1. Presented by: Michael Weinstein, AVP, Division Financial Officer
2. Welcome Notes
    a. Presentation outline and additional resources available at: www.ChicagoNCSctic.com/news-events/webinars/
    b. Questions will be answered at the conclusion
    c. Brief survey provided when you log-out
        - Attorneys seeking Illinois CLE credit must complete the survey
3. Today's Goals:
    a. BEC Explained
    b. "Our Crime": Wire Fraud
    c. Provide real world example relating to wire fraud in the industry
    d. Learn common red flags to identify Business Email Compromise (BEC)
    e. How to avoid becoming a victim
    f. Learn about what Chicago Title is doing to prevent wire fraud
    g. Containment: Steps to consider if you've been compromised
4. Stats:
    a. Global Problem: Complaints from victims in every U.S. State and 100 countries
    b. IC3 BEC Reported Crime Statistics (time period Oct. 2013-May 2016)
        - Total Victims = 22,143
        - Total Exposed dollar loss = $3,086,250,090
        - Total Take = $1.2 Billion – ($1.5 Billion)
        - Majority of transfers going to Asian banks located within China & Hong Kong
        - 1,300% increase in identified victims and exposed loss since January 2015
5. Business Email Compromise – Defined
    a. BEC: A sophisticated scam targeting businesses working with foreign suppliers and/or businesses that regularly perform wire transfer payments. The scam is carried out by compromising legitimate business email accounts through social engineering or computer intrusion techniques to contact unauthorized transfers of funds. Most victims report using wire transfers as a common method of transferring funds for business purposes.
    b. Key points:
        - Targets businesses that regularly perform wire transfers
        - Uses social engineering and computer intrusion to conduct unauthorized wire transfers
        - Transfers can begin in U.S. but are usually quickly transferred many times overseas and then disbursed
        - **Unwitting** "money mules" in the U.S. are recruited to receive funds in their personal accounts and then directed to quickly transfer them to accounts overseas (usually 48-72 hours)
        - Mules are sometimes directed to open fictitious business accounts or fake corporations in the true name of the Mule
6. "Our Crime": Wire Fraud
    a. Begins as phishing attempt. **Often web based emails are targeted.** Fraudster will send an email note impersonating a victim's email provider and request that the victim log in, or otherwise enter their email

credentials (logon ID and password). Again, a successful phishing attempt is the key to the email compromise!!! If the phishing attempt has links and those links are clicked on, bad things can follow.

b. Fraudster COULD download malware/virus: If malware is not stopped or contained by anti-virus software it could allow direct unlimited access to data, passwords, bank account information, your camera or microphone on your PC. It could download key logging software to record your keystrokes.
c. Good news is that our crime is a **phishing attempt that will try to redirect you to a fraudster's fake site and have you voluntarily give them your logon password to your email account.**
d. ONCE THAT HAPPENS THE EMAIL COMPROMISE HAS OCCURRED!
    - WATCHING ALL OF YOUR EMAIL COMMUNICATION
    - WHO YOU COMMUNICATE WITH, YOUR ADDRESS BOOK, THE TRANSACTION DETAILS ON YOUR REAL ESTATE DEALS, YOUR CLIENT AND CUSTOMER COMMUNICATONS, YOUR SUPPLIER COMMUNICATIONS
    - YOU ARE THEIR CYBER RAG DOLL!!
    - A Fraudster can insert themselves ANYWHERE in your business (or personal) life to try to steal money that is due to you (clients/customers) or money that you owe to others (suppliers/vendors)
    - Once they own your communications your business is compromised
e. NEXT STEP: WATCH – WAIT – ATTACK
    - **WATCH & WAIT**: After gaining your email access your email will be monitored
        - Sometimes for great lengths of time
        - Your email can remain compromised and no action is taken. Fraudster doesn't see a good enough opportunity
    - **ATTACK**: At the right "time" a fraudulent email will be sent out to person who is in control of disbursing funds with an attachment that includes fraudulent wire instructions
        - Most common attack timing (wait for a good wire instruction to be sent out and soon thereafter follow it with a fraudulent one)

      Three email methods used:
        1) Using actual email account (risky for detection)
        2) Using a spoofed email (close to actual email address)
            - Examples: Real email address is "**jonathan.doe@chicagotitle.com"** but one sees:
                - jonathan.doe@chicag**0**title.com ←the number "0" is suspect
                - jonathan.doe@chicagotit**1**e.com ←the number "1" is suspect
                - jonathan.doe@chicagotitl**e**.com ←the extra "e" is suspect
                - jonathan.doe@chicago**tt**le.com ←the missing "i" is suspect
            - Real email address is "**jane.doe@fsu.edu** but one sees:
                - jane.doe.fsu.edu@gmail.com ←where the ".fsu.edu@gmail.com" is suspect
                - jane.doa@fsu.edu ←where the "a" is suspect
        3) Masking identity with the actual email address in the header text (looks like actual sender, requires header examination to detect)

7. Commercial real estate transaction – Example

Wire Fraud Webinar – June 23rd

OUTLINE

8. Social engineering red flags
    a. UNSOLICITED email from someone you don't know
    b. UNSOLICTED attachments/links from known contacts (could be imposter)
    c. Overly formal language (doesn't match tone), bad grammar, misspelled words, bad syntax
    d. Incorrect facts in an email
    e. Timing/Pressure/sense of urgency
        - Email arriving or requesting your response at odd "business" times – times that a legitimate owner would not access their account
        - Commuting time (gives fraudster time to send, receive, and delete correspondence)
        - At end of week or day, or holiday (allows more time to divert funds)

    f. Look for email asking you to take important action (like wiring to a different account) and requesting you to confirm via email (not phone)Emails from same recipient with significant changes in grammar, sentence structure, and spelling when comparted to previous emails

        - Real examples of fraudulent communications
            - Incorrect grammar, misspellings, phrases that fall outside of our normal business cadence

              "I will forward you the new account details, tomorrow, please confirm to me when you receive it before wire."

              "Kindly confirm to me if wire has not been done yet."

              "The sellers forwarded this new details for the funding to me this morning. I can ask seller to write a letter of direction to me and I will forward it to you. Is that okay?"

              "I will be awaiting for the confirmation".

    g. Email from previous commercial real estate transaction example

9. How to AVOID becoming a victim

a) Train employees to recognize phishing attempts and be alert for communication red flags. Consider outsourcing this ONGOING training if you don't have or desire to have dedicated resources for phishing training. (Ex: Knowbe4)

b) Two factor authentication (at least on email account):

- SMS message
    - Most popular, everyone carries their phone with them (one time passcode)
- Voice
    - Need a phone, can be landline or cell
- Smart Phone Soft Token (via app)
    - Available when no cell service available, "App" generates numbers

- Hardware token
    - USB device on keychain. Plugs into PC (and works with some phones)
    - No codes to enter
    - Requires you Plug in and touch device when authentication is needed

10. CT Chicago NCS wire fraud prevention
    a. Call to verify authenticity of wire instructions received via email
    b. Disbursement of funds only to parties to the transaction
    c. 2 Factor Authentication
    d. Staff awareness
        - Obey red flag protocol (wire "corrections", change in disbursement method check→wire)
        - Training for escrow and accounting employees
        - Sharing of industry examples/information in Corporate newsletters
        - Corporate Internet Security
11. Containment: Steps to consider if you've been compromised
    a. STOP ALL EMAIL COMMUNICATION (assume it is being monitored)
    b. If an outgoing wire transfer (seller's proceeds) call Chicago Title
    c. If an incoming wire transfer (and you are the Buyer's Attorney)
        - Along with Buyer, call the bank that sent the wire transfer to the fraudster and have them RECALL the wire
        - Call the Receiving Bank and notify them of fraudulent activity on their customer's account
        - Follow Bank protocol (all are slightly different)
12. Use Chicago Title as your resource
    a. Leverage banking relationships with large lenders
        - We have partnerships with high level fraud department contacts
        - Internal process to ensure quick action when level of suspicion is high or a known fraud occurs
    b. Leverage our relationships with H.U.D., F.B.I., IC3, D.O.J.
        - We can coordinate efforts between front line, Accounting, Law Enforcement, Bank, IT and other Corporate departments, as well as the parties to the transaction
13. Consider Cyber insurance as a safety net. If you have it already, examine it for social engineering coverage.
14. Q & A
15. Contact Us
16. Before you go!
    a. Complete brief survey. Please note: survey must be completed in order to receive Illinois CLE credit.
17. Thank you!

CHICAGO TITLE INSURANCE COMPANY

NATIONAL COMMERCIAL SERVICES | CHICAGO

WIRE FRAUD WEBINAR
THURSDAY, JUNE 23, 2016

ADDITIONAL RESOURCES

1. Law enforcement source on BEC/EAC crime
   - FBI / Internet Crime Compaint Center (IC3): www.ic3.gov

2. General Cyber-Safety
   - STOP. THINK. CONNECT
     - www.stopthinkconnect.org
     - General tips & advice: www.stopthinkconnect.org/tips-advice/general-tips-and-advice

3. Cybersecurity Breach Plans
   - Best Practices for Victim Response and Reporting of Cyber Incidents by the United States Department of Justice Cybersecurity Unit
   - Data Breach Response Guide by Experian Data Breach Resolution

4. Phishing TRAINING and General Info
   - KnowBe4
     - www.knowbe4.com

5. 2 Factor Authentication Information
   - Two Factor Auth: Click on "Email" services that offer 2-factor and what types offered
     - https://twofactorauth.org
   - How to set up various types of email on "2 factor"
     - https://www.turnon2fa.com/tutorials/
   - Two Steps Ahead Campaign
     - https://www.stopthinkconnect.org/campaigns/two-steps-ahead-campaign
   - Naked Security by Sophos
     - The power of two – All you need to know about two-factor authentication

6. Password Manager/Locker Information
   - Five Best Password Managers
     - http://lifehacker.com/5529133/five-best-password-managers

Social Engineering Red Flags

FROM:

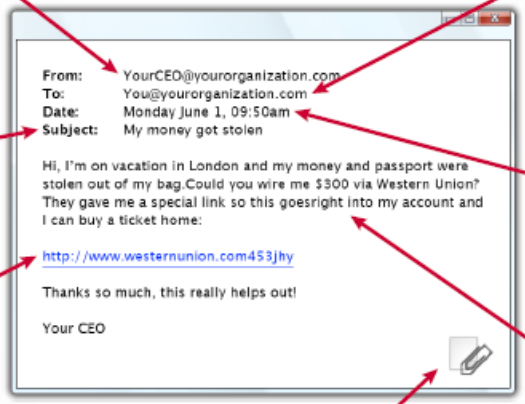
- I don't recognize the sender's email address as someone **I ordinarily communicate with**.
- This email is from **someone outside my organization and it's not related to my job responsibilities**.
- This email was sent from **someone inside the organization** or from a customer, vendor, or partner and is **very unusual or out of character**.
- Is the sender's email address **from a suspicious domain**? (like micorsoft-support.om)
- **I don't know the sender personally** and they **were not vouched for** by someone I trust.
- **I don't have a business relationship** nor any **past communications** with the sender.
- This is an **unexpected or unusual email** with an **embedded hyperlink or an attachment** from someone I hadn't communicated with recently.

TO:

- I was cc'd on an email sent to one or more people, but I **don't personally know** the other people it was sent to.
- I received an email that was also sent to an **unusual mix of people**. For instance a seemingly random group of people at your organization whose last names start with the same letter, or a whole list of unrelated addresses.

SUBJECT:

- Did I get an email with a subject line that is **irrelevant** or **does not match** the content?
- Is the email message a reply to something I **never sent or request**?



DATE:

- Did I receive an email that I normally would get during regular business hours, but it was **sent at an unusual time** like 3 a.m.?

HYPERLINKS:

- I hover my mouse over a hyperlink that's displayed in the email message, but the **link to address is for a different web site**. (This is a **big** red flag.)
- I received an email that only has **long hyperlinks with no further information** and the rest of the email is completely blank.
- I received an email with a **hyperlink that is a misspelling** of a known web site. For instance, www.bankofarnerica.com - the "m" is really two characters – "r & n")

CONTENT:

- Is the sender asking me to click on a link or open an attachment to **avoid a negative consequence**, or to **gain something of value**?
- Is the email **out of the ordinary**, or does it have **bad grammar** or **spelling errors**?
- Is the sender asking me to click a link or open up an attachment that **seems odd** or **illogical**?
- Do I have an **uncomfortable gut feeling** about the sender's request to open an attachment or click a link?
- Is the email asking me to look at a **compromising or embarrassing picture** of myself or someone I know?

ATTACHMENTS:

- The sender included an email attachment that I **was not expecting** or that **makes no sense** in relation to the email message. (This sender doesn't ordinarily send me these types of attachment(s).)
- I see an attachment with a **possibly dangerous file type**. The only file type that is **always safe to click on is a .TXT** file.)

KnowBe4.com
Human error. Conquered.