TruStage®

RISK Alert

Actionable insights for bond policyholders

Awareness | **Watch** | Warning

Fraudulent instruction incidents & compromised email leads to wire fraud

Fraudulent instruction incidents – such as Business Email Compromise (BEC) and vendor impersonation scams – have seen an increase involving credit unions. Nearly 30% of new cyber claims in Q1 2026 have been related to BEC according to Beazley.

BEC scams typically involve fraudsters that impersonate executives to fraudulently request urgent wire transfers, while the vendor impersonation has fraudsters impersonating a vendor and send a fraudulent email to the credit union to update banking information for remittances. These attacks are highly targeted, often leveraging compromised email accounts or convincing spoofed domains to appear legitimate.

Alert details

The severity of wire transfer fraud losses attributable to BEC and vendor impersonation scams has increased significantly with multiple reported large dollar losses.

Business email compromise

- Typically begins with fraudsters compromising the CEO or other executive's corporate email account. In some cases, the fraudsters write email rules to send incoming and outgoing email to the executive's trash folder to conceal the scam.
- Fraudsters send a fraudulent email to the CFO or other executive from within the compromised email account requesting a large dollar wire to pay a vendor or purchase an investment. Alternately, the fraudsters send a spoofed email appearing to come from the CEO or other executive requesting the wire. The fraudulent emails create a sense of urgency to process the wire ASAP.
- The fraudulent emails requesting the wire often coincide with when the CEO, or other executive, is out of the office. The fraudsters would know this since they have access to their calendar.
- The fraud is typically discovered after the requester returns to the office.

Vendor impersonation

Fraudsters typically send a spoofed email to the credit union - appearing to come from a vendor. This email contains updated banking instructions for remitting payments. As legitimate invoices are received from the vendor, the credit union remits payment via wire or ACH credit transfer – using the updated banking information. The fraud is discovered when the legitimate vendor contacts the credit union regarding a delinquent payment.

Date:
July 7, 2026

Risk category:
Fraudulent instruction; Business email compromise; BEC; Wire fraud; Fraud; Scams; Deepfakes

States:
All

Share with:

- Branch operations
- Board of directors
- Executive management
- IT
- Risk manager

Facing risk challenges?:
Schedule a no-cost, personalized discussion with a Risk Consultant to learn more about managing risk.

Artificial intelligence (AI) - deepfake technologies have been a game-changer for the BEC scam. Fraudsters can create a deepfake voice of a credit union executive to scam the CFO into wiring funds or create a deepfake video of the executive to scam another executive or employee in a video conference call.

As deepfakes attacks become more prevalent and more advanced, you must adapt your controls and strategies. With respect to the BEC scam, credit unions should take a zero-trust approach for authentication and communication. Training is critical as employees tend to believe what they see and hear.

Risk mitigation

Credit unions should consider these risk mitigation strategies:

- Confirm the legitimacy of internal requests for wire transfers received via email, voice message, live voice calls, or video conference calls. Authenticate requests by using a different communications channel (out-of-band authentication), such as face-to-face with the requester or calling the requester's phone extension or cell phone.
- Avoid processing the wire until you are able to authentic the request.
- Establish formal procedures for handling internal wire transfer requests. Implement dual controls – using two employees - for handling internal wire transfer requests or payments.
- Limit the number of employees granted authority to submit or approve wire transfers.
- Prohibit employees from writing an email rule to send all incoming and outgoing email to their trash folder.
- Require multifactor authentication to access corporate email accounts.
- Add an "EXTERNAL" warning in subject line for incoming emails originating outside of your organization.
- Ensure all employees are trained on scams, how to recognize it, and the correct internal processes.
- Conduct periodic staff training, such as quarterly, on how fraudsters can use deepfake technology (manipulation of voice, image, or video) in social engineering and fraudulent instruction scams.
- Avoid using public email accounts when communicating with staff.
- Verify updated banking instructions for remittances received from vendors by calling the vendor using a reliable phone number.
- Consider implementing a deepfake detection solution. These solutions employ AI and machine learning to analyze digital media, such as images, videos and audio for signs of manipulation.

Risk prevention resources:

Access the **Business Protection Resource Center** for exclusive risk and compliance resources (user ID and password required).

Access related RISK Alerts within the RISK Alerts Library. Simply use the search or other filtering features using keywords such fraud, scams, deepfake and business email compromise.

- Business email compromise & fraudulent instruction risk overview
- Deepfake risk overview
- Emerging Risk Outlook: Business email compromise and fraudulent instruction scams

For additional support, call 800.637.2676 or email riskconsultant@trustage.com

TruStage®