TruStage™

RISK Alert

Actionable insights for bond policyholders

Awareness | **Watch** | Warning

Vendor impersonation fraud sets up fraudsters to intercept payments

In a scam closely related to the business email compromise (BEC) or fraudulent instruction scam, fraudsters are impersonating vendors/suppliers used by credit unions. Credit unions receive a spoofed email – appearing to come from the vendor/supplier – with updated banking information for paying invoices by ACH or wire. The fraudulent emails do not request payment from credit unions. As legitimate invoices are received from the actual vendors/suppliers, credit unions remit payment by ACH or wire using the updated, fraudulent banking information allowing the fraudsters to intercept payments.

Alert details

Fraudsters are impersonating vendors/suppliers used by credit unions to intercept payments made by credit unions. Credit unions receive a spoofed email – appearing to come from the vendor/supplier – with updated banking information (new routing and account number) for paying invoices by ACH or wire. The fraudulent emails do not request payment from credit unions.

As legitimate invoices are received from the actual vendors/suppliers, the credit union remits payment by ACH or wire using the updated banking information. The fraud is discovered when the vendor/supplier contacts the credit union inquiring about a delinquent payment. The losses have reached mid to high six-figures.

These losses are generally not insurable under the Funds Transfer coverage in the Fidelity Bond. The fraudulent emails contained updated banking information for remitting payments via ACH or wire. They do not request a wire or ACH credit transfer that causes an account to be debited or credited.

The scam generally starts with fraudsters compromising the email account of a vendor/supplier or credit union accounting department employees. The fraudsters search through the emails for payment indicators (e.g., emails containing invoices to be paid). They frequently write rules to send incoming and outgoing emails to the trash folder to prevent the fraud from being discovered.

After sending the spoofed email to the credit union, the fraudsters rely on the actual vendors/suppliers to send invoices to the credit union. They simply wait for the credit union to transmit payments to the fraudulent account. Upon receipt, the funds are typically transferred elsewhere.

Date:
June 27, 2023

Risk category:
Fraud; scams; business email compromise; fraudulent instruction; vendor; funds/wire transfer; ACH

States:
All

Share with:

- Accounting
- Executive management
- Risk manager
- Transaction services

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

Risk mitigation

Alert accounts payable staff at the credit union of this vendor impersonation scam.

If the credit union receives an email purportedly from a vendor/supplier with updated banking information for remitting payments, the instructions should be verified by calling the vendor/supplier using a reliable phone number.

Credit unions victimized in this scam should consider these steps for recovering the funds:

- Contact the institutions where the transfers were sent in an attempt to recover the funds. The institutions will likely require an indemnification agreement before returning any funds.
- Report the fraud to the FBI by filing a complaint through the **Internet Crime Complaint Center** (IC3). IC3's Recovery Asset Team (RAT) tracks the funds down and works with financial institutions to freeze the funds for the victims.

  In 2022, RAT initiated the Financial Fraud Kill Chain (FFKC) on 2,828 business email compromise complaints involving domestic transfers with potential losses of over $590 million. A monetary hold was placed on approximately $433 million, which represents a 73% success rate.

Risk prevention resources:

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

Access the RISK Alerts Library and enter key words in the search feature.

Review these resources:

- **Emerging risk outlook web series**: Wire fraud and business email compromise
- **Business email compromise & fraudulent instruction risk overview**
- **Fraud & scams eBook**

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