Business Email Compromise 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

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

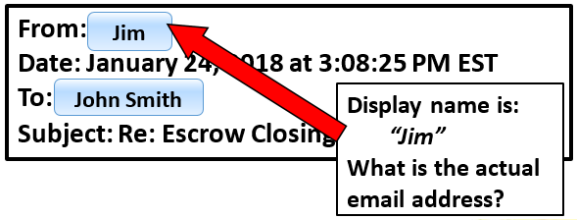
Internal Actions

- ☐ 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. ***

PREVENTION & RECOGNITION

- ☐ Hover you cursor over, or expand contact details on, 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.
- ☐ Call a known/trusted phone number or meet in person to confirm that the wire transfer information provided to you, matches the other party's information
- ☐ Does the Routing Number or SWIFT 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 or SWIFT Number:
  a. Any reputable search engine
  b. The Federal Reserve www.FRBServices.org
  c. American Bankers Association https://routingnumber.aba.com

- ☐ Regularly check your email account log-in activity for possible signs of email compromise
- ☐ Develop an intrusion detection system to identify emails from extensions that are similar to your company email.
- ☐ 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?