Simple Cyber

GUIDANCE FOR C&F INSUREDS

EST. 1822
A FAIRFAX COMPANY

Best Practices for Responding to Payment Fraud

Payment fraud – transferring funds to a criminal posing as a legitimate business associate –requires immediate action to stop the payment and restore the funds.

1. Contact your bank to request a recall of the wire transfer due to fraud and confirm the request in writing.
2. Notify the receiving bank about the recall/reversal of the wire.
3. Notify the local Secret Service office (where either bank is located) of the fraud and file a complaint.

You can find the local office here:
www.secretservice.gov/contact/field-offices

Request they initiate the FBI's Financial Fraud Kill Chain.

4. Preserve records of the incident, including original electronic emails. These files help investigators analyze the crime.
5. Preserve records of the incident including email sent and received *in their original electronic state*. The email file(s), which contain(s) message header and content, helps investigators to perform a thorough analysis of the crime that occurred.
6. After completing the above steps, contact your insurer as per your policy's requirements.

While recalling the wire transfer and reporting to the Secret Service can't guarantee fund recovery, these steps can help mitigate loss, assist in tracing funds, and support any potential insurance claim.[1]

SIMPLE STEPS TO REDUCE THE RISK OF PAYMENT FRAUD

Email communication is efficient, but it's not the most secure method of communication. Anyone's emails can be intercepted, altered, or fabricated - and can fool a recipient. You can reduce probability of payment fraud risk by following these best practices:

1 Verify Email Requests by Telephone Require

Require those responsible for paying invoices or changing bank routing information to verify payment details over the phone, not by email or electronic documents. Be aware of "deepfake" technology that can mimic someone's voice. Using known phone numbers and established authentication procedures (e.g., having a unique identification code for each person and known only to the relevant individuals) can help protect against deepfakes.

2 Segregate Wire Transfer Responsibilities

Implement a policy requiring at least three people to review and approve wire transfer requests, invoice payments, or changes to bank account information. The initiator should enter requests, which are then verified by two independent signatories.

3 Enforce Multifactor Authentication (MFA) for Email and Remote Access

Payment scams often start with comprised access credentials to email accounts. Use MFA for all remote system access, including email, to help prevent criminals from using compromised credentials to impersonate company employees. Major email providers offer MFA, adding security beyond account names and passwords.

4 Regular Training on Business Email Compromise (BEC) and Payment Fraud

Technology alone isn't enough because employees are often the weakest link. Regular, documented training on BEC and payment fraud is essential.

1 Reporting the loss to your insurer does not guarantee coverage. Rather, coverage will be determined based on the nature of the loss and the provisions of any pertinent policy.

If you have questions about this advisory, your policy, or risk mitigation opportunities, please contact **CyberSolutions@cfins.com.**