FRAUD FIGHTER

ACCOUNT TAKEOVER FRAUD (ATO)

What is ATO Fraud?

ATO fraud is recognized as a top threat to financial institutions and their customers due to the major direct financial losses experienced, as well as the lengthy and costly post-incident mitigation efforts required.

Whether initiated by a lone individual, criminal groups, or rogue stats, hackers today conduct industrial scale data mining and social media phishing operations to acquire consumer login credentials at scale. This not only leads to a host of direct losses but also raises the costs of **security**, **investigation**, and **remediation costs**.

Today, ATO fraud is gaining traction as unregulated sections of the internet, the so-called "Dark Web", have created a marketplace for stolen information. Concurrently, with more digital accounts being opened every day, fraudsters have more opportunities to exploit vulnerabilities such as duplicate passwords.

Typical ATO Scenario

Criminal obtains consumer account information, such as username and password, which have often been illicitly obtained in a data breach.

Criminal takes control of the accout by changing password, ownership information, security questions, 2-factor authentication devices etc.

Criminal is free to conduct activities, such as accessing bank funds, stored ACH information, transferring funds via Venmo/PayPal, open new accounts, and make purchases.

ATO Fraud Methods

Phishing

Data breaches are not exclusively caused by external actors. Sometimes, employee can inadvertently communicate sensitive information or provide unauthorized access to third parties. Hackers continue to develop new means of exploiting people's trust and attentiveness to small details. Unfortunately, these types of attacks, in their various formats, have been wildly successful in the past:

Email Phishing
Most common method, with emails widely blasted to a large respondent base

Spear Phishing
Emails sent to a targeted individual vor group

Whaling
Phishing attack specifically aimed at high net worth individuals

Vishing
Voice / phone fraud where a fraudster impersonates a bank employee under the pretext of calling to warn about account access issues

Smishing
SMS text messages containing a link to a fake banking portal; can also take the form of a messenger-based scam

Credential Stuffing

This method preys on the tendency of individuals to reuse passwords and other credentials on multiple online accounts. When acquiring lists of stolen credentials on the Dark Web, hackers utilize bots to log the stolen credentials automatically and rapidly into multiple websites and services.

Malware

Malicious software is a widespread and lucrative method for a hacker to take control of an individual's bank account, the entire bank itself, or even shut down or damage an entire organization's technology infrastructure.

Malware can be welcomed and walked into a company's network via emailed phishing links, but can also be introduced via downloaded apps. Whether it is a disguised weather or chat app downloaded onto a user's smartphone using company Wi-Fi, or a known plug-in mistakenly downloaded from an unsanctioned website, malware can be easily pulled in and wreak all sorts of havoc that might take weeks or months to recover from.

Overlay Attacks

Fake screens created for smartphones or tablets, to impersonate legitimate banking / ecommerce sites and collect login credentials.

These fake screens are "Mobile Banking Trojan" malware that captures the victim's authentication credentials and can remain active while other banking transactions are performed. The malware can then intercept a funds transfer and redirect the money to a fraudulent account. As our use of smartphones and tablets to conduct remote financial transactions grows, breaches and losses from these types of attacks are expected to skyrocket globally.

Man-in-the-Middle Attacks

In a Man-in-the-Middle attack, hackers exploit weak, unsecured Wi-Fi hotspots to monitor and intercept private data transmitted by users to their target website or financial institution. Using software obtained on the Dark Web, the coffee drinking customer next to you could be a hacker viewing all traffic on the Wi-Fi network, able to intercept, edit, send, and receive your data without being noticed.

Sim Card Swapping

1. Fraudster steals customer credentials and mobile phone number.
2. Fraudster manipulates the mobile operator to perform as sim Swap.
3. Fraudster uses the new credentials to log into victim's bank account.
4. Bank sends an SMS OTP or 2FA to victim's phone number.
5. The verification arrives on the fraudster's phone, which can be used to access the account.

A fraudster's goal in SIM card swapping is to intercept / access the "one-time" recovery PIN texted to our phones in the event we cannot remember our login credentials.

In fact, more and more websites are deploying texted PINs after every login, used as automatic 2FA (Two Factor Authentication) or MFA (Multi Factor Authentication) identity verification security. Unfortunately, this system can easily be defeated by, again, human social engineering tactics.

In a SIM card swap scam, the fraudster contacts a customer's mobile phone carrier and successfully impersonates the customer, using "knowledge data" collected from a data breach. He then convinces the call center agent to port the (real customer's) mobile phone number to the illegal SIM card, which is then inserted and activated in the fraudster's phone.

You're Not Alone

Vendors such as Uveritech in the anti-fraud industry have developed solutions that combine best-class identity authentication with an automated, transparent, and multi-layered approach to security. Contact us or visit our website to learn more about our wide range of identity and currency verification solutions.