RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

Alert Type | Awareness | Watch | **Warning**

Fraudulent Wire Transfers Impact Corporate Accounts

Cyber criminals are again targeting credit unions' corporate accounts via fraudulent wire transfers. They do this by compromising employees' login credentials and accessing the ACH/wire transfer systems to initiate a wire transfer out of the credit union's corporate account.

Details

There has been an uptick in fraudulent wire transfers from credit union corporate accounts at corporate credit unions. Fraudsters access the corporate credit union's ACH / wire systems using stolen login credentials to request wires.

These losses can be significant and has exceeded $1million. In a few cases, the thieves circumvented the dual control requirement that requires a second credit union employee to login to the wire transfer system to approve a wire entered by another employee. The fraudster knew both usernames and passwords.

The most common form of stealing these credentials is through spear phishing attacks specifically targeting certain staff. The employee's computer then becomes infected with malware or keyloggers capture the employees' log-in credentials. One credit union experienced a compromise of several email accounts. This resulted in several fraudulent emails being sent to the corporate credit union requesting wires.

Risk Mitigation Tips

Consider these risk mitigation tips:

- Use a dedicated computer to access third party ACH and wire transfer systems and prohibit using such computer for email or internet browsing.
- An alternative to using a dedicated computer is to use a separate operating system and browser written to a USB flash drive. When the user needs to access the third-party vendor's system, they would boot the operating system from the flash drive on their existing computer or a dedicated computer and use the browser from the flash drive to access the system.
- Prohibit telecommuters from accessing the ACH and wire transfer systems using their home computers.
- Use the strongest form of multifactor authentication offered by the corporate credit union or bank to access the ACH and wire systems.

Continued…

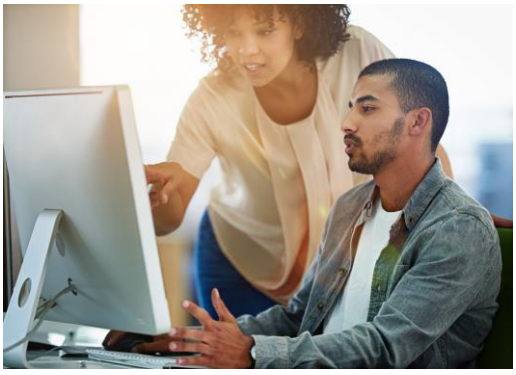
Date: October 5, 2021

Risk Category: Funds / Wire Transfer; Fraud; Malware

States: All

Share with:

- ☐ Executive Management
- ☐ Legal / Compliance
- ☐ Risk Manager
- ☐ Transaction Services



Facing risk challenges?

Schedule a free personalized discussion with a Risk Consultant to learn more about managing risk.

Risk Mitigation (continued)

- Deploy the following controls, if offered:
  - Restrict the days and hours of access to the ACH and wire transfer systems
  - Restrict the credit union's IP addresses with access to the ACH and wire transfer systems
  - Set individual transaction limits
  - Enforce dual control feature and
  - Validation and confirmation process for transfers exceeding a specific dollar amount.
- Notify your corporate credit union or bank immediately when there is a change in employees authorized to access the ACH and wire systems.
- Deploy up to date antivirus, anti-malware and anti-spyware which should be configured to allow for automatic updates.
- Install patches to operating systems as soon as they are available.
- Deploy anti-spam controls.
- Deploy content filtering software to block employee access to unauthorized websites; and
- Establish and enforce a credit union wide acceptable use policy for credit union owned computers which should include internet browsing and email.

Risk Prevention Resources

Access CUNA Mutual Group's **Protection Resource Center** at cunamutual.com for exclusive risk and compliance resources to assist with your loss control efforts. The Protection Resource Center requires a User ID and password.

- Wire Transfer Risk Overview
- Cybersecurity Threat Outlook

Access the Protection Resource Center for exclusive resources:

- Loss Prevention Library for resources & checklists
- Webinars and Education
- RISK Alerts Library
- Report a RISK Alert

The Protection Resource Center requires a User ID and Password.