TRUSTAGE Account takeovers

Losses from account takeovers can escalate very quickly as a large number of members can be targeted.

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.

Fraudsters have launched sophisticated social engineering attacks against credit union members, and, in turn, member accounts have been drained by fraudsters and their fraudulent transactions.

These fraudsters typically are:

- Manipulating your members getting them to provide login credentials, and two-factor authentication passcodes, by spoofing the credit unions' phone number.
- Targeting your call center employees and getting them to reset member passwords and change member contact information.
- Simply asking the member for missing pieces as they already have some information from previous compromises.

From that point, they gain necessary access to fraudulently transfer the funds that they want.

FAQs

- **How are fraudsters able to access and transfer funds out of our members' accounts?**+

Once fraudsters gain access to your members' online banking account through social engineering, they typically access funds one of these ways:

  - They conduct a transaction through an external transfer service sending money to another financial institution. Think of commonly used peer-to-peer (P2P) services like Zelle, Venmo and PayPal.
  - They make external transfers to an account at another financial institution, or use internal member-to-member account transfers.

No matter the method, the fraudsters have usually blocked the member from accessing their account by changing the password on the account. Then, they will begin to transfer funds out of the account, typically to a money mule account.

- **How do money mules participate in account takeovers?**+

Money mules are typically recruited by fraudsters to assist in laundering funds derived from criminal activities — knowingly or unknowingly. Unfortunately, these individuals add layers of recipients to the money trail, making it difficult for law enforcement to trace the money.

In account takeover schemes, money mules are usually instructed to open accounts at financial institutions and may do so using stolen or synthetic identities. After the accounts are opened, the money mules generally receive unusually large electronic deposits, such as ACH credit transfers or wires. Of course, they are instructed to transfer the funds elsewhere.

Fraudsters will target account-to-account (A2A) or external transfer services to transfer funds out of member accounts to accounts under their control at other institutions.

While the fraudsters typically transfer funds from the compromised member accounts to external money mule accounts, a recent trend has the account takeovers and transfers to money mule accounts occurring at the same credit union.

- **Do you have controls in place to minimize account takeover fraud and losses?**+

Managing the risks of account takeovers through online banking requires a layered security program. One of the most common tools is the use of two-factor authentication relying on a passcode. Transmitting one-time passwords in SMS text messages continues to be a common delivery method. However, fraudsters' social engineering tactics allow them to successfully hijack incoming calls and SMS text messages.

Consider either:

  - Push notifications to a dedicated app residing on the member's mobile device which alerts the member of attempted logins. The member is given a choice to approve or deny the login attempt.

- Implement a soft token that resides on the member’s mobile device which generates a one-time-passcode that the member must enter to complete the login.

Other risk mitigation strategies to help combat account takeover trends and losses include, but are not limited to:

- Educate and warn members of scams designed to obtain their login credentials and/or debit card details. Don’t forget to explain that phishing, SMiShing and vishing attempts will often spoof phone numbers and websites that appear to be from the credit union.
- Deploy an identity verification solution capable of detecting synthetic identities.
- Don't allow members to use the "forgot password" feature using an unregistered device.
- Require signed authorizations before allowing member-to-member transfers.
- Implement reasonable monetary limits for the member-to-member transfer feature.