## Common Variations

- Hacked accounts via spear phishing
- Spoofed accounts made to look similar to authentic accounts (john.kelly@abc.com vs. john.kelley@abc.com)
- Spoofed accounts with slight variations in domains (abc@lawfirm.com vs. abc@lawflrm.com)
- Spoofed accounts mimicking the real account until one reviews the extended header

## Common Targets

- Free web based e-mail users
- Bookkeepers, accountants, controllers
- Title companies, buyers/sellers, or attorneys in the midst of a real estate transaction
- Businesses who deal with overseas vendors/ suppliers

## Statistics

The Internet Crime Complaint Center (IC3) has seen a 1300% increase in identified exposed losses since January 2015. The scam was reported in all 50 states and in 100 countries. Fraudulent transfers were sent to 79 countries; however, the majority went to banks in China and Hong Kong. Over 15,000 domestic and international victims with an exposed loss of over $1 billion were reported to the IC3 from October 2013 to May 2016.

## Suggestions for Protection

- Educate employees on how to identify a BEC scam before sending payments to fraudsters.
- Verify wire transfer requests and changes to vendor bank accounts with two-factor authentication such as a secondary sign-off and/or using voice verification over known phone numbers.
- Create intrusion detection system rules that flag e-mails with extensions similar to company e-mail or differentiate between internal and external e-mails.
- Be wary of free, web based e-mail accounts, which are more susceptible to being hacked.
- Be careful when posting financial and personal information to social media and company websites.
- Be suspicious of requests to send a wire "discreetly" or secretly and requests to send a wire quickly.
- Register domains that are slightly different than your actual domain.
- Know the habits of your customers, including payment details, reasons for payment, and typical payment amounts.
- Scrutinize all e-mail requests for transfer of funds.

# Business E-Mail Compromise

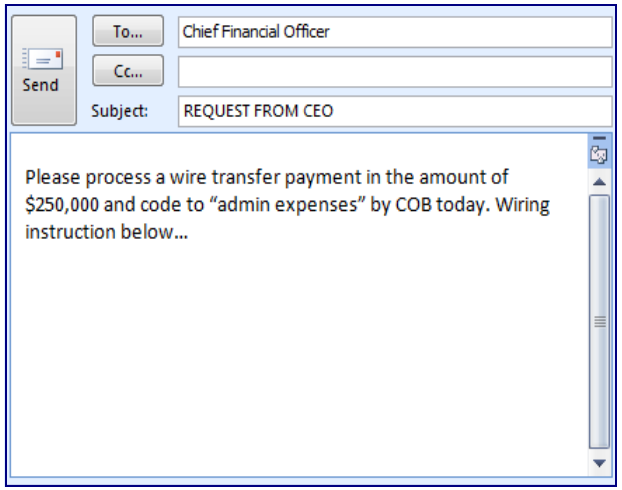
## How and When to Report to the Federal Bureau of Investigation

U.S. Immigration and Customs Enforcement

## Chicago Field Office

## Business E-mail Compromise (BEC)

The CFO of a U.S company received an e-mail from her CEO while the CEO was on vacation out of the country. The CEO requested a transfer of funds for a time-sensitive payment that required discretion. The CFO followed the instructions and wired $250,000 to a bank in Hong Kong.




The next day, the CEO called about another matter. The CFO mentioned she had completed the wire the day before, but the CEO said he never sent the e-mail and knew nothing about the transaction.

The company was the victim of a BEC. BEC is a sophisticated financial fraud targeting businesses of all types and sizes. BECs are carried out through social engineering or computer intrusions to conduct unauthorized transfers of funds.

## What to do if you are a victim

1. Report the matter to your bank: On international transactions, contact your financial institution to issue a **"SWIFT recall."** For domestic transfers, request your financial institution send a **"hold harmless letter"** to the beneficiary bank.

2. Report to law enforcement: After contacting your financial institution, immediately report the incident to the FBI Chicago Field Office at **ChicagoBEC@ic.fbi.gov** or **(312)421-6700.** Provide the following information:

   - Date of the incident
   - Summary of the incident
   - Victim Name
   - Victim location (City, State)
   - Victim bank name
   - Victim bank account number
   - Beneficiary name
   - Beneficiary account number
   - Beneficiary bank location
   - Intermediary bank name
   - SWIFT/IBAN number
   - Date of transaction
   - Amount of transaction
   - Copies of emails, including header information

3. Notify your bank and/or law enforcement of unauthorized wires as soon as possible. Days, hours, and minutes can make a big difference in preventing monetary loss.

## What if there is no financial loss?

Report the matter to the FBI via the Internet Crimes Complaint Center (IC3) at www.ic3.gov. You also may want to consider notifying local law enforcement. Please be sure to provide the transaction information and copies of the e-mails.

For additional information on Business E-mail Compromise, go to www.ic3.gov/media/. Specific public service announcements on this scam include:

- Alert Number I-082715a-PSA dated 8/27/2015
- Alert Number I-082715b-PSA dated 8/27/2015
- Alert Number I-061416-PSA dated 6/14/2016

**FBI Chicago Field Office**
**2111 W. Roosevelt Rd.**
**Chicago, IL 60608**
**(312)421-6700**