FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

MISSING the days of mortgage fraud

By Lisa A. Tyler
National Escrow Administrator

The articles contained in this edition make us miss the days when the biggest thing the real estate industry was combating was mortgage fraud.

The April 2019 issue of this newsletter featured an article that discussed how experts predicted ransomware attempts would increase in the coming months. Unfortunately, it seems to be true. I recently attended a conference where the CEO of a lending company shared a story about one of his peers: The CEO of another lending company was victimized by this crime. In the end, the CEO paid the equivalent of $1.5 million in bitcoin to the hackers, in order to restore his computer systems. Lenders must be a target, because that same week another lender reported they were successfully attacked and were held for ransom. Read "RANSOMWARE" for more details about how the crime affected one city.

Buyers all over the country are the targets of hackers attempting to steal their life savings. They strike innocent, hard-working homebuyers when they are most vulnerable: Engaged in the process of buying a home. The process of buying a home is described by buyers as, "crazy challenging." There are a lot of "i's" to be dotted and "t's" to be crossed, which is why hackers are successful in their attempts. This article will demonstrate steps the Fidelity National Title Group takes to prevent this; but the thieves are still winning. Read "HOW to lose your life savings" for all the details.

Wire transfer fraud is the fastest growing real estate cybercrime in the United States. Attempts by fraudsters to divert wire transfers have not weakened. Instead, the hackers have broadened their horizons. Although homebuyers are the most common target for this fraud, anyone involved in wiring money during the closing process are vulnerable. Recently, the fraudsters have figured out how to infiltrate documents sent via eFax® systems and alter payoff demands.

Stephanie Cannon, Closing Services Manager for Title Underwriters Agency, knows all too well the schemes and scams used to succeed at this type of fraud. She tirelessly reminds her staff to be alert and to look for any discrepancies to avoid falling victim. Her efforts have paid off. Read "CLEVER wire fraud schemes" for more details.

Nationally, title insurance companies belong to the American Land Title Association (ALTA). ALTA works throughout the year on behalf of the industry. For the last several years, the ALTA has put together some terrific resources for home buyers through their Homebuyer Outreach Program (HOP). They have put together informative materials which can be shared with consumers to describe what title insurance is, since many consumers do not truly understand the value of an owner's title insurance policy. Read more in the article entitled "AMERICAN land title association."

IN THIS ISSUE

Share Fraud Insights
via email, mail or word of mouth.

volume 14 issue 9
September 2019

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

RANSOMWARE

Simply put, ransomware works like this: A criminal hacks into a computer, deploys malicious software to block access or take over a computer system with unbreakable encryption, and then demands a ransom for the encryption key needed to re-gain access and unscramble the files.

In May 2019, the City of Baltimore fell victim to this crime. Hackers were successful in encrypting about 10,000 of their computers. The hackers sent a ransom demand, but the Mayor refused to pay.

The *Baltimore Sun* reported that the demand said, "We've watching you for days and we've worked on your systems to gain full access to your company and bypass all of your protections," and demanded the City pay 13 bitcoins within four days to unencrypt the computers, or the price would go up. They claimed after 10 days, the data would be lost forever. The hackers threatened, "We won't talk more, all we know is MONEY!...Hurry up! TikTok, Tik Tok, Tik Tok!"

The 13 bitcoin added up to approximately $103,000. The hackers threatened to stop all future communications if the city called the FBI, and claimed any attempt to use any other software would permanently damage their computers and the files contained on them.

Experts reported the hackers utilized RobbinHood malware. RobbinHood is a very powerful program which seems to gain access through hacked remote desktop services or other Trojans, rather than spam.

The attack affected phone lines, email accounts, the ability to collect payments for utilities, even parking fines and many more services the public relies on. Most notably to the title insurance industry, the attack affected the recorder's office causing a delay in real estate transactions.

It does not end there. The County of Harrison, West Virginia, was the victim of a ransomware attack on Thursday, June 13, 2019. The County was forced to revert to manually recording documents, thus exposing title insurance companies to bigger gap periods and requiring manual title searches for pending transactions.

Our Company has guidelines on how operations can continue business as usual in the event a county recorder's office is attacked by ransomware. It is more important than ever we all work together.

Anyone located in a municipality who falls victim to this type of cyber incident should be sure to consult with their Underwriter for approval to close any transaction.

The FBI has provided advice to organizations to protect themselves from a ransomware attack. The FBI's tips can be found on their website: https://www.fbi.gov/investigate/cyber.

Article provided by contributing author:
Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

HOW *to lose your life savings*

Imagine setting a goal of buying a home. For many, this means sacrificing for years to save enough for the down payment. The buyers find their dream home. They make an offer to purchase the home, the offer is accepted, and the escrow and title order is opened with a title company. The settlement agent sends an email to the buyer similar to this:

From: Officer, Starr sofficer@fntg.com
Sent: Monday, January 1, 1019 2:52 PM CT
To: Doe, John (Buyer) jdoe@yahoo.com
Subject: Document Delivery Notice – Order # 56565656 Ref

Good Afternoon,

Due to the continued rise in wire fraud we now require the attached alert to be signed and returned back to Fidelity National Title Group. Please read it in its entirety to help prevent wire fraud in our transaction.

Please do not wire your closing funds before verbally verifying wiring instructions with an employee of Fidelity National Title Group.

Please do not hesitate to contact Fidelity National Title Group with any questions or concerns.

Thanks you!!!

Starr Officer
Fidelity National Title Group

Here are a few excerpts from the alert:

WIRE FRAUD ALERT
IMPORTANT! YOUR FUNDS MAY BE AT RISK

Please be advised that the wire instructions listed below are the only wire instructions we will send you. This is the only form that should be used to wire funds to us in this transaction. If you receive another email or unsolicited call purporting to alter these instructions, please immediately call us at: 888-934-3354

BANK NAME: Large Bank, N.A.
ADDRESS: 1234 Everywhere, Anytown, USA, 11223
ABA NO: 090909090909
ACCOUNT HOLDER: Fidelity National Title Group
ACCOUNT NO: 987654321 REFERENCE: 1212121212

The transaction progresses. The closing date is only a few days away when the settlement agent sends an estimated closing statement along with the same wire instructions illustrated above.

The settlement agent calls the buyer, at a known trusted phone number to review the wire instructions and confirm he agrees to the amounts reflected on the closing statement. At the end of the conversation, the settlement agent reminds the buyer the wire instructions will never change.

The next morning the buyer receives an email from someone whom he believes is the settlement agent, stating something has gone awry with the Company's bank account and provides him with new wiring instructions. He prints off the new instructions, goes to his bank and initiates a wire.

Two days later the buyer goes to the title company to sign his closing documents. The settlement agent asks him when he will be wiring in his down payment and closing costs.

That is when the buyer's stomach does a few flips and he instantly recalls all of her warnings. He tells her he sent the wire a couple of days ago. She asks him where he sent the funds. He pulled out the wiring instructions shown here:

Fidelity National Title Group
601 Riverside Avenue, Jacksonville, FL 32204
WIRE INSTRUCTIONS

REGIONAL BANK
1122 Central Ave.
Big, USA 98765

ABA Routing No.: 9898989898
For credit to: Fidelity National Title Group
Account No.: 101010101010

THANKS.

The settlement agent confirms they are wrong and shows him the correct ones. She tells the buyer to go to his bank right away and request they recall the wire for fraudulent reasons. He leaves.

This is an all too common story. Buyers all over the country are losing $50,000, $100,000, $500,000 or more, to fraudsters posing as someone in a real estate transaction and providing the buyer with alternate wire instructions. This crime is devastating.

Everyone gets harmed by this scam. Sellers lose the buyer of their home. Real estate agents lose their commission. Lenders and settlement agents cannot close their files. Worst of all, buyers lose their lifesavings!

How can we stop it? By working together. Talk about the scam. Discuss how it works and how it can be prevented. Share this article with anyone and everyone you know who may just be thinking of buying a home.

Tell homebuyers wire fraud is real and they are one of the biggest targets. Give them these four steps to avoid being a victim:

1. **Call, do not 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 is 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:** Call the title company to confirm the funds were received.

By working together and getting the word out we can help stop the hackers from succeeding at this crime.

Article provided by contributing author:
Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration

FRAUD Insights

CLEVER wire fraud schemes

Title Underwriters Agency was processing a sale transaction. The title report was completed and Andrew Wessels, a Title Services Coordinator, was working on clearing title. The payoff demand was ordered and received. A homeowners' association statement had been requested and the property taxes were confirmed. Everything was progressing smoothly.

Andrew received an email from the listing agent asking for a copy of the payoff demand. The email stated the seller was questioning the amount due. Andrew emailed a copy of the payoff to the listing agent.

Later that same day the listing agent responded and included an attachment with an updated payoff amount, and stated this was the correct payoff letter. Andrew thought it was strange since the amount did not change, so he began to look everything over very closely.

The payoff demand was received via eFax®. The seller's mortgage was with ABC Bank. Andrew compared the email address he had on file for the real estate agent to the email he just received and it was a match. He compared the two payoff demands side by side and noticed they did not match.

	CORRECT Wire Instructions	ALTERED Wire Instructions
Bank	ABC Bank	XYZ Bank
Bank Address	1234 Adams Street Anywhere, USA 12345	1234 Adams Street Anywhere, USA 12345
Credit	ABC Mortgage 0987654321	Darius Lesgettham LLC/ Payoff Funding
ABA#	042000314	320825331
Account # / (Reference #)	1234567890 (Account #)	0123456789 (Reference #)

Andrew called the listing agent to confirm his suspicions were correct. The real estate agent neither sent over an updated payoff nor did he request a copy of the original payoff demand. Andrew urged the listing agent to change his email password and have his system scanned, since it appeared his email account had been compromised.

The file successfully closed, Andrew paid over $95,000 to ABC Bank and the satisfaction of mortgage was recorded. Not only did he save his company from a monetary loss, he also avoided a public relations nightmare.

Had Andrew simply sent the payoff funds per the altered demand, the seller would have most likely ended up with derogatory marks on his credit history for failure to make his mortgage payments. The buyer would have had a cloud on his title and the new lender would not be in first lien position. All resulting in unhappy customers and a mess to be cleaned up.

Stephanie Cannon, Closing Services Manager, remitted this story to recognize Andrew Wessels for protecting the Company. Way to go Andrew! We appreciate your efforts and attention to detail.

To assist her staff, Stephanie has established a database where they log payoff lender wire instructions. Now they check this database against new payoff demands before they send out a wire to pay off a mortgage.

MORAL OF THE STORY

Having a confirmation process in place is key to defending against this type of theft. Whether the wire transfer instructions are coming from a trusted party or a new party, it is important to verify any new wiring instructions received.

Article provided by contributing author:
Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration

AMERICAN land title association

The American Land Title Association (ALTA) has short videos targeted for real estate agents and for buyers. The Homeowner Outreach Program (HOP) was designed to help provide information about the benefits of owner's title insurance. They provide more than sixty convenient resources that are informative and provide easy to understand explanations for our customers about the values of title insurance.

For instance, one of the great resources are simple scripts to describe what we do and how we do it, in the simplest of terms — whether you are speaking to your grandmother, a homebuyer or a seasoned real estate agent.

In addition, there are other tools they provide for real estate agents:

- Homebuyer Checklist PowerPoint
- 10 Steps to Buy Your Home with Confidence
- What Every REALTOR® Should Know About Owner's Title Insurance
- 7 Reasons Why Every Homebuyer Needs Owner's Title Insurance

To view all the resources visit: https://www.alta.org/homebuyer/.

Next month we will share with you 10 values of title insurance.