Cybersecurity

Policies, Processes, Procedures, & Insurance Coverage

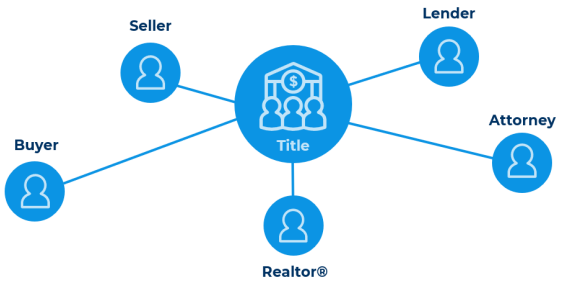
Presented by:

Adam E. Gwaltney, President & COO of EnO Professional Insurance Solutions
Cindy Immonen, NTP, CLTP, VP, Account Manager of FNF MI Agency

Brief Introduction

Our Real Estate Ecosystem is not *SAFE*

1 in 3 real estate transactions are targeted!



Protecting the Ecosystem

Extend training throughout ecosystem

- Consumers
- Realtors®
- Lenders

Benefits include prevention of YOUR brand exploitation

Have Policies, Processes, Procedures, & Insurance Coverage

03/09/2022

War in Ukraine Increases *Cyber Risk*: Social Engineering Red Flags

Cyberattacks on businesses and government agencies have increased following the Russian invasion of Ukraine, with the risk of spillover cyberattacks against non-primary targets becoming much more widespread.

The U.S. Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security (DHS), urged corporate leaders to prepare for attacks and adapt their C-suites accordingly.

"We assess that Russia would consider initiating a cyberattack against the Homeland if it perceived a U.S. or NATO response to a possible Russian invasion of Ukraine threatened its long-term national security," according to a bulletin from the DHS Intelligence and Analysis bulletin.

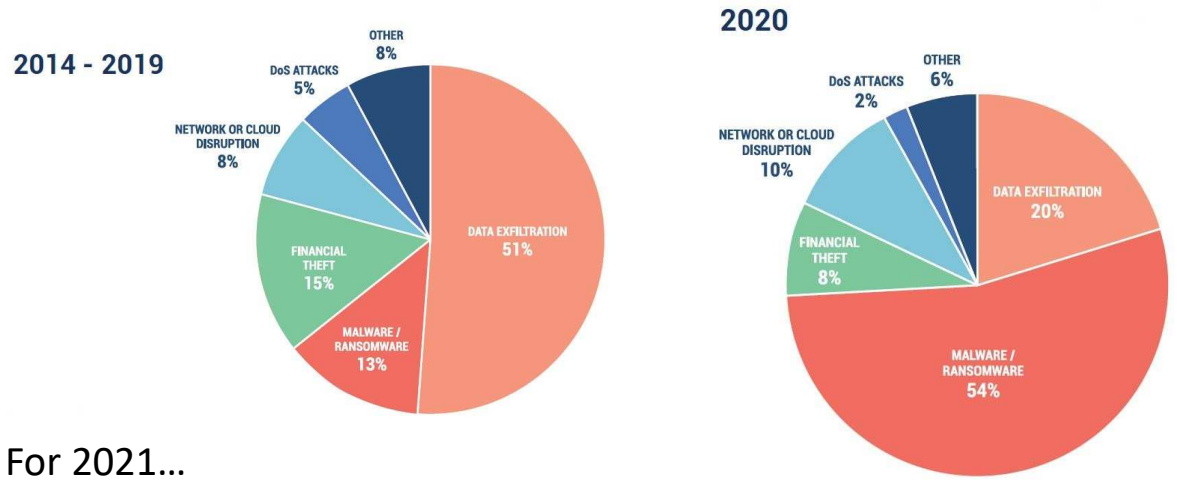
Some immediate actions that can be taken to strengthen cyber posture include:

- •Enable multifactor authentication
- •Set antivirus and antimalware programs to conduct regular scans
- •Enable strong spam filters to prevent phishing emails from reaching end users
- •Update software
- •Filter network traffic

Experts also expect an increase in sophisticated social engineering schemes centered around the war. Avanan, an email cybersecurity firm, reported an 800% increase in phishing attacks since February 27.

“We are seeing cybercriminals use Russia and Ukraine-centric social engineering efforts, like phishing emails, leveraging current events to solicit an emotional response to the war,” says Ros Smothers, former CIA cyber threat analyst and technical intelligence officer, now at KnowBe4. “In other words, people are less likely to think before they click.”

Cyber insurance claims by cause



For 2021…

Corporate Cyber Attacks Up 50% in 2021 - WHY…

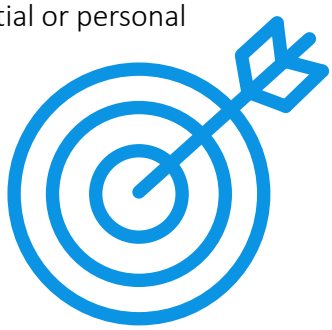
Cybercriminals can penetrate **93** percent of company networks!

Cyber-attacks are varied and involve several possibilities, including:

- Ransomware – attackers seize control of your systems and files until you pay a ransom to get control back.
- DDoS attack (Distributed Denial-of-Service)- your systems are put to a halt by overloading them.
- Data theft – attackers access your customer data and sell it online.
- Man-in-the-middle attack – a hacker alters communications between two-parties without being detected.
- Phishing – an attacker will pose as someone trustworthy in order to gain sensitive information such as usernames or bank details.
- Password attack – your password has been compromised and an attacker can gain access to your accounts.
- Viruses, worms and bots – these are little snippets of code that get embedded into your systems and used for malicious purposes, such as corrupting your system, stealing data, or spreading malware.
- By Using Phone Apps - Even the latest Smart phones are not fully secure. Application programming interfaces (API) and applications can be used to fool customers.
- Wi-Fi Hotspots – This method is commonly called 'Evil Twin'; an attacker fools a wireless user into connecting their mobile device to a tainted hotspot disguised as a legitimate provider. In actual fact the hotspot was setup for the hacker to eavesdrop on the unsuspecting victims' personal details.

so·cial en·gi·neer·ing / ˈsōSHəl ˌenjəˈni(ə)riNG/ *noun*

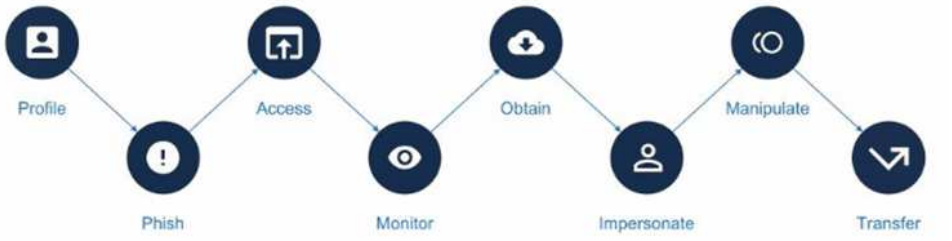
The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes



Don't be a target!

- Be careful what you share and who you share it with!
- Restrict social media posts to real-life friends.
- Avoid using social media to sign into third party platforms and/or applications.
- Consider what privacy you are trading when allowing apps to track your use across other apps.
- Your 'friend' sends you a strange message via any method. You're receiving help you didn't ask for.
- The sender can't prove their identity.
- Your emotions are heightened. The request is urgent. The offer feels too good to be true.

SOCIAL ENGINEERING PLAYBOOK



phish·ing /ˈfiSHiNG/ *noun*

The fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

- Takes a "Blockbuster" approach

  (Phishing often takes the form of a spam email paired with malicious offerings.)

- Phishing emails rarely trigger security policy alerts. *Why?*
  - Look and feel legitimate
  - May not include malicious links or malware attachments
  - Do not arrive in high enough volume to raise red flags

PHISHING WORKS BECAUSE…

In a Rush

Multitasking

Customer Oriented

How Big is the problem?

- Real estate fraud continues to be one of the most prevalent cybercrimes in the U.S *(NARS)*
- **19,369** Business Email Compromise (BEC)/Email Account Compromise (EAC) complaints with adjusted losses exceeding 1.8 billion dollars *(2020 iC3 Report)*
- **13,638** individuals fell victim of wire fraud in the real estate and rental sector in 2020 *(2020 iC3 Report)*
  - Losses totaled over **$213M**
  - **17%** increase from 2019

$4,200,000,000 *(internet crime losses)* / **$300,000** *(avg. sales price)* = **14,000** *Stolen homes*

Cybersecurity is everyone's ***responsibility***

ALL Employees can –
Create a breach
Prevent a breach
Detect a breach

ALL Employees possess credentials and overall knowledge that is critical to the success of a breach.
All it takes is **ONE** employee - to take the bait.

Add additional funds
for hiring security talent
and/or training **ALL** employees.

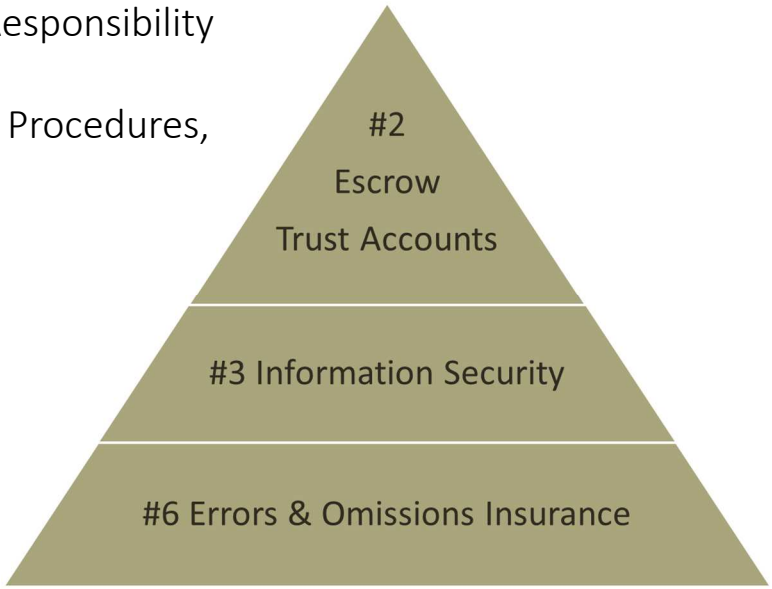
- In most cases employees are not cautious enough to question whether they should open an attachment or click on a link to a site without verifying that the attachment is legitimate, and the website is valid.
- Employees likely have a false sense of security that their anti-virus would catch any attachment if it is bad.
- Another issue is - the bad guys are getting very good at emails! They are doing their research on companies, news articles and other information to determine who works at a company, what their email address is, what their position is and with whom they might be communicating with. The result is a well-crafted email catered to the recipient.

Educating **everyone** at your office and **everyone** in a transaction
– Real Estate Agents –Loan Offers – Sellers – Buyers –
This is the most effective way to combat attacks.

91% of all data breaches are caused by human error

ALTA Best Practices
Dealing with Financial Responsibility

Have Policies, Processes, Procedures,
& Insurance Coverage

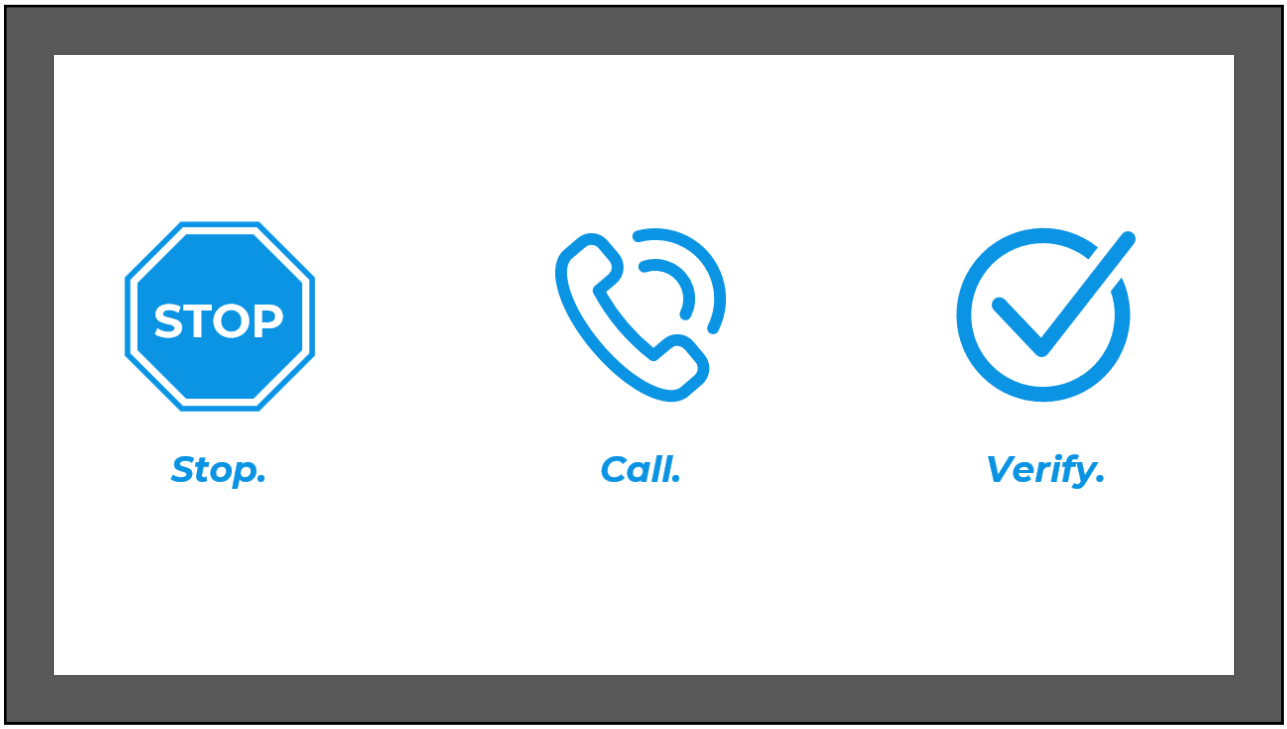


Pillar 2: Adopt and maintain appropriate written procedures and controls for Escrow Trust Accounts allowing for electronic verification of reconciliation

The ALTA Best Practices Framework: Assessment Procedures…
There are ***39*** Assessment Questions that should have

Policies, Processes, Procedures

Network Security
Physical Security
Privacy
Disposal
Disaster
Employee Requirements
Third Party Requirements



NEVER RELY

On emails or other communications purporting to change wire instructions.

Parties to a transaction rarely change wire instructions in the course of a transaction.

Have a three-step process in place for wire transfers. This can include verbal communication using a telephone number known by both parties.
Know your customer. Be aware of your client's typical wire transfer activity and question any variations.

ALWAYS VERIFY WIRE INSTRUCTIONS
Specifically, the ABA routing number and account number, by calling the trusted source who is receiving the funds. **DO NOT RELY** on other parties calling you. **DO NOT** use the phone number provided in the email containing the revised instructions, use phone numbers you have called before or can otherwise verify. **DO NOT** send an email to verify as the email address may be incorrect, or the email may be intercepted by the ***fraudster***.

#3 – Adopt and maintain a written privacy and information security program to protect Non-public Personal Information (NPI or PII) as required by local, state and federal law.

** NOWHERE in Best Practice #3 does it stated that insurance should part of your "program." However, is it implied?

The ALTA Best Practices Framework: Assessment Procedures…
There are ***24*** Assessment Questions that should have

Policies, Processes, Procedures

Network Security
Physical Security
Privacy
Disposal
Disaster
Employee Requirements
Third Party Requirements

Nonpublic Personal Information

Do **not** provide personal information online:

- Social Security Number / Tax ID Number
- Date of Birth
- Credit Card or Account Numbers
- Login Credentials

Safeguard transaction information as if it were your own!

How does a breach occur?
Preventing this from happening

- Unpatched software
- Weak/guessable passwords
- Exposed vulnerabilities
- Phishing

LEADING THREATS

Social Engineering

Phishing/Spear-Phishing

Diversion Theft

Ransomware

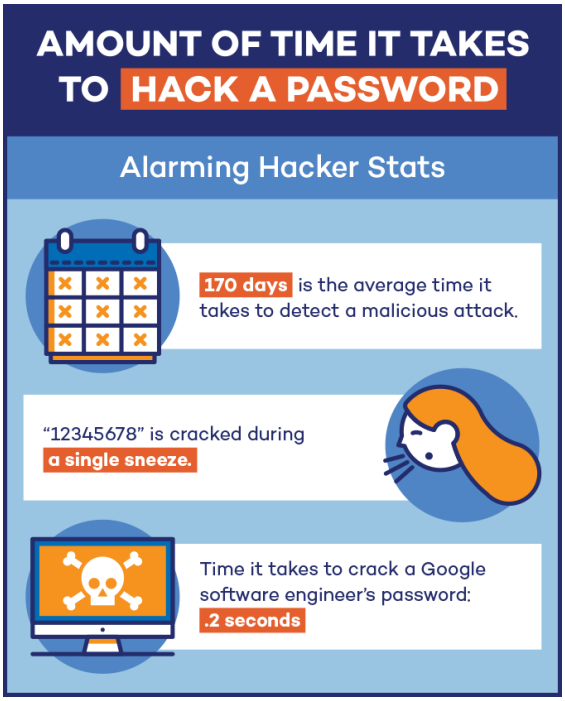
Password Policies, Processes, Procedures

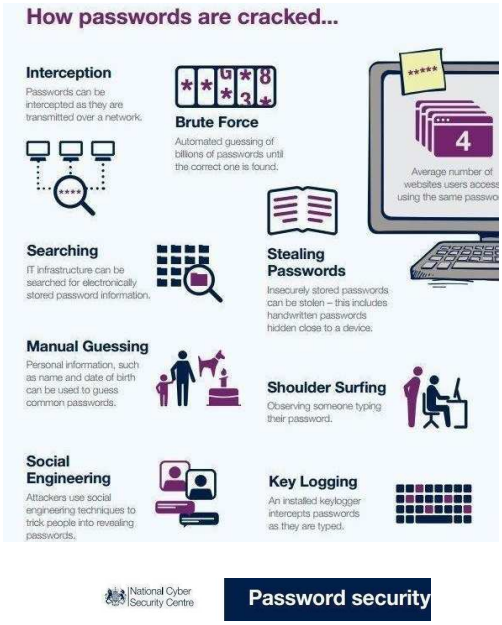
01 Create unique passwords

02 Different passwords for each account

03 Update frequently

04 2 Factor Authentication
Multi Factor Authentication





Some Tips for *Prevention*:

Use Multiple Authentication Methods

"**Two Factor Authentication**" can help; you add an extra layer of security to your account by requiring two key elements:

1. Something you know - your password or pin
2. Something you physically have – a smart phone - most commonly a code sent to your phone
3. Something you are - fingerprints

Articles:

Two-factor authentication: What you need to know (FAQ)
https://www.cnet.com/news/two-factor-authentication-what-you-need-to-know-faq/

Free email services have Multiple Authentication Methods -

- Gmail (https://myaccount.google.com/security/signinoptions/two-step-verification/enroll-welcome)
- Yahoo (https://help.yahoo.com/kb/SLN5013.html)
- MSN (https://support.microsoft.com/en-us/help/12408/microsoft-account-about-two-step-verification)
- Apple (https://support.apple.com/en-us/HT204915)

Mobile & WiFi Considerations

*Mobile devices represent one of the **fastest growing** "attack surfaces" for cybercriminals.*

Exploits take advantage of:

- *Bluetooth*
- *Wi-Fi*
- *Cellular Connections*

DO'S AND DON'TS

- ✓ *Disable auto-join unfamiliar networks*
- ✗ *Avoid use of public WiFi*
- ✗ *Check personal email on work devices.*
- ✓ *Never leave your devices unattended.*

#6 – Maintain appropriate professional liability insurance and fidelity coverage.

- Professional liability (E & O) to protect your professional errors
- Fidelity (coverage for theft) – can also be referred to as Crime
- So why doesn't ALTA specifically address Cyber Insurance as they do E & O and Fidelity…?

Part of the ALTA Best Practices Framework: Assessment Procedures…
There are ***4*** Assessment Questions that should have

Policies, Processes, Procedures

Partial Coverage for the Risks…

- **Business Owners** – can only endorse the insurance policy.
  Limited coverage
  Will only cover nominal loss, not designed for a true breach or theft
- **E & O** – very few carriers even offer Cyber Endorsements.
  limited scope, not recommended as coverage is limited
  is not designed for a true breach or theft
- **ESB** – limited scope of coverage, low limits, used as a stop gap measure

How do I Insure the Risks - Crime

Crime Insurance Protects money and securities.

Employee Theft (FIDELITY)
Forgery or Alteration
Inside the Premises - theft of money and securities
Inside the Premises - robbery or Safe burglary of other property
Outside the Premises
Computer Fraud
Funds Transfer Fraud
Money Orders and Counterfeit money

Crime Insurance

Designed to cover money AND securities **NOT** data OR information!

Social Engineering Fraud – the fraudulent email/internet/telephone burglar

Can purchase high limits of coverage

You can tailor the policy to your agency's needs

Loss payee endorsements can be added to cover your underwriter(s)

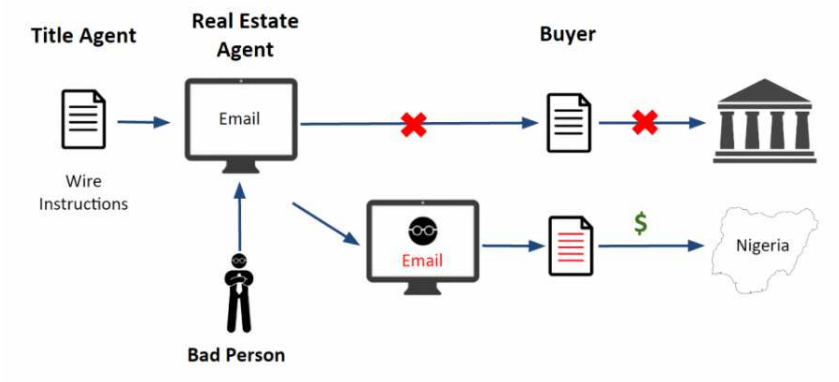
Very broad coverage form as compared to the ESB

Premiums can be substantially lower than those of the ESB

Storytelling Time

An Example how Fraud Happens – When the Buyer sends their $ to the fraudsters!

Crooks are hacking the weak email accounts and waiting for the opportunity to send a buyer false wire instructions that are directed to a "Nigerian Prince".
Then, POOF, the money is gone. The closing doesn't happen, and everyone gets sued.



Is the Title Agency Covered under their INSURANCE?

An Example how Fraud Happens – When the Buyer sends their $ to the fraudsters!

Breakdown of the fraud and what transpired…

This story was $3,748,118.28
February 24, 2022

Commercial property scheduled to close on Wednesday

The Fraud (Friday):

10 am: Commercial broker receives an email from a fraudster posing as an escrow officer with fraudulent wiring instructions (title company logo, name, and account holder on instructions)

4 pm: Commercial broker forwards email to buyer, buyer wires funds to fraudster's account

The Recovery (Monday/Memorial Day - banks are closed):

10 am: Title Company is alerted of the fraud and follow Wire Fraud Recovery Roadmap

11 am: FBI - IC3 report is filed with the FBI and direct contact is made to federal law enforcement to assist

11:15 am: The fraud desk of the bank is notified and IC3 report is included in communications

Tuesday:

1:00 pm: Title Company receive confirmation that the $$$ was gone!

Is the Title Agency Covered under their INSURANCE?

An Example how Fraud Happens
- When the Payoff $ goes to the fraudsters!

This story was $201,978.02
February 14, 2022

Breakdown of the fraud and what transpired…

- Residential property scheduled to close on Friday

The Fraud (Friday):

- 9 am: Escrow Officer received "updated" payoffs purportedly from lender's attorney. Escrow Officer used number from payoff to verify information.
- 1 pm: Shortly after initiating wire, Escrow Officer followed up with borrower who advised the banking information was incorrect.
- 1:30 pm: Escrow Officer alerted Title Companies management about the fraud and followed Wire Fraud Recovery Roadmap
- 1:45 pm: FBI - IC3 report is filed with the FBI and direct contact is made to federal law enforcement to assist
- 2:00 pm: The fraud desk of the bank is notified and IC3 report is included in communications
- 4:00 pm: Title Company receive confirmation that the *$$$* was gone!

Is the Title Agency Covered under their INSURANCE?

An Example how Fraud Happens
- When a Lien Payoff $ goes to the fraudsters!

This story was $7,090.83
February 22, 2022

Breakdown of the fraud and what transpired…

- Residential property scheduled to close on Tuesday

The Fraud (Tuesday) :

- 9:00 am: The Contractor who is not a party to the transaction but has a lien that will be paid off received an email purportedly from Seller asking for ACH information – a form to be filled out - so that payment could be made.
- 9:30 am: The Contractor filled out the form - emailed the Escrow Officer with an updated Lien Payoff statement from for the Seller's construction lien with ACH information and Wire information.
- 1:00 pm: Escrow Officer used number from new Construction Lien Form / Payoff statement to verify information.

2 Weeks later:

- 1:30 pm: Title Agent notified two weeks later by the Contractor that the lien was not paid and still had a balance. Title Company receive confirmation that the $$$ was gone! Manager alerted Title Companies management about the fraud and followed Wire Fraud Recovery Roadmap
- 1:45 pm: FBI - IC3 report is filed with the FBI and direct contact is made to federal law enforcement to assist
- 2:00 pm: The fraud desk of the bank is notified and IC3 report is included in communications

Is the Title Agency Covered under their INSURANCE?

An Example how Fraud Happens
- When the Sellers $ goes to the fraudsters!

This story was $50,046.85
February 11, 2022

Breakdown of the fraud and what transpired…

- Residential property scheduled to close on Thursday

The Fraud (Thursday):

- 11:00 am: Shortly after seller's Broker got added to an email chain, a different set of disbursement instructions were sent to the Escrow Officer. Was asked to have proceeds a wired instead of a check.
- 1:00 pm: The Escrow Department then received another email purportedly from Seller's Attorney with bank information for the payoff as well.
- 4:00 pm: Shortly after initiating wire, Escrow Officer followed up with Seller who advised the banking information was incorrect!

On Friday:

- 8:30 am: Escrow Officer alerted Title Companies management about the fraud and followed Wire Fraud Recovery Roadmap
- 10:15 pm: FBI - IC3 report is filed with the FBI and direct contact is made to federal law enforcement to assist
- 2:00 pm: Escrow Officer spoke with the Broker who advised the new instructions were fraudulent and he had been compromised.
- 4:00 pm: Title Company receive confirmation that the $$$ was gone!

Is the Title Agency Covered under their INSURANCE?

Bain V. Platinum Realty, LLC

Is Everyone on the Hook for Wire Fraud?

- Buyer purportedly receives email from listing broker with new wiring instructions.
- Buyer wires funds to the fraudulent instructions produced resulting in an unrecoverable loss in the amount of **$196,662.**
- Jury finds the Broker **85% responsible** for the loss.
  - Judgment entered against the broker in the amount of **$167,129.**
- Broker files post-trial motion seeking a determination in her favor.
  - *United States District Court for the District of Kansas affirms jury verdict.*

Was the Title Agency Covered under their INSURANCE?

How does a Title Company Insure the Risks of Cyber Liability?

Cyber liability Insurance Protects Information and Data

Policy affords coverage in two sections:

First Party – losses that directly affect the insured
Third Party – losses arising from a breach but originating from a third party

*SOME Cyber Liability policies are adding Social Engineering coverage for additional premium – this covers MONEY – currently very expensive

Cyber Liability Insurance – 1st Party

Will cover costs incurred by the insured (You):

- Breach notification/response expenses
- Public relations
- Forensic consultants/investigation
- Credit monitoring
- Cyber extortion
- Business interruption/extra expense
- Loss of actual data-system restoration
- PCI (Payment Card Industry) fines and penalties

✓ First party coverage is the lynch pin of coverage and is generally UNDERINSURED!

Cyber Liability Insurance – 3rd Party

Will cover claim expenses and damages you are legally obligated to pay as a result:

- A network security breach
- Loss of private information – privacy liability
- Regulatory actions or proceedings, penalties
- Website media content

*Third party coverage is generally offered in higher limits as compared to first party and is the lesser of the two risks monetarily speaking.

Cybersecurity and Strategies for Safety and Privacy:

Know your "**Third Party Service Provider**" – they must have a Security Policy or agree to yours

Who is responsible for their disaster recovery planning?

What disasters are they prepared to withstand?

How frequently do they test their plan?

Where is their disaster recovery site located?

Do they have a backup power supply?

Are they currently utilizing a disaster recovery provider?

Misconceptions in the Market…Crime

- My Fidelity Bond covers my crime risk – does it really?
- Crime insurance is unavailable to the title industry - WRONG
- My underwriter requires a loss payee provision on my Fidelity Bond – Crime can allow for this too!
- It's very expensive- WRONG – in most cases, the crime insurance policy is LESS expensive than a Fidelity Bond
- Protects from internal and external risks
- Protects escrow and operating accounts

Misconceptions in the Market…Crime

- Coverage is expensive (compared to ESB, Crime, E & O v. overall monetary risk)
- No markets for title industry – actually dozens of markets are "open" to title industry.
- Cookie cutter policies can expose your company!
- I have my "other" insurance policies endorsed and that's all I need
- My Best Practice security is in place therefore I do not need Cyber Insurance - - a cyber crime can be the most catastrophic loss facing your agency
- It's the Third-Party lawsuit that's going to bankrupt me – NOT TRUE! First Party losses can bankrupt you
- Public relations won't help after a data loss – breach coach can be critical at the onset

Summary for Cyber & Crime Insurance Policies

- Both Cyber Liability and Crime Insurance policies should be carried by all title agencies
- They actually work in tandem
- Cyber will protect data and Crime will protect money, both from internal and external risks
- Many experts predict that a full, stand-alone Cyber Liability policy will soon become one of the top three insurance policies in any business insurance portfolio
- Policy endorsements for cyber and crime simply do not cover your risk properly
- Stand-alone policies are recommended

Panic
Cry – Scream - Curse
Call the Bank
Cry – Scream – Curse
Lose sleep
Deny
Write a Big Check
Cry – Scream - Curse

Create a Cyber-Fraud Response Plan that includes:

Contact the Banks involved – **1st the receiving Bank *<u>then</u>* your Bank**
Do not solve the issue on your own
Have definition of clear roles and responsibilities
Outline levels of decision-making authority
Alerting all internal employees
Know your external communication
Secure your office and the network
Maybe take all computers Offline <u>if</u> Directed by IT Professionals
Document the specifics of the breach and / or loss
Report - have a list of all possible places to report to
Contact: Cyber-Fraud Insurance Carriers
Errors & Omissions Carrier
Title Insurance Underwriters
When building your plan Know:
Your State Laws
Your Clients State Laws
Review and Update your plan – OFTEN!

Industry Standard Policies and Tools

- **ALTA Outgoing Wire Preparation Checklist:** Use this checklist as a best practice for verifying outgoing wire information.
- **ALTA Rapid Response Plan for Wire Fraud Incidents:** Use this tool to customize your action plan when a wire fraud attempt occurs.
- **Video: How To Complete an IC3 Report**. Watch the video to see how easy it is to help law enforcement gather information.
- **ALTA Cybersecurity Incident Response Plan:** Use this tool to help your team to establish and maintain secure systems and be prepared to act quickly if an incident occurs.
- **ALTA Best Practices.** The third pillar of ALTA's "Title Insurance and Settlement Company Best Practices" provides procedures that should be taken to protect non-public personal information (NPI)

Employee Training and Awareness

•Monitor and Improve Employee Skills.
Consider a phishing security test for all of your employees. These companies can help:

- Security Planner: **https://securityplanner.org**
- PhishMe: **https://phishme.com/free**
- KnowBe4: **https://www.knowbe4.com/resources**

•Webinars to Watch:

- **Data Security Essentials: Strategies to Protect Non-public Personal Information** (**Download copy of presentation**)
- **Fortify Your Business: Lock Down Data and Protect Client Funds** (**Download copy of presentation**)
- **Safeguarding Escrow Trust Accounts**
- **Best Practices: Protecting Non-public Personal Information** (**Download copy of presentation**)
- **Fraud and Your Escrow/Trust Accounts** (**Download copy of presentation**)

AMERICAN LAND TITLE ASSOCIATION

Resources for Your Clients and Consumers

•**Wire Fraud Tips Video:** Share this 1-minute video with homebuyers so they know how to protect their money.

•**ALTA Wire Fraud Video:** This 2-minute video provides four tips on how consumers can protect their money and offers advice on what to do if they have been targeted by a scam. Link to this video from your website, include in your email or share on social media.

•**ALTA Wire Fraud Infographic**: ALTA has produced this Rack Card explaining Wire Fraud. ALTA Members can brand the infographic with their own information at the **ALTAprints website**.

•**ALTA Wire Fraud PowerPoint for Consumer Education:** (**Member-only content**) Use this presentation to educate consumers about the dangers of phishing emails and wire transfer fraud. The presentation provides information on what to do if you've fallen victim to a scam and also highlights 10 tips to prevent wire fraud.

https://stopwirefraud.org/

COALITION TO STOP REAL ESTATE WIRE FRAUD

FEDERAL BUREAU OF INVESTIGATION
Internet Crime Complaint Center IC3

FBI CYBER Strategy

FBI's Internet
Crime Complaint Center
www.ic3.gov

Keep items in a safe location in the event you are requested to provide them for investigations or use as evidence.

Q: What type of information would possibly be considered evidence in regard to my complaint?

A. It is important that you keep any evidence you may have related to your complaint. Evidence may include, but is not limited to, the following:

- Canceled checks
- Credit card receipts
- Money order receipts
- Certified or other mail receipts
- Wire receipts
- Virtual currency receipts
- Pre-paid card receipts
- Envelopes (if you received items via FedEx, UPS, or U.S. Mail)
- Facsimiles
- Pamphlets or brochures
- Phone bills
- Printed or preferably electronic copies of emails (if printed, include full email header information)
- Printed or preferably electronic copies of web pages
- Hard drive images
- PCAP files containing malicious network traffic
- Network, host system, and/or security appliance logs
- Copies of malware
- Chat transcripts and/or telephony logs

APWG is the global industry, law enforcement, and government coalition focused on unifying the global response to cyber crime through development of data resources, data standards and model response systems and protocols for private and public sectors.
www.antiphishing.org

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

Alerts and Tips Resources Industrial Control Systems

https://www.cisa.gov/uscert/report

Official website of the Department of Homeland Security

Report Incidents Report Phishing Report Malware Report Vulnerabilities Share Indicators

Contact Us

(888) 282-0870

Send us email

Download PGP/GPG keys

Report Incidents, Indicators, Phishing, Malware, or Vulnerabilities

MLTA est. 1901
MICHIGAN LAND TITLE ASSOCIATION
Integrity ◆ Responsibility ◆ Service