TESTIMONY OF DANIEL D. MENNENOH ITP, NTP

PRESIDENT, H.B. WILKINSON TITLE COMPANY, INC.

ON

DATA SECURITY: VULNERABILITIES AND OPPORTUNITIES

FOR IMPROVEMENT

BEFORE

THE HOUSE FINANCIAL SERVICES COMMITTEE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

WEDNESDAY, NOVEMBER 1, 2017

WASHINGTON, D.C.

Chairman Luetkemeyer, Ranking Member Clay and members of the subcommittee, my name is Daniel Mennenoh. I am President of H.B. Wilkinson Title Company, a title insurance agency headquartered in Galena, Illinois. I have been in the title insurance and settlement business for nearly 36 years. I purchased the company from my father. My wife and I have operated the company together for 20 years.

H.B. Wilkinson has 28 employees and has offices in seven counties, the most populated of which is Rock Island, which includes the Quad-Cities and has a population of approximately 150,000. We close about 70 real estate transactions a month or roughly 800 a year. By industry standards we are considered a large title company. The average title agency has less than five employees and revenue between $250,000 and $499,000 annually.

For the past year I had the honor of serving as the President of the American Land Title Association (ALTA). ALTA is the national trade association representing more than 6,300 title insurance companies, title and settlement agents, independent abstracters, title searchers, and real estate attorneys. ALTA represents many small businesses that serve their local communities and operate in every county in the United States.

One of my favorite responsibilities serving as ALTA president was traveling the country to meet with members of the association and hearing what was happening in their businesses and local markets. In those conversations, the one topic that always topped the list of concerns for title professionals was data security and the growing threat of criminals trying to steal our customers' closing funds. These small business owners were not just worried about the future of their business but also the threat to their customers potentially losing their life's savings.

With the spike in security incidents and fraud, the title industry has spent millions to protect its customers' money and data. Like other financial companies, members of the title industry must comply with the data safeguarding requirements of the Gramm Leach Bliley Act (GLBA).[1] GLBA places strict requirements on title companies and financial institutions to safeguard "nonpublic personal information". In addition to GLBA, title companies must comply with various state data security and breach notification laws and state insurance department rules like the recent regulation developed by the New York Department of Financial Services. Unlike most federal laws, GLBA does not preempt state law that gives greater privacy protection.

[1] Pub.L. 106–102, 113 Stat. 1338, enacted November 12, 1999.

Several years ago, ALTA developed a set of voluntary industry best practices for members to use as part of their compliance programs. These best practices include guidelines on data security and stronger accounting procedures. This includes things like using secure systems when transmitting a consumer's personal information and ensuring that third parties abide by the title company's data security standards.

While companies are not required to follow the ALTA Best Practices, a significant portion of our membership has adopted them as part of their compliance management program.

Increase in Criminal Activity

Having sound policies and procedures to protect data and money is more important than ever due to the barrage of cyber attacks. Earlier this year, the FBI reported a 480 percent increase in criminals attempting to steal consumer's closing funds.

The growth in the crimes is due in part to their profitability. The average successful bank robber's haul is $3,816. The average successful wire fraud loss is $129,427. This is a much better return for a much less expensive and dangerous crime to commit. Overall, these scams have cost Americans $5.3 billion.

Often, a first step for criminals trying to steal closing funds is deploying a common social engineering technique called phishing. This is a method used by criminals to get you to share your personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. They accomplish this by sending email messages, texts, websites or phone

calls that seem legitimate. Some criminals attempt to get the unsuspecting person to download malicious code. Oftentimes the only goal is to obtain login and password information for your email so that they can use it in another scheme. When these attacks target companies or people that regularly send wire transfer payments, it is called Business E-mail Compromise (BEC) or Email Account Compromise (EAC).[2]

In a typical scheme targeting homebuyers, the criminal monitors real estate transaction information. In many instances, they obtain access to email accounts, most commonly those used by real estate professionals who are trusted by the consumer. Criminals use this access to find transaction patterns and details to make their fraudulent communications seem legitimate.

Once the criminals gain access to an email account, they will monitor messages to find someone in the process of buying a home. They then use the stolen information to email fraudulent wire transfer instructions disguised to appear as if they came from a professional to the buyer, seller, real estate agent or title company. These emails look legitimate. They often use an actual party's logo, nearly identical email addresses as the supposed sender and use words or phrases gleaned from legitimate emails.

Homebuyers are the most common target. Criminals will monitor email traffic about a transaction to get ahead of common deadlines for the buyer to send the earnest money or down payment. When this occurs, it is not uncommon for the fraud to be discovered weeks later when

[2] BEC https://www.ic3.gov/media/2017/170504.aspx

the buyer shows up to settlement with insufficient funds. This delay in detection also makes it nearly impossible to recover the stolen funds.

In one instance that I am familiar with, a woman in Texas lost her entire life savings to the hands of these sorts of cyber criminals. She had saved nearly $25,000 and planned to use it as a down payment on a house. Prior to the lender finalizing the Closing Disclosure Form, the woman's email was hacked.

Using information gathered by accessing her email account, a fraudster impersonated the title agency closer, used the closer's name, and instructed the buyer to send the purchase proceeds amount using fraudulent wire instructions. The buyer, believing it was the title agency closer, followed the instructions and wired the funds to the fraudster's account the day before closing. On the day, of closing the title agency closer contacted the buyer with the correct amount she needed to purchase the house. Confused, the buyer told the title agency closer that she had already wired the funds according to the closer's earlier instructions. After reviewing the fraudulent wire instructions that the buyer had been sent, the closer contacted the receiving bank to halt the transaction. But it was too late, and the funds had already been sent out. The money was gone. Not only did the home purchase fall through, but the woman lost her life savings.

This form of cybercrime can also wreak irreparable damage on small businesses. In another instance, the email account of an attorney customer of an Illinois based title agency was hacked into. However, the closer at the title agency wasn't aware of the hack. As a result, when the title agency closer was emailed a set of fraudulent disbursement instructions sent by the

fraudster following an initial set of legitimate disbursement instructions sent by the attorney, they simply used what appeared to be the most recent set of instructions sent by their client.

It first became clear that something had gone wrong later that day when the attorney checked with his client as to whether the funds had been received. They had not and so the attorney reached out to the title agency. The title agency immediately reviewed the altered wire instructions and found the owner of the account on those instructions to be different than the sellers. The agency then contacted the bank that wire that received the wire and notified them that it had been fraudulent.

Ultimately the bank on the other end of the transaction was able to freeze the funds, but there were already other wires that had been sent to the same fraudulent account. The title company made the sellers whole by paying them the full sales proceeds of about $127,000. The company received all but about $4,000 back, and has used the incident as a valuable training tool for its employees. But had the crime not been detected so early on, this title agency could have suffered a devastating financial loss. Title companies in each of your districts have stories like these.

With the amount of personal data obtained through publicly known data breaches, the risk only increases. In today's environment, criminals can obtain verified email accounts, passwords and security questions on the dark web for as little as $10.[3] Increasingly, criminals do

[3] https://www.bloomberg.com/news/articles/2017-09-15/equifax-hack-your-social-security-and-identity-are-for-sale

not need to use phishing schemes or other hacking attempts to gain access a real estate professional's email account to perpetuate these crimes.

How the Industry Responded to these Crimes

Title Companies have taken an array of steps to combat this fraud. Some of these steps include using secured email communications, calling homebuyers on a known phone number before sending wire instructions, and asking their banks to match both the recipient's account number a payee information when sending wires. Many of our member companies issue warnings to their customers. They commonly put these warnings on their websites and at the bottom of every email they send.

This is not a problem that we as an industry can fix on our own. What is so frustrating is that there is no amount of money we can spend to protect our consumers from being targeted by these criminals. The only thing that will help is to increase awareness so that our customers can help protect themselves.

At ALTA, this has been our guiding principle this year. In April, we issued a consumer alert outlining five tips that people can use to protect against wire fraud:

1. **Call, don't email:** Confirm all wiring instructions by phone before transferring funds. Use the phone number from the title company's website or a business card.
2. **Be suspicious:** It's not common for title companies to change wiring instructions and payment information.

3. **Confirm it all:** Ask your bank to confirm not just the account number but also the name on the account before sending a wire.
4. **Verify immediately:** You should call the title company or real estate agent to validate that the funds were received. Detecting that you sent the money to the wrong account within 24 hours gives you the best chance of recovering your money.
5. **Forward, don't reply:** When responding to an email, hit forward instead of reply and then start typing in the person's email address. Criminals use email address that are very similar to the real one for a company. By typing in email addresses you will make it easier to discover if a fraudster is after you.

We then converted that alert into a 2-minute video that title companies, real estate agents and lenders can use to help educate consumers about how they protect their money.[4] We also developed an info-graphic that members can use to inform homebuyers about the wire fraud scams and what to do if they've been targeted by a scam.

Our members know the key to keeping these crimes from happening in their community is awareness, and they know they cannot do it alone. This needs to be a coordinated awareness effort across the industry between all players including real estate agents, policy makers, consumer groups, title insurance companies, title and settlement agents, real estate attorneys and customers themselves.

In January of this year, I along with the ALTA Board of Governors met with Consumer Financial Protection Bureau Director Richard Cordray. In that meeting, we provided examples of

[4] Video (linked)

these crimes and asked for the CFPB's help in increasing awareness. They were not aware of this crime and asked for more information, which our members were happy to provide. We followed up with a letter to the Bureau in April. We said, "Despite efforts by the title industry and others to educate consumers about the risk, homebuyers continue to be targeted. If we are going to protect consumers from these schemes during the upcoming home buying season we will need your help." We encouraged the Bureau to work with its fellow financial regulators and law enforcement officials to prevent these criminals from utilizing our country's financial system.

In July, the CFPB published a warning to help alert consumers about wire fraud schemes.[5] Other regulators have also issued warnings including the Missouri Department of Insurance (DOI), the Colorado Division of Real Estate at the Department of Regulatory Agencies, the Federal Trade Commission and the Financial Crimes Enforcement Network (FinCEN).

While this is a step in the right direction, this alone will not solve this problem. We all need to use consumer alerts to help educate our buyers, sellers and real estate partners about the risks. We need to carry an urgency about this problem. Consumers need to not just be aware of the danger, but empowered to help protect themselves.

Additional Practices to Prevent Fraud

Along with increasing awareness for homebuyers, we are working with our industry partners to make simple process changes to help consumers.

[5] https://www.consumerfinance.gov/about-us/blog/buying-home-watch-out-mortgage-closing-scams/

Probably the single biggest preventative measure that real estate and banking professionals can take is to encourage consumers to call the title company or real estate agent to verify wire instructions before transmitting funds. We encourage regulators to work with banks to include this simple practice into their training in working with customers that are sending wires for real estate purchases.

Another banking practice that would help reduce the risk is payee matching. We encourage financial institutions to match not only the account number of the recipient but also the payee's name. Oftentimes the fraudulent instructions will say the transfer is to be sent to the title company's trust account but instead it goes to the criminal's personal account. Just matching the account number on the request with an account number at the beneficiary bank will not catch this. Some banks have voluntarily added additional capabilities to match the payee's names, and it is proving useful in catching these schemes.

Conclusion

Consumer losses due to a data breach (even a massive one like Equifax), pales in comparison to the loss of their down payment or earnest money. We believe policy makers should focus on two key areas to stop these crimes.

First, we need to increase public awareness of these schemes. In an advisory last year, the Financial Crimes Enforcement Network (FinCEN) stated that due to the irrevocable nature of these transfers, the best first line of defense is to prevent Americans from falling victim to these scams.

Second, a simple change in practices can be the single biggest deterrent to wire fraud. We encourage financial institutions to match not only the account number of the beneficiary but also the payee's name.

Lastly, policymakers should consider ways to better use both suspicious activity reports and IC3 data to better detect accounts used by these criminals and their mules. We need to provide financial institutions with as much information as possible to uncover these networks. Even if more information does not lead to prosecutions of these criminals, it can help banks decide to place holds on the account preventing the criminal or the mule from withdrawing funds while they conduct a more thorough investigation.

I appreciate the opportunity to discuss one of the largest threats to consumers, title companies and the U.S. real estate system. ALTA is eager to serve as a resource to this Subcommittee, and I am happy to answer any questions.