JAVELIN ADVISORY SERVICES | FRAUD MANAGEMENT

Account Takeover:

Static Authentication Enables Access Without Confirmation

javelin

JUNE 2025

MEET THE AUTHOR

Jennifer Pitt
Senior Analyst,
Fraud Management

AUDIENCE

Financial providers: Banks, credit unions, fintechs, insurance companies, payment processors, and credit card companies; chief information risk officers, corporate social responsibility officers, CEOs, CISOs, communications teams, fraud investigators.

Vendors: Retailers, prepaid program managers, prepaid management providers, online and mobile banking platform providers, online and mobile banking vendors, identity protection service providers, and card processing companies.

CONTRIBUTORS

Suzanne Sando
Lead Analyst, Fraud Management

Overview

Ongoing and pervasive exposure of U.S. consumers' personal information has made account takeover (ATO) the lowest-hanging fruit for criminals. Criminals are using legitimate credentials and mimicking typical customer behavior to impersonate accountholders to slip past fraud controls. ATO risk signals are often subtle and difficult to detect, especially with outdated authentication models that validate users only at login. To thwart ATO risks, financial institutions must address gaps in user authentication and use identity-proofing and authentication solutions that go beyond onboarding or initial login.

This Javelin Strategy & Research report examines the growing impact of ATO and identifies where static authentication falls short. It outlines what financial institutions must do to strengthen their defenses to detect and thwart account takeover fraud in real time to protect customers and their holdings.

Primary Questions

- How can FIs strengthen identity verification and authentication strategies to stop account takeover?
- Why should FIs move away from static fraud defenses?
- Why is it so critical for banks and consumers to address ATO fraud immediately?

javelin

Table of Contents

Table of Figures

javelin

Executive Summary

Victims of account takeover fraud lost almost $16 billion in 2024. This represents a jump of $2.9 billion from the prior year. Criminals can obtain a higher return by taking over existing accounts, which have already undergone initial onboarding and know-your-customer checks. By gaining unauthorized account access and changing account information, such as the email address and phone number, criminals can use the account longer without detection.

Less than 10% of account takeover victims reported that their FI is doing enough to protect them against identity fraud. That means that more than 90% of ATO victims think their financial institution is not doing enough to combat the problem. This underscores a serious gap in the fight against account takeover fraud.

Unfortunately, 42% of ATO victims closed the accounts where the fraud occurred. After the significant toll of account takeover fraud, victims often take steps to avoid being victimized again. And in the customer's mind, the liability of failing to detect and prevent fraud lies with the bank. Stopping account takeover fraud from happening in the first place, or at least significantly reducing its overall incidence, is critical for customer retention.

Existing checking and email accounts were the favorite targets of fraudsters in 2024. In fact, 39% of account takeover fraud victims reported that their checking accounts were taken over, and 23% experienced the takeover of their email accounts. Checking accounts are favored targets among fraudsters because consumers often keep most of their money in checking accounts (rather than savings). Checking accounts are also often linked to accounts at different banks and online merchants. And email accounts are linked to most (if not all) financial and non-financial accounts. Taking over checking or email accounts provides criminals with easy access to a variety of account types.

Recommendations

Continuously authenticate users throughout the entire login session—from login to logout. Validating a user during just the initial login is not sufficient to protect against account takeover. Without continuous authentication, criminals using legitimate credentials often have unfettered access to accounts. Financial institutions must monitor behavior throughout the entire login session to ensure that the verified customer is the same person still using the account. Continuous authentication strategies should include a layered approach of behavioral biometrics, device analytics, and real-time monitoring.

Assess each login session for risk signals of account takeover. These signals include multiple failed login attempts, immediately changing personal or account information after login, device identification and behavior changes, geolocation changes, use of a VPN, and changes in customer behavior. Each indicator on its own may not indicate account takeover, but several indicators together increase the risk of allowing the user to access the login session without further verification and checks for fraud.

Employ a perpetual know-your-customer (KYC) solution. KYC does not stop with account onboarding. Perpetual KYC solutions utilize AI and machine learning technologies to verify customer identification, assess risk, monitor customer accounts and behavior, and alert bank systems to anomalies or fraud signals. Perpetual KYC processes address compliance concerns and mitigate the risks of money laundering and fraud in real time. And even though KYC is typically associated with anti-money-laundering processes, continuous KYC solutions can be used to combat different types of fraud, like account takeover.

Educate customers about the signs of account takeover. Consumers may not recognize subtle changes that signal fraud, like an added name, username, email address, or phone number. FIs should advise their customers and members to regularly monitor their accounts for unusual and unauthorized transactions as well as any changes to their account profiles.

Partner with vendors that offer identity verification and protection against account takeover. These solutions look at multiple risk signals like device fingerprints, IP address, login velocity, and behavioral anomalies. These solutions also evaluate unusual account behavior and unauthorized device access. Partnering with these vendors helps reduce costs, prevent account takeover, assist with regulatory compliance, and minimize customer attrition.

Require phishing-resistant multifactor authentication (MFA). Organizations must require consumers to use phishing-resistant MFA protocols, which can include behavioral and device analytics and biometrics (including fingerprint, voice, photo, and video) or passkeys. This type of authentication protects against password cracking, social engineering, and SIM swaps, which can all be used to gain the necessary information and access to take over accounts.

Current Bank Defenses Are No Match for ATO

Ongoing and pervasive exposure of consumers' personal information has made account takeover (ATO) the lowest-hanging fruit for criminals. Attackers are using legitimate credentials and mimicking typical customer behavior to impersonate accountholders and bypass fraud controls. ATO risk signals are often difficult to detect, especially with outdated authentication models that validate users only at login. These static defenses create the perfect opportunity for account takeover fraud to flourish. Financial institutions must address gaps in authentication and identity verification and instead use solutions that can better differentiate the bad actors from the verified accountholders.

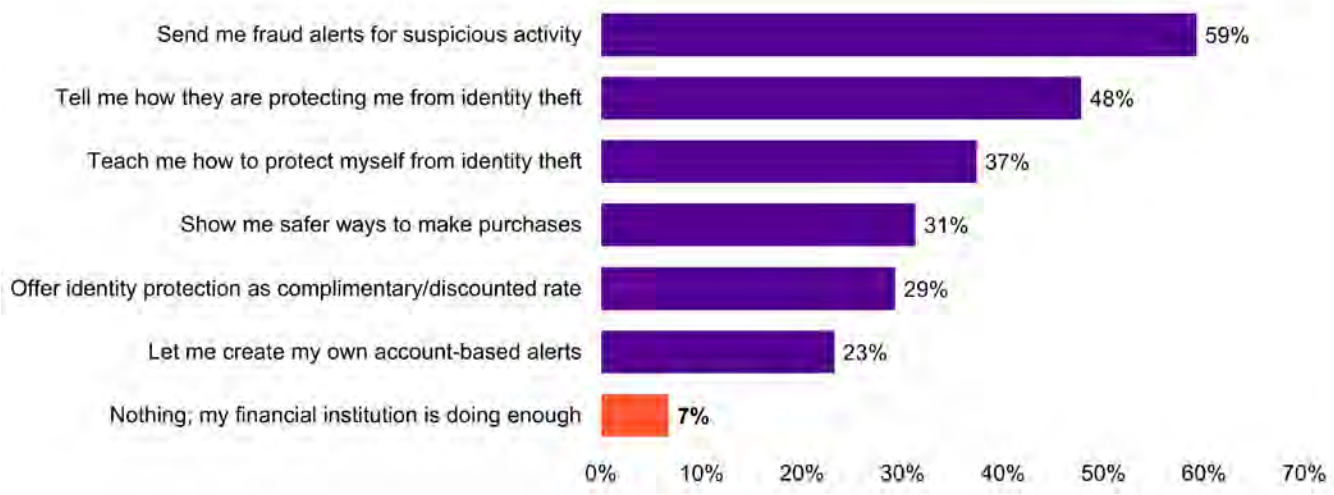
The problem is that banks have been slow to upgrade outdated fraud solutions, allowing attackers to capitalize on these vulnerabilities. According to Javelin's *2025 Identity Fraud Study: Breaking Barriers to Innovation*, 5.1 million consumers were victims of ATO fraud in 2024, a 9% increase from the prior year.[1] And cybersecurity company Kasada noted that ATO attempts against consumers increased by 250% in 2024.[2] This surge in attacks shows that fraudsters are taking advantage of gaps that banks still haven't addressed.

Consumers have taken notice. According to Javelin research, less than 10% of account takeover victims said their financial institution is adequately protecting them against fraud. That means that more than 90% of ATO victims think their bank is not doing enough. This underscores a serious gap in the fight against account takeover fraud.

One of the biggest failures is that many banks still don't send fraud alerts to consumers. Unfortunately, this could indicate a larger problem—that banks are not adequately detecting suspicious activity. Additional failures include neglecting to offer or advise members about customer-initiated fraud alerts and neglecting to advise customers on how they can protect themselves from fraud. In customers' minds, the liability for failing to detect and prevent all fraud lies solely with the bank.

FIs Are Not Doing Enough to Prevent ATO

Figure 1. Percentage of ATO Victims Who Need Additional Help to Feel Safe From Fraud, by Method



Source: Javelin Strategy & Research, 2025

javelin

These significant process gaps make it easier and more profitable for criminals to take over existing accounts, which have already undergone initial onboarding and KYC checks.[3] By gaining unauthorized account access and changing account information—such as the email address and phone number—criminals can use the account for an extended period without being detected.

It's important for banks to understand that no person or institution is immune to account takeover, and with the increasing use of bots and AI, these attacks are becoming more and more sophisticated.

AI is no longer just speeding up fraud. It's changing the way these attacks are carried out.

Fraudsters are using AI to automate credential testing, personalize phishing attacks, and simulate normal user behavior to avoid detection.

Some AI tools used by fraudsters can even adjust automatically in real time based on the security controls they encounter, helping criminals remain undetected while they try to access or take control of an account. Examples of these AI-assisted fraud tactics include solving CAPTCHAs (challenges designed to distinguish humans from bots), slowing down login attempts to avoid being blocked by login limits, or changing how their device identifies itself. Even when continuous authentication is in place, fraudsters who mimic normal customer behavior may be able to avoid detection and maintain control of the account.

And because of allowed weak credentials and lax authentication protocols, it's often simple for fraudsters to change account credentials and take over an account.

Account takeover can occur in various ways: phishing (impersonating a legitimate organization to trick users into providing sensitive information), credential stuffing (using stolen login credentials from one account to access another), malware, and man-in-the-middle attacks (intercepting user communication).[4]

Through phishing, attackers can easily obtain sensitive information directly from accountholders. Before the actual accountholder even realizes that they've been conned, the attacker has already changed key information, often locking out the accountholder or, in the case of financial accounts, draining the account entirely.

Data breaches and leaks are other common ways fraudsters gain information needed to take over an account. Information already on the surface or dark web—like usernames, passwords, email addresses, phone numbers, or other detailed PII—can be used to easily take over existing financial and non-financial accounts. FIs can help address data-breach-related fraud by partnering with identity protection service providers, which can detect leaked information, notify the user, and even help with deleting information.

Although many account takeovers begin with compromised credentials (as in the case of phishing and data breaches), some start by targeting the device itself, like what happens in SIM swapping. SIM swaps involve a fraudster persuading a phone carrier representative to transfer control of the number to a SIM card controlled by the attacker.[5] The attacker can then take over the device, gaining unauthorized access to contacts, messages, apps, and

passcodes. The prevalence and success of SIM swapping are the biggest reasons that banks should stop sending their customers one-time passcodes (OTPs) via text message. This tactic allows fraudsters to easily access accounts and make immediate transfers out of the account, as bank personnel often believe they are speaking with the legitimate customer who just verified the provided one-time passcode.

Text-based OTPs are not a secure form of authentication. Instead, FIs should provide and require phishing-resistant authentication options like passkeys.[6] The implementation of passkeys not only mitigates the risk of SIM swaps but also reduces the reliance on outdated and insecure credentials like passwords, which are easy to crack and often reused across multiple platforms,[7] aiding in easy account takeover fraud.

LEGITIMATE CREDENTIALS MAKE DETECTION CHALLENGING

As account takeover involves criminal use of real usernames and passwords—often stolen from data breaches, obtained from the internet, or gained from scam victims—and because those credentials belong a real, verified user, these attackers can easily go undetected for long periods.

Although these criminals may log in using the correct username and password and they may attempt to mimic the accountholder's typical actions, some behaviors may not align with those of the true accountholder. Attackers might use an unrecognized device or log in from an unusual location, or their typing and keystroke patterns may be inconsistent with the verified user. When considered together with other risk signals, these anomalies can indicate a compromised account. With ATO, behavioral red flags and risk signals may be more subtle than with other fraud typologies. As a result, ATO is harder for many legacy fraud systems to detect. Failing to address the growing account takeover problem can lead to increased transaction disputes, loss of consumer trust, reputational damage, and possible fines.[8]

FIs must conduct a holistic fraud review, not only for each customer but also across all accounts and customers in their organization. This will help determine if there are patterns across the organization that may indicate ATO— like several customers' information being changed (including email address or name), multiple accounts being accessed by the same device, and other patterns detected across accounts. Fraud teams should investigate not just the fraudulent transactions but also every action the fraudster takes once inside the account. This will provide valuable insight into fraud tactics.

FIs can no longer rely on reactive fraud detection strategies. Account takeover must be stopped earlier, before criminals have a chance to change account information or steal money. To keep up with evolving threats, financial institutions must move beyond static login checks and adopt adaptive authentication methods that evaluate risk throughout the customer's entire login cycle, from login to logout.

Additionally, FIs should set limits on login attempts and notify the account holder of any changes in account information, transaction behavior, login changes or failures, and changes in account behavior (which refers to how a customer typically interacts with their account once logged in). This can include what they access (such as settings instead of transaction history), when they access it, how they interact with the account (such as staying logged in longer, changing settings, or skipping common steps), and where they access the account from (such as a new IP address or a change in language settings).

Account Takeover Carries a Heavy Cost

In 2024, consumers lost almost $16 billion (a $2.9 billion increase from 2023) (see Javelin's *2025 Identity Fraud Study: Breaking Barriers to Innovation*). The average dollar loss per victim was $2,575 (up from $2,519 the previous year).[9] Because nearly 60% of Americans don't have enough savings to cover an unexpected $1,000 expense, this loss from account takeover may be too much to bear.[10]

The significant and unexpected financial loss, coupled with extreme emotional and psychological stress, takes a serious toll on victims. Nearly half of all account takeover victims (49%) say their lives were affected by their fraud victimization.

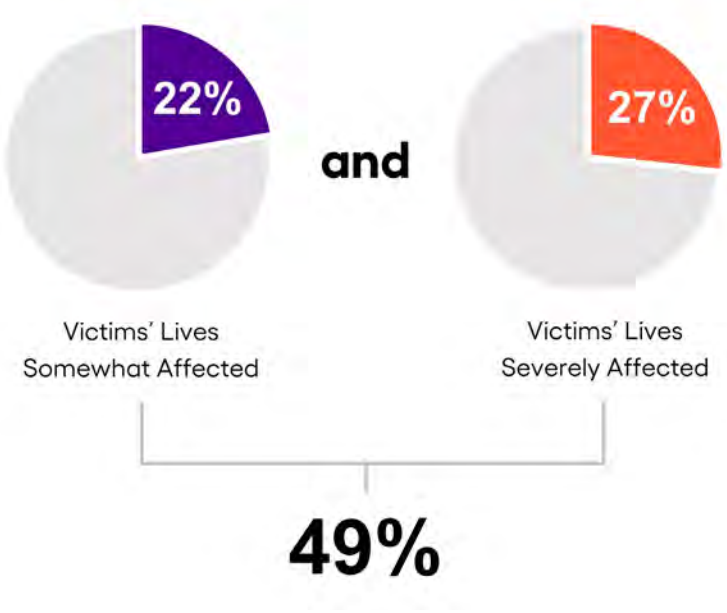
Financial services providers should be very concerned about the impact of fraud on consumers. Account takeover fraud is often reported by victims as a personal violation, and as a result, they may be more hesitant to conduct financial transactions or participate in a digital world at all.

Account takeover fraud can be devastating. And consumers may not even realize the violation is happening until it's too late. The signs may initially be subtle, like an added name, username, email address, or phone number. But if these subtle changes are not flagged by the organization, the accountholder may experience complete devastation. Eventually, the actual accountholder may be locked out of their account, or their hard-earned money may be stolen from that account.

The damage may not end there; criminals rarely stop with just one account. As existing accounts are often tied to other financial and non-financial accounts, the takeover of one account often leads to the seizing of several accounts, leaving victims distraught and unsure of what to do next.

Almost Half of ATO Victims Say Their Lives Were Affected by Fraud

Figure 2. Percentage of ATO Victims Whose Lives Were Affected by Fraud



Source: Javelin Strategy & Research, 2025

javelin

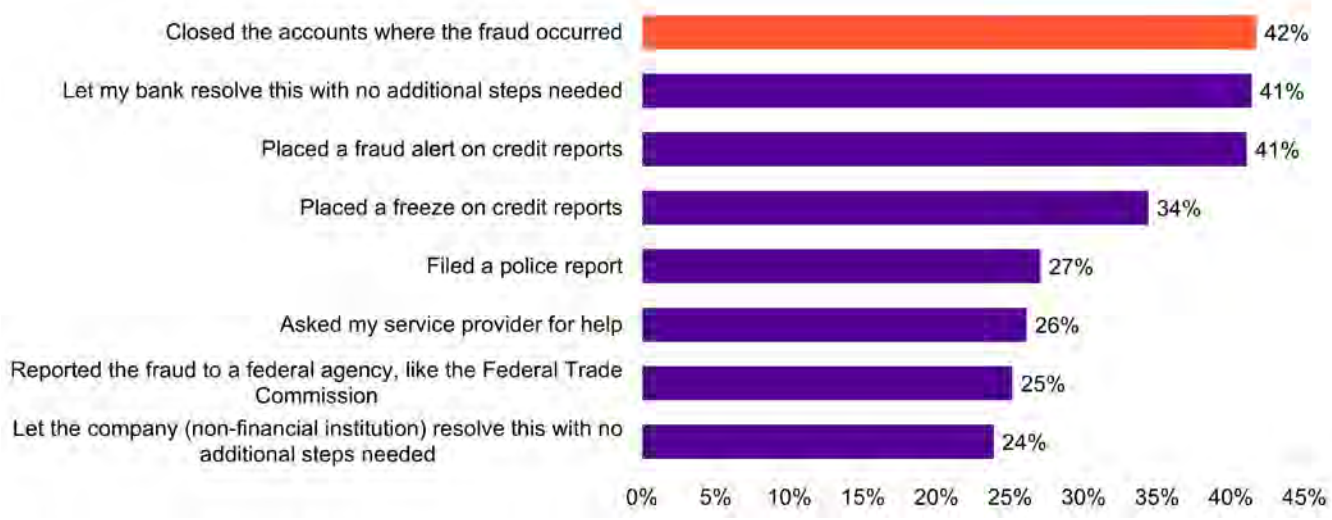
Recovery is often costly and extremely time-consuming, and victims may not even be aware of the full extent of the fraud. Fraudsters can lie dormant in an account before making any major changes or draining the account. If one account has been taken over, consumers should expect that other accounts may also have been compromised. FIs must help their consumers resolve fraud in its entirety, with the expectation that other financial and non-financial accounts have already been affected.

Account takeover fraud is one of the most destructive types of identity fraud. ATO victims must be on constant alert and be diligent about continually checking all of their financial and non-financial accounts for signs of tampering. Victims often enlist the help of others—including their financial institution, law enforcement, and credit monitoring services— in this long, drawn-out recovery process. Many fraud victims even take steps to avoid future victimization, including placing credit freezes and enabling fraud alerts.

But the bigger problem with account takeover fraud is the erosion of trust. When people no longer feel safe, they stop doing business with the organization involved. In fact, 42% of ATO victims closed the accounts where the fraud occurred. Considering that account takeover can often involve multiple financial and non-financial accounts (and therefore mean the closure of multiple accounts), that figure is staggering. This highlights the importance of preventing account takeover fraud from occurring in the first place (or at least significantly mitigating it).

More Than 40% of ATO Victims Close Accounts After Fraud

Figure 3. Percentage of Account Takeover Victims Who Took Various Steps After Victimization



Source: Javelin Strategy & Research, 2025

When fraud does happen, FIs should guide their customers through the entire resolution process so they no longer feel alone in the aftermath of their traumatic fraud event. FIs should also encourage victims to change their login information, switch to multifactor authentication, and add fraud alerts to their accounts. This can help minimize the overall impact by stopping the takeover before additional accounts are compromised or significant financial losses occur.

javelin

ATO Affects More Than Financial Accounts

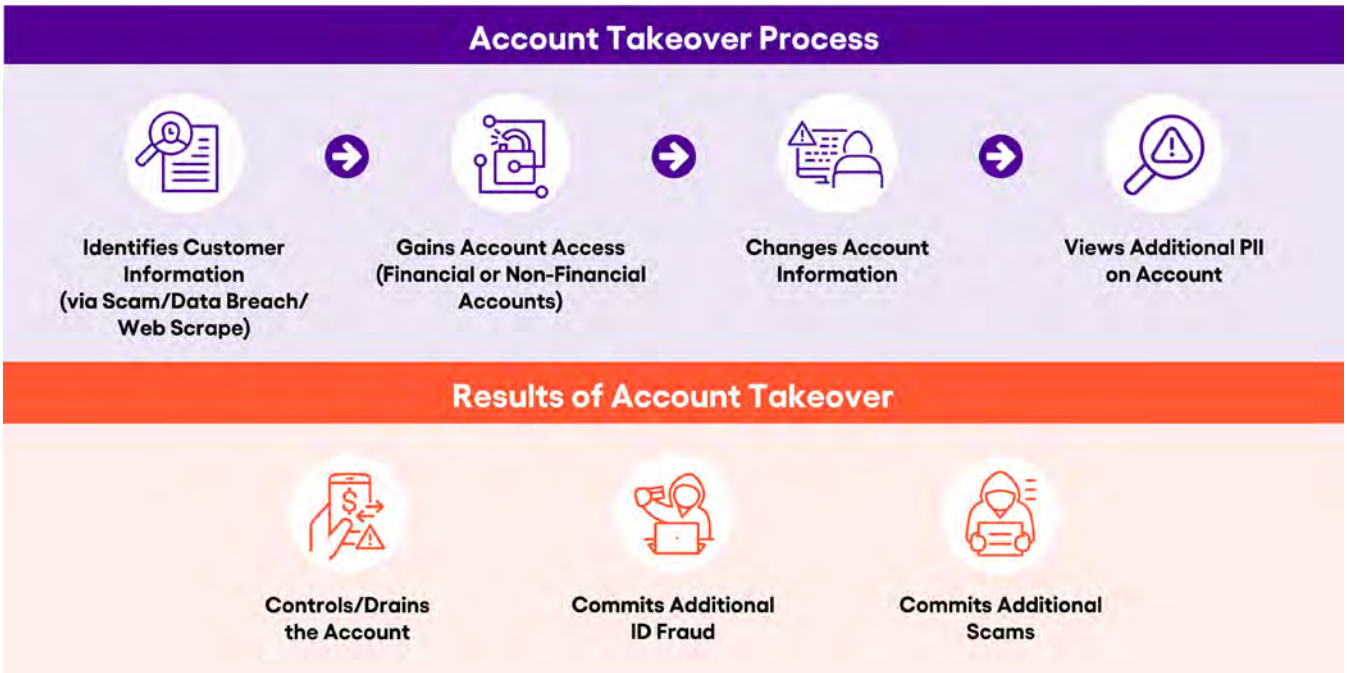
All sectors are susceptible to account takeover: financial services, retail and e-commerce, social media, higher education, and healthcare, to name a few. Consumers' financial and non-financial accounts are always at risk because these accounts provide attackers with valuable information. As the world shifts everything to digital channels and more people link their accounts, criminals have access to a larger pool of information they can use to commit additional identity fraud or scams.[11]

Account takeover fraud starts with the fraudster identifying and accessing customer information, usually through already-compromised information or social engineering attacks. The attacker then uses this information to gain unauthorized access to financial and/or non-financial accounts. To remain undetected as long as possible, the fraudster adds or changes information on the account (like email address or password), redirecting account-related communication and locking out the legitimate accountholder.

ATO not only offers attackers access to the initial account that's taken over but also allows access to other valuable information in that account—information that can provide access to other accounts or can help facilitate additional identity fraud or scams. For example, financial accounts often contain sensitive information like Social Security numbers. The attacker may not have had knowledge of this number or access to it before they took over one financial account. But after the ATO, the attacker can access a plethora of sensitive information.

ATO Can Lead to More Than the Compromise of Just One Account

Figure 4. Account Takeover Process, With Actions by Fraudster and Results

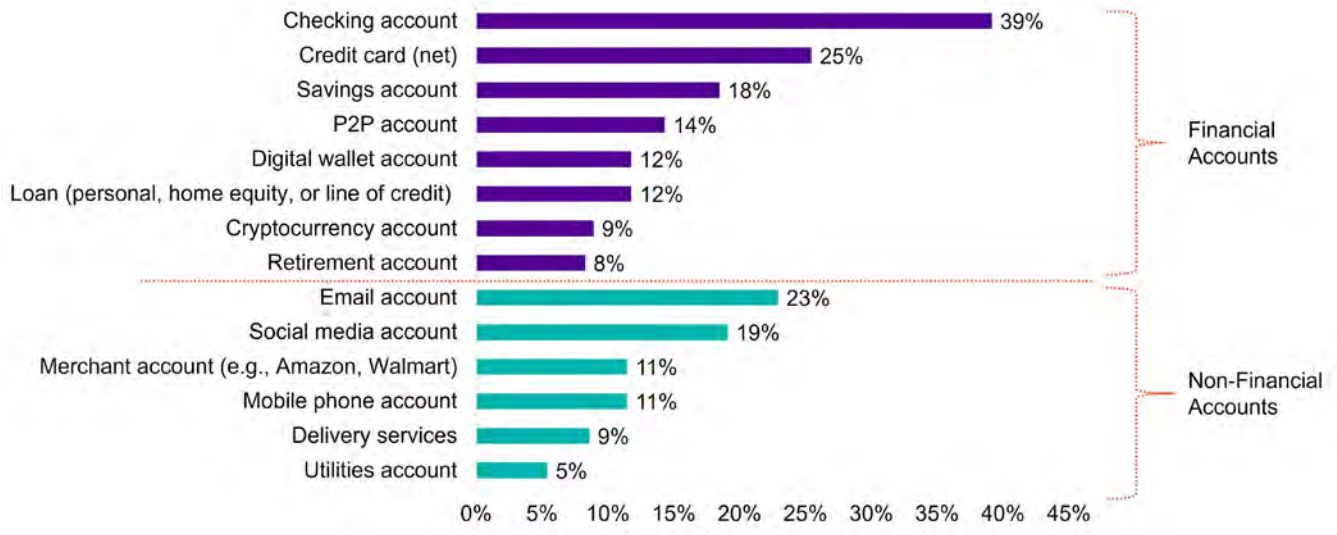


Source: Javelin Strategy & Research, 2025

The threat is not limited to a single type of account, though some account types are targeted more than others. The top financial account types taken over were checking accounts (39%) and credit card accounts, both store-specific and major credit cards (25%). The top non-financial account types taken over were email accounts (23%) and social media accounts (19%).[12]

Checking and Email Accounts Top the List of Accounts Taken Over

Figure 5. Percentage of Account Takeover Victims, by Account Type



Source: Javelin Strategy & Research, 2025

This is not surprising, as most consumers own these types of accounts. Checking accounts at one bank are often linked to checking accounts at another bank. And because of low and sometimes nonexistent interest rates on traditional savings accounts, consumers often keep what little they have for liquid money in checking accounts. Email accounts are linked to nearly all financial and non-financial accounts. And most people have one or more social media accounts, which contain swaths of personal and professional details. Taking over a checking, email, or social media account provides criminals with easy access to a sea of information. The more personal information these attackers have, the more devastation they can cause.

Fraud Protection and User Experience Can Co-Exist

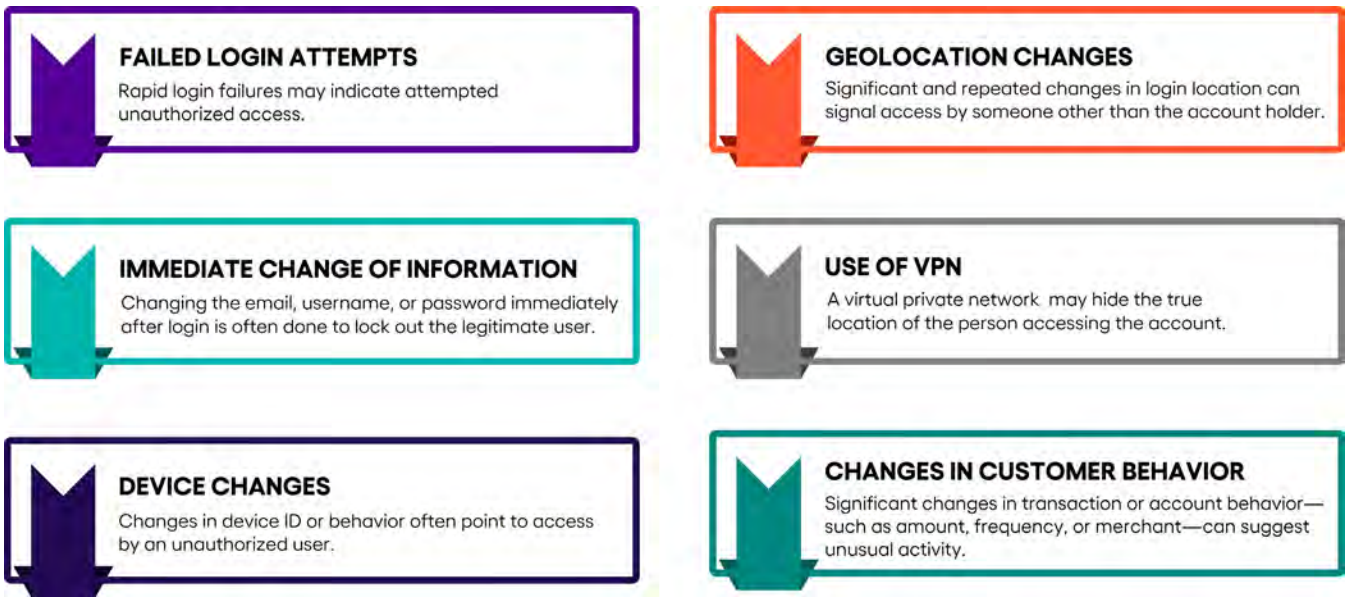
Many organizations are concerned that requiring strong authentication methods, including multifactor authentication or step-up authentication (commonly used during high-risk actions like large-dollar transfers or account detail changes), will cause too much customer friction, ultimately leading to dissatisfaction and attrition. But strong authentication doesn't have to mean entering a username and password multiple times. Authentication methods (like passkeys) are more secure, easier to use, and don't require customers to remember them.

Strong authentication can work in the background, using contextual and behavioral signals to assess risk in real time. When implemented correctly, it strengthens security without significantly increasing customer friction. Because account takeover involves the initial use of the customer's real credentials, banks must use a layered and continuous approach to defeat this problem. FIs must use a combination of identity verification and authentication strategies, including physical biometrics, behavioral biometrics, AI-powered real-time fraud detection tools, and robust consumer education campaigns on phishing, social engineering, and malware attacks.[13]

FIs need to assess each login session for risk and signs of account takeover like multiple failed login attempts, immediately changing personal or account information after login, device identification and behavior changes, geolocation changes, use of a VPN, and changes in customer behavior (which may indicate that someone other than the initial verified user is using the account).[14]

The Presence of Multiple Risk Signals May Indicate ATO

Figure 6. Indicators of Account Takeover Fraud



Source: Javelin Strategy & Research, 2025

Each indicator on its own may not point to account takeover, but several of these indicators together should raise the risk level and require additional verification. Rather than validating authentication only during the login process, the user needs to be continuously authenticated during the entire login session. Using AI-powered solutions, this can be done in the background in real time to more effectively assess risk while mitigating customer friction.

To mitigate ATO, FIs must view customers and accounts holistically, looking at each customer throughout the entire account lifecycle and comparing that activity to that of known good customers and expected behavior as well as known detected fraud accounts.

Implementing strong perpetual or continuous KYC processes (often reserved for AML teams) can help protect against account takeover. Perpetual KYC uses AI and machine learning to verify identity, assess risk, and alert systems to suspicious activity. When these checks run continuously, not just at onboarding, financial institutions can detect account takeover attempts earlier and take action before the damage spreads.[15] As identity verification alone isn't often enough to prevent ATO, strengthened authentication is needed. When strong identity verification is combined with robust authentication strategies and consortium-based data sharing,[16] financial institutions can better detect anomalies and prevent ATO early.

Banks don't need to start from scratch when implementing solutions to prevent account takeover. Several vendors offer ATO fraud prevention and mitigation solutions.[15] These solutions look at multiple risk signals—like device fingerprints, IP address, login velocity, and behavioral anomalies— and evaluate unusual account behavior and unauthorized device access. Partnering with vendors that offer robust ATO prevention solutions—like Signifyd, Memcyco, Telesign, Beyond Identity, Forter, Okta, Imperva,[17] PingIdentity,[18] Mitek,[19] and BioCatch[20]—can help reduce costs, prevent account takeover, assist with regulatory compliance, and help reduce customer attrition.

ATO fraud solutions alone are not going to solve this problem for banks.
FIs need help from their customers and members, too.

FIs must educate their customers and members on how to protect themselves from account takeover fraud by using strong authentication and reporting any unexpected or unauthorized transactions or account changes to the FI.

FIs must proactively advise their customers on how to determine if their account may have been taken over. Some of these initial indications of account takeover include suspicious account activity, unrecognized login attempts, added usernames, added email addresses, and suspicious communications.[21] Consumers should monitor their accounts, whether through their financial institution, through an identity protection service provider, or on their own. Bank personnel should advise every customer and member to proactively check their accounts regularly, looking for unusual activity and reviewing their account profile for information that has been added or changed. This extra vigilance by consumers (coupled with automatic fraud alerts from the bank and customer-initiated fraud alerts) can help better protect consumers from account takeover.

The widespread exposure of consumers' personal information and the rapid advancements in technology exploited by fraudsters have made account takeover one of the most prevalent and damaging forms of fraud. To combat this growing threat, financial institutions must prioritize strong, continuous authentication, dynamic identity verification, comprehensive fraud alerts, and consumer education.

Methodology

Consumer data in this report is based on information gathered from Javelin's 2024 Identity Fraud study. This survey was conducted online among 5,023 U.S. adults over the age of 18; this sample is representative of the U.S. census demographics distribution. Data collection took place Oct. 11-Oct. 30, 2024. Data is weighted using 18-plus U.S. population benchmarks on age, gender, race/ethnicity, education, census region, and metropolitan status from the most current CPS targets. Due to rounding errors, the percentages on graphs may add up to 100% plus or minus 1%. To preserve the independence and objectivity of this annual report, the sponsors of this project were not involved in the tabulation, analysis, or reporting of final results. The ID Fraud Study estimates key fraud metrics for the current year using a base of consumers who have experienced identity fraud in the past six years. Other behaviors are reported based on data from all identity fraud victims in the survey (i.e., fraud victims experiencing fraud up to six years ago) as well as total respondents, where applicable. For questions answered by all respondents, the maximum margin of sampling error is +/-1.41 percentage points at the 95% confidence level. For questions answered by all identity fraud victims, the margin of sampling error is +/-3.3 percentage points at the 95% confidence level.

Endnotes

1 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

2 Kasada, "4 Data-Driven Takeaways from Kasada's 2025 Account Takeover Trends Report." Published Feb. 6, 2025; accessed May 27, 2025

3 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

4 Privacy, "Account Takeover Faud—How To Detect It and Protect Yourself." Published April 22, 2025; accessed May 22, 2025

5 Digital Credit Union, "Common Account Takeover (ATO) Fraud Examples." Published Feb. 26, 2025; accessed May 22, 2025

6 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

7 Javelin Strategy & Research, "Password Fatigue: A Case for Multilayered Passwordless Authentication." Published June 4, 2024; accessed May 22, 2025

8 DataDome, "Account Takeover Prevention: How to Prevent ATO & Mitigate Fraud." Published Nov. 10, 2022; accessed May 22, 2025

9 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

10 CBS News, "Most Americans can't afford a $1,000 emergency expense, report finds." Published Jan. 23, 2025; accessed June 9, 2025

11 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

12 Ibid.

13 Ibid.

14 Incognia, "Account Takeover Prevention." Published 2025; accessed May 12, 2025

15 Javelin Strategy & Research, "2025 Identity Fraud Study: Breaking Barriers to Innovation." Published March 25, 2025; accessed Jan. 12, 2024

16 Javelin Strategy & Research, "Identity Verification Demystified: Share More, Secure More." Published Oct. 31, 2024; accessed May 27, 2025

17 Memcyco, "Top 7 Account Takeover Solutions." Published April 2, 2025; accessed May 22, 2025

18 Ping Identity, "Prevent & Mitigate Account Takeover Fraud." Published 2025; accessed May 22, 2025

19 Mitek Systems, "Account Takeover Fraud Prevention." Published 2025; accessed May 12, 2025

20 BioCatch, "Account Takeover Protection." Published 2025; accessed May 12, 2025.

21 Privacy, "Account Takeover Faud—How To Detect It and Protect Yourself." Published April 22, 2025; accessed May 22, 2025

javelin

Related Research

Fraud in the Age of Agentic Commerce
May 2025
Agentic commerce is coming, and so are the fraud opportunities. Consumers, agent services, and merchants must all be prepared for an onslaught of fraud and scams, with cybercriminals looking to take advantage of this new technology. Identity verification and authentication of all parties involved in the transaction will be critical in thwarting fraudsters who attempt to exploit agent services.

Fraud Prevention: Managing The Entire Customer Lifecycle
September 2024
This report, sponsored by TransUnion, explores the immediate and long-term risks associated with new-account fraud (NAF) and account takeover (ATO) fraud for organizations and consumers and establishes a case for employing comprehensive identity-proofing and authentication solutions to stop fraud throughout the entire account lifecycle.

ATO Fraud: Why It Remains FIs' Greatest Fraud Risk
August 2024
Despite years of anti-fraud investment, account takeover (ATO) continues to plague financial institutions and consumers. Traditional authentication methods offer too many gaps of opportunity for cybercriminals, primarily because of easily compromised or acquired credentials. Among traditional identity fraud typologies tracked by Javelin Strategy & Research, ATO losses are among the most impactful to consumers. In 2023, ATO fraud losses suffered by consumers increased 15% from the previous year. This report explores why FIs' short-term focus on identity verification and authentication is adversely affecting their ability to dramatically reduce ATO.

About Javelin

Javelin Strategy & Research, part of the Escalent Group, helps its clients make informed decisions in a digital financial world. It provides strategic insights to financial institutions including banks, credit unions, brokerages and insurers, as well as payments companies, technology providers, fintechs and government agencies. Javelin's independent insights result from a rigorous research process that assesses consumers, businesses, providers, and the transactions ecosystem. It conducts in-depth primary research studies to pinpoint dynamic risks and opportunities in digital banking, payments, fraud & security, lending, and wealth management. For more information, visit www.javelinstrategy.com.

Follow us on LinkedIn

javelin