Life

NORTH AMERICAN®
A Sammons Financial Company
North American Company for Life and Health Insurance®

Field Bulletin

Account Takeover (ATO) – What is it?

514NB

Account Takeover is a type of theft where an unauthorized 3rd party, known as a "Fraudster" gains access to an account with the intent of stealing funds. This usually happens when the fraudster has acquired another person's personally identifiable information ("PII") and uses the information to create an online account or impersonate a policy owner by phone. Once the fraudster takes over an account, they change contact information (such as email, phone number, or address) to keep the policy owner unaware and divert company communication. The fraudster can then begin requesting electronic funds transfer ("EFT") change forms, partial withdrawal/loan request forms, or full surrender forms to be mailed or emailed to the new contact information to complete and submit back to the Company.

Fraudsters are often patient, holding information for long periods of time before launching an attack when vigilance decreases.

Industry ATO data*

- ATO incidents overall increased by 13% in 2023. Attacks are often initiated through contact centers, agent/producer portals and customer portals. Customer portal attacks have been rising steadily: 63% of portals were accessed by fraudsters.
- Customer remains the top detection method.
- On average, detection takes 9.5 days.

ATO Red Flags for Producers

- Urgent disbursement requests from clients via email.
- Multiple changes to a client's contact information, including, but not limited to email, phone number, address, and banking information.
- Requests to assist a client in accessing the web portal.
- Clients become unreachable by phone and/or they are out of the country after changes/transactions have been requested.

Tips for Protecting yourself and Your Client's Information

- Opt for multifactor authentication when available.
- Regularly change email passwords or web login passwords.
- Use Strong Passwords
    - Passwords should consist of 12-14 characters with a combination of numbers, letters, and symbols.

- Do not use the same username or password across multiple platforms.
- Do not send PII information (including Policy/Contract/Account Numbers) via an unsecure email platform; use encryption if possible.
- Keep virus software and malware programs updated.
- Monitor other financial accounts for suspicious activity.
- Stay informed about phishing scams.
- Use secure networks; avoid using public Wi-Fi for accessing sensitive information unless you are connected via a VPN.
- Educate Clients about common security practices.
- Regularly backup data to prevent loss due to system failures or cyber-attacks.

What are we doing to prevent this activity?

Today, we are seeing an increase in this type of activity specifically through policyholder or agent's email or web portal accounts being compromised.

To help prevent fraudsters from accessing online accounts, North American's Special Investigations Unit has many procedures in place to alert us of suspicious account activity. Additionally, we conduct regular training with our internal business partners to help enhance their fraud detection skills as early detection increases the chance of recovery.

How Can You Help?

In addition to the red flags listed above, please review your client's contracts regularly and alert us immediately if you suspect any unusual activity. Referrals can be reported directly to our internal Special Investigations Unit at SIU@sfgmembers.com or by calling our Customer Contact Department.

If you have questions about this bulletin, please email the Compliance Team at SIU@sfgmembers.com.

* Data is obtained from FraudShare, a 3rd party platform used by multiple insurance carriers to report known fraudulent data.