What to do if you are a victim of a Business Email Compromise Scheme

NOTE: This information is being provided to victims or potential victims of BEC schemes to ensure appropriate action is taken to try to recover the stolen funds.

A Business Email Compromise (BEC) scheme targets businesses and/or individuals performing wire transfer payments (e.g., for the payment of an invoice or purchase of real estate). These rely on social engineering and deception to convince victims to send their money, usually a wire transfer, to criminal actors and are initiated when a victim receives false wire instructions from someone masquerading as a trusted business contact. In most cases, legitimate email accounts have been spoofed or compromised to lend legitimacy to the emails purporting to be from trusted contacts.

According to the FBI's Internet Crime Complaint Center (IC3), the area covered by FBI Tampa is #2 in the country in terms of losses incurred by victims of BEC schemes. Due to the sophisticated nature of the scheme, it is critical for victims to take action **as soon as the fraud is discovered**. The FBI has established protocols for both domestic and international wire transfers.

If you are a victim of a BEC scam, please take the below actions immediately:

- ☐ **Contact your bank**
  - ☐ Determine the appropriate contact at your bank who has the authority to reverse or "recall" the wire transfer you made.
  - ☐ Ensure the bank understands you have been the victim of a Business Email Compromise.
  - ☐ Request a Wire Recall or SWIFT Recall Message
  - ☐ Request your bank to fully cooperate with law enforcement
- ☐ **Contact FBI Tampa (813-253-1000) and follow the prompts to speak with an operator**
- ☐ **Report the incident to the FBI at: www.IC3.gov**

  Be prepared to provide all details related to the transaction (date, amount, sending and receiving bank names, account numbers, contact information, etc.).

For additional information, please contact FBI Tampa at:

TP-CTOC@fbi.gov

Public Service Announcement
FEDERAL BUREAU OF INVESTIGATION

10 September 2019

Alert Number
I-091019-PSA

BUSINESS EMAIL COMPROMISE THE $26 BILLION SCAM

This Public Service Announcement is an update and companion piece to Business Email Compromise PSA 1-071218-PSA posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center complaint information and updated statistics from October 2013 to July 2019.

DEFINITION

Business Email Compromise/Email Account Compromise (BEC/EAC) is a sophisticated scam that targets both businesses and individuals who perform legitimate transfer-of-funds requests.

The scam is frequently carried out when a subject compromises legitimate business or personal email accounts through social engineering or computer intrusion to conduct unauthorized transfers of funds.

The scam is not always associated with a transfer-of-funds request. One variation involves compromising legitimate business email accounts and requesting employees' Personally Identifiable Information or Wage and Tax Statement (W-2) forms.[1]

STATISTICAL DATA

The BEC/EAC scam continues to grow and evolve, targeting small, medium, and large business and personal transactions. Between May 2018 and July 2019, there was a 100 percent increase in identified global exposed losses[2]. The increase is also due in part to greater awareness of the scam, which encourages reporting to the IC3 and international and financial partners. The scam has been reported in all 50 states and 177 countries. Fraudulent transfers have been sent to at least 140 countries.

Based on the financial data, banks located in China and Hong Kong remain the primary destinations of fraudulent funds. However, the Federal Bureau of Investigation has seen an increase of fraudulent transfers sent to the United Kingdom, Mexico, and Turkey.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and July 2019**:

Domestic and international incidents: 166,349
Domestic and international exposed dollar loss: $26,201,775,589

[1] Reference PSA 1-022118-PSA Increase in W-2 Phishing Campaigns
[2] Exposed dollar loss includes actual and attempted loss in United States dollars

The following BEC/EAC statistics were reported in victim complaints to the IC3 between **October 2013 and July 2019**:

Total U.S. victims: 69,384
Total U.S. exposed dollar loss: $10,135,319,091

Total non-U.S. victims: 3,624
Total non-U.S. exposed dollar loss: $1,053,331,166

The following statistics were reported in victim complaints to the IC3 between **June 2016 and July 2019**:

Total U.S. financial recipients: 32,367
Total U.S. financial recipient exposed dollar loss: $3,543,308,220

Total non-U.S. financial recipients: 14,719
Total non-U.S. financial recipient exposed dollar loss: $4,843,767,489

BEC AND PAYROLL DIVERSION

The IC3 has received an increased number of BEC complaints concerning the diversion of payroll funds. Complaints indicate that a company's human resources or payroll department receives spoofed emails appearing to be from employees requesting a change to their direct deposit account. This is different from the payroll diversion scheme in which the subject gains access to an employee's direct deposit account and alters the routing to another account.[3]

In a typical example, HR or payroll representatives received emails appearing to be from employees requesting to update their direct deposit information for the current pay period. The new direct deposit information provided to HR or payroll representatives generally leads to a pre-paid card account.

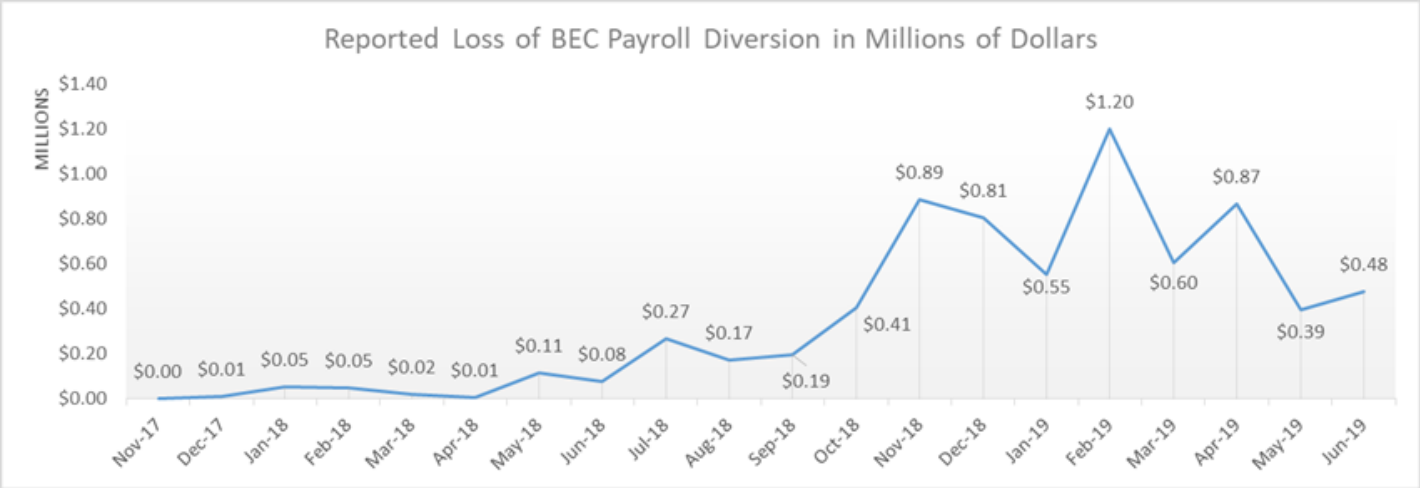
Some companies reported receiving phishing emails prior to receiving requests for changes to direct deposit accounts. In these cases, multiple employees may receive the same email that contains a spoofed log-in page for an email host. Employees enter their usernames and passwords on the spoofed log-in page, which allows the subject to gather and use employee credentials to access the employees' personal information. This makes the direct deposit requests appear legitimate.

Payroll diversion schemes that include an intrusion event have been reported to the IC3 for several years. Only recently, however, have these schemes been directly connected to BEC actors through IC3 complaints.

A total of 1,053 complaints reporting this BEC evolution of the payroll diversion scheme were filed with the IC3 between Jan. 1, 2018, and June 30, 2019, with a total reported loss of $8,323,354. The average dollar loss reported in a

[3] Reference PSA I-091818-PSA Cybercriminals Utilize Social Engineering Techniques to Obtain Employee Credentials to Conduct Payroll Diversion

complaint was $7,904. The dollar loss of direct deposit change requests increased more than 815 percent between Jan. 1, 2018, and June 30, 2019 as there was minimal reporting of this scheme in IC3 complaints prior to January 2018.



SUGGESTIONS FOR PROTECTION

Employees should be educated about and alert to this scheme. Training should include preventative strategies and reactive measures in case they are victimized. Among other steps, employees should be told to:

- Use secondary channels or two-factor authentication to verify requests for changes in account information.
- Ensure the URL in emails is associated with the business it claims to be from.
- Be alert to hyperlinks that may contain misspellings of the actual domain name.
- Refrain from supplying login credentials or PII in response to any emails.
- Monitor their personal financial accounts on a regular basis for irregularities, such as missing deposits.
- Keep all software patches on and all systems updated.
- Verify the email address used to send emails, especially when using a mobile or handheld device by ensuring the senders address email address appears to match who it is coming from.
- Ensure the settings the employees' computer are enabled to allow full email extensions to be viewed.

If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds and your employer to report irregularities with payroll deposits.

As soon as possible, file a complaint regardless of the amount with www.ic3.gov or, for BEC/EAC victims, BEC.IC3.gov.

Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

May 04, 2017

Alert Number
I-050417-PSA

Questions regarding this PSA should be directed to your local **FBI Field Office**.

Local Field Office Locations: www.fbi.gov/contact-us/field

BUSINESS E-MAIL COMPROMISE
E-MAIL ACCOUNT COMPROMISE
THE 5 BILLION DOLLAR SCAM

This Public Service Announcement (PSA) is an update to Business E-mail Compromise (BEC) PSAs 1-012215-PSA, 1-082715a-PSA and I-061416-PSA, all of which are posted on www.ic3.gov. This PSA includes new Internet Crime Complaint Center (IC3) complaint information and updated statistical data as of December 31, 2016.

DEFINITION

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

The techniques used in the BEC/EAC scam have become increasingly similar, prompting the IC3 to begin tracking these scams as a single crime type[1] in 2017.

The scam is carried out when a subject compromises legitimate business e-mail accounts through social engineering or computer intrusion techniques to conduct unauthorized transfers of funds.

Most victims report using wire transfers as a common method of transferring funds for business purposes; however, some victims report using checks as a common method of payment. The fraudsters will use the method most commonly associated with their victim's normal business practices. The scam has evolved to include the compromising of legitimate business e-mail accounts and requesting Personally Identifiable Information (PII) or Wage and Tax Statement (W-2) forms for employees, and may not always be associated with a request for transfer of funds.

BACKGROUND

The victims of the BEC/EAC scam range from small businesses to large corporations. The victims

continue to deal in a wide variety of goods and services, indicating that no specific sector is targeted more than another.

It is largely unknown how victims are selected; however, the subjects monitor and study their selected victims using social engineering techniques prior to initiating the BEC scam. The subjects are able to accurately identify the individuals and protocols necessary to perform wire transfers within a specific business environment. Victims may also first receive "phishing" e-mails requesting additional details regarding the business or individual being targeted (name, travel dates, etc.).

Some individuals reported being a victim of various Scareware or Ransomware cyber intrusions immediately preceding a BEC incident. These intrusions can initially be facilitated through a phishing scam in which a victim receives an e-mail from a seemingly legitimate source that contains a malicious link. The victim clicks on the link, and it downloads malware, allowing the subject(s) unfettered access to the victim's data, including passwords or financial account information.

The BEC/EAC scam is linked to other forms of fraud, including but not limited to: romance, lottery, employment, and rental scams. The victims of these scams are usually U.S. based and may be recruited as unwitting money mules[2]. The mules receive the fraudulent funds in their personal accounts and are then directed by the subject to quickly transfer the funds to another bank account, usually outside the U.S., upon direction, mules may open bank accounts and/or shell corporations to further the fraud scheme.

STATISTICAL DATA

The BEC/EAC scam continues to grow, evolve, and target small, medium, and large businesses. Between January 2015 and December 2016, there was a 2,370% increase in identified exposed losses[3]. The scam has been reported in all 50 states and in 131 countries. Victim complaints filed with the IC3 and financial sources indicate fraudulent transfers have been sent to 103 countries.

Based on the financial data, Asian banks located in China and Hong Kong remain the primary destinations of fraudulent funds; however, financial institutions in the United Kingdom have also been identified as prominent destinations.

The following BEC/EAC statistics were reported to the IC3 and are derived from multiple sources, including IC3 and international law enforcement complaint data and filings from financial institutions between **October 2013 and December 2016:**

Domestic and international incidents:	40,203
Domestic and international exposed dollar loss:	$5,302,890,448

The following BEC/EAC statistics were reported in victim complaints to the IC3 from **October 2013 to December 2016:**

Total U.S. victims:	22,292
Total U.S. exposed dollar loss:	$1,594,503,669
Total non-U.S. victims:	2,053
Total non-U.S. exposed dollar loss:	$626,915,475

The following BEC/EAC statistics were reported by victims via the financial transaction component of the new IC3 complaint form, which BECame available in June 2016[4]. The following statistics were reported in victim complaints to the IC3 from **June 2016 to December 2016:**

Total U.S. financial recipients:	3,044
Total U.S. financial recipient exposed dollar loss:	$346,160,957
Total non-U.S. financial recipients:	774
Total non-U.S. financial recipient exposed dollar loss:	$448,464,415

SCENARIOS OF BEC/EAC
Based on IC3 complaints and other complaint data, there are five main scenarios by which this scam is perpetrated.

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 account. The 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. This particular scenario has also been referred to as the "Bogus Invoice Scheme," "Supplier Swindle," and "Invoice Modification Scheme."

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 made to a second employee within the 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 financial institution with instructions to urgently send funds to bank "X" for reason "Y." This particular scenario has been referred to as "CEO Fraud," "Business Executive Scam," "Masquerading," and "Financial Industry Wire Frauds."

Scenario 3: Business Contacts Receiving Fraudulent Correspondence through Compromised E-mail
An employee of a 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 this 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 to follow up on the status of an 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.

Scenario 5: Data Theft
Fraudulent requests are sent utilizing a business executive's compromised e-mail. The entities in the business organization responsible for W-2s or maintaining PII, such as the human resources department, bookkeeping, or auditing section, have frequently been identified as the targeted recipients of the fraudulent request for W-2 and/or PII. Some of these incidents are isolated and some occur prior to a fraudulent wire transfer request. Victims report they have fallen for this new BEC scenario even if they were able to successfully identify and avoid the traditional BEC scam. This data theft scenario of the BEC scam first appeared just prior to the 2016 tax season.

TRENDS

W-2/PII Data Theft

This scenario of BEC/EAC was identified in 2016 in which a human resource department or counterpart was targeted with a spoofed e-mail seemingly on behalf of a business executive requesting all employee PII or W-2 forms for tax or audit purposes. The request appeared to coincide with the 2016 U.S. tax season, which runs from January through April. The number of complaints and reported losses peaked in April 2016, although complaints were still submitted by victims throughout 2016. Victims appeared to be both the businesses responsible for maintaining PII data and the employees whose PII was compromised. In several instances, thousands of employees were compromised. Employees filed identity theft–related complaints with IC3 that included reported incidents of fraudulent tax return filings, credit card applications, and loan applications.

Resurgence of Original Scheme

The IC3 saw a 50% increase in the number of complaints in 2016 filed by businesses working with dedicated international suppliers. This scenario was described in the earliest BEC/EAC complaints and quickly evolved into more sophisticated scenarios . In some instances, instead of requesting a change in a single remittance or invoice payment, BEC/EAC perpetrators changed the remittance location to redirect all incoming invoice payments. The fraudulent request appeared to be facilitated through a spoofed e-mail or domain.

Real Estate Transactions

The BEC/EAC scam targets all participants in real estate transactions, including buyers, sellers, agents, and lawyers. The IC3 saw a 480% increase in the number of complaints in 2016 filed by title companies that were the primary target of the BEC/EAC scam. The BEC/EAC perpetrators were able to monitor the real estate proceeding and time the fraudulent request for a change in payment type (frequently from check to wire transfer) or a change from one account to a different account under their control.

SUGGESTIONS FOR PROTECTION

Businesses with an increased awareness and understanding of the BEC/EAC scam are more likely to recognize when they have been targeted by BEC/EAC fraudsters, and are therefore more likely to avoid falling victim and sending fraudulent payments.

Businesses that deploy robust internal prevention techniques at all levels (especially for front line employees who may be the recipients of initial phishing attempts) have proven highly successful in recognizing and deflecting BEC/EAC attempts.

Some financial institutions reported holding their customer requests for international wire transfers for an additional period of time to verify the legitimacy of the request.

The following list includes self-protection strategies:

- Avoid free web-based e-mail accounts: Establish a company domain name and use it to establish company e-mail accounts in lieu of free, web-based accounts.
- Be careful what you post to social media and company websites, especially job duties and descriptions, hierarchal information, and out-of-office details.
- Be suspicious of requests for secrecy or pressure to take action quickly.
- Consider additional IT and financial security procedures, including the implementation of a two-step verification process. For example:
    - Out-of-Band Communication: Establish other communication channels, such as telephone calls, to verify significant transactions. Arrange this two-factor

authentication early in the relationship and outside the e-mail environment to avoid interception by a hacker.

- Digital Signatures: Both entities on EACh side of a transaction should utilize digital signatures. This will not work with web-based e-mail accounts. Additionally, some countries ban or limit the use of encryption.

- Immediately report and delete unsolicited e-mail (spam) from unknown parties. DO NOT open spam e-mail, click on links in the e-mail, or open attachments. These often contain malware that will give subjects access to your computer system.
- Do not use the "Reply" option to respond to any business e-mails. Instead, use the "Forward" option and either type in the correct e-mail address or select it from the e-mail address book to ensure the intended recipient's correct e-mail address is used.
- Consider implementing two-factor authentication for corporate e-mail accounts. Two-factor authentication mitigates the threat of a subject gaining access to an employee's e-mail account through a compromised password by requiring two pieces of information to log in: (1) something you know (a password) and (2) something you have (such as a dynamic PIN or code).
- Beware of sudden changes in business practices. For example, if a current business contact suddenly asks to be contacted via their personal e-mail address when all previous official correspondence has been through company e-mail, the request could be fraudulent. Always verify via other channels that you are still communicating with your legitimate business partner.
- Create intrusion detection system rules that flag e-mails with extensions that are similar to company e-mail. For example, a detection system for legitimate e-mail of abc_company.com would flag fraudulent e-mail from abc-company.com.
- Register all company domains that are slightly different than the actual company domain.
- Verify changes in vendor payment location by adding additional two-factor authentication such as having a secondary sign-off by company personnel.
- Confirm requests for transfers of funds. When using phone verification as part of two-factor authentication, use previously known numbers, not the numbers provided in the e-mail request.
- Know the habits of your customers, including the details of, reasons behind, and amount of payments.
- Carefully scrutinize all e-mail requests for transfers of funds to determine if the requests are out of the ordinary.

A complete list of self-protection strategies is available on the United States Department of Justice website www.justice.gov in the publication titled "Best Practices for Victim Response and Reporting of Cyber Incidents."

WHAT TO DO IF YOU ARE A VICTIM

If funds are transferred to a fraudulent account, it is important to act quickly:

- Contact your financial institution immediately upon discovering the fraudulent transfer.
- Request that your financial institution contact the corresponding financial institution where the fraudulent transfer was sent.
- Contact your local Federal Bureau of Investigation (FBI) office if the wire is recent. The FBI, working with the United States Department of Treasury Financial Crimes Enforcement Network, might be able to help return or freeze the funds.
- File a complaint, regardless of dollar loss, with www.ic3.gov or, for BEC/EAC victims, bec.ic3.gov

When contacting law enforcement or filing a complaint with IC3, it is important to identify your incident as “BEC/EAC”; also consider providing the following information:

- Originating business name
- Originating financial institution name and address
- Originating account number
- Beneficiary name
- Beneficiary financial institution name and address
- Beneficiary account number
- Correspondent bank if known or applicable
- Dates and amounts transferred
- IP and/or e-mail address of fraudulent e-mail

Detailed descriptions of BEC/EAC incidents should include but not be limited to the following when contacting law enforcement:

- Date and time of incidents
- Incorrectly formatted invoices or letterheads
- Requests for secrecy or immediate action
- Unusual timing, requests, or wording of the fraudulent phone calls or e-mails
- Phone numbers of the fraudulent phone calls
- Description of any phone contact, including frequency and timing of calls
- Foreign accents of the callers
- Poorly worded or grammatically incorrect e-mails
- Reports of any previous e-mail phishing activity

---

1. The IC3 uses descriptions of crime types for categorization purposes. ↩
2. Money mules are defined as persons who transfer money illegally on behalf of others. ↩
3. Exposed dollar loss includes actual and attempted loss in United States dollars. ↩
4. “Financial Recipient” is defined as an account holder who receives the fraudulent funds. ↩