BEC AWARENESS

Definitions

- **Business E-mail Compromise** (BEC) - a scam targeting *businesses* working with foreign suppliers and/or businesses that regularly perform wire transfer payments.
- **E-mail Account Compromise** (EAC) - a component of BEC which targets *individuals* who perform wire transfer payments.

Overall

- Any business or government entity is a target.
- Types of payments targeted can be CEO payroll checks, invoice payments, attorney fees, litigation settlements, government contractor payments, home down payments to title companies, etc.
- Perpetrators will masquerade as "known" or "new" business affiliations to trick victim businesses
- The "masquerade" is carried out by the perpetrator through computer intrusions such as email phishing scams, spoofing, or hacking to gather business information. This information is then used by the perpetrator to send fraudulent emails to victim businesses and financial institutions to the initiate the financial transactions.
- The perpetrators may involve the name of a 3rd party, legitimate entity, which can be easily verified, to add false validity to their financial transaction request.
- The perpetrators typically target large dollar transactions, although some will target payroll ACH payments.
- The perpetrator may set a false "deadline" to create unnecessary urgency or pressure, to cause the financial transaction take place, all to avoid due diligence by the victim business or financial institution.
- Bank accounts used by the criminals can be domestic or foreign bank accounts. Banks in Asia—particularly in China and Hong Kong—are common destinations for these fraudulent transactions.
- BEC/EAC scams are linked to other forms of fraud, including but not limited to: money mules, romance, lottery, employment, and rental scams
- A BEC/EAC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

Red Flags – "Known Business" Affiliations

- A perpetrator will masquerade as a "known business" of the victim, such as an existing customer, vendor, contractor, or employee, in order to trick the victim business.
- An email, fax, or phone request is made by the "known business" to change/update their bank account information, for a future ACH, payroll, or wire transfer.
- The "known business" email contains different language, timing, and amounts than previously verified and authentic transaction instructions.

- The transaction instructions originate from an e-mail account closely resembling a known customer's e-mail account; however, the e-mail address has been slightly altered by adding, changing, or deleting one or more characters.
- Emailed transaction instructions originate from a customer's employee who is a newly authorized person on the account or an authorized person (CEO, CFO, payroll manager, accounts payable manager) who has not previously sent wire transfer instructions.

Red Flags – "New Business" Affiliations

- A perpetrator will masquerade as "new business" to target victim businesses such as real estate agents, title companies, attorneys, and vendors in large dollar transactions involving unknown individuals.
- Perpetrators monitor real estate transactions and listings and inject themselves into the process, causing the down payment to be diverted through a wire transfer to an account controlled by the perpetrator.
- A victim's employee e-mails a financial institution transaction instructions on behalf of the customer/perpetrator based exclusively on e-mail communications allegedly originating from executives, attorneys, or their designees. The victim employee indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.
- E-mailed transaction instructions include markings, assertions, or language designating the transaction request as "Urgent," "Secret," or "Confidential."

Prevention & Recovery

- Best prevention – if a potential victim business, individual, or financial institution receives an email, fax, or telephone call requesting to change bank account information, deposit an unknown check and transfer the proceeds, or make an ACH, payroll, or wire transfer payment –
    - If the requesting party is "known" – contact the requesting party using a different and separate verifiable method of contact to confirm the account change request or financial transaction is valid.
    - If the requesting party is "new" – contact your financial institution to advise them of your suspicions; conduct due diligence of the requesting party name, address, email address, telephone numbers; contact the FBI.
    - Do not reply to the perpetrator making email the request, to attempt to verify their information.

If you believe you are a victim of a BEC/EAC

- Contact your bank immediately.
- To request immediate assistance in recovering BEC-stolen funds, file a complaint with FBI's IC3 at www.ic3.gov immediately and contact your local FBI field office. While the recovery of BEC stolen funds is not assured, there is greater success in recovering funds when victims or financial institutions report BEC-unauthorized wire transfers to law enforcement within 24 hours.

Examples:

BEC Schemes

Scenario 1: Business Working with a Foreign Supplier

A business that typically has a longstanding relationship with a supplier is requested to wire funds for an invoice payment to an alternate, fraudulent bank account. The account change request may be made via telephone, facsimile, or e-mail. If an e-mail is received, the subject will spoof the e-mail request so it appears similar to a legitimate request. Likewise, requests made via facsimile or telephone call will closely mimic a legitimate request.

Scenario 2: Business Executive Receiving or Initiating a Request for a Wire Transfer

The e-mail accounts of high-level business executives (Chief Financial Officer, Chief Technology Officer, etc.) are compromised. The account may be spoofed or hacked. A request for a wire transfer from the compromised account is sent to a second employee at the victim company who is typically responsible for processing these requests. In some instances, a request for a wire transfer from the compromised account is sent directly to the victim business financial institution with instructions to urgently send funds to bank "X" for reason "Y."

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail

An employee of a victim business has his or her personal e-mail hacked. This personal e-mail may be used for both personal and business communications. Requests for invoice payments to fraudster-controlled bank accounts are sent from the employee's personal e-mail to multiple vendors identified from this employee's contact list. The business may not become aware of the fraudulent requests until that business is contacted by a vendor following up on the status of the invoice payment.

Scenario 4: Business Executive and Attorney Impersonation

Victims report being contacted by fraudsters who typically identify themselves as lawyers or representatives of law firms and claim to be handling confidential or time-sensitive matters. This contact may be made via either phone or e-mail. Victims may be pressured by the fraudster to act quickly or secretly in handling the transfer of funds. This type of BEC scam may occur at the end of the business day or work week and be timed to coincide with the close of business of international financial institutions.

EAC Schemes

Scenario 1 – Lending/Brokerage Services:

A perpetrator hacks into and uses the e-mail account of a financial services professional (such as a broker or accountant) to e-mail fraudulent instructions, allegedly on behalf of a client, to the client's bank or broker age to wire-transfer client's funds to an account controlled by the perpetrator.

Scenario 2 – Real Estate Services:

The perpetrator compromises the e-mail account of a realtor or of an individual purchasing or selling real estate, for the purposes of altering payment instructions and diverting funds of a real estate transaction (such as sale proceeds, loan disbursements, or fees

Scenario 3 – Legal Services:

A perpetrator compromises an attorney's e-mail account to access client information and related transactions. The criminal then e-mails fraudulent transaction payment instructions to the attorney's financial institution.