



*Law Office of*

**MICHELLE L. GLASS, PA**

REAL ESTATE

# Cyber and Wire Fraud: Know the Signs

**Presented By: Michelle L. Glass, Esq.**

Information Received From: Fidelity National Financial

# Business Email Compromise (BEC)

- **Sophisticated fraud scheme targeting businesses who regularly perform wire transfer payments**
- **Involves targeting of all participants of a real estate transaction, gaining entry into their computer systems and posing as those parties via compromised emails**
  - real estate agents
  - loan officers
  - mortgage brokers
  - title agents
  - buyers and sellers
  - closing attorneys
- **A/K/A account hijacking**

# FBI Real Estate Scheme Diagram

## (U) E-mail Account Spoofing Techniques

**Using existing e-mail account:** Actual sender is masked and does not appear in the "reply to" field, yet does appear in email header.

**Adding/removing characters:** From legitimate widgets@freemail.com to widget@freemail.com

**Rearranging characters:** From acme868@freemail.com to acme686@freemail.com.

**Replacing characters:** In a sans serif font frequently used in e-mail to Arial, different characters appear to be similar: sales@freemail.com to sales@freemail.com; sales@freemail.com to sales@freemail.com



Victims are identified by browsing websites such as Zillow.com and Flipkey.com to identify and target realtors. Criminal actors (CAs) also use Internet chat rooms to communicate the details of the scheme, content of language used in spam, and malicious links sent to victims.



CA uses social engineering and computer intrusion techniques such as malware and spear phishing to gain access to target's email account and/or others whom the target corresponds such as title agent, builder, buyer, borrower, seller, etc.



CA peruses target victim's email account messages and determines the timing of deposit/closing/settlement dates.



CA hijacks/intercepts the upcoming transaction by spoofing a transactional participant's email account. CA does this by 1) creating a similar domain account; and/or 2) using existing email account. If an existing e-mail account is used, CA will often code any incoming email to go directly to the trash bin to further conceal the fraud.



CA presents to be a transactional participant and sends an email to another participant in the transaction with alternative wire transfer instructions. In a title company this may be sent to the individual in charge of disbursements or the title agent themselves; if the target is a borrower, the e-mail may contain wire transfer instructions purportedly from the title company or real estate agent requesting earnest money or down payment funds or a change to the previously legitimate instructions sent by the actual title agent or realtor; if the target is the seller, it may be instructions on where to wire their settlement funds.



Wire transfer request is assumed to be legitimate and is authorized and submitted to victim's bank using the beneficiary account information provided by the CA in the email.



Victims bank submits the wire transfer to a bank account in the United States controlled by the CA.



CA usually requires confirmation from the victim that the wire was sent/deposited. Once confirmed, the CA will take immediate steps to withdraw the funds from the account in question.

# BEC Details

**With access to the email account, the fraudster will either:**

- Intercept and send emails directly from within the participant's email account, or
- Set up a similar, but separate, "spoofed" account to send emails.

From: [REDACTED] <[officeemailins@comcast.net](mailto:officeemailins@comcast.net)>  
Date: August 17, 2017 at 6:40:08 AM MDT  
To: [REDACTED] <[\[REDACTED\]@gmail.com](mailto:[REDACTED]@gmail.com)>  
Subject: CD and Wire balancing - [REDACTED]  
Reply-To: [REDACTED] <[officeemailins@comcast.net](mailto:officeemailins@comcast.net)>

Good Morning,

Can you please send me the buyer's email for this file?


[REDACTED]

*Escrow Officer*

[REDACTED]

[REDACTED] Email: [REDACTED] <[\[REDACTED\]@fnf.com](mailto:[REDACTED]@fnf.com)>

[REDACTED]

 **Care to be Aware**  
Always call a verified phone number before you wire.  
Call us immediately if you receive an email with wire instructions.



From: "[REDACTED]" <[REDACTED]@ltic.com>

Date: 2/16/18 9:00 AM (GMT-08:00)

To: [REDACTED]@yahoo.com (REAL BUYER)

Cc: [REDACTED] (REAL LENDER)

Subject: FHL13102 / 6729 50th St- wire receipt



[REDACTED] (BUYER'S LAST NAME USED)

Look at the receipt carefully, the account number is not correct. Please call your bank or go into the bank to rectify this. You mistakenly put ABA routing number in place of account number. It should be (Account Number: 149681779, Bank Routing Number: 263191387).

[REDACTED]  
Escrow Officer  
Lawyers Title Company

[REDACTED] FAX  
[REDACTED]@ltic.com

**\*\*Be aware! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS call your escrow officer immediately to verify the information prior to sending funds.\*\***

From: [REDACTED] <[REDACTED]@yahoo.com>

Date: 2/16/18 12:19 PM (GMT-08:00)

To: "[REDACTED]" <[REDACTED]@lti-c.com>

Subject: Re: FHL13102 / 6729 50th St- wire receipt

Yes thank you. I will be fixing this by 1:30pm today.

Sent via the Samsung Galaxy S7 edge, an AT&T 4G LTE smartphone

# 2016 FBI Findings

## **Most prevalent fraud scheme targeting businesses today.**

- Scam has been reported in all 50 states and in 131 countries
- More than 40,000 victims of cyber fraud attacks resulting in over \$5 Billion in losses.

## **Title companies, law firms, realtors, sellers and buyers were the most often targeted victims of wire fraud**

- 480% increase in the number of complaints filed by title companies in 2016 resulting in an estimated \$19M diverted from real estate transactions
- Nearly 1 Billion dollars targeted in 2017 from real estate transactions

# Additional Costs Associated with BEC

- **Investigation**
- **Litigation**
- **Brand and Reputation Erosion/Customer Churn**

# Recognition

is the **KEY!**



# Common Indicators of BEC

- **Emails requesting last minute changes to wiring information (i.e. change in beneficiary and/or receiving bank).**
- **Time of day the wire transfer was requested.**
  - End of the week or end of business day
  - Outside normal business hours
- **Emails from same sender that have significant changes to grammar, sentence structure or spelling compared to previous emails.**
- **Requests for secrecy or pressure to take action quickly.**
- **Sudden changes in business practices.**
  - Current business contact suddenly asks to be contacted via a different e-mail account

# Application in a Transaction

- **Seller Proceeds:** Escrow receives email from fraudster posing as seller to amend wire instructions for sale proceeds.
- **Buyer Funds:** Buyer receives email from fraudster posing as escrow agent or real estate agent with wire instructions for deposit or cash to close
- **Lender Funds:** Escrow receives email from fraudster posing as lender requesting return of loan proceeds or payoff funds.
- **Realtor® Commissions:** Escrow receives email from fraudster posing as Realtor® with wire instructions for commissions.

# Suggestions for Protection

- **EDUCATION- Best defense is awareness and understanding of the BEC scam.**
- **Avoid sending sensitive or confidential information via e-mail.**
- **Be careful of what is posted on social media sites and websites, especially job duties and descriptions, hierarchal information, and out-of-office details.**



## Suggestions for Protection (cont'd)

- **Establish other communications channels, such as a known, trusted telephone number to verify transactions.**
  - Establish early in the relationship
  - Establish outside the e-mail environment to avoid interception
- **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.**

## Suggestions for Protection (cont'd)

- **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 your email address book to ensure the intended recipient’s correct e-mail is used.
- **Use two-factor authentication** for e-mail accounts. This mitigates the threat of access through a compromised password by requiring two pieces of information to log in: 1) something you know (password) and 2) something you have (dynamic pin or code)
- **Use complex passwords that employ a combination of mixed case, numbers and symbols.**
  - Consider using a password manager



## Suggestions for Protection (cont'd)

- **ALWAYS verbally confirm requests of transfer of funds. Use previously known and trusted numbers, not the numbers provided in the e-mail request.**
- **Carefully scrutinize all e-mail requests for transfers of funds to determine if they are out of the ordinary.**
- **Regularly purge email**
  - Why? So the threat actor/hacker cannot look at your prior e-mails for information gathering purposes.
- **Consider implementing standard warning notice to your customers of the scam.**

# Wire Fraud Alerts

## Wire Fraud Alert

*This Notice is not intended to provide legal or professional advice. If you have any questions, please consult with a lawyer.*

Realtors®, Real Estate Brokers, Closing Attorneys, Buyers and Sellers are targets for wire fraud and many have lost hundreds of thousands of dollars because they simply relied on the wire instructions received via email, without further verification.

A fraudster will hack into a participant's email account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a closing, the fraudster will send an email to the Buyer purporting to be the escrow agent or another party to the transaction. The fraudulent email will contain new wiring instructions or routing information, and will request that the Buyer send funds to a fraudulent account.

Please be advised that the wire instructions listed below are the only wire instructions we will send you. If you receive another email or unsolicited call purporting to alter these instructions, please immediately call us at (insert phone number).

Insert Wire instructions

In addition, the following non-exclusive self-protection strategies are recommended to minimize exposure to possible wire fraud.

- **NEVER RELY** on email's purporting to change wire instructions. Parties to a transaction rarely change wire instructions in the course of a transaction.
- **ALWAYS VERIFY** wire instructions, specifically the ABA routing number and account number, by calling the party who sent the instructions to you. **DO NOT** use the phone number provided in the email containing the instructions; use phone numbers you have called before or can otherwise verify. **Obtain the number of your Realtor®, Real Estate Broker and your escrow officer as soon as an escrow account is opened. DO NOT** send an email to verify as the email address may be incorrect or the email may be intercepted by the fraudster.
- **DO NOT** forward wire instructions to other parties without first verbally verifying the instructions from the sending party.
- **USE COMPLEX EMAIL PASSWORDS** that employ a combination of mixed case, numbers, and symbols. Make your passwords greater than eight (8) characters. Also, change your password often and do NOT reuse the same password for other online accounts.
- **USE MULTI-FACTOR AUTHENTICATION** for email accounts. Your email provider or IT staff may have specific instructions on how to implement this feature.

For more information on wire fraud scams or to report an incident, please refer to the following links:

Federal Bureau of Investigation: <http://www.fbi.gov>

Internet Crime Complaint Center: <http://www.ic3.gov>

### ACKNOWLEDGEMENT OF RECEIPT

Your signature below acknowledges receipt of this Wire Fraud Alert.

Buyer 1

Signature \_\_\_\_\_

Printed Name \_\_\_\_\_

Address \_\_\_\_\_

Date \_\_\_\_\_

Phone Number \_\_\_\_\_

Buyer 2

Signature \_\_\_\_\_

Printed Name \_\_\_\_\_

Address \_\_\_\_\_

Date \_\_\_\_\_

Phone Number \_\_\_\_\_

**WIRE SAFE.**

IMPORTANT WIRE FRAUD ALERT FOR HOME BUYERS



Realtors®, real estate brokers, closing attorneys, buyers and sellers are targets for wire fraud and many have lost hundreds of thousands of dollars because they simply relied on the wire instructions received via email.

A fraudster will hack into a participant's email account to obtain information about upcoming real estate transactions. After monitoring the account to determine the likely timing of a closing, the fraudster will send an email to the buyer purporting to be the escrow agent or another party to the transaction. The fraudulent email will contain new wiring instructions or routing information, and will request that the buyer send funds to a fraudulent account.

We are urging everyone to **INQUIRE BEFORE YOU WIRE** and to never rely solely on email communication. Always follow these two simple steps:

## INQUIRE BEFORE YOU WIRE.

When in doubt, always call our office or your escrow officer.

For the best in service, remember to always insist on



**STEP 1**



Obtain the phone number of your Real Estate Broker, Realtor®, Closing Attorney (if applicable) and your Escrow Officer as soon as an escrow is opened. Complete the information below and keep this flyer in your escrow folder. If you are reading this at one of our offices and you don't have a copy of this flyer, simply ask the receptionist for a copy.

**STEP 2**



Prior to wiring, call the phone number you wrote down from step #1 above to speak directly with your Escrow Officer to confirm wire instructions. If you receive a change in wiring instructions supposedly from us or your Escrow Officer, be suspicious as we rarely change our wiring instructions.

ESCROW NUMBER

BROKER'S NAME/PHONE

REALTOR'S NAME/PHONE

ESCROW COMPANY

ESCROW OFFICER'S NAME/PHONE

# Wire Account Notification

## WIRE ACCOUNT NOTIFICATION

Property Address: \_\_\_\_\_

Project Reference: \_\_\_\_\_

Due to the increased wire fraud activity, the Company has instituted procedures to assist in the protection of parties to the Real Estate Settlement from these illegal activities.

Below you will find the wire account information for this transaction. Please be advised that the wire instructions, listed below, are the only wire instructions we will send you. **Verbally verify these wire instructions with us prior to forwarding to other parties.**

*If you receive another e-mail or unsolicited call purporting to alter these instructions, please immediately call us at (\_\_\_\_)\_\_\_\_-\_\_\_\_\_.*

BANK NAME: \_\_\_\_\_

ABA NUMBER: \_\_\_\_\_

ACCOUNT NAME: \_\_\_\_\_

ACCOUNT NUMBER: \_\_\_\_\_

ESCROW NUMBER: \_\_\_\_\_

EMPLOYEE TO NOTIFY: \_\_\_\_\_

EMPLOYEE PHONE NUMBER: \_\_\_\_\_

**If you have any questions, contact the Employee listed above at the number shown above.**

# Business Practices

- **Protect your house**
  - Department of Justice Cyber Incident Preparedness Checklist ([www.justice.gov](http://www.justice.gov))
- **Limit opportunities**
- **Standardize procedures**



# What To Do If a Party to the Transaction is a Victim

- **The account owner should contact the financial institution immediately upon discovering the fraudulent transfer.**
- **Request that the financial institution contact the corresponding financial institution where the fraudulent transfer was sent.**
- **Contact the local police department and Federal Bureau of Investigation (FBI) office.**
- **File a complaint with the Internet Crime Complaint Center at [www.ic3.gov](http://www.ic3.gov), regardless of the dollar amount.**



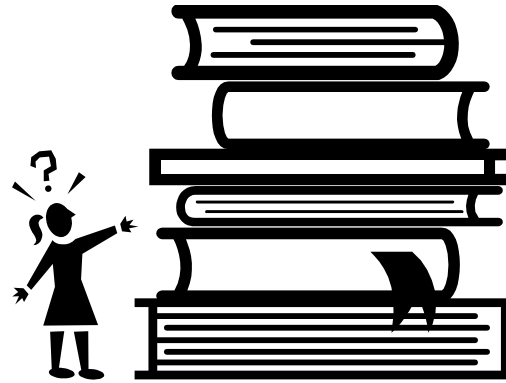
## **What To Do If a Party to the Transaction is a Victim (cont'd)**

- **Inform all parties to the transaction via a known, trusted phone number, that electronic communications may have been compromised and that all further activity should occur outside of electronic methods.**
- **DO NOT continue to communicate with persons who believe may not be proper parties to the transaction. Ignore further e-mails or other requests for updates.**
- **Recommend all parties to the transaction review email account security, including changing passwords, reviewing email login history and conducting security reviews of computers and networks.**

**ALWAYS:**

**Inquire before you wire!**

# Any Questions?



Michelle L. Glass, Esq.  
Law Office of Michelle L. Glass, PA  
Telephone: (904) 606-3903  
Facsimile: (904) 606-3936  
[michelle@glass-law.net](mailto:michelle@glass-law.net)