

CEO & Wire Transfer Fraud Checklist

Have you been a victim of CEO or Wire Transfer Fraud, commonly known as Business Email Compromise (BEC)? Review the checklist below for immediate actions:

IMMEDIATE ACTIONS

Internal Actions

- Review all IP logs accessing the relevant infrastructure (internal mail servers or other publically accessible infrastructure) – looking for unusual activity
- Scan for log-in locational data. Was there a log-in from an unknown country or location, specific to that email account?
- Review the relevant email account(s) which may have been spoofed or otherwise compromised for any rules such as “auto forward” or “auto delete”
- Inform employees/agents of the situation and require they contact clients and customers who are near the wire transfer stage
- Review all requests that asked for a change in payment type or location. ***Remain especially vigilant on transactions expected to occur immediately prior to a holiday or weekend. ***

Reporting the Incident

- Contact your bank
 - Determine the appropriate contact at your bank, who has the authority to recall a wire transfer
 - Notify your bank you have been the victim of a Business Email Compromise
 - AND -
 - Request a wire recall or SWIFT Recall Message
 - AND -
 - Request they fully cooperate with law enforcement
- Report the incident (or attempt) to the FBI at www.IC3.gov
- Provide all details for the beneficiary: account numbers, contact information, names
- Contact your local FBI Field Office

PREVENTION & RECOGNITION

- Does the Routing Number provided to you, resolve to the expected bank used by the other party? (*Example: Have you received wire information for an account at a Hong Kong bank; however, your other party only banks in the U.S.?*)

Possible websites to verify a Routing Number:
 - a. The Federal Reserve
www.FRBServices.org
 - b. American Bankers Association
<https://routingnumber.aba.com>
- Call a known/trusted phone number or meet in person to confirm the wire transfer information provided to you, matches the other party's information
- Hover you cursor over suspicious email addresses – Looking for indications of Display Name Deception or Spoofing
- DO NOT hover on **links** within emails, as simply hovering *may* execute commands.
- Regularly check your email account log-in activity for possible signs of email compromise
- Regularly check your email account for new “rules”, such as email forwarding and/or auto delete
- Be cautious of “new” customers, suppliers, clients and/or others you don't know who ask you to:
 - a. ...open or download any documents they send
- OR -
 - b. ...sign into a separate window or click on a link to view an invoice or document
- OR -
 - c. ...provide sensitive Personal or Corporate information
- Verify the wire instructions you provide to your customers/clients are accurate for both the pertinent bank and pertinent account.
 - a. Where did you get the account data?
 - b. Is this the correct account number?