BankUnited

Business Email Compromise
Fraud Prevention
Understanding and Preventing Cyber/Email Fraud

Stewart Title Guaranty Company 2020

Bain v. Platinum Realty, LLC ,

https://www.nar.realtor/legal-case-summaries/licensee-liable-for-wire-fraud-losses

- Read the full decision: Bain v. PLATINUM REALTY, LLC(link is external)
- Kansas federal court upholds jury verdict that determined that the buyer's representative was 85% responsible for the buyer's losses, which occurred when the buyer transferred purchase money to fake account after buyer's representative allegedly forwarded email containing false wiring instructions to the buyer.
- A real estate buyer ("Buyer") purportedly received an email from her real estate representative ("Buyer's Representative") that provided new wiring instructions for the upcoming closing on a property. The Buyer used the false instructions to wire the purchase money to the fraudulent account and lost $196,622. The criminal had infiltrated the email exchanges between the parties to the transaction and created fake email accounts that were very similar to the email accounts used by the parties. The criminal had used these accounts to transmit the false wire instructions that were eventually sent to the Buyer.
- The Buyer brought a lawsuit against a number of parties, including the Buyer's Representative. The Buyer's Representative claimed that she had never sent the email with the false wiring instructions. She had initially forwarded an email with the false wire instructions but she had sent it to one of the fake accounts set up by the criminal. She claimed that she had not sent the later email that the Buyer did receive and used to send the purchase money to the fraudulent account.
- The case went to trial, and the jury found that the Buyer's Representative was 85% responsible for the loss and the court entered judgment against the Buyer's Representative for $**167,129.** The Buyer's Representative filed a post-trial motion seeking a determination in her favor.
- The United States District Court for the District of Kansas affirmed the jury verdict. The court rejected the Buyer's Representative's argument that she did not send the email to the Buyer that was used to send the wire, finding this was an issue of fact for the jury to resolve as there was some evidence that the Buyer's Representative had sent the later email. The jury determined that the Buyer's Representative had sent the email, and so the court affirmed the jury verdict in favor of the Buyer.
- ***Bain v. Platinum Realty, LLC*** , No. 16-2326-JWL, 2018 WL 3105376 (D. Kan. June 25, 2018). [This is a citation to a Westlaw document. Westlaw is a subscription, online legal research service. If an official reporter citation should become available for this case, the citation will be updated to reflect this information.]

MALWARE:

- Malicious software, known as Malware is intended to disrupt computer operations, collect sensitive information, or gain unauthorized access. Malware includes computer viruses, worms, Trojan horse, spyware, adware and more.
- Malware is distributed by a variety of means, most often email where the user is asked to click on a link that purports to be legitimate. Recent example include IRS, NACHA, Federal Reserve, FDIC. Malware is also distributed through websites, Pop-ups, Social Network sites, Removable Media.

SIGNS OF MALWARE:

Computer -is slow or locks up, reboot unexpectedly, unusual pop-ups appear, new or unexpected toolbars pop up- (ANY PERFORMANCE ISSUES)

Online Banking- repeats prompts for ids/passwords, elements of page are missing, unusual prompts to enter sensitive information (ANY UNUSUAL BEHAVIOR)

What if?- if you experience these signs- STOP and call your bank immediately, do not attempt to sign-on to banking site, have PC rebuilt or cleaned by professional IT.

BEC Headlines

BankUnited

HEADLINES:

- Austrian Firm Fires CEO After $56-million Cyber Scam.
- Cybercriminals Steal $54 Million from Aircraft Parts Maker
- Firm Sues Cyber Insurer Over $480K Loss.
- Denver Couple (Buyers) scammed out of $300K-kills purchase
- Tech Firm Suffers $46M Cyberheist.
- FBI Warns of Dramatic Increase in Business E-Mail Scams
- Thar she blows: Whaling attacks likely to rise in 2018.
- US and European companies Top Targets of CEO Fraud.
- Ransomware payments to hit the $1B+ mark for 2018.

BankUnited

RECENT HEADLINES (Courtesy of ALTA):

•**Maryland:** The FBI says fraudsters used fake emails to fool a settlement company into wiring them the proceeds of the sale of a couple's home. **Amount lost: $411,548**

•**New York:** A judge trying to sell her apartment received an email she thought was from her real estate lawyer telling her to wire money to an account. **Amount lost: $1 million.**

•**Washington:** The homebuyers sued the title company for the lost money, but also close to $5 million for an alleged violation of the RICO Act. The title company, which denies it had anything to do with the money going missing, said that it immediately contacted the FBI when the attack was discovered. **Amount lost: $1.57 million.**

•**Colorado:** A couple, who lost their life savings while trying to buy their dream retirement home, has filed suit alleging that none of the companies involved in the transaction—including a title company—did enough to protect sensitive financial information. **Amount lost: $272,000**

•**Minneapolis:** A retired couple hoping to buy a townhouse to be closer to their grandchildren received an email that looked like it came from the title company with instructions to wire money before the closing. They did. The email was fake. **Amount lost: $205,000.**

Updated BEC Statistics

Historical Data:

- 10/13 - 2/16: $2.3B
- 2/16 – 5/16: $3.1B
- 5/16 - 5/17: $5.0B
- 5/17-12/18: $12B
- **Thru 7/2019 $26B in exposed dollar loss-domestic and international**

- Business Email Compromise **(BEC)** attacks have expanded tremendously over the past few years, with a projected growth of over **$26 billion in 2019.**

- Average Bank Robbery **$4000.00**
- Average BEC **$170,000.00**

- A total of 1,053 complaints reporting the 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 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**

- **The combination of simplicity and effectiveness have ensured that BEC will continue to be one of the most popular attacks, especially for those who lack special tools and knowledge to pull off more complicated schemes.**

- **How BEC Schemes Work**

Unlike account takeover activity, e-mail-compromise schemes involve impersonation and social engineering resulting in victims submitting 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.

BEC schemes focus on using compromised e-mail accounts to mislead financial institutions and their customers into conducting unauthorized wire transfers. BEC schemes can be broken down into three stages:

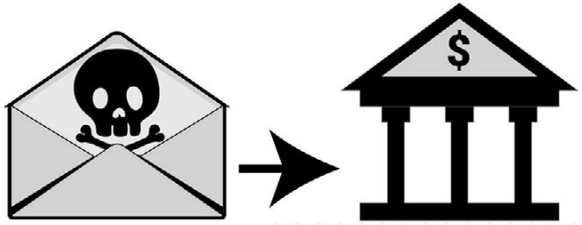
How BEC and EAC Schemes Work

BankUnited

- **Stage 1 – Compromising Victim Information and E-mail Accounts**:

Criminals first unlawfully access a victim's e-mail account through social engineering or computer intrusion techniques. Criminals subsequently victim's e-mail account to obtain information on victim's financial institutions, account details, and related information.

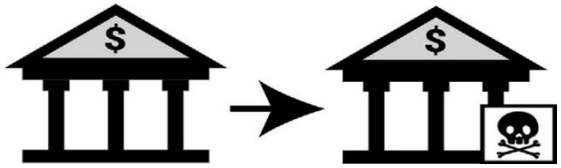
- **Stage 2 – Transmitting Fraudulent Transaction Instructions**:



Criminals then use the victim's stolen information to e-mail fraudulent wire transfer instructions in a manner appearing to be from the trusted counter party. 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.

How BEC and EAC Schemes Work

- **Stage 3 – Executing Unauthorized Transactions**: Criminals trick the victim 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

BankUnited

- BEC schemes target financial institutions' Customers. Criminals seek to unlawfully access the e-mail accounts of a company's Executives (RE Brokers), Employees (Agents) and or **Buyers/Sellers** to:
- a) Directly submit fraudulent transaction instructions by impersonating above through e-mails and documentation related to the requested transfer; or
- b) Mislead a company employee into submitting fraudulent transaction instructions to the company's financial institution by impersonating a supplier, company executive, and or a **Trusted Counter Party** to authorize or order payment through seemingly legitimate internal e-mails**.**
- c) BEC Scams are rampant in the Mortgage/Title/Settlement industries. Cyber Fraudsters are preying on unsuspecting Buyers and Sellers through compromised email accounts.

BE AWARE!!

Current BEC scheme effecting the Real Estate Industry:

- ***Scenario 1– Criminal Impersonates a TRUSTED Counter Party in the RE Transaction***: A criminal hacks into and uses the e-mail account of a Borrower's RE Agent or Settlement Attorney to send fraudulent wire transfer instructions to the ***Borrower/Buyer***. Based on this request, the Borrower requests their financial institution issues a wire transfer and sends funds to an account the criminal controls. *In this scenario, the criminal impersonating the Borrower/Buyer's Trusted Counter Party (RE Agent) prompted the Buyer's financial institution to execute an* ***authorized*** *wire transfer*.

BEC schemes often take the following forms:

- ***Scenario 2 – Criminal Impersonates a Financial Institution's Customer***: A criminal uses a "spoofed" e-mail account of a Company A's Customer (Borrower) to send fraudulent wire transfer instructions to Company A. Company A then sends **APPROVED** wire instructions to their financial institution (Bank). 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*.

BEC schemes often take the following forms: “Whaling”

- ***Scenario 3 – Criminal Impersonates an Executive***: A criminal uses a “SPOOFED” e-mail account of a Company B’s executive (CEO) to send wire transfer instructions to a Company B employee (CFO) who is responsible for processing and issuing payments. The employee, believing the executive’s e-mailed instructions are legitimate, orders Company’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*.

BEC schemes often take the following forms:

- ***Scenario 4 – 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*.

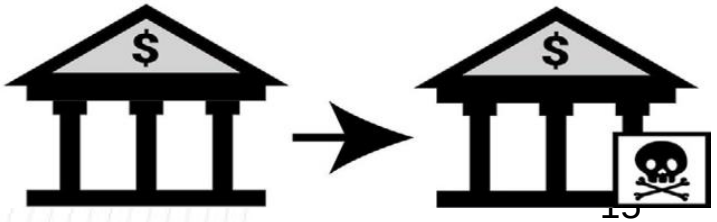
Anatomy of a BEC
The Players:

- The Cyber Thief

- The Title/Exchange Company

- The Taxpayer/Seller/Buyer

- The Remitting Bank
- The Beneficiary Bank



- Realtor

- Settlement Attorney

- Appraiser

- Home Inspector

Anatomy of a BEC-Scenario 1

- ***Scenario – Criminal Impersonates a Financial Institution's Commercial Customer***:
- Through the distribution of MALWARE, A Cyber Thief hacks into the email account of Mr. John Smith. Mr. Smith (Taxpayer) is presently scheduling the closing of a purchase of a $500,000.00 Investment Property.
- Mr. Smith previously sold a like-kind Investment Property 5-months prior to this purchase. Mr. Smith is currently working with his Real Estate Attorney and USA Title & Exchange, a national provider of Title Insurance and 1031-Exchange services.
- The Cyber Thief has been following the email traffic between Mr. Smith**, His Realtor**, Closing Attorney and USA Title & Exchange for the **past 60 days** and is fully aware of the scheduled date of the closing, the amount of the transaction and who at USA Title is the primary contact to receive information pertaining to the transaction
- Prior to the scheduled closing the Cyber Thief creates a fraudulent email address to mimic that **of Mr. Smith's Realtor** and sends false wire transfer instructions for USA Title& Exchange Company to Mr. Smith via email.
- Mr. Smith receives the instructions and issues outbound wire transfer instructions to his Bank via online.
- Bank receives the instructions and sends funds as instructed , however the funds are being remitted to an account the criminal controls.
- The funds are received at the Beneficiary Bank, deposited to an account set up by the Cyber Thieves, with further wire instructions to send the funds to a offshore bank account.
- Mr. Smith receives the Fed# from and proceeds to forward the information to USA Title & Exchange and his Attorney in preparation for the closing.
- **All are notified of the Fed# but the funds never get there……. What now……**

In this scenario, the criminal impersonating the Customer's Trusted Counter Party prompted the Individual to execute an authorized wire transfer.

How can you defend your company from BEC?

- Businesses are advised to **educate employees** on how BEC scams and other similar attacks work. These schemes do not require advanced technical skills, use tools and services widely available in the cybercriminal underground, and only needs a single compromised account to steal from a business. As such, here are some tips on how to stay safe from these online schemes:
- Carefully **scrutinize all emails**. Be wary of irregular emails sent by high-level executives, as they can be used to trick employees into acting with urgency**. Review and verify** emails requesting funds to determine if the requests are out of the ordinary.
- **Raise employee awareness**. While employees are a company's biggest asset, they can also be its weakest link when it comes to security. **Commit to training employees**, review company policies, and develop good security habits.
- **Verify any changes in vendor payment location by using a secondary sign-off by company personnel.**
- **Stay updated** on customers' habits, including the details, and reasons behind payments.
- **Verify requests**. Confirm requests for fund transfers when using phone verification as part of two-factor authentication, use known familiar numbers, not the details provided in the email requests.
- **CLIENT ENGAGEMENT: *Establish communication protocol when Client is engaged***
- **Report any incident immediately to law enforcement or file a complaint with the IC3 (Internet Crime Complaint Center: . https://www.ic3.gov/default.aspx**

BEWARE!!!
BEC SCAM 101

---------- Forwarded message ---------
From: **ROBERT Bxxxx** <officedocs@cox.net>
Date: **Tue, Oct 9, 2018 at 8:37 AM**
Subject: Re: FW: Sxxxxx Nxxx and Lxxxxx Nxxx from Lobain / 38 Beachtree Terrace, Rockaway, NY 10786/MT-20836
To: **Sxxxxx Nxxx** nxxxxx@mail.montvail.edu

- Your wire amount is $18,348.30 please ensure wire is sent today and send me an email once completed, see below wire instructions:
- **Bank Name:**
  Bank Of America
  315 Main Street,
  Western, NY 10870
  Routing# 026009593

- **Account Name:**
  ACME **Debra Ardis** Settlement Services
  100 Lake Avenue
  Western, NY 10871
  Account# 446040991720

- **Report any incident immediately to law enforcement or file a complaint with the IC3 (Internet Crime Complaint Center): . https://www.ic3.gov/default.aspx**

BEC Email Trail Red Flags

From: Robert Stillwell <closingdpt@comcast.net>
Sent: Monday, December 10, 2018 9:34 AM
To:
Subject: 36 Flagstaff Ave, Pittstown, NY 12891

Good Morning, What's the update regarding my loan proceed? Is there any possibilities I could have my proceed from my loan wired to my trust investment account today? I just discovered that my bank now maintain a 14 days hold mandatory policy before clearing wire and check deposits. I would rather pay the wire fee to have my proceed wired to my trust to ensure immediate access to the funds. Please advise!

Thank you,

Robert.

BEC Email Trail Red Flags

From: Robert Stillwell <closingdpt@comcast.net>
Sent: Monday, December 10, 2018 9:34 AM
To:
Subject: 36 Flagstaff Ave, Pittstown, NY 12891

Good Morning, What's the update regarding my loan **proceed**? Is there any **possibilities** I could have my **proceed** from my loan wired to my trust investment account today? **I just discovered that my bank now maintain a 14 days hold mandatory policy before clearing wire and check deposits**. I would rather pay the wire fee to have my **proceed** wired to my trust to ensure immediate access to the funds. Please advise!

Thank you,

Robert

BEC Email Trail Red Flags

From: Robert Stillwell <closingdpt@comcast.net>
Sent: Monday, December 10, 2018 11:59 AM
To:
Subject: RE: 36 Flagstaff Ave, Pittstown, NY 12891

The account is on our names and we'll like it wired to the account, The policy also applied to certified checks. Please advise!

Thank you,

Robert.

BEC Email Trail Red Flags

From: Robert Stillwell <**closingdpt@comcast.net**>
Sent: Monday, December 10, 2018 11:59 AM
To:
Subject: RE: 36 Flagstaff Ave, Pittstown, NY 12891

The account is on our names and **we'll like it wired to** the account, The policy also **applied** to certified checks. Please advise!

Thank you,

Robert.

BEC Email Trail Red Flags

From: Robert Stillwell <closingdpt@comcast.net>
Sent: Monday, December 10, 2018 11:59 AM
To:
Subject: RE: 36 Flagstaff Ave, Pittstown, NY 12891

Below is the account I will like to have my proceed wired too.

Bank: Main Street Bank
Account Name: Samantha Robert Stillwell Smith
Account #: 123456789
Routing #: 1000301567

Please kindly acknowledge the wire transfer confirmation receipt immediately the wire has been transmitted.
Thank you,
Robert.

BEC Email Trail Red Flags

From: Robert Stillwell <closingdpt@comcast.net>
Sent: Monday, December 10, 2018 11:59 AM
To:
Subject: RE: 36 Flagstaff Ave, Pittstown, NY 12891

Below is the account I will like to have my proceed wired too.

Bank: Main Street Bank
Account Name: Samantha Robert Stillwell Smith
Account #: 123456789
Routing #: 1003015678

Please kindly acknowledge the wire transfer confirmation receipt immediately the wire has been transmitted.
Thank you,
Robert.

What to do IF & WHEN a BEC Occurs

- Have a Continuation of Business **(COB)** Plan for IF and WHEN a BEC occurs.
- Contact your Banking team **IMMEDIATELY** via Telephone AND email. KNOW WHO TO CONTACT, Sales, Service, All!
- Ensure **ALL** Employees have Bank CONTACT INFO.
- Inform Banking Team of the **FRAUDULENT** transaction.
- Provide a **screen shot** of the outbound wire if possible.
- Once informed, Bank Team should alert the **Corporate Fraud Division** of the transaction.
- Bank should submit a wire recall on Client's behalf to the **Beneficiary Bank** and report the fraudulent transaction in an attempt to have the funds held.
- Bank should complete an FBI, **Internet Complaint Form (IC3)** and contact law Enforcement on Client's behalf for immediate action.
- Bank should keep the Client(s) fully informed of **the status** and any additional steps such as completion of an Affidavit of ***Unauthorized Transaction***.
- Upon receipt of recovery, funds will be returned to the originating account.

Red Flags

- **Red Flags**
  - Changed email address, often subtle (hover cursor over email address)
  - Multiple parties on prior emails; fraudulent email is only 2-party
  - Changed or multiple sets of wiring instructions – **WIRE INSTRUCTIONS SHOULD NEVER CHANGE!**
  - Poor grammar or odd use of terms / phrases
  - Sense of urgency – funds must be wired immediately
  - Recipient bank account doesn't make sense
    - ✓ Payee not a party to transaction
    - ✓ Payee is law firm not involved in the transaction
    - ✓ Payee in an unrelated location (another state)
  - Email sent outside of normal business hours or using 24 hour clock (22:00 hrs. instead of 10:00pm)
  - Unexpected email with link to a document – likely a link with malware
    (hover cursor over the link)

BEWARE!!!
FAXING is Now Vulnerable!!

BankUnited

- There has been a recent move to go back to utilizing FAXING as a method of sharing and obtaining banking and wire information between Settlement Agents and Buyers/Sellers.

- Although using FAX technology MAY negate systemic hacking, **REMEMBER** that if email exchange was used in any part of the communication chain, using FAXES to share banking information is open to **CYBER FRAUD.**

- **CASE STUDY:**
  - Prior to closing, Seller of property communicated via email with the Title/Settlement Company on obtaining their FAX number to provide Loan Payoff Information for their loan.
  - 2 weeks prior to the closing the Seller faxed the Pay Off Information they received from their Lender directly to the Settlement Company. Banking Information included the account title: **Payoff Clearing Account**
  - 2 Days prior to the Closing the Settlement Company received an updated FAX "From the Seller" which had a change to the pay Off Account Number and Information at the same Lender Bank: **Payoff Toneberg Enterprise**
  - Settlement Company used the banking information from the second FAX and wired **$390,000.00** to the Lender Bank to "Pay Off" the Seller's Mortgage.
  - Cyber Fraudsters compromised the Seller's email and followed the communication between the Settlement Company and The Seller. They gained access to the original payoff letter the Seller received from the Lender and created an exact duplicate of the original FAX. The second FAX made no reference of being an update.
- **Report any incident immediately to law enforcement or file a complaint with the IC3 (Internet Crime Complaint Center): . https://www.ic3.gov/default.aspx**

Q&A