

FIN-2016-A003

September 6, 2016

# Advisory

## Advisory to Financial Institutions on E-Mail Compromise Fraud Schemes

***Criminals are actively using e-mail schemes to defraud financial institutions and their customers—billions of dollars in possible losses.***

The Financial Crimes Enforcement Network (FinCEN) is issuing this advisory to help financial institutions guard against a growing number of e-mail fraud schemes, in which criminals misappropriate funds by deceiving financial institutions and their customers into conducting wire transfers. This advisory also provides red flags—developed in consultation with the Federal Bureau of Investigation (FBI) and the U.S. Secret Service (USSS)—that financial institutions may use to identify and prevent such e-mail fraud schemes.

***E-mail Compromise Fraud:*** Schemes in which criminals compromise the e-mail accounts of victims to send fraudulent wire transfer instructions to financial institutions in order to misappropriate funds. The main types of e-mail compromise fraud include:

***Business E-mail Compromise (BEC):*** Targets a financial institution’s *commercial* customers.

***E-mail Account Compromise (EAC):*** Targets a victim’s *personal* accounts.

### This Advisory should be shared with:

- *Cybersecurity departments*
- *Risk departments*
- *Fraud prevention units*
- *BSA/AML management*
- *AML intelligence units*
- *AML analysts/investigators*

BEC and EAC schemes are among the growing trend of cyber-enabled crime adversely affecting financial institutions. Since 2013, there have been approximately 22,000 reported cases of BEC and EAC fraud involving \$3.1 billion.<sup>1</sup> In some cases, financial institutions have absorbed losses through reimbursing customers victimized by e-mail compromise fraud. Financial institutions can play an important role in identifying, preventing, and reporting fraud schemes by promoting greater communication and collaboration among their internal anti-money laundering (AML), business, fraud prevention, and cybersecurity units.

1. See the FBI Internet Crime Complaint Center (IC3) Public Service Announcement “[Business Email Compromise: The 3.1 Billion Dollar Scam](#)” (June 14, 2016) and [2015 Internet Crime Report](#).

## How BEC and EAC Schemes Work

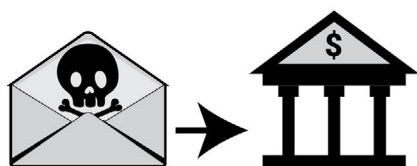
Unlike account takeover activity, e-mail-compromise schemes involve impersonating victims to submit seemingly legitimate transaction instructions for a financial institution to execute. In account takeover activity, criminals access victims' accounts and are able to directly execute transactions without submitting transaction instructions.<sup>2</sup>

While BEC and EAC schemes have unique aspects, as noted below, both focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. Both BEC and EAC schemes can be broken down into three stages:

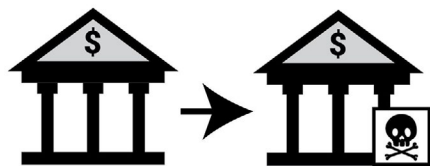
**Stage 1 – Compromising Victim Information and E-mail Accounts:** Criminals first unlawfully access a victim's e-mail account through social engineering<sup>3</sup> or computer intrusion techniques. Criminals subsequently exploit the victim's e-mail account to obtain information on the victim's financial institutions, account details, contacts, and related information.



**Stage 2 – Transmitting Fraudulent Transaction Instructions:** Criminals then use the victim's stolen information to e-mail fraudulent wire transfer instructions to the financial institution in a manner appearing to be from the victim. To this end, criminals will use either the victim's actual e-mail account they now control or create a fake e-mail account resembling the victim's e-mail.



**Stage 3 – Executing Unauthorized Transactions:** Criminals trick the victim's employee or financial institution into conducting wire transfers that appear legitimate but are, in fact, unauthorized. The fraudulent transaction instructions direct the wire transfers to the criminals' domestic or foreign bank accounts. Banks in Asia—particularly in China and Hong Kong—are common destinations for these fraudulent transactions.



### Business E-Mail Compromise (BEC) Schemes

BEC schemes target financial institutions' commercial customers. Criminals seek to access unlawfully the e-mail accounts of a company's executives or employees to:

- a) Directly submit fraudulent transaction instructions to the company's financial institution by impersonating company employees through e-mails and documentation related to the requested transfer; or

2. See FinCEN Advisory FIN-2011-A016 "[Account Takeover Activity](#)" (December 2011).

3. Social engineering refers to human interaction tactics used to deceive an individual into revealing information.

- b) Mislead a company employee into submitting fraudulent transaction instructions to the company’s financial institution by impersonating a supplier or a company executive to authorize or order payment through seemingly legitimate internal e-mails.

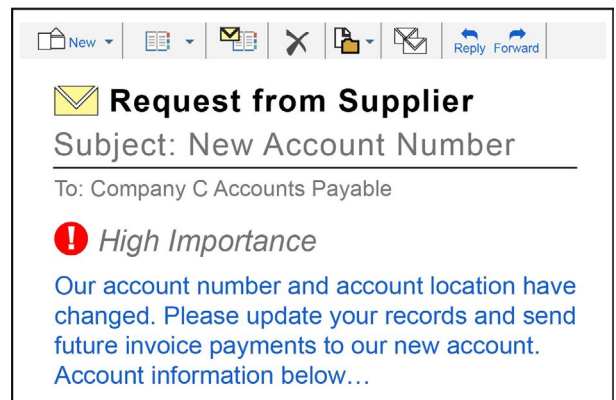
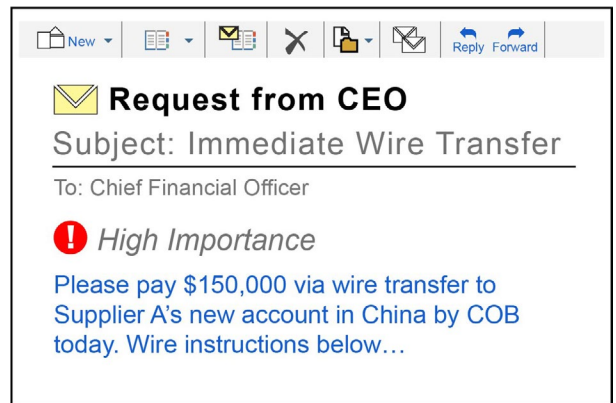
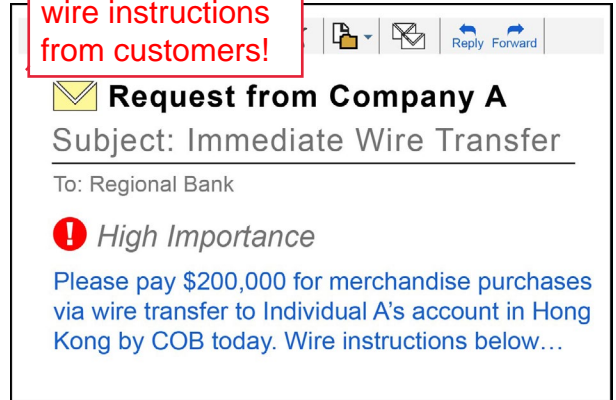
To illustrate, BEC schemes often take the following forms:

**Scenario 1 – Criminal Impersonates a Financial Institution’s Commercial Customer:** A criminal hacks into and uses the e-mail account of a Company A employee to send fraudulent wire transfer instructions to Company A’s financial institution. Based on this request, Company A’s financial institution issues a wire transfer and sends funds to an account the criminal controls. *In this scenario, the criminal impersonating the financial institution’s customer prompted the financial institution to execute an unauthorized wire transfer.*

**Scenario 2 – Criminal Impersonates an Executive:** A criminal hacks into and uses the e-mail account of a Company B executive to send wire transfer instructions to a Company B employee who is responsible for processing and issuing payments. The employee, believing the executive’s e-mailed instructions are legitimate, orders Company B’s financial institution to execute the wire transfer. *In this scenario, the criminal impersonating a company executive misled a company employee into unintentionally authorizing a fraudulent wire transfer to a criminal-controlled account.*

**Scenario 3 – Criminal Impersonates a Supplier:** A criminal impersonates one of Company C’s suppliers to e-mail and inform Company C that future invoice payments should be sent to a new account number and location. Based on this fraudulent e-mailed information, Company C updates its supplier’s payment information on record and submits the new wire transfer instructions to its financial institution that direct payments to an account controlled by the criminal. *In this scenario, the criminal impersonating a supplier provided fraudulent payment information to mislead a company employee into unintentionally directing wire transfers to a criminal-controlled account.*

Unibank does not accept emailed wire instructions from customers!



## E-Mail Account Compromise (EAC) Schemes

Unlike BEC, EAC schemes target individuals instead of businesses. Individuals who conduct large transactions through financial institutions, lending entities, real estate companies, and law firms are the most likely targets of this type of scheme. EAC schemes often take the following forms:

**Scenario 1 – Lending/Brokerage Services:** A criminal 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 brokerage to wire-transfer client’s funds to an account controlled by the criminal.

**Scenario 2 – Real Estate Services:** A criminal 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). Alternately, a criminal hacks into and uses a realtor’s e-mail address to contact an escrow company, instructing it to redirect commission proceeds to an account controlled by the criminal.

**Scenario 3 – Legal Services:** A criminal 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. Alternatively, the criminal may compromise a client’s e-mail account to request wire transfers from trust and escrow accounts the client’s attorney manages.

### BEC and EAC Fraud Red Flags

Success in detecting and stopping BEC and EAC schemes requires careful review and verification of customers’ transaction instructions and consideration of the circumstances surrounding such instructions.

In applying the red flags below, financial institutions are advised that *no single transactional red flag necessarily indicates suspicious activity*. Financial institutions should consider additional indicators and the surrounding facts and circumstances, such as a customer’s historical financial activity and whether the customer exhibits multiple red flags, before determining that a transaction is suspicious. Financial institutions should also perform additional inquiries and investigations where appropriate.

BEC and EAC schemes are similar and, therefore, 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 and 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. For example:







Legitimate e-mail address

john-doe@abc.com

Fraudulent e-mail addresses

john\_doe@abc.com

john-doe@bcd.com

-  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 financial institution 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, however, the wire transfer 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, while thinking the new account belongs to the known supplier/vendor, as described in the above BEC Scenario 3. This red flag may be seen by financial institutions *receiving* wire transfers sent by another financial institution as the result of e-mail-compromise fraud.