Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

SUMMARY

Account takeover fraud is hitting financial institutions hard! This type of fraud occurs when a fraudster gains access to a legitimate user's account to make unauthorized transactions. Typically, attackers employ phishing techniques – sending deceptive emails or messages that appear to be from your credit union, tricking users into revealing their login credentials or other sensitive information voluntarily.

REAL LIFE EXAMPLE OF HOW THESE ATTACKS ARE PERPETRATED

An accountholder lost $70,000 after receiving an urgent text message that appeared to come from his financial institution telling him to log onto a website. The accountholder clicked the website link and provided the requested information. Four days later the accountholder discovered that the scammer had changed his password and transferred $70,000 into a new account that the scammer had opened at the accountholder's financial institution the day before the fraud was perpetrated. The scammer then sent the money to a reloadable gift card. *Member education is critical, but it's not stopping these scams from happening.*

MITIGATION STEPS

- Only allow account-to-account transferers if the member is joint on the account
- Review recent account-to-account transfer enrollees
- Double Multi-Factor Authentication (MFA) is critical
- Compare geolocation of IP address used to accountholder's address
- IP blacklisting
- Utilize device recognition
- Device fingerprinting
- Don't allow accountholders to use "forgot password" feature using unregistered devices
- Deploy real time fraud monitoring for suspicious transactions with behavioral analytics
- Block headless browsers
- Disallow email addresses as user IDs
- Warn your members about this type of scam with a 90-second video that all Allied Solutions policyholders can request at no cost by contacting risk_specialist@alliedsolutions.net

NOTE: MEMBERS VICTIMIZED IN THESE SCAMS ARE ENTITLED TO REG E PROTECTION

- **Reg E's definition of an unauthorized EFT [§1005.2(m)]:** Unauthorized electronic fund transfer means an electronic fund transfer from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit.

RISK MITIGATION RESOURCES

- FAQ: Electronic Fund Transfers
- Visit Allied's Risk Alerts Library

LinkedIn Facebook