RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Fraudulent Wire Transfers Generated From Email Scams

Cybercriminals have gone to great lengths throughout 2020 to commit theft or fraud by manipulating credit union executives, employees, and even business members using fake or doctored emails. The surge of business email compromise (BEC) and fraudulent instruction scams typically request large wire transfers. These urgent requests often exceed $1 million.

Details

Business Email Compromise (BEC) scams – fraudsters impersonating an organization's CEO or another executive through a spoofed email – often request other employees to send a wire transfer as part of a fraudulent transaction. However, this sophisticated form of social engineering appears now to be compromising business members emails as well.

Similar to the scam targeting credit union CEOs, fraudsters compromise or spoof the business member's email and send an email to the credit union requesting a wire transfer. A social engineering attack in which compromised email credentials or spoofing are used to induce a credit union employee to make a wire transfer or other electronic payment to a bank account controlled by a cybercriminal is commonly referred to as **fraudulent instruction**.

Both fraudulent instruction and business email compromise scams often focus the request as "urgent" or "pay immediately" in hopes that the employee does not take time to scrutinize the request. Once the criminals find the weak link, they continue to send these requests which can add up to large losses for a credit union.

According to Beazley, an increase in these scam-related losses coincides with the increase in remote working during the second quarter, suggesting that detecting and preventing social engineering scams has become more difficult with the increase in distractions working remotely.

A 96% increase in loss frequency and a 950% in credit union loss dollars paid related to business email compromise has occurred from 2018-2019 according to Beazley Breach Solutions claims data. In fact, financial institutions were among the most targeted industries in Q2 2020.

Protecting your credit union organization from social engineering and BEC doesn't need to be expensive. Making an investment in training and process changes can often reduce the likelihood of falling victim.

Date: October 6, 2020

Risk Category: Scam; Fraud; Fraudulent Emails; Business Email Compromise; Wire Transfer; Social Engineering

States: All

Share with:

- ☐ Accounting
- ☐ Executive Management
- ☐ Risk Manager
- ☐ Transaction Services
- ☐ People Leaders

Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Risk Mitigation Tips

Credit unions should consider these mitigation tips

- Train staff to be able to identify these types of scams and the procedures for handling internal wire transfer requests
- Avoid using public email accounts when communicating with staff and watch for email domains that may vary such as: ABC1cu.com vs. ABClcu.com
- Require credit union staff to match the email on file with the email involved with the wire transfer request
- Be alert for urgent wire requests or last-minute changes to wire instructions.
- Establish formal procedures for handling internal wire transfer requests. Confirm all requests involving vendors.
- Internal emails requesting a wire transfer should be authenticated using a different communications channel (out-of-band authentication), such as verifying face-to-face with the requestor or calling the requestor's phone extension or mobile phone. One successful practice is to have the accounting department verify internal requests for wires
- Limit the number of employees that have the authority to submit or approve wire transfers.
- Consider removing or not publishing employee information (names, titles and email addresses) on the credit union's website
- Don't trust contact details provided in the request. If the request is fraudulent, the criminal will have supplied fake contact information, too
- Adopt a written wire transfer agreement for business members due to the size of their potential wire transfer requests. In the absence of a signed wire transfer agreement, require business members to request large dollar wires in person.
- Alert business members of this scam
  - Suggest they avoid using public email accounts (e.g., Gmail, AOL, etc.). It is best to establish a company website domain and use it to create company email accounts.
  - Be aware of information posted on company websites and social media such as job duties, organizational structure or out of office details.

Risk Prevention Resources

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

- Business Email Compromise Risk Overview
- Online Risk Assessment: Funds and Wire Transfer
- Wire Transfer Risk Overview
- Cybersecurity Threat Outlook eBook

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.

Facing risk challenges?

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