E-MAIL COMPROMISE FRAUD SCHEMES

RED FLAGS FOR BEC & EAC SCAMS

E-MAIL COMPROMISE FRAUD consists of schemes where criminals compromise a victim's e-mail account and send fraudulent wire transfer instructions to Financial Institutions (FIs).

22,000

Since 2013 there have been approximately **22,000** reported cases.

$3.1B

Reported E-mail Compromise Fraud cases have involved **3.1 billion dollars.*** *includes actual and attempted loss.

Both domestic and foreign accounts have been **recipients** of fraudulent funds.

EAC SCAMS

Also known as **E-MAIL ACCOUNT COMPROMISE.** These schemes target a victim's personal accounts. They often target individuals who conduct large transactions through FIs, lending entities, real estate companies and law firms.

BEC SCAMS

Also known as **BUSINESS E-MAIL COMPROMISE.** These schemes target a FI's commercial customers. Criminals access the e-mail accounts of a company's executives or employees.

HOW THESE SCHEMES PLAY OUT

STAGE 1
Compromising Victim Information and E-mail Accounts

STAGE 2
Transmitting Fraudulent Transaction Instructions

STAGE 3
Executing Unauthorized Transactions

In some cases, financial institutions have **absorbed losses** through reimbursing customers victimized by e-mail compromise fraud.

BEC and EAC schemes are similar and may exhibit similar suspicious behavior, which can be identified by one or more of the following red flags:

- **A customer's seemingly legitimate e-mailed transaction instructions contain different language, timing, and amounts** than previously verified, authentic transaction instructions.
- **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.
- **E-mailed transaction instructions direct payment to a known beneficiary; however, the beneficiary's account information is different from what was previously used.**
- **E-mailed transaction instructions direct wire transfers to a foreign bank account that has been documented in customer complaints** as the destination of fraudulent transactions.
- **E-mailed transaction instructions direct payment to a beneficiary with which the customer has no payment history or documented business relationship,** and the payment is in an amount similar to or in excess of payments sent to beneficiaries whom the customer has historically paid.
- **E-mailed transaction instructions include markings, assertions, or language designating the transaction request as *Urgent*, *Secret*, or *Confidential*.**
- **E-mailed transaction instructions are delivered in a way that would give the FI limited time or opportunity to** confirm the authenticity of the requested transaction.
- **E-mailed transaction instructions originate from a customer's employee who is a newly authorized person on the account** or is an authorized person who has not previously sent wire transfer instructions.
- **A customer's employee or representative e-mails a financial institution transaction instructions** on behalf of the customer that are based exclusively on e-mail communications originating from executives, attorneys, or their designees. However, the customer's employee or representative indicates he/she has been unable to verify the transactions with such executives, attorneys, or designees.
- **A customer e-mails transaction requests for additional payments immediately following a successful payment** to an account not previously used by the customer to pay its suppliers/vendors.

  Such behavior may be consistent with a criminal attempting to issue additional unauthorized payments upon learning that a fraudulent payment was successful.
- **A wire transfer is received for credit into an account, and names a beneficiary that is not the account holder of record.** This may reflect instances where a victim unwittingly sends wire transfers to a new account number, provided by a criminal impersonating a known supplier/vendor.

  This flag may be seen by financial institutions receiving wire transfers sent by another FI as the result of e-mail-compromise fraud.

Source: *FinCEN Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes*, FIN-2016-A003, September 6, 2016

The above red flags have been summarized from FinCEN's Advisory. For the original list of red flags and more comprehensive information on Business E-mail Compromise and E-Mail Account Compromise, see ***https://www.fincen.gov/sites/default/files/advisory/2016-09-09/FIN-2016-A003.pdf***

VERAFIN A STEP AHEAD.
1.877.368.9986 info@verafin.com www.verafin.com