Cyber-Fraud and Real Estate

.....

Recent Trends and Tips

.....

Mike Koutnik
Matt O'Neill

Apartment Association of Southeastern Wisconsin
March 19, 2018

FOX | O'NEILL | SHANNON s.c.

Roadmap

- What is the Nature of the Risk
- Tips for Protecting Yourself from Becoming a Victim
- Steps to Take in the Event You Are Affected

Risks - Overview

- Nature of Threat and Targets
- Increased Activity in Real Estate
- Examples

Risks – Targets

Big Names

- Equifax (2017) – 145,000,000 People Affected
- Uber (2016) – 57,000,000 Customers' Personal Information Compromised
- Target (2013) – 41,000,000 Customers' Payment Card Accounts
- Yahoo! (2013) – 3 Billion Accounts Compromised

Risks – Targets

- Big Names Grab Headlines, But Smaller Players are also Targeted

- 43% of Attacks in 2015 Targeted Companies with 250 or Fewer Employees
  - Typically Less Protected

Risks – Increased Activity in Real Estate

- Annual Global Cost of Cybercrime Estimated to Total $2.1 Trillion by 2019
- Wire Fraud is Fastest Growing Form of Cyber-Crime in Real Estate
- Weaknesses Inherent to Real Estate
  - Smaller Companies or Individuals Often Involved
  - Speed of Transactions
  - Number of Parties
  - Large Sums of Money

Risks – Example: Wire Fraud

Hacker Breaks into an Email Account of Involved Party

Hacker Observes Correspondence and Collects Information

Scam Email Sent Prior to Closing With Wiring Instructions

Money is Wired to Hacker's Account and Often Transferred Again Out of the Country

Risks – Example: Wire Fraud

Broker Representing Seller Emails Closer With Wire Instructions

- Email Was From Broker's Account
- Broker Was In Fact Representing Seller
- Email Referred to Previous Communication

Title Company Wired $126,000 to Fraudulent Instructions

Risks – Example: Wire Fraud

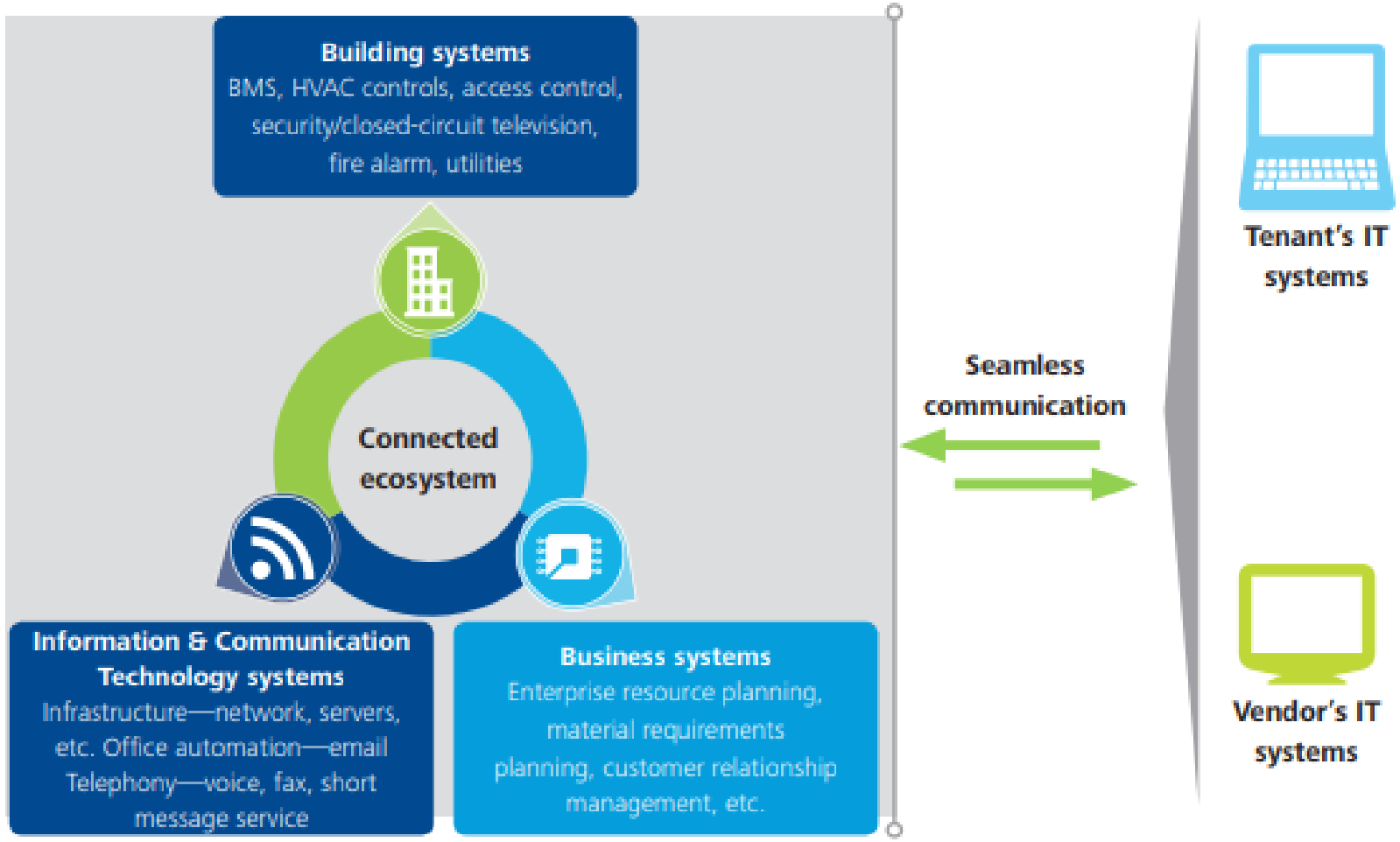
Denver Couple Loses $272,535.96

- March 30, 2017 – Email Purportedly From Broker Informs Couple That Shannon From Title Company Would be Sending Wiring Instructions
- April 3, 2017 – Couple Receives Email From Someone Identified as “Shannon Ryon” at the Title Company Requesting the $272,535.96 Wire
- April 3, 2017 – Seller Receives Email from “Ashley Johnson” at Mortgage Company With a Final Closing Disclosure Showing $272,535,96
- Emails Were Fraudulent, Sellers Sent Money

Risks – Increased Activity in Real Estate

Changing Interaction Between Property, Property Owner, and Tenant

Figure 1: Illustrative IT ecosystem of a CRE company[3]



Source: The Institution of Engineering and Technology, UK, and Deloitte Center for Financial Services analysis

Risks – Example: Target

1. Install Malware that Steals Credentials
2. Use Credentials to Access Target Hosted Web Services
3. Access Target Through a Vulnerability in Target's Web Services
4. Modify Credentials of Administrators of Target's Systems
5. Steal Personally Identifiable Information ("PII") from Servers
6. PII Unsuccessful, Install Malware on PoS to Mine Credit Card Info
7. Save Credit Card Info to Local File, Extract File, Sell

Risks – Other Examples

- Overpayment Scams
- Links by Text Message
- Referral Emails

Prevention – Overview

- Security of Email Accounts
- Update Software
- Utilize Antivirus and Firewall Protections; Regularly Back-Up Data
- Find an IT Vendor/Contractor You Trust
- Review Insurance Policy
- Keep Current on the Types of Scams
- Talk

Prevention – Pick up the Phone

- Easiest Way to Reduce Risk is to Verbally Confirm Wiring Instructions
- Use a Verified Phone Number to Confirm Instructions
- Build Relationships with Other Parties

Prevention – Email Security

Hacker Needs a Way In

- Often a Link or Attachment from a Legitimate Looking Email
- The Link or Attachment may:
    1. Install Password Cracking Malware
    2. Direct You to a Page that Mirrors the Log-In Page for a Transaction-Related Website or Email
- Guessing Email Passwords
    - Common Passwords
    - Using Social Media

From: Bryan Johnsen [mailto:B.Johnsen@tcnb.com]
Sent: Monday, September 25, 2017 1:06 PM
Subject: Bryan Johnsen sent you a File

Hello,

Please see attached

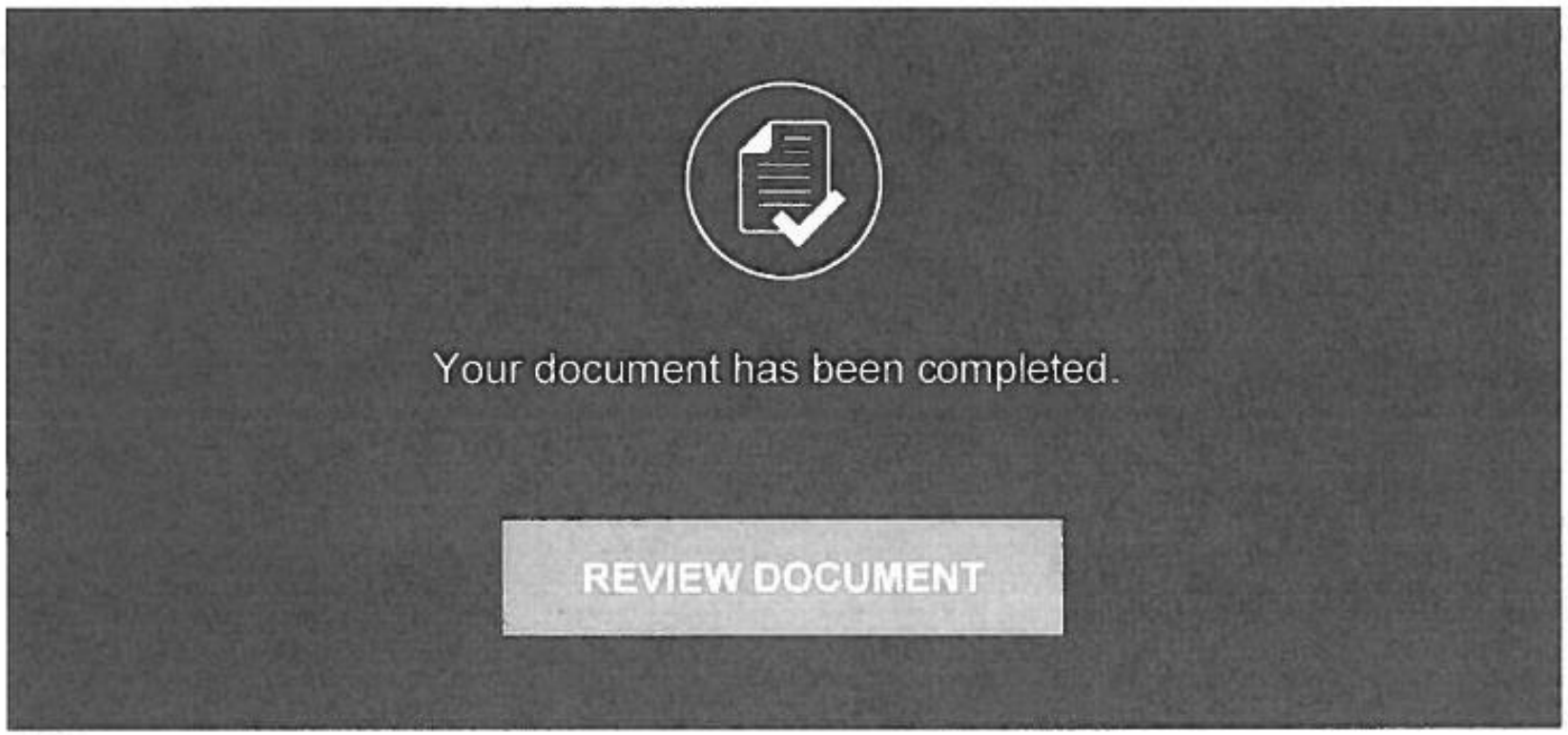
Bryan Johnsen
Vice President - Commercial Lending
P: 414-305-1157 | **F:** 414-403-2291
E: w855176@tcnb.com
A: 6400 S. 27th St., Oak Creek, Wisconsin 53154

Bryan Johnsen
Vice President - Commercial Lending, Tri City National Bank
P: 414-525-7664 | **F:** 414-425-1328 | **M:** 608-574-4080
E: B.Johnsen@tcnb.com
A: 5555 S. 108th St., Hales Corners, WI 53130

Our mission is to be the Community Bank that defines our success by yours.

From: DocuSign via DocuSign [mailto:dse@computershare.com]
Sent: Tuesday, November 22, 2016 10:00 AM
To: Michael G. Koutnik
Subject: (mgkoutnik@foslaw.com)DocuSign Amend

DocuSign



All signers completed Please DocuSign this document: Amend.pdf

From: Laurna Kinnel [mailto:presidentnewe@gmail.com]
Sent: Wednesday, November 08, 2017 9:52 AM
To: [redacted]
Subject: URGENT

Hello,

Kindly confirm to me the available account balances, as I would need you to initiate a bank transfer for a payment, let me know so I can forward you the details. I'm in a meeting currently and won't be able to pick calls.

Waiting for your reply.

Thanks

Laurna Kinnel

Sent from my iPhone

Prevention – Email Security

- Review Sent Folder and Other Folders for Anomalies
- Use Strong Passwords
  - Current Advice is Long Phrases
- Use a Variety of Passwords
- Use Two-Factor Authentication
- Use Encrypted Email When Possible
- Document Sharing Platform
  - (ShareFile, Zip Logix, etc.)

Thu 1/18/2018 1:44 PM

B [redacted]Brandon <b[redacted]@firstam.com>

RE: FW: FA-Secure Wiring instructions

To [redacted]; [redacted]

Cc [redacted]; [redacted]; Michael G. Koutnik; [redacted]

SecureMessageAtt.html
1 MB

First American

In order to serve you better now and in the future, First American has a Secure E-Mail system. As a result, all users will be prompted to register a user name and password the first time they access this system.

You have received an encrypted Secure E-Mail from the First American Financial Corporation or one of its subsidiaries that may contain private and/or sensitive data. If you have questions or concerns about this secure E-Mail Notification, please contact your First American representative.

Click here to read your secure message, which expires 2018-01-28 11:44 PST. Please save or export this message and any attachments to a separate system before the expiration to avoid losing this information.

More Info

First American

Login

Log in to read your secure message.

mgkoutnik@foslaw.com

Password

Forgot Password

Continue

Wed 1/24/2018 10:58 AM

[redacted]@ctt.com>

RE: Return of Earnest Money [redacted]

To Michael G. Koutnik

Cc [redacted]

Thank you so much, we will get that wire out today.

[redacted]

CHICAGO TITLE

20825 SWENSON DR SUITE 200 WAUKESHA, WI 53186

[redacted]

www.wisconsin.ctic.com | www.chicagoagent.com | www.etitle.ws

CHICAGO TITLE

Chicago Title Company is a subsidiary of Fidelity National Financial, Inc. (NYSE: FNF), a Fortune 500 company

Your experience with Chicago Title is extremely important to us! Share feedback with my manager by clicking here.

From: Michael G. Koutnik [mailto:MGKoutnik@foslaw.com]
Sent: Wednesday, January 24, 2018 10:36 AM
To: [redacted]
Cc: [redacted]
Subject: Return of Earnest Money [redacted]

IMPORTANT NOTICE - This message sourced from an external mail server outside of the Company.

[redacted]

Mike

Prevention – Email Security

Remember – Best Security, Password, or Technology is Worthless if the User is Careless With Login Information or Clicks on an Infected Link.

Prevention – Software Updates

- Increased Security
  - WannaCry Ransomware
- Auto-Updates May be Disabled
- New Features

FOX | O'NEILL | SHANNON s.c.

Prevention – IT Vendors/Contractors

Best Practices When Selecting:

- Review Vendor's Reputation

- Discuss Specific Questions or Concerns and Ensure you Receive Satisfactory Answers

- Review the Contract; May Be Online/Click-Through
  - Vendor Liability

Prevention – Review Insurance Policy

Contact your Insurer to Discuss:

1. Various Scenarios of Cyber-Fraud and Whether Any Coverage is Provided by Your Current Policy
2. Discuss Whether Insurance for Cyber-Fraud is Available/Makes Sense
3. These Products Are New, So Make Sure That You Understand the Policy and the Coverage Provided
4. Periodically Review the Policy – Risks Are Rapidly Changing

Prevention – Why Do It

- Reputation
  - U.S. National Cyber Security Alliance Found that 60% of Small Companies Close Within 6 Months of a Successful Cyber Attack

- Related Costs Mount Rapidly:
  - Ponemon Institute - Average All-In Cost Related to a Successful Attack of a Small to Mid Sized Company at $690,000.

Steps To Take If Affected & Remedies

Contact Bank and Title Company Immediately

Contact Local Police

Contact FBI

- Milwaukee Field Office - 414-276-4684 (covers Dodge, Milwaukee, Ozaukee, Washington, Waukesha, Kenosha, Racine and Walworth)
- Financial Fraud Kill Chain (72 hour window)

Contact Insurer, if applicable

Work with IT Vendor/Contractor to Change All Passwords, Run Anti-Virus, and Otherwise Ensure Systems are Clear

Required Disclosure of Data Breach Involving Personal Information

Treatment of Personal Information (Wis. Stat. 134.98)

- "Personal information" means an individual's last name and the individual's first name or first initial, in combination with and linked to any of the following elements, if the element is not publicly available information and is not encrypted, redacted, or altered in a manner that renders the element unreadable: 1. The individual's social security number. 2. The individual's driver's license number or state identification number. 3. The number of the individual's financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual's financial account. ~~4. The individual's deoxyribonucleic acid profile, as defined in s. 939.74 (2d) (a). 5. The individual's unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.~~

Personal Information; Data Breaches; Disclosure

Notice Must:

- Inform Affected Individuals
- Be Given Within a Reasonable Amount of Time, Not to Exceed 45 Days After Learning of Breach

Contact Us

Mike Koutnik

mgkoutnik@foslaw.com

FOX | O'NEILL | SHANNON s.c.

Matt O'Neill

mwoneill@foslaw.com

622 N. Water Street, Suite 500

Milwaukee, WI 53202

414-273-3939