Social Engineering Tips:
Take Immediate Action!

CHUBB

If you believe you have transferred funds to a criminal posing as a legitimate business associate, you should act quickly and do the following:

1. Immediately contact the originating bank, **request a recall of the wire transfer,** and confirm that recall in writing.

2. Immediately **file a complaint with the FBI** at www.ic3.gov.
   This reporting triggers the FBI's Recovery Asset Team and the FBI's assistance seeking return of the wire transfer.

3. **Preserve records of the incident,** including emails sent and received in their original electronic state. Correspondence and forensic information contained in these electronic files help investigators shed light on the perpetrator(s) and parties responsible for the incident.

4. Once the above steps are complete, **contact Chubb** per the instructions in your policy.

While neither recalling the wire transfer nor reporting to the FBI guarantees the return of your funds, they maximize the opportunity to mitigate your loss, assist the FBI in tracing the funds, and help establish any insurance claim.

Simple Steps to Prevent Fraudulently Induced Wire Transfers

While email promotes efficient communication, it is not always secure. Regardless of your familiarity with a contact, **email may be intercepted, altered, and fabricated**. You can reduce the chances of fraud with these best practices:

1. **Verify Email Requests** by Telephone: Require those responsible for paying invoices or changing bank routing information to verify payment details over the phone (rather than by email or documents sent electronically). Making a phone call to a known, pre-existing telephone number remains the single best protection against fraud.

2. **Segregate Wire Transfer Responsibilities:** Establish a standing policy that requires at least three people to review and approve wire transfer requests, pay an invoice or change a business partner's bank account information. Such request should be entered by the initiator of the wire and verified by two independent signatories.

3. **Turn on MFA for Cloud Email:** "Multifactor Authentication" (MFA) is available from all major email providers. It provides a layer of security to email accounts beyond a user's account name and password, making it harder for criminals to impersonate you, your executives and your employees.