TruStage™

Account takeovers

Risk overview

Losses from account takeovers of member accounts have increased significantly in frequency and severity in recent years. Several credit unions have incurred seven-figure account takeover fraud losses.

Account takeover is a type of identity fraud where fraudsters leverage a person's existing credentials to take control of their legitimate financial, credit, email, or social media accounts. This unauthorized access to user accounts can lead to various account takeover attacks.

Unfortunately, just about every type of industry that holds sensitive data is at risk of account takeover-based fraud.

Fraudsters have launched sophisticated social engineering attacks against credit union members to scam them into providing their online banking login credentials, including two-factor authentication passcodes.

How account takeovers happen

There are a variety of methods used by fraudsters in their account takeover efforts, including:

- Social engineering
- Phishing, SMiShing & Vishing
- Brute force attacks
- Credential stuffing
- Malware
- Man-in-the-browser attacks
- Application flaws

⚠ Losses from account takeovers can escalate very quickly as fraudsters can potentially target a very large number of members every day over the course of consecutive days. A credit union could potentially incur thousands of dollars in daily losses.

The dark web has made account takeover fraud much more attractive to attackers by reducing liability as they no longer need to steal directly from targeted users. Fraudsters can simply purchase valid login credentials instead of performing the tiring task of cracking passwords.

The network of increased online financial accounts and offerings also fuel account takeovers.

A significant negative impact is having member accounts drained by fraudsters and their fraudulent transactions. However, these financial losses can also bring on significant organizational reputation damage and potential legal ramifications due to data security and protection of personal data.

Social engineering against members

Fraudsters deploy the same social engineering tactics used in the P2P/Zelle scam to scam members into providing their login credentials – usernames and two-factor authentication passcodes.

Here's how the scam works:

- Fraudsters send text alerts to members – appearing to come from the credit union – warning them of suspicious transactions on their accounts.
- Members responding to the text receive an immediate phone call from the fraudsters spoofing the credit union's phone number. The fraudsters claim to be from the credit union's fraud department and are calling to discuss the suspicious transactions.
- Fraudsters ask for members' online banking usernames to verify their identity. In the background, the fraudsters use the usernames with the "forgot password" feature which triggers a two-factor authentication passcode to members that must be entered to reset the passwords.
- Fraudsters tell members they will receive a passcode and the members must provide it over the phone to the fraudsters as an additional identity verification step.
- Members receive the passcode and provide it to the fraudsters who use it to successfully reset members' online banking passwords.
- Fraudsters login to the accounts and use external transfer service to transfer funds to external money mule accounts.

Upon logging into member accounts, the fraudsters typically change their contact information (home and mobile phone numbers and email addresses) through the member profile feature. This allows the fraudsters to intercept any notifications or fraud alerts from the credit union regarding suspicious transactions.

Account takeover fraud: $2M loss

- Members received a text alert – appearing to come from the credit union – warning them of a suspicious debit card transaction.
- Members responding to the text received an immediate phone call from the fraudsters spoofing the credit union's phone number. The fraudsters claimed to be from the credit union's fraud department.
- Fraudsters conned the members into providing their online banking username which the fraudsters used with the "forgot password" feature triggering a two-factor authentication passcode to the members.
- Members provided the passcode to the fraudsters who used them to reset the passwords.
- Fraudsters logged into the accounts and used external transfer service to transfer funds to external money mule accounts.

In some cases, the fraudulent text alerts contain a link to a spoofed website that is made to appear like the credit union's online banking login page. Members click on the link and enter their usernames and passwords to the spoofed website. The fraudsters use the credentials to login to member accounts; however, the logins trigger two-factor authentication passcodes to the members due to the fraudsters using unregistered devices. However, the members enter the passcodes to the spoofed website which the fraudsters immediately use to complete the login to member accounts.

In another version, fraudsters call members directly - spoofing the credit union's phone number – and claim to be from the credit union's fraud department. The fraudsters then use the same tactics to con the members into providing online banking usernames and two-factor authentication passcodes triggered by the fraudsters using the "forgot password" feature to reset member passwords.

Social engineering against members

A newer trend has the compromised member accounts, and the money mule accounts at the same credit union. The fraudsters recruit money mules to open accounts at the target credit union for an opportunity to earn easy money.

Once the mule accounts are opened, the fraudsters launch their social engineering attack against existing members to harvest login credentials. Fraudsters use the member-to-member transfer feature to make large dollar transfers from the compromised accounts to the money mule accounts. The money mules withdraw the funds through various means, including in person large cash or check withdrawals at a branch, requesting a wire transfer, and debit card transactions (ATM withdrawals and/or POS transactions to purchase gift cards).

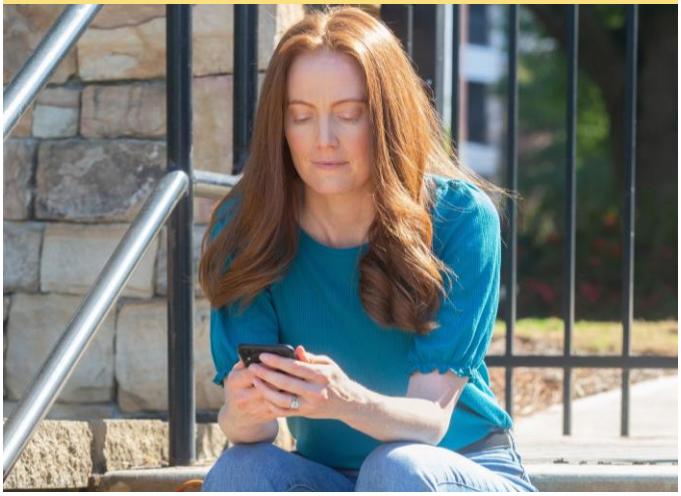
Who are money mules?

- **Unwitting participants** - These money mules are typically recruited through online job scams, won a sweepstakes, or strike up an online relationship and are unaware that they are engaged in criminal activity.
- **Witting participants** - These money mules are aware that they may be involved in suspicious activity but engage in it anyway.
- **Complicit participants** - These money mules are fully aware that they are engaged in criminal activity.

Money mules may open accounts under their own identity. Alternately, they may be instructed to open the accounts using a stolen or synthetic identity.

Account takeover fraud: $2.5M loss

- Fraudsters recruited money mules through social media to open accounts at a specific credit union.
- Once the mule accounts were opened, the fraudsters launched their social engineering attack against existing members.
- Rather than start with sending fraudulent text alerts, the fraudsters called members – spoofing the credit union's phone number – impersonating employees from the credit union's fraud department.
- Fraudsters conned members into providing their online banking usernames which the fraudsters used with the "forgot password" feature triggering a two-factor authentication passcode to the members.
- Members provided the passcode to the fraudsters who used them to reset the passwords.
- Once logged into the compromised accounts, the fraudsters initiated large dollar member-to-member transfers to the money mule accounts.
- The money mules withdrew the funds through various means.



Social engineering against members

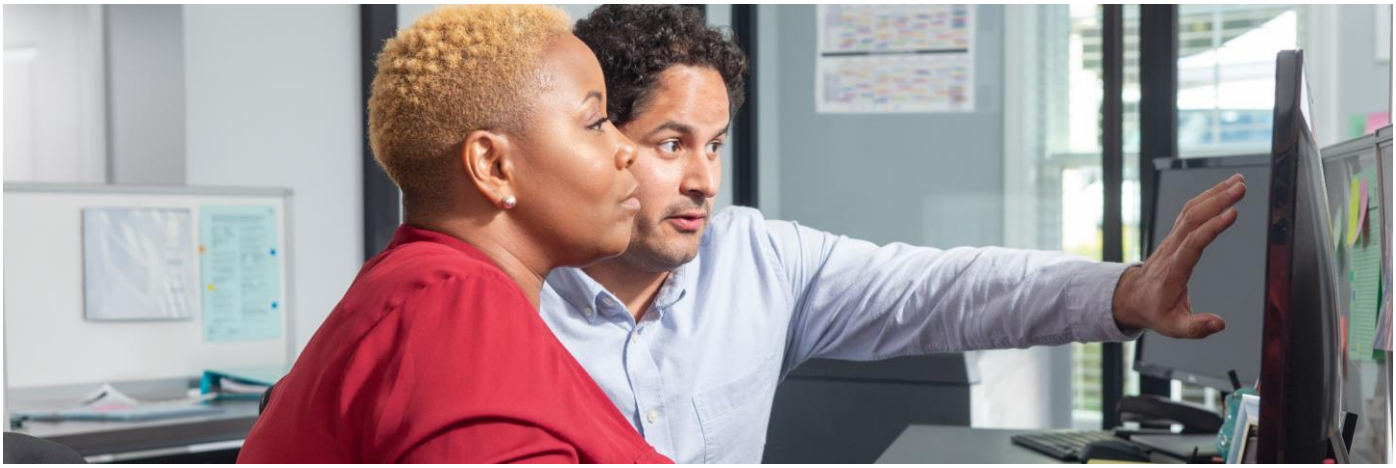
Other less common social engineering tactics used in fraudsters' account takeover efforts include:

- Fraudsters may **enroll member accounts for online banking** through the credit union's website. They have enough of the members' personal information to enroll the accounts. Credit unions typically send an online banking enrollment passcode to members by text message, email or automated phone call and members must enter the passcode to complete the online enrollment. Fraudsters generally request the passcode to be delivered via email since they hacked the member's email account to intercept the passcode.
- Fraudsters may **launch a phishing attack against members with a link to a spoofed website** made to appear like the credit union's online banking login page. Fraudsters harvest members' usernames, passwords, and two-factor authentication passcodes.
- Fraudsters may **deploy social engineering tactics against credit union call centers** by impersonating members to reset member passwords or to have member contact information, such as mobile phone numbers, changed on the accounts.

  A credit union reported an $800k online wire fraud loss when a fraudster impersonated the member and social engineered a call center employee into changing the member's home and mobile phone numbers and resetting the member's online banking password. A two-factor authentication passcode was triggered when the fraudster attempted to login to the account, but the passcode was sent to the fraudster's mobile device. The fraudster requested two wires totaling $800k. A callback verification was made for each wire request, but the calls went to the fraudster who answered the security questions.
- Fraudsters may **deploy social engineering tactics against mobile carriers**, such as the case in the SIM swap and port-out scams. This allows the fraudsters to intercept two-factor passcodes transmitted in text messages that may be used by fraudsters to enroll member accounts for online banking, reset member passwords using the "forgot password" feature, or when logging into member accounts with an unregistered device.

  In the SIM swap scam the fraudster impersonates a mobile phone user and social engineers the user's mobile phone carrier into activating a replacement SIM card the fraudster has in their possession.

  In the port-out scam the fraudster social engineers a mobile phone carrier into porting the user's service to a different carrier using the same mobile phone number.



Other account takeover methods

While fraudsters have often relied on sophisticated social engineering tactics to scam members out of their login credentials, there are other methods being used by fraudsters in their account takeover efforts.

Brute force attacks

In a brute force attack, fraudsters deploy trial and error techniques to guess login credentials. It is a simple yet effective tactic for gaining unauthorized access to individuals' accounts through online banking. Using bots and botnets, fraudsters can continuously try to guess login credentials at a frequency and speed that humans cannot replicate.

A security feature built into web application login forms blocks user IP addresses after a certain number of failed login attempts. By using bots to launch their attack, the logins appear to come from a variety of devices and from different IP addresses.

Credential stuffing

Credential stuffing is a subset of brute force attacks. Fraudsters use login credentials obtained from a data breach or from the dark web. It is particularly effective as people frequently use the same login credentials for multiple websites.

Similar to brute force attacks, fraudsters use bots and botnets for automation and scale and to circumvent the security feature for failed login attempts.

Malware

Credential stealing malware – also referred to as banking trojans – is another method deployed by fraudsters to steal login credentials. Fraudsters commonly distribute malware in phishing attacks – either as an infected attachment or a link to an infected/malicious website.

Cybercriminals have developed sophisticated malware toolkits that are sold on the dark web. The toolkits can be customized to target specific online banking websites. The malware lays dormant on the user's browser and springs to life when the user visits a targeted online banking website.

These toolkits are frequently used in **man-in-the-browser** (MITB) attacks. In a MITB attack, the malware lays dormant in the user's browser and is activated when the user navigates to a targeted online banking website. Once the user logs into their account the MITB can piggyback on the online banking session and overwrite transfers entered by the user changing the amounts and destination accounts without the user's knowledge. Authentication methods, including two-factor authentication, are generally ineffective against MITB attacks.

Application flaws

Fraudsters may exploit vulnerabilities in one of the software applications an organization uses. Simply put, a flaw in a company's database management software, e-commerce platform, or email system can provide an open door through which a hacker can walk in and wreak havoc, including brute force attacks.

The unauthorized retrieval, transfer, or copying of data from a device or server can provide attackers access to login credentials, such as usernames and passwords, to gain control of an account.

Key risk mitigation actions

- Educate members on the social engineering tactics used by fraudsters to obtain online banking login credentials.
- Warn members that the credit union would never ask for login credentials including two-factor authentication passcodes.
- Warn members to not rely on caller ID and instruct them to call the credit union using a reliable phone number if they receive a text or call from someone purporting to be from the credit union.
- Use strong passwords and do not re-use the same passwords for other e-commerce sites.
- Educate members on proper email hygiene.
- Properly authenticate members enrolling for online banking through the credit union's website. Avoid sending online banking enrollment passcodes via email due to the risk of email hacking.
- Avoid resetting passwords based on a member's phone request.
- Change the settings to the "forgot password" feature so that members cannot use it with an unregistered device.
- Deploy a more secure form of two-factor authentication, such as a token or push notifications to a dedicated app residing on the member's device.
- Deploy a real-time fraud monitoring solution with behavioral analytics that leverages the use of artificial intelligence and machine learning.
- Require signed authorizations before members can make member-to-member transfers.
- Block and review large dollar external transfers and large dollar member-to-member transfers that occur immediately following a password reset.
- Ensure transaction limits – single transaction and daily limit – for payment types offered through online banking, including member-to-member transfers, are reasonable.

Important note: Fidelity Bond Condition 12

If you find yourself in the midst of an account takeover spree with a large number of members targeted every day while racking up thousands in daily losses; remember that **Condition 12 in the Fidelity Bond** requires credit unions to take all reasonable measures to minimize the loss after its discovered. Failure to do so could jeopardize a claim.

In these cases, credit unions often take a step ladder approach to stop the fraud. For example, a credit union may lower the transaction limit for the payment type targeted by the fraudsters and/or develop a fraud rule to block and review transfers that meet certain criteria.

If these steps are not effective at stopping the fraud, the credit union may deploy additional controls. There are times when the only way to stop the fraud is to temporarily disable the payment type targeted by the fraudsters.

For additional support, contact a TruStage risk consultant at **800.637.2676** or email **riskconsultant@trustage.com**

TruStage