity. What sets these leaders apart is their commitment to including cybersecurity in their broader strategic initiatives and empowering every stakeholder—from frontline staff to technology teams—to help detect and deter threats.

For community banks and credit unions, meeting rising expectations for transparency remains a challenge, but it's also a major opportunity to build trust. Three ways that your institution can close the gap are by clearly communicating your security strategy, making cybersecurity a visible part of your platform and experience, and keeping customers informed about emerging scams.

85%

of account holders view **transparency in cybersecurity communication as essential.**

Source: Accenture

APITURE®
now part of CSI

Building a Culture of Security

Begin building your proactive strategy by investing in systems and tools that detect high-risk activity in real time, ensuring the safety of payment processes and sensitive data. Your success depends on selecting the right technology partners that meet rigorous standards, such as SOC 2, FFIEC, and NACHA compliance.

You should also seek platforms that provide intuitive dashboards, real-time alerts, and the ability to act quickly on suspicious activity. Finally, understand that your culture of security will not function without transparency. Regularly communicating security policies, reinforcing good habits, and alerting account holders to ongoing scams strengthens trust while making security a shared responsibility.

By embedding security into both technology and culture, you not only protect your institution's assets, you also strengthen trust, retain existing account holders, and attract younger, more security-conscious consumers.

SCHEDULE A DEMO