Allied Solutions

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

SUMMARY

Fraudsters are phishing, spoofing, and employing social engineering against your members using phone calls, text messages, emails, and chat and pretending to be your credit union. In these attacks, the bad actors ask your members for multiple authentication information such as online banking username and, PIN number, security code, account number, card number, and more with the intent to gain access to the members' account/s and drain their funds.

With the holidays upon us, bad actors are boosting their efforts. It's critical that we collaborate and share the following information with your team and membership to prevent them from being defrauded.

FRAUD IS EVOLVING

Fraudsters continue to evolve and find new ways to perpetrate fraud and trick credit union members. Below are recent examples of how bad actors are defrauding well-meaning individuals.

- Bad actors forward member calls to their credit union to a different number at which the member is unknowingly speaking to the fraudster.
    - Allied Solutions encourages credit unions to block call forwarding functionality.
- Fraudsters obtain authentication layers from members then contact the credit union, credit union call center, or the credit union's 3rd party vendor's call center and place a travel alert on their account so they can commit fraud in other states.
    - It's critical that you validate with your members that they did in fact place a travel alert on their account/s; this may include calling the member directly to confirm the alert. If using a 3rd party, require them to take extra steps before implementing a travel alert.
- Bad actors access members' online banking and reset their username and password. After they've gained control of the account, they change the phone number, email, and/or address of the member so they can intercept micro deposits or security codes that are sent.
    - Allied recommends that you, your call center, and/or your 3rd party call center be on high alert if these types of requests are received. You may want to consider not offering phone, email, or address changes on your online banking platform.

EDUCATING YOUR MEMBERS

Frequently educate your members that your credit union will never reach out to them via call, text, email, or chat requesting authentication, financial, or personal information. If your members are contacted requesting such information, inform them that bad actors have likely spoofed the credit union, and they should:

1. Not respond in any way
2. Contact the credit union directly to report the incident

RISK MITIGATION RESOURCES

- Visit Allied's Risk Alerts Library

LinkedIn Instagram