TLTA Webinar – Cyber Security for the Title Industry

Supporting Documentation to Webinar

To be included with Power Point Presentation

Disclaimer: There are IT and Cyber Security companies referenced in this presentation. Their inclusion is not an endorsement or recommendation of those vendors, but rather is intended to be a helpful tool in researching available vendors. Individual companies should do their own due diligence in selecting which vendor(s) with which to do business.

This information is being provided by TLTA for educational and reference purposes only and should not be construed as legal, financial or business advice from or on behalf of TLTA. Users should consult their own legal counsel and subject-matter experts to ensure that any policies adopted or actions taken meet the requirements unique to their company.

Title Company Cyber Security Challenges: Wire Fraud, Ransomware and Data Breaches

Summary: Title companies and especially their customers are vulnerable to wire fraud caused by Business Email Compromise. Additionally, companies of all types, including title companies, are at risk from increasingly aggressive and sophisticated ransomware attacks and data breaches. Challenges and guidelines for how title companies can prevent these types of attacks are reviewed in this presentation.

1) **Business Email Compromise (BEC)/Wire Fraud Update.** Threat actors are increasingly targeting the real estate transaction, and specifically buyer's funds for closing, through BEC wire fraud scams. The latest reports, including the FBI Internet Crime report published on 4/22/2019 shows the following:
    a. The FBI received 351,937 complaints in 2018 or over 900 complaints per day. The Internet Crime Center (IC3) was formed in May of 2000 and has received a total of 4.4 million complaints.
    b. In the US, BEC scams accounted for 1.3 billion in losses. Global losses were 12.5 billion in 2018. (According to a report published earlier this spring by Proofpoint, the number of BEC attacks per targeted organization increased 476% year-over-year in the last quarter of 2018.)
    c. The FBI formed the **Recovery Asset Team (RAT)** in February 2018. Its purpose is to streamline communications with financial institutions in order to block and recover transfers to U.S. accounts made under fraudulent pretenses. So far, RAT has had a recovery rate of 75% of transactions involving wire fraud that were reported to RAT. Title companies are invited to immediately notify the Federal Bureau of Investigation Internet Crime Complaint Center (IC3), the FBI's **Recovery Asset Team** and utilize the FBI's Financial Fraud Kill Chain Process if they or their clients have been the victim of a wire fraud through any means including BEC.
    d. The FBI stated: "*It is worth noting that these are not national crime statistics, but just statistics from internet crimes reported to IC3.* ***The true figures will almost certainly be higher.***" The FBI also stresses that wire fraud scams "*are constantly evolving as scammers become more sophisticated.*" The FBI went on to say that wire fraud involving buyers is even more underreported than CEO imposter wire fraud as typical buyers would not have the knowledge of how to report this crime. **The bottom line: Wire Fraud attacks on title companies and their clients is increasing dramatically as criminals continue to have success and develop better tools for their attacks.**
    e. The FBI also reported:

"Business Email Compromise (BEC/EAC) actors will use information that is publicly available on real estate listing sites to target victims. This may include homes that are for sale and the progress of the sale such as “under contract”, as well as the contact information of the real estate agent. Be wary of any communication that is exclusively e-mail based and establish a secondary means of communication for verification purposes. **(NOTE: BEC by Threat Actors who identify the target transaction through listing and just sold notices in the MLS, FaceBook, Instagram and Realtor websites helps explain one more way that victims are identified and data for wire fraud is obtained.)**

Be mindful of phone conversations. Victims have reported receiving phone calls from BEC/Email Account Compromise (EAC) actors requesting personal information for verification purposes. Financial institutions report phone calls acknowledging a change in payment type and/or location. Some victims report they were unable to distinguish the fraudulent phone conversation from legitimate conversations." **(NOTE: Title agents and underwriters have reported multiple contacts from varied sources to create a sense of urgency and legitimacy – BEC threat actors have spoofed/faked emails from multiple parties, followed by faxes, followed by texts followed by phone calls, all creating a coordinated, realistic sounding scenario to trick title companies and their customers into being the victim of wire fraud.)**

f. Symantec Security Response Team discussed what the future holds for Business Email Compromise:

"What lies ahead for BEC scams? As artificial intelligence (AI) and machine learning (ML) become more developed, we may very well see BEC scammers adopting these technologies in the near future to make their attacks even more convincing. Both ML and AI could be used to power audiovisual "deepfakes" that target or impersonate C-Suite executives. Already we have seen deepfakes that use only audio, as it is easier to leverage than both audio and visual elements.

A BEC scammer using ML/AI could target an organization's senior financial executive or employee who has direct access to the CEO and who could authorize money transfers. When the employee tries to verify the request, the scammer might use audio featuring the CEO—such as earning calls, YouTube footage, TED talks, and other previous recordings—to fool the employee into believing it is indeed the CEO's voice on the other end ordering the transfer. The employee could then execute the request fully believing it was legitimate. While this is a scary prospect, future BEC scam scenarios may just play out this way." **(NOTE, an AI "deepfake" could pull audio from a Realtor/title company /lender's pod cast or YouTube to make the BEC wire fraud attack even more believable and persuasive.)**

g. Title company-specific issues regarding wire fraud:
    i. Title companies are at risk of both **direct loss** from BEC/Wire Fraud scams and losses from **lawsuits** by customers who experience wire fraud losses. Title

Companies who implement good procedures to protect buyers and sellers from wire fraud also help protect their company from lawsuits. See TLTA Cyber Fraud Resources for avoiding wire fraud. Documenting standard business practices followed on each file is critical.

ii. Threat actors increasingly gain access to critical real estate information through a variety of sources of information (vulnerable systems, data breaches and the dark web).

iii. Threat actors are getting better with their BEC/Wire Fraud scams. Emails are more persuasive, more detailed and are part of coordinated effort of phone calls, texts, and fake emails from other related parties.

iv. New targeting tactics are also being used such as behavioral analysis to determine the vulnerably of victims. Tools like https://www.crystalknows.com can mine LinkedIn and gather social intelligence.

v. Title companies gain find more to help them fight wire fraud at Coalition to Stop Real Estate Wire Fraud and the TLTA Cyber Fraud site.

2) **Data Breach –** the title companies store billions of records containing Private Non-public and Confidential Information and handles trillions of dollars through their escrow accounts. This makes our industry a tempting target and they will be increasingly targeted by cyber criminals.

a. Impact of data breach. Suffering a data breach can cause irreparable financial and reputational damage. For example, in the Equifax breach, if all 148.5 million affected and were put at risk received the proposed $125 settlement, Equifax would be liable for about **$18.5 billion**, or about five-times the company's 2018 revenue. The Federal Trade Commission (FTC) now recommends everyone accept the 10-year Credit Reporting. There has been such a strong interest in $125 settlement per person settlement that it far exceeds the pool available for payments. The FTC estimates Equifax will pay $700 million in damages and penalties.

b. There are 6,500,000 data records compromised every day or 75 records compromised every second. There have been 14 billion records compromised, lost or stolen since 2013.

c. 20 breaches have involved over 100,000,000 records, 7 of which have occurred so far in 2019.

d. Here's a list where data was compromised, exposed or breached where 100 Million or more records were involved per incident:

Data Compromised, Exposed or Breached - 100 Million+ Records

Company	Number of Records	Year
Yahoo	3,000,000,000	2013
Verifications IO LLC	2,000,000,000	2019
First American	885,000,000	2019
Facebook	540,000,000	2019
Marriott	500,000,000	2018
Friend Finder Networks	400,000,000	2016
MySpace	360,000,000	2016
Truecaller	300,000,000	2019
Massive Business hack (7-Eleven & Nasdaq)	160,000,000	2012
Adobe Systems	152,000,000	2013
Under Armour	150,000,000	2018
eBay	145,000,000	2014
Equifax	143,000,000	2017
Canva	140,000,000	2019
Heartland	130,000,000	2009
LinkedIn	117,000,000	2016
Target	110,000,000	2013
Capital One	106,000,000	2019
Quora	100,000,000	2018
Justdial	100,000,000	2019
	9,538,000,000	

3) **RansomWare –** Ransomware attacks have increased dramatically in 2019. See Exhibit A for example of Ransomware attacks for one month in 2019.

   a. **How ransomware works:** Ransomware identifies the drives on an infected system and begins to encrypt the files within each drive. Ransomware generally adds an extension to the encrypted files, such as .aaa, .micro, .encrypted, .ttt, .xyz, .zzz, .locky, .crypt, .cryptolocker, .vault, or .petya, to show that the files have been encrypted—the file extension used is unique to the ransomware type. Once the ransomware has completed file encryption, it creates and displays a file or files containing instructions on how the victim can pay the ransom. If the victim pays the ransom, the threat actor may or may not provide a cryptographic key that the victim can use to unlock the files, making them accessible. A recent article in PC Magazine provides a description of how RansomWare works:

> *Two relatively recent types of malware—Ryuk and SamSam—enter your systems under the guidance of a human operator. In the case of Ryuk, that operator is probably located in North Korea, and with SamSam, in Iran. In each case, the attack starts with finding credentials that allow entry into the system. Once there, the operator examines the content of the system, decides what files to encrypt, elevates privileges, looks for and deactivates anti-malware software and links to backups to also be encrypted, or in some cases, deactivates backups. Then, after perhaps months of preparation, the encryption malware is loaded and launched; it may finish its job in minutes—far too quickly for a human operator to intervene.*

Example of the type of notice a user may see on their screen after a ransomware attack.

b. **How ransomware is delivered:** Ransomware is commonly delivered through phishing emails or via "drive-by downloads." A "drive-by download" is a program that is automatically downloaded from the internet without the user's consent or often without their knowledge. It is possible the malicious code may run after download, without user interaction. After the malicious code has been run, the computer becomes infected with ransomware.

c. **To prevent ransomware and increase the ability to recover from an attack, implement the recommendations listed below.** Additionally, KnowBe4 provides a Ransomware Rescue Manual with detailed information on how to prevent and recover from a ransomware attack. Additional resources on how to protect your company from Ransomware attacks can be found here: Carnegie Mellon University Ransomware: Best Practices for Prevention and Response; and here: Center for Internet Security - Ransomware Impacts and Defense Controls

Recommendations for Title Insurance Companies

The following IT and Operational recommendations will help fight all of the above attacks: Wire Fraud, Ransomware and Data Breaches.

1) **High priority IT procedures every title company is advised to implement**
   a. **Inform yourself.** Keep yourself informed about recent cybersecurity threats and be up to date on ransomware techniques. You or your IT manager can find information about known phishing attacks on the Anti-Phishing Working Group website. You or your IT manager may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
   b. **Email Encryption.**
      i. **What is Email Encryption?** Email encryption makes the contents of email, both the text and any attachments, indecipherable to unauthorized individuals. Encryption is used while the emails are in transit, that is, while they are passing

through the public Internet, so that if an unauthorized individual intercepts an email while it moves across the Internet it cannot be read. Also, if human error causes a leak where client NPI is sent to the wrong recipient, that recipient will be unable to read the NPI. The greatest benefit of encrypting emails in transit is that the emails are protected while exposed to the Internet.

Look for email encryption products that integrate with your normal workflow. Encryption and decryption should happen automatically and invisibly, keeping your business flowing and allowing your company to protect email as it travels outside your network.

ii. **Transport Layer Security (TLS).** Transport Layer Security are cryptographic protocols designed to provide communications security over a computer network. TLS can be used to encrypt most of the email traffic of a title company. The use of products that can automatically encrypt on the fly is recommended. If TLS is not available on the recipient's side then email should automatically fall back to an alternative method of encryption.

c. **Password Management.** It is recommended that title companies should eliminate password reuse across all online accounts, personal or private and change passwords for all accounts with companies that have suffered a breach. See: Choosing and Protecting Passwords - Homeland Security and https://www.cnet.com/news/the-best-password-managers-of-2019/. Data breaches are also being enabled by use of passwords that have been compromised and made available on the dark web. Google found 300,000 compromised passwords being used when they tracked passwords through their 'Password Checkup' Chrome extension. Computer users must change their passwords if there is any possibility their password has been compromised.
d. **Enable/Implement Two-Factor/Multi-Factor Authentication** (2FA/MFA) for all accounts where available. Two-factor authentication does not eliminate all risk of compromised passwords but it greatly reduces that risk. An example of a product that helps implement 2FA/MFA is Authy – https://authy.com/. If your email and application's provider do not provide for enable 2FA/MFA, you need a new provider.
e. **IMAP.** It is recommended that title companies should disable IMAP connections on email services. If your provider only has the option to connect via IMAP, you need a new service provider.
f. **Backing up computers and servers.** Title companies must perform frequent backups of their systems and other important files and verify their backups regularly. If a computer becomes infected with ransomware, a company can restore their system to its previous state using their backups. Complete backups must be taken and verified daily including the operating system, all applications and all data. **NOTE: If the system that preforms the backups becomes encrypted from malware/ransomware, the company will not be able to recover their data. It is not uncommon for ransomware infections and other malware attacks to also infect and encrypt backup systems.** A company needs to perform its backups in such a way as to protect them from becoming infected, and if they do, the damage is limited to a small amount of data. Internal or external IT teams are advised to provide title company executives and owners with monthly reporting on backup success. Also, it's equality important to test recoverability of your data to

confirm a full restore can actually be accomplished and determine how long a full restore will take. Nothing replaces performing full and complete test.

g. **Title companies must update and patch PC's, Applications, Servers and Network Security Devices.** Applications and operating systems (OSs) must be updated with the latest patches, including any Microsoft products the company is utilizing. See timely patching of Microsoft Windows/MacOS/Microsoft Office. Vulnerable applications and operating systems are the target of most ransomware attack. (See Understanding Patches and Software Updates.) Internal or external IT teams are advised to status and explain any deviations.

Note: In the EquiFax data breach, the attack process started when hackers learned of new server operating system vulnerabilities published by US-CERT. They began searching the web for any servers with vulnerabilities that the US-CERT warned about. Two months later they hit the jackpot with an Equifax portal. The hackers used a month-old vulnerability where a security patch had not been applied and gained access to login credentials for three servers. They were then able to access another 48 servers containing personal information. The thieves spent 76 days within Equifax's network before they were detected. The hackers stole the data piece by piece from 51 databases so they wouldn't raise any alarms. The result was the theft of 143 million records. A GAO Report details the following failures:

Further, Equifax violated Gramm-Leach-Bliley Safeguards Rule in the following ways:

- *Equifax did not check to make sure employees followed through on the patching process;*
- *Equifax failed to detect that a patch was needed because the company used an automated scan that wasn't properly configured to check all the places that could be using the vulnerable software;*
- *Equifax failed to segment its network to limit how much sensitive data an attacker could steal;*
- *Equifax stored admin credentials and passwords in unprotected plain-text files;*
- *Equifax failed to update security certificates that had expired 10 months earlier;*
- *Equifax didn't detect intrusions on 'legacy' their systems*

Note: Title companies could be equally vulnerable to similar attacks caused by failure to promptly apply all software security patches. Equifax's 48-hour patch rule (Equifax had not actually applied the patch after two months) was identified by the FTC *as insufficient and they should have applied patches more quickly*. Title companies also store confidential customer data and would be subject to similar patch application requirements.

h. **It is recommended that title companies ensure Anti-Virus (AV) is installed and up to date.** Ideally desktop computers would have AV enabled (built-in Windows Defender works well if you are on Windows 10) and systems would be configured so updates are applied automatically and all security features are enabled. **Note:** Windows 7 will reach

its "End-of-Life" and support, including security patching, will be discontinued January 2020. A company's Internal or external IT team are advised to provide title company executives and owners with monthly reporting on AV status and explain any deviations from 100%.

i. **Monitoring.** Network Monitoring/Intrusion Detection is just as important as the preventative measures that you are taking because without it a malicious actor could go undetected forever. For title companies can implement products from vendors like Alienvault, Arctic Wolf, or Perch that offer network monitoring. This can be much more cost effective that hiring a dedicated cybersecurity skilled employee. Title companies without a dedicated IT team can utilize IT vendor offering Network Monitoring as a managed service.

j. **Content scanning.** Title companies are advised to implement content scanning and filtering on mail servers. Ideally inbound e-mails would be scanned for known threats and any attachment types that could pose a threat would be blocked.

k. **URL Defense.** Title companies are advised to implement URL defense solutions such as Proofpoint or Cisco Umbrella which protects network resources by blocking access to malicious websites. Links in all email messages are evaluated using a variety of sophisticated techniques to determine the likelihood that they lead back to phishing or malware websites.

l. **Standard Benchmark Settings.** Title companies are advised to configure the security settings of Microsoft Windows machines using guidance "Microsoft Security Baselines", "CIS Benchmarks" or other reputable options.

NOTE: Before implementing the changes suggested in these documents, companies should test them for compatibility with their business prior to deploying company wide.

2) **High Priority operational procedures title companies are advised to implement**:

   a. **Verify Wire Instructions.** Title companies are advised to verify all wire instructions received from sellers or lenders from previously validated phone number (See TLTA Cyber Fraud Resources for avoiding wire fraud). Additionally, they are advised to use an outgoing wire checklist to insure all the steps are followed and that compliance/audit documentation is created for each transaction. See: ALTA Outgoing Wire Preparation Checklist.

   b. Buyer education to protect against wire fraud. Title companies are advised to educate buyers and realtors to follow best practices for avoiding wire fraud.

      i. Educate buyers by:

         1. Sending notifications and wire fraud alerts through email
         2. Having buyers sign wire fraud warning pre-closing
         3. Calling buyers to discuss wire fraud best practices
         4. Sending follow-up email confirming phone conversation and requesting buyer reply back acknowledging title company has advised them regarding risks involved with wire transfers

      ii. Educate buyers to do the following:

         1. Do not ever accept wire instructions via unencrypted email from anyone
         2. Do not accept wire instructions that they did not request from the title company
         3. Do not accept wire instructions from anyone (such as the lender, Realtor) other than the title company

4. Do not accept last minute changes to wire instructions from anyone Title companies will never change wire instructions that were sent upon request and properly verified
5. When the buyer requests wire instructions and those instructions were provided by a secure delivery method, the buyer should always contact the title company through a validated phone number to verbally confirm the wire instructions

iii. Educate Realtors on common social engineering dangers
1. Free email services can be easily compromised
a. Yahoo, Gmail, Etc…
b. Buyers, Sellers, and even Realtors often use these services
c. All email systems should have 2-factor authentication enabled
2. Private email servers can be compromised as well
a. A Realtor's email address is readily available to anyone online which means a Realtor can more easily be targeted and email account compromised and the Realtors email address can imitate
b. Realtors often access email via mobile devices making it more difficult to detect fraudulent email markers
i. Smaller screens make it more difficult to spot suspicious emails
ii. Email headers are usually hidden making it more difficult to detect spoofed or fraudulent email senders

c. **Security Awareness Training.** Organizations are advised to ensure that they provide cybersecurity awareness training to their personnel. Ideally, organizations will have regular, mandatory cybersecurity awareness training sessions to ensure their personnel are informed about current cybersecurity threats and threat actor techniques. To improve workforce awareness, organizations can test their personnel with phishing assessments that simulate real-world phishing emails. Regardless of the technology implemented, it is imperative that company executives/owners outline, document and implement a company-wide Security Awareness Training and Testing Solution and **make training mandatory for ALL employees**. It is recommended that reporting that tracks the success rate of the training be implemented and reported to company executives and ownership monthly.
i. Additionally, company policies and procedures should
1. Ensure all new employees are educated on proper cyber security procedures
2. Ensure current employees stay aware of new and emerging scams
3. Reassess the security training program at least annually making sure the program stays relevant and updated with current best practices
ii. Here is a link of Comments from IT professional on implementing security awareness training
iii. **Note: More than 75 percent of title professionals don't conduct simulated phishing tests, according to a survey conducted by ALTA's Data & Analytics Work Group** https://tiacrrg.com/survey-75-percent-of-title-agents-dont-conduct-phishing-tests/.
iv. **Example of how users are tricked into disclosing their username and password:**

"It's easy to successfully obtain the mortgage or title company portal's username and password by sending a phishing email to the customer. So the portal actually offers a false sense of security and does not protect the customers' confidential information. A portal is not a magic bullet because all the cybercriminal needs to do is send an email that the user's portal account has been suspended or that account needs a new password and about 90 percent of the people are going to fall for it." Greg McDonald, CEO of Cloudstar. All users and certainly company employees must become much better educated about suspicious, phishing emails designed to trick them into clicking on malware or revealing confidential information.

v. **Effectiveness of Security Training for Phishing**.

12-month test. KnowBe4 tested 9 million employees with 20 million phishing security tests across 18,000 organizations. The failure rate (where users are tricked into clicking on links or opening attachments with simulated malware) dropped from an average of 30% to 2% after 12 months of training/testing.

vi. **Open email attachments with caution.** Employees must be educated to be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

vii. **Verify email senders.** If employees are unsure whether an email is legitimate, it is recommended that they stop and verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous, verified and legitimate email to ensure the contact information you have for the sender is authentic before click on any links or open any attachments.

d. **Cyber Insurance.** Secure as broad of cyber insurance (See TLTA article on Cyber insurance) coverage as possible. Cybersecurity Insurance coverage for small title companies that provides coverage for legal fees, Incident Response and other title company related losses can be obtained for reasonable costs. These policies also include dark web monitoring and alerting for compromised email/passwords within their organization and the companies and organization they do business with. Title companies are advised to:

i. Ensure their policy includes coverage for social engineering

ii. Ensure their police includes additional Social Engineering coverage called Technology Theft Fraud that is now available. Technology Theft Fraud will help in the situation where the title agent's email is compromised, the criminal pretends to be the title agent and a fraudulent wire is then sent by a client of vendor. The term Technology Theft Fraud extends the definition of social engineering. As of August 2019, the coverage has limits of $100K-$250K. This coverage can also be obtained without the call back provision requirement that many other insurance companies require as a condition of the policy.

iii. Confirm there is no "look back" provision where a carrier can deny coverage if any of the standard verification procedures were not followed

iv. Secure coverage from an insurance company familiar with title company operations (Utilize resources from TLTA, ALTA, & your underwriters) and understands their unique and industry specific needs

e. **Data Breach Response Plan.** Prepare a company response plan in the event of a data breach.
f. **Wire Fraud Response Plan.** Prepare a company response plan in the event the company is the victim of wire fraud.

TLTA has created a Cyber Fraud Resource page with additional resources for title companies.

Exhibit A

Example of Ransomware Attacks

Recorded attacks for the month of July, 2019

https://techtalk.pcpitstop.com/2019/01/09/ransomware-attacks-2019/

- Georgia Courts Agency – Ransom demands were not disclosed, and officials will not comment on intentions to pay.
- Richmond Heights City Hall – Ransom demands were not disclosed, but officials reported they did not pay them.
- City of La Pointe – Indiana – Ransom demands were not disclosed, and city officials did not confirm if they will pay the demands. However, they did state the city has a cyber insurance policy which will help restore systems.
- Humboldt State University KHSU Radio – California – Ransom demands were not disclosed, nor was it confirmed if officials will pay these demands to restore the station's networks.
- Monroe College – New York – Hackers demanded a ransom payment of $2M. It is unclear if the college will pay those demands, or restore networks using backup files.
- Daviess County Library – Kentucky – Ransom demands were not disclosed; although, officials did report they do not intend to pay.
- City of Collierville – Tennessee – Ransom demands were not disclosed, nor were intentions to pay.
- Butler County Library – Pennsylvania – Ransom demands were not disclosed, nor did officials confirm if they intended to pay ransom demands.
- Onondaga County Library – New York – Ransom demands were not disclosed, nor did officials confirm if they intended to pay ransom demands.
- Lawrenceville Police Department – Georgia – Ransom demands were not disclosed, nor did officials confirm if they intended to pay ransom demands.
- Henry County – Georgia – Ransom demands were not disclosed, nor did officials confirm if they intended to pay ransom demands.
- Vigo County – Indiana – Ransom demands were not disclosed, nor did officials confirm if they intended to pay ransom demands.
- Bilancione Dentistry – Florida – Hackers demanded a payment of $10,000; however, Dr. Bilancione stated he had no intention to pay those demands.
- Johannesburg Utility – South Africa – The ransom demands have not been disclosed, nor have the department's intention to pay.
- Lincoln County Sheriff – North Carolina – The ransom demands have not been disclosed, nor have the department's intention to pay.
- New Haven Public School – Connecticut – The ransom demands have not been disclosed, nor have the department's intention to pay. However, last fall when the school was hit with ransom, they paid a $2,000 ransom demand.
- Spring Hill Medical Center – Alabama – The ransom demands have not been disclosed, nor have the department's intention to pay.
- Department of Public Safety – Georgia – Officials stated they will not pay the ransom demands; however, they have yet to disclose what those ransom demands were.
- St. John's Ambulance – England – The ransom demands have not been disclosed, nor have the organization's intention to pay.
- Park DuValle Community Health Center – Kentucky – Healthcare officials confirmed they paid the $70,000 ransom demands through a bitcoin payment.
- Houston County Schools – Alabama – The ransom demands have not been disclosed, and school officials have not confirmed any intention to pay.
- Sabine School District – Louisiana – The ransom demands have not been disclosed, and school officials have not confirmed any intention to pay.
- Morehead Schoool District – Louisiana – The ransom demands have not been disclosed, and school officials have not confirmed any intention to pay.
- Ouachita School District – Louisiana – The ransom demands have not been disclosed, and school officials have not confirmed any intention to pay.
- Gadsden School District – New Mexico – The ransom demands have not been disclosed; however, school officials confirmed they have no intention to pay.
- Broken Arrow Schools – Oklahoma – Ransom demands have not been disclosed, and school officials have yet to comment on their intentions to pay.
- Lyons County Schools – Nevada – School officials they did not pay the ransom, but their cyber insurance did negotiate a payment with the hackers. The amount was not disclosed.

ALTA Outgoing Wire Preparation Checklist

Visit the ALTA Website: https://www.alta.org/business-tools/information-security.cfm

Date: _____

File Number: _____

Company Name/Location: _____

Section 1: Provide the source of the wiring instructions:

☐	I received the initial outgoing wire instructions directly from the **payee in person**. The instructions have not been modified or amended. ***Proceed to Section 2.***
☐	I received the initial outgoing wire instructions directly from the **payee via the United States Postal Service or a known overnight mail or messenger service** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. ***Proceed to Section 2.***
☐	I received the initial outgoing wire instructions directly from the **payee via fax** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the package. The instructions have not been modified or amended. ***Proceed to Section 2.***
☐	I received the initial outgoing wire instructions from the **payee**, which have been modified or amended in writing in person at the following date/time: _____. ***Proceed to Section 2.***
☐	I received the initial outgoing wire instructions directly from the **payee by email** and **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number shown in the email. The instructions have not been modified or amended. ***Proceed to Section 2.***
☐	I received the initial outgoing wiring instructions **via a 3rd party** (e.g., attorney, realtor, lender) and have **verified** the accuracy of the instruction by **calling the payee** at a phone number obtained independently from any phone number obtained via the 3rd party. The instructions have not been modified or amended. ***Proceed to Section 2.***

Section 2: Verify instructions received by email or from someone other than the payee.

☐	Wire Payee Name:	
☐	Wire Amount:	
☐	Payee Phone Number:	
☐	Source of Phone Number (*never use the phone number included in an email*):	
	☐	Original Order or Contract:
	☐	Secure Portal:
	☐	Internet Search:
	☐	Other (*describe*):

☐	Name of Person I Spoke With: Date:
☐	Wire Information confirmed. Account and ABA Routing Number, and Account Name match payee in the file. Wire instruction notes indicate correct payment information (e.g., loan number, beneficiary, other information).
☐	Wire Information confirmed. Account and ABA Routing Number match an entry on our company's list of validated wire instructions for common bank payoffs.

Wire Creator: _____ _____

(Signature) **(Date)**

_____

(Printed Name)

Wire Authorizer: _____ _____

(Signature) **(Date)**

_____

(Printed Name)

Section 3: Verify Delivery of Wired Funds.

☐	Date Wire Was Sent:	
☐	Date Wire Was Received:	
☐	Name of Person Who Confirmed Receipt:	
☐	Purpose of Wire:	
	☐	Loan Payoff
	☐	Equity Loan Payoff
	☐	Seller Proceeds
	☐	Real Estate Commission
	☐	Other (*describe*):

Verified By: _____ _____

(Signature) **(Date)**

_____

(Printed Name)

Disclaimer: There are IT and Cyber Security companies referenced in this presentation. Their inclusion is not an endorsement or recommendation of those vendors, but rather is intended to be a helpful tool in researching available vendors. Individual companies should do their own due diligence in selecting which vendor(s) with which to do business.

This information is being provided by TLTA for educational and reference purposes only and should not be construed as legal, financial or business advice from or on behalf of TLTA. Users should consult their own legal counsel and subject-matter experts to ensure that any policies adopted or actions taken meet the requirements unique to their company.