Allied Solutions

Thursday | March 31, 2022

Fraud Risk Bulletin

Exclusive, As-It-Happens Risk Updates and Insights

RISK ALERT

Before You Wire Money, Verify! Verify! Verify!

SUMMARY

Bad actors have become increasingly sophisticated and capable of a variety of tactics to obtain information for authenticating a wire transfer, such as:

- Forging a notary signature
- Forwarding calls from the accountholder's phone number
- Phishing accountholders
- Spoofing an accountholder's email
- Moving funds from one account to another
- Requesting changes on an accountholder's account before requesting the outgoing wire transfer

We strongly recommend your financial institution implement robust security measures with multiple layers of authentication before processing a wire transfer.

RISK MITIGATION STEPS

1. Since most wire fraud instances are happening in non-face-to-face environments, consider not offering outgoing wire transfers when the accountholder is not present.
2. Require signed wire transfer agreements (contracts) that include verification procedures determined by the accountholder (e.g., password, callback/text, security questions, etc.).
3. Use 3FA (3 factor authentication); 2FA at a minimum.
    - Something you know, such as a password or security questions
        - Create a unique PIN, password, or passcode for outgoing wire requests.
        - Confirm a security question between the financial institution and the accountholder.
        - Obtain and call back multiple telephone numbers, such as cell, work, and home. Never rely on only one call back telephone number.

Only use telephone numbers that you have on file for at least 30 days, not the phone number given to you at the time of the request.

- Something you have, such as a smart phone and APP such as DUO
  - A text with a code sent to your phone. If this method is used, include language such as, “ABC FCU will never call you for this code: 123456; it’s for online use only. Call ABC FCU now if you did not request or if you released it to someone who called you.”
- Something you are, such as your voice or other biometric method

4. Do not post your wire policies and procedures publicly. Doing so enables the bad actors to spot weaknesses.
5. Set a daily dollar limit for non-face-to-face wires without a wire transfer agreement.
6. Limit employees authorized to perform wire transfers and set dollar limits by employee, such as: over $5,000 requires manager approval, over $25,000 requires VP approval.
7. Call back to a phone number that you have, not the one the caller is giving you or including in an email. Be sure that phone number has not been changed within the last 60 days.
8. Restrict the IP address(es) for financial institution for all outgoing wires.
9. Pay special attention to wires from a HELOC or transfer of HELOC funds to another account of the accountholder.
10. Be aware of mortgage wire fraud during closing. Take extra steps to protect your accountholder from falling victim to scams directing payments to be wired to bad actors.
    - Did the wiring instructions come from the actual closing agent? Was an email address or phone number that matches the closing agent’s used?
    - Was there a last-minute change in wiring instructions (e.g., changes in the recipient financial institution, address, or email)?
11. Flag outgoing international wire requests "high risk" and take extra measures before performing the wire request or consider not offering international wire requests.
12. Educate accountholders and staff at all levels about wire fraud prevention.
13. Audit wire transfers performed to ensure compliance with your written procedures.

RISK MITIGATION RESOURCES

Sign up for our fraud risk e-newsletter and our webinar series, Let's Talk Fraud.

Visit our website for fraud prevention resources.

Contact a risk specialist here

LinkedIn Twitter Facebook