



# Simple Cyber

## GUIDANCE FOR C&F INSUREDS

## Simple Steps 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. File a complaint with the FBI's Internet [Crime Complaint Center \(IC3\)](#). This reporting triggers the FBI's Recovery Asset Team and the FBI's assistance seeking return of the wire transfer.
  - a. Report to Law Enforcement in the jurisdiction where the crime has occurred.
  - b. Local Police/Sheriff: (Local law enforcement report is often needed to reverse the wire)
  - c. [Secret Service](#)
  - d. [FBI Field Office](#)
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.

Ask your Field Office to initiate the FBI's Financial Fraud Kill Chain.

<sup>1</sup> 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.

## Simple Steps to Avoid 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 compromised 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.

If you have questions about this advisory, your policy, or risk mitigation opportunities, please contact [CyberSolutions@cfins.com](mailto:CyberSolutions@cfins.com).

Crum & Forster prepared this content for informational purposes only. It does not represent coverage or insurability, and it does not provide legal, tax, accounting, or other professional advice. Consult your professional advisors about this content. The C&F logo, C&F, and Crum & Forster are registered trademarks of United States Fire Insurance Company.

This content cannot address every payment fraud scenario relevant to your premises or operations, and the content might be out-of-date. You should independently implement a reasonable loss mitigation program to identify and mitigate risks relevant to your premises and operations, including the risk of payment fraud. Crum & Forster provides this content "AS IS" and without any representation, guaranty, or warranty.