RISK Alert

ACTIONABLE INSIGHTS FOR BOND POLICYHOLDERS.

CUNA MUTUAL GROUP

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

Business Email Compromise Scams Look to Exploit Remote Workers

Fraudsters have jumped on the opportunity to exploit weak security measures as employees adjust to remote working environments. By using a Business Email Compromise scam, fraudsters request wire transfers to pay vendors under the guise of executive management. According to Beazley Breach Solutions, there has been a 96% increase in loss frequency and a 950% increase in loss dollars paid to credit unions related to business email compromise.

Details

Business Email Compromise (BEC) scams – fraudsters impersonating an organization's CEO or another executive through a spoofed email requesting a wire transfer - have been around for several years. However, with the recent shift of many Americans working at home, the FBI expects an increase in BEC scams.

With credit union staff working remotely, fraudsters will likely pursue newer remote workers that aren't familiar with proper security protocols or follow lax controls. Additionally, fraudsters may use the excuse of the pandemic to urge staff to make payments they would not normally perform.

A BEC scam typically involves an executive level employee's email that has been compromised or spoofed through a phishing attack. The fraudsters create an email appearing to be sent from the executive's email to another individual within the organization requesting a payment – typically wire transfer – or purchase of gift cards.

Some red flags include:

- Urgency of the message
- Request to keep transaction confidential
- Communication only through email and refuses other communication channels
- Requests change in direct deposit information
- Requests for payments to be made to a different account since they are inaccessible due to the COVID-19 crisis

According to Beazley Breach Solutions claims data, there has been a 96% increase in loss frequency and a 950% in loss dollars paid in credit unions related to business email compromise from 2018-2019.

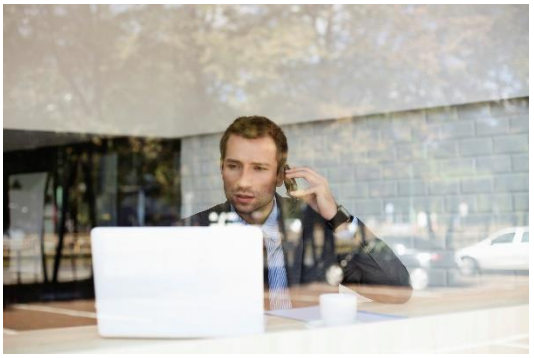
Date: May 12, 2020

Risk Category: Scams; Fraudulent Emails; Business Email Compromise; Wire Transfer

States: All

Share with:

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



Your feedback matters!

Was this RISK Alert helpful?

Vote Yes | Vote No

Risk Mitigation Tips

To manage risks related to business email compromise fraud, consider adopting these risk mitigation tips:

- Consider removing or not publishing employee information (names, titles and email addresses) on the credit union's website.
- Establish formal procedures for handling internal wire transfer requests. Confirm all requests involving vendors.
- Limit the number of employees that have the authority to submit or approve wire transfers.
- 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.
- All employees involved with wire transfers should receive training on this scam and the procedures for handling internal wire transfer requests.
- Be alert for urgent wire requests or last-minute changes to wire instructions.
- Verify information from the sender via telephone if remote.
- Avoid using public email accounts when communicating with staff and watch for email domains that may vary such as ABC1cu.com vs. ABClcu.com.

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. Review these resources to learn more:

- Business Email Compromise Risk Overview
- Online Risk Assessment: Funds and Wire Transfer
- Wire Transfer Risk Overview
- COVID-19 Outbreak 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.

© CUNA Mutual Group, 2020.

Insurance products offered to credit unions are underwritten by CUMIS Insurance Society, Inc., a member of the CUNA Mutual Group. This RISK Alert is intended solely for CUNA Mutual Group Fidelity Bond policyowners to prevent fraud losses. Any further distribution of this information could subject you to liability under common law and various statutes including the Fair Credit Reporting Act.

This resource was created by CUNA Mutual Group based on our experience in the credit union, insurance, and risk management marketplace. It is intended to be used only as a guide, not as legal advice. Any examples provided have been simplified to give you an overview of the importance of selecting appropriate coverage limits, insuring-to-value, and implementing loss prevention techniques. No coverage is provided by this resource, nor does it replace any provisions of any insurance policy or bond. Please read the actual policy for specific coverage, terms, conditions, and exclusions.