Seeing beyond your walls

An enhanced approach to fighting Account Takeover

$16B+	24%	1 in 4
in ATO losses annually [1]	year-over-year increase in ATO attacks [2]	consumers reported experiencing ATO in 2025 [3]

THE CONTINUED THREAT OF ACCOUNT TAKEOVER

Account takeover (ATO) remains the most significant fraud threat facing financial institutions today. In 2024, ATO losses reached $16 billion annually, representing more than half of all identity fraud losses that year. ATO attack volumes grew 24% year-over-year, with nearly 1 in 4 consumers (24%) reporting being victims of account takeover.

At Anti Fraud Advisors, we assess and stress-test fraud programs across the industry. What we have consistently found is that most organizations have expanded and improved their fraud capabilities, but those capabilities have grown inward. More sensors, more models, more friction at the transactional and authentication layer, but all focused on activity observable within the institution's own walls. Adversaries have taken note and focus on what you cannot control within your own walls.

BUILDING STRONGER WALLS

In response to rising ATO losses, we've noted that institutions are focusing investments in strengthening their external walls (i.e., stronger access controls). Institutions have moved from passwords to multi-factor authentication, deploying one-time passcodes via SMS and authenticator apps. More recently, Passkeys and biometrics have been increasingly adopted to reduce reliance on passwords and strengthen authentication, but they are not a solution for consistently combating fraud. Risk engines now evaluate hundreds of signals at login to verify the end-user. The premise is sound: stronger verification at the point of access should prevent unauthorized access. Furthermore, as threats grow in speed and volume, correlating multiple signals in real time becomes increasingly unworkable, resulting in reduced precision, security gaps, and excessive user friction. Yet no matter how robust the authentication layer, it does nothing to prevent credentials from being compromised in the first place. And that is precisely where fraudsters are gaining the upper hand.

Today, ATO attacks are engineered to circumvent authentication controls by going upstream to acquire user credentials. Through tactics such as phishing, Adversary-in-the-Middle attacks, malware, and impersonation scams, fraudsters don't start by directly attacking the institution or attempting to break its controls; they target end users themselves. This allows fraudsters to defeat the intent of login controls by intercepting credentials and one-time passcodes upstream through fake portals and adversary-in-the-middle workflows, then using them to access the legitimate institution.

The most important moment in an ATO attack is not the login attempt. It is the moment an end-user's credentials are stolen. That moment occurs entirely outside your environment, and in most cases, the victim never knows it happened.

[1] 2025 Identity Fraud Study: Breaking Barriers to Innovation | Javelin
[2] Q3 2024 DIGITAL TRUST INDEX | Sift
[3] Sift Q3 2025 Digital Trust Index

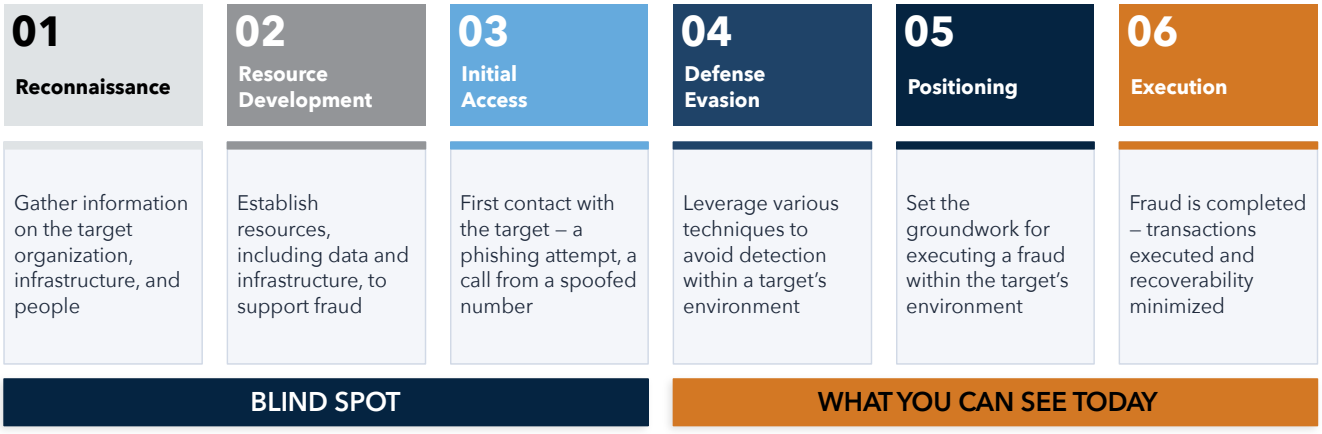
© 2026 Anti Fraud Advisors (AFA LLC) & Memcyco. Confidential & Proprietary.

THE BLIND SPOT

To understand why institutional controls have fallen short, it's important to understand the lifecycle of an ATO attack. An ATO attack consists of many steps or phases. However, most institutions today only have visibility into the latter half of that process. Thus, there's a critical blind spot in their defenses.

Let's use a phishing attack to illustrate this.

1. **Reconnaissance:** Fraudsters identify a target institution for a phishing campaign based on known control weaknesses or availability of targets within the institution's user base. They acquire information about end-users to target.
2. **Resource Development:** Fraudsters register lookalike domains (e.g., Internationalized Domain Name homograph) and leverage tools to clone the target institution's website. Fraudsters also develop ads, design Search Engine Optimization (SEO) poisoning campaigns, and prepare phishing campaign material.
3. **Initial Access:** Fraudsters deploy ads, SEO poisoning, and phishing campaigns to redirect and lure unsuspecting victims to the lookalike domains via search engines, emails, SMSs, and social media. Victims' credentials are harvested through these campaigns.
4. **Defense Evasion:** Fraudsters leverage a combination of tactics to deceive both the institution and victims. Fraudsters log in with credentials unknowingly supplied by end-users visiting the cloned site, with the institution having limited visibility of this.
5. **Positioning:** Fraudsters apply for additional credit products and add payees (e.g., wire recipient, Zelle recipient) in preparation for fund extraction.
6. **Execution:** Fraudsters execute transfers to accounts in their control and carry out credit bust-out frauds.



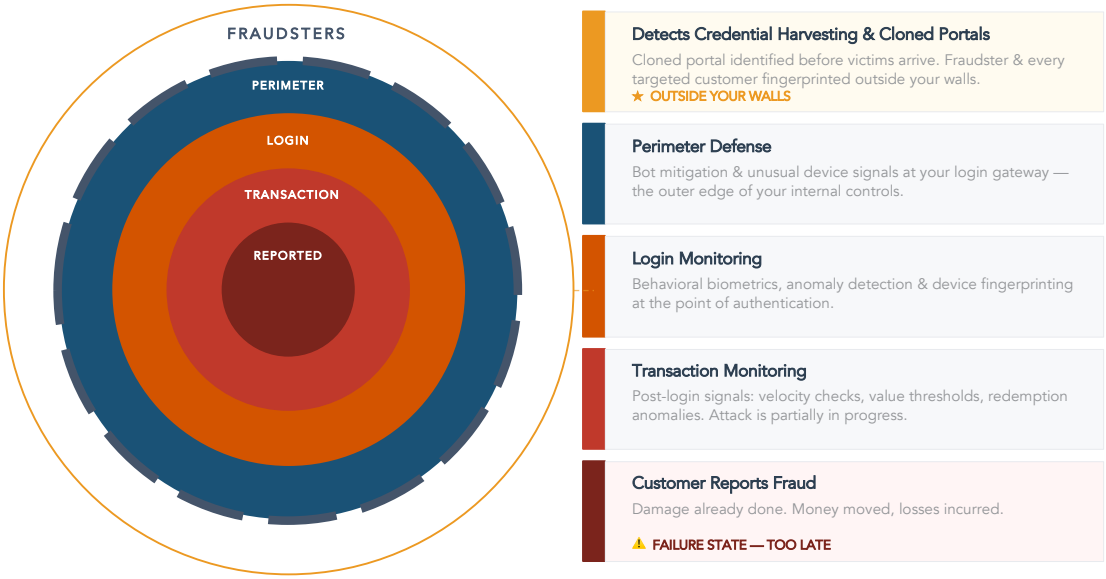
Our threat research finds that there is often a 48 to 72-hour period from when the credentials were compromised and the first fraudulent login. This presents an opportunity for institutions to identify end-users that may be compromised and take action to protect the end-user and the institution.

© 2026 Anti Fraud Advisors (AFA LLC) & Memcyco. Confidential & Proprietary.

SEEING BEYOND YOUR OWN WALLS

Closing this gap requires extending your fraud-detection perimeter beyond your own walls. If the first phases of an ATO attack are upstream of your environment, detection must operate there as well. This is not a replacement for your existing fraud stack. This helps bridge the visibility gap your current tools cannot address.

Memcyco is uniquely positioned to provide intelligence beyond your own walls. When a fraudster clones your institution's website to harvest users' credentials, they believe they are working undetected. However, Memcyco changes the economics of cloned-site attacks. When attackers copy protected elements from the legitimate site, Memcyco can surface signals from the cloned environment, identify affected users and suspicious devices, and give institutions earlier visibility before stolen credentials are used for account takeover.



This allows institutions to have immediate awareness of the creation of cloned sites, access to a registry of known fraudsters' devices, and the ability to identify every one of their end-users who visits the cloned site. The result is intelligence beyond what traditional vendors can provide: a real-time view of an active attack and a verified list of exposed end-users before any login attempt is made. This attack-level and victim-level visibility is unique to this class of tooling and goes beyond what tools limited to activity inside your own walls are designed to provide.

- ✓ **Cloned Portal Detection**: Identifies fake banking portals and credential-harvesting kits the moment they are assembled, giving your fraud team hours or days of advance warning before stolen credentials are used.
- ✓ **Exposed User Identification**: When end-users unknowingly submit credentials to a fake portal, Memcyco identifies exactly which end-users were exposed, enabling proactive account protection before an attacker acts.
- ✓ **Credential Deception and Attack Intelligence**: When end-users unknowingly submit credentials to a fake portal, Memcyco scrambles what the attacker receives and embeds a unique tracer. Stolen credentials become actionable intelligence, rather than a point of compromise.

© 2026 Anti Fraud Advisors (AFA LLC) & Memcyco. Confidential & Proprietary.

HOW WE CAN HELP

Extending the observability of your fraud program is not simply a technology decision. It requires a clear assessment of where your current program has gaps, a strategy for deploying new controls in the right sequence, a defensible business case, and validation that new controls perform as intended. Anti Fraud Advisors brings specialized expertise at each stage.

Fraud Program Assessment

We can evaluate your current fraud program capabilities against your relevant fraud risks, mapping where your controls provide coverage, where gaps exist, and how well you are positioned to be able to manage your current and emerging fraud risks.

Fraud Red Team

We actively attack your institution the way a sophisticated fraudster would. This allows you to assess your program's performance in a "live-fire" exercise, but unlike actual fraudsters, we share with you how your controls are being defeated and provide recommendations to enhance your program, before fraudsters further exploit gaps in your defenses.

Fraud Controls Strategy

We work with your fraud, risk, and technology teams to define a prioritized roadmap for enhancing, rationalizing, and deploying new controls. This includes sequencing, integration architecture, control interdependencies, and which actions are invoked, at what point, so new capabilities complement, rather than conflict with your existing fraud stack, and you're able to convert information into actions.

Business Case Development

We build the financial and operational case for introducing new capabilities into your technology stack, quantifying the risk exposure addressed, expected loss reduction, cost of inaction, and ROI of upstream detection. We translate fraud program improvements into the language of risk and finance that executive and board-level stakeholders require.

Conclusion

Almost all anti-fraud tools deployed by financial institutions today focus on what happens within their own walls. Authentication controls are circumvented upstream, detection models fire only after the attacker has already logged in, and end-users are victimized without any awareness. These are not edge cases. They are the structural consequence of fraudsters adapting their attack techniques, steadily eroding the effectiveness of stronger authentication controls.

Closing this gap requires visibility beyond what can be observed inside your own walls: identifying fake portals before credentials are harvested, flagging exposed end-users before accounts are accessed, and acting before losses occur. Yet visibility alone is not enough. Even when threats are identified, institutions face the added challenge of translating that awareness into fast, accurate, and coordinated action, without overwhelming already stretched teams or introducing new friction into operations.

Anti Fraud Advisors and Memcyco are helping institutions make this shift, shining a light on what may not be visible today and enabling the decisive action that follows.

© 2026 Anti Fraud Advisors (AFA LLC) & Memcyco. Confidential & Proprietary.