C.Y.B.E.R
Can You Be Entirely Ready?

Jonathan W. Biggs, J.D.
Vice President, Risk Management & Education – Investors Title

NCPA’s 38th ANNUAL MEETING & SEMINAR
March 22, 2018 – March 24, 2018
Jonathan W. Biggs
Vice President & Director of Risk Management & Education

Jon Biggs oversees risk management functions related to Investors Title’s approved provider system. In this role, he oversees the approval process, develops educational seminars and communications-based initiatives involving approved providers and agents, and manages provider data and analysis related to the company's risk management efforts.

Prior to joining Investors Title in 2012, he was partner at a firm in Durham, North Carolina where he practiced residential and commercial real estate law for more than 20 years. Mr. Biggs holds a bachelor’s degree from Duke University and a Juris Doctor from Wake Forest University School of Law.
C.Y.B.E.R. – Can You Be Entirely Ready?

Investors Title Risk Management

Continuing Legal Education Seminar

Jonathan W. Biggs, J.D.

Vice President - Risk Management & Education
Two Part Test:

1) Do I Have a Computer?
2) Do I Have a Cellular Phone?

If You Answered “YES” to either, then you **NEED** to watch this presentation on Cyber Fraud and Cyber Security!
“I am convinced that there are only two types of companies – those that have been hacked and those that will be... and even they are converging into one category - companies that have been hacked and will be hacked again.”


from Ponemon Institute

70% of organizations report having been compromised by a successful cyberattack in the past 12 months.
Online You can make 3400% of Bank Robbery Haul

“You know, you can do this just as easily online.”

Average Bank Robbery = $3,816
Average Wire Fraud Loss = $129,427
Yahoo!

Equifax Data Breach

What Are The Odds I Was Affected?

- Roughly 323 Million people in the United States.
- 24% of them are under the age of 18, which leaves about 245 million people that potentially have credit histories.
- Odds that you were affected are roughly 3 out of 5.
Dan Mennenoh, ALTA Past-President

Appeared before House Subcommittee on Financial Institutions & Consumer Credit

“This is a problem we can’t fix on our own. What is so frustrating is that there is no amount of money we can spend to protect consumers from being targeted by these criminals.”
1) Introduction
2) Definition of Cyber Fraud
3) Three Categories of Cyber Fraud
4) Cyber Breach & Data Breach
5) C.Y.B.E.R. – Can You Be Entirely Ready?
6) Cyber Crime and Cyber Theft
7) F.A.S.T. – Fast Action Stops Theft
8) Social Engineering
9) W.I.R.E – What I Require Every time
10) Cyber Fraud Insurance
11) Conclusion

What is CYBER - Fraud?
- Same as Fraud Generally
  - A **false representation** of a material of fact
  - is **intended to deceive** another
  - so that the individual **will act in reliance** upon it
  - that, in fact, **deceives** and
  - to her or his **legal injury** (DAMAGE)

- **ADDITIONAL ELEMENT**
- **Uses phone, computer or digital network to perpetrate the fraud**
What is CYBER - Fraud?

*N*Cyber-Fraud* is an all-encompassing term that includes a wide variety of types of fraud. It is often confused and identified with each of the sub-classes of *Cyber-Fraud* and used interchangeably.

### Three Categories of Cyber-Fraud

1. **Cyber Breach**
   - When **DATA** or **INFORMATION** is stolen

2. **Cyber Theft or Cyber Crime**
   - When **MONEY** is stolen

3. **Social Engineering Fraud**
   - When victim is tricked into turning over **MONEY** or **INFORMATION**
Three Categories of Cyber Fraud

1) Cyber-Breach – INFORMATION STOLEN

The cyber-breach fraud can be perpetrated many ways, including the following:

- Gaining credentials (login and password) for access to a computer network that contains NPI;
- Intercepting un-encrypted or improperly encrypted communication containing NPI;
- Improper disposal of NPI;
- Sharing NPI with a source that is believed to be trusted (but is not); and
- Many more.

2) Cyber-Theft or Cyber-Crime – MONEY STOLEN

- Cyber-Theft is what people generally think of when they think of Cyber-Fraud – someone stole MONEY from an account using the internet
- A separate flavor of cyber-fraud
- Even separate type of insurance coverage
  (Crime Insurance or Cyber-Theft Insurance Policy)
- Involves a computer and/or a computer network in order to steal or misappropriate money.
- Log into your online banking and transfer funds to themselves.
- Many banks will not reimburse a business for money lost if the transfer is made with the correct account number, login, and password.
Social Engineering – Tricked Out of **MONEY** or **INFO**

- This fraud is a type of theft that is more dependent upon the traditional elements of fraud and designed to trick an authorized individual into sending money to an incorrect recipient or location.

- Hacked the person and not the computer.
- Generally performed through a computer, phone or other digital network.
- A separate flavor of cyber-fraud.
- Even separate type of insurance coverage (Social Engineering Insurance Policy).
Non-Public Personal Information Definition

Personally identifiable information or data such as information provided by a customer on a form or application, information about a consumer’s transactions, or any other information about a consumer which is otherwise unavailable to the general public. NPI includes first name or first initial and last name coupled with any of the following:

- Social Security Number
- Driver’s License Number
- State-issued ID Number
- Credit Card Number
- Debit Card Number; or
- Other Financial Account Numbers

Not Really

NO!

But Try Anyway!
Guide to Setting Up Your Information Security Plan

Protections to Put in Place To Protect NPI

1. Risk Assessment
2. Access Limited To Authorized Personnel Only
3. Implement Wire Security Policy
4. Implement Physical Security of NPI
5. Implement Digital and Electronic Security aka Network Security
6. Insure Proper Disposal and Decommissioning of NPI
7. Disaster Management Plan
8. Oversight of Service Providers Handling NPI
1. Risk Assessment

Take an honest, deep look at every aspect of your business

- Front door lock
- File storage
- Network security
- Clientele
- Employees

...to evaluate what risk are present that could stop you from doing business tomorrow...
1. Risk Assessment
   a) Initial Examinations:
      • Where and how is NPI stored?
      • Who has vs. who needs access to NPI?
      • How is NPI communicated?
      • Identify where you are vulnerable
   b) Some Specific Questions:
      • Unauthorized access to NPI or sensitive information in the Company records
      • Interception of data during transmission
      • Loss of data in a natural disaster
      • Corruption of data or systems
      • Misplacement or loss of paper records containing NPI
      • Compromise of NPI from disposal of records or equipment
      • Unauthorized or unintended disclosure of electronic or printed NPI
      • Failure to adequately monitor third party service providers and NPI risks

2. Access Limited to Authorized Personnel Only
   • Acknowledge Information Security Policy
   • Criminal Background Checks (Going Back 5 Years)
     • Pre-Hire
     • Every 3 Years Post Hire
   • Only Authorized Employees Access NPI and Accounts
   • Assign User Rights To Employee
   • Terminate Employee Privileges Immediately Upon Separation
3. Implement Wire Security Policy

- Investors has another brochure to help you set up your wire security policy
- More on this later

5. Implement Physical Security of NPI

- Clean Desk Policy
  - Keep paper files closed during the day, when not being used, and secured at night
- Implement written Privacy Policy
- Employee access to NPI
- Physical/Location Security
  - Secure points of entry to building and computers
- Computers should have auto-locking screen savers
- Removable Media

- **Digital Security** - Updated Systems, including OS security updates
- **Backup Data** - Performed Daily & Stored in a Secure Offsite Location.
- **Internet Security** - Antivirus, Anti-Malware, Firewalls Anti-Spyware
- **Password Policy**
  - Strong Passwords
  - At least 8 Characters Long
  - Upper case, Lower case, Number & Special Character
  - Changed At Least Every 3 Months
- **Encrypted Email** – Use it

5. Implement Digital & Electronic Security (Network Security)

The Secret Number is:

<table>
<thead>
<tr>
<th>POST CARD</th>
</tr>
</thead>
<tbody>
<tr>
<td>U Ben Took</td>
</tr>
<tr>
<td>1 Unprotected Lane</td>
</tr>
<tr>
<td>Vulnerableville, NC</td>
</tr>
<tr>
<td>Unsuspecting Suckers Of America</td>
</tr>
</tbody>
</table>

Always Encrypt Email Containing Sensitive Information
6. Insure Proper Disposal & Decommissioning of NPI
   - Shred or Burn Paper & Files Containing NPI
   - Computers and Digital Devices Containing NPI

7. Disaster Management Plan
   - Create an Information Systems Disaster Recovery Plan
   - Protect Against:
     - Interruption To Business
     - Hardware Failures
     - Software Failures
     - Environmental Events
     - Theft
8. Oversight of Service Providers Handling NPI

Types of Third Party Service Providers

- Independent Searchers
- Couriers
- Janitorial Service
- Alarm Company
- HVAC, Plumbing, Electrical
- Off Site Storage
- **IT Professionals**

---

Cyber Breach & Data Breach

**Common Types of Cyber Breach and Data Breach Fraud**

1) Ransomware
2) Identity Theft
3) Network Intrusion
4) Advanced Persistent Threat/Key Loggers
1) **Ransomware**

Prevents or limits users from accessing their system.

**There are two primary types:**

1) **Encrypting Ransomware**
   - Incorporates advanced encryption algorithms.
   - Designed to block system files and demand payment to provide the victim with the key that can decrypt the blocked content.

2) **Locker Ransomware**
   - Locks the victim out of the operating system, making it impossible to access the desktop and any apps or files.
   - The files are not encrypted in this case, but the attackers still ask for a ransom to unlock the infected computer.
Cyber Breach & Data Breach

GLOBAL MENTIONS OF RANSOMWARE

- Up 500% in 3 Years
- Up 100% in Last 6 Months of 2015
Who Pays Ransom & How Much?

- OVER 70% of infected businesses **PAY THE RANSOM**
- OVER 50% of infected businesses paid between $10K - $40K
- Ransom for home users generally between $200 - $10,000

Who Recovered Their Data?

- ONLY 42% of Ransomware victims recover their data
- ONLY 25% of PAYING victims recover their data

How is Ransomware Deployed?

- 97% of Ransomware is delivered by Phishing Emails

2) Identity Theft

- Gain Access To Data Source, Computer or Network
- Usually Login is your Email Address
- Only Need your Password
- Steal More Than Account Numbers
- Steal Ability To Open Accounts
- Steal Ability To Verify Information at Banks, etc.
- Steal Ability To Verify Information at Retirement Accounts
- Steal Ability To Perpetrate a Crime in Your Name
CYBER-FRAUD GOLD MINE

1.6 +/- Billion Social Network Users Worldwide
64% of Internet Users Access Social Media Online
EVERY DAY more than 600,000 Facebook accounts are compromised

Cyber Breach & Data Breach

Universal Loan Application
Fannie Mae 1003
Freddie Mac 65

1. Deal Specific Information
2. Borrower Information
3. Employment Information
4. Income Information
5. Assets & Liabilities Info
6. Net Worth Information
7. (Total) Real Estate Info
8. Transaction Details
9. Borrower Declarations
10. Borrower Affirmation & Sigs
11. Additional Liabilities
3) Network Intrusion

Microsoft Security Essentials

Attention

Microsoft Security Essentials detected 1 potential threat and suspended it.

Click 'Clean computer' to remove this threat.

Show details | Clean computer

4) Advanced Persistent Threat/Key Loggers
Why Is It Soooooooo Effective?

- Most home users do not have even baseline cyber security
- Most users do not have cyber security education or ignore it
- Most users have sensitive / irreplaceable data on their PC
- Most users do not back up regularly or at all
- Most users do not update their software when available
- Most users rely on PURE LUCK to be safe online
- Most users feel useless without their computer
- Many offices have a “Bring Your Own Device Policy” and the home user’s problems become the company’s problems
- The human factor is a huge weakness for any computer
- The internet is a “target rich environment” for victims
- Most users would rather pay than admit to being duped.
Cyber Breach & Data Breach

Sad Prince of Nigeria

No One Takes His Emails Seriously

Cyber Crime and Cyber Theft
F.A.S.T. — Can You Be Entirely Ready? — Jonathan W. Biggs, Vice President Risk Management and Education

- You Must Act F.A.S.T.
- You Need:
  - A Cyber-Fraud Response Team
  - A Cyber-Fraud Response Plan
- Keep Calm & Follow the Plan Fast Action Stops Theft

Many Attorney’s Existing Cyber-Fraud Response Plan

1. Discover Breach or Loss
2. Panic, Curse & Throw Things
3. Cry
4. Call The Bank
5. Cry Again
6. Deny
7. Write a Big Check
8. Curse Again
9. Lose Sleep
10. Go To Dental School

They Need A New Plan! Fast Action Stops Theft!
Steps in Cyber Fraud Response Plan

1. Alert the Cyber Fraud Response Team
2. Alert All Internal Employees
3. Take Computers OFF-Line (Do Not Turn Them Off)
4. ALERT BANK – “Letter of Instruction”
5. File a Report with FBI Internet Crime Complaint Center (IC3.gov)
6. Secure Your Office and Network
7. Document Specifics of the Breach or Loss
8. Contact Cyber Fraud Insurance Carrier
9. Contact Your Errors & Omissions Carrier
10. Contact Law Enforcement (Local & State)
11. Contact State Bar
12. Contact Title Insurance Underwriters
13. Follow Laws Regarding Notification
14. Review and Update Your Cyber Fraud Response Plan

(Include Central Fraud Departments and Your Local Branch)
Funds Lost Are Tough To Recover

- **68%** of Funds Lost as a Result of a Cyber Attack Are Declared **Unrecoverable**

- Must Act Quickly to Contact Bank and Authorities

  **LETTER OF INSTRUCTION**
  
  **FROM WIRING BANK TO RECIPIENT BANK**

- If within 24 Hours, then up to **70%** chance to recover
- If within 48 Hours, then only **25%** chance to recover
- If Over 48 Hours, then money is usually overseas
Social Engineering Defined

1) Social engineering is the art of manipulating people so they give up confidential information. (passwords or bank info)

2) The Fraudster “hacks an individual” and not necessarily the computer. **P-I-C-N-I-C.**

3) Usually begins with the digital compromise of the computer or email of a person involved in the transaction.

4) Fraudsters use social engineering it is usually easier to exploit your natural trusting nature than hack your system.
FBI Numbers

- FBI reported that there was a **2,370% increase in wire fraud loses** nationally. [https://www.ic3.gov/media/2017/170504.aspx#ref3](https://www.ic3.gov/media/2017/170504.aspx#ref3)


Social Engineering

**Social Engineering and Business Email Compromise both Lead to Wire Fraud**

1) Once a victim is compromised, the Fraudster exploits the position of confidence gained to convince the victim to send the fraudster money or more information.

2) Frustrating fraud because the fraudster did not take the money or info.

3) Fraudster convinces victim to willingly turn over the money or info.
Social Engineering

Red Flags of Social Engineering Fraud & BEC

Red Flags

- “Red Flags” are not absolute rules
- An indication that there may be something out of order
- There may be reasons for the “Red Flag”
- Upon proper investigation, may be very legitimate.
- Should look out for the following and investigate each instance of a “Red Flag” when they are discovered.

Below is not an “all inclusive” list, but rather some of the more prevalent “Red Flags.”
Red Flags

- Wires to be sent outside of the United States
- Changes in Wiring Instructions
  - Very few individuals or corporations change their bank accounts in the middle of a transaction. **Be very suspicious of change wiring instructions.**
- Similar But Slightly Different Email Addresses
  - Many cyber criminals will attempt to defraud you by communicating with a very similar (but slightly different email address)
- Wire to a different geographic location than Recipient
- Wire to account which is not in the name of the Recipient

- Individual Wire Sent to Corporate Account
- Corporate Wire Sent to Individual Account
- Broken English
  - Many cyber criminals are outside of the United States and English may not be their first language
  - Not an absolute, but worth checking out
- Unnecessary Speed Requirements or Demands
  - Everyone understands the desire to receive their money from a third party, but extraordinary pressure for the speed of the wire is generally a sign that they do not want you to investigate this “Red Flag.”
Social Engineering

Be on the Look Out for Phishing Emails

Pretending To Be From:
- Banks
- IRS
- Credit Card Companies
- Ebay.com
- Amazon.com
- Paypal.com
- Mortgage Companies
- Social Media (Such as Facebook)

War Stories

*Hover Over Links To See True Identity*

- IGotYou@FailToHover.com
- http://YouWishItWasWells.com
- http://GiveMeYourPassword.com
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> john.podesta@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.

From: synp.zep@gmail.com
To: john.podesta@gmail.com
Date: 2015-02-19 06:35
Subject: 2 things

Though CAP is still having issues with my email and computer, yours is good to go.

jpodesta
p@ssw0rd

I warn you, the Windows 8 system is VERY different from what we had back at the WH. Might require a tutorial. It's an operating system that is best with touch screens, which we obviously don't have. If you need tech's help, they're at x5683. Otherwise, I can show you some tricks when I get in. I have it on my home computer, and it took a while to get used to completely.
Social Engineering

Spoof Email Video

Create your Google Account

One account is all you need
One free account gets you into everything Google.

Take it all with you
Switch between devices, and pick up wherever you left off.
What I Require Every Time

W. I. R. E. When you Wire

1. Proper Identification
2. Verbal Confirmation
3. Delivery Verification

What Require Every Time
**Lawyers Mutual – “Financial Fraud Exclusionary Endorsement”**

- November 2017
- Excludes coverage for wire or financial fraud unless you fall into one of two safe harbors

**Outgoing Wires**

You must disburse trust funds in accordance with a

1) Written
2) Original
3) Notarized disbursement instruction
4) Authorizing the wiring/electronic transmission of funds
5) Received prior to disbursement
When All Else Fails;  
Have a Plan B – Cyber-Fraud Insurance
Cyber Fraud Insurance

Truth #2 – You Are A Target
- Wrong Direction
- Only Road
- People Trying To Hit You
- Not Nimble Enough To Avoid Getting Hit
- No One Is!

With Social Engineering Online You can make 3400% of Bank Robbery Haul

Social Engineering
Average Fraud Loss =$129,427
I TOLD YOU SO . . . Comes 2 Ways

1) When You Look In The Mirror After A Loss
2) When Your Insurance Agent Tells You, When He Gives You a Check

Either Way, I Told You So Is Coming.

Simple Steps To Avoid Being a Victim

REMEMBER:
- Slow Down – Follow Company Procedures
- Do what in necessary or required, not just what is wanted

ALWAYS:
- Be on Your Guard – Be Suspicious
- Look for Red Flags
- Use Encrypted Email for **ALL** Sensitive Information
  - Remember that email thread is contained in forward or reply
- Type Your Own Email Addresses (or use your contact list)
- Roll Over / Hover Over Links to See Their Actual Destination
- Follow Company Policies
- Use Complex Password and Keep Them Confidential
Simple Steps To Avoid Being a Victim

NEVER:

• Assume Email is Safe (even if encrypted)
• Trust Emails From Free E-Mail Accounts (gmail, yahoo, hotmail etc.)
• Click on Links in Email
• Click on Attachments in Email (unless you have verified sender)
• Send Sensitive Information in Email
• Wire Funds Without Call Back Procedure
• Bypass Company Policies
**Conclusion**

http://InvTitle.com/wire

**SELLER/BUYER BEWARE**

Protect Yourself from Fraud

Since 2014 the real estate industry has experienced a drastic increase in escrow fraud theft. Criminals are getting smarter and more sophisticated.

**Actual Trust Account Fraud Cases**

Often the fraudster uses email addresses and domains identical to those of the actual attorney and will even use their company logo.

- Fraudster intercepts buyer’s and/or seller’s email to their realtor or attorney.
  - Fraudster pretends to be the buyer or seller and inserts their wiring instructions to the attorney. Funds are wired to the fraudster’s account.
- Fraudster impersonates attorney or realtor (they even use the names of the actual employees) and emails the buyer instructing them to wire the funds needed for closing to a fraudulent account.
- Fraudster impersonates seller and tells attorney they want their sale proceeds to be wired to a fraudulent account.

http://InvTitle.com/fraud
Conclusion

Credits

Chubb – Social Engineering Fraud
https://youtu.be/nknq9sUu8ko

Cisco – Anatomy of an Attack
https://www.youtube.com/watch?v=4gR562GW7TI

WRAL - Mortgage Closing Scam

Jimmy Kimmel - What is Your Password?
https://youtu.be/opRMrEfAil