FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

YOUR automobile extended warranty is about to expire

By Lisa A. Tyler
National Escrow Administrator

There has been a steady rise in online scams, and fraudsters are relentless with online attacks. This is why it is important for our readers to stay vigilant and learn how to avoid newly trending scams. Most recently, there has been an increase in calls from fraudsters claiming to be representatives of Apple® or Amazon Support. Since both companies are so widely known, fraudsters are often successful using this tactic. Read more about it in "TRENDING scams."

Settlement agents nationwide have been asked by customers about deed theft. These questions may arise from commercials advertising a service which purports to protect homeowners from becoming a victim of title theft. Here is an example of one such inquiry: *"I am hearing a lot of buzz about how easy it is for thieves to submit a title change on a property that allows them to own the deed so they can take loans out against the property using its equity, and then leaving the problem and debt to the real property owner. Apparently, this is as easy as filling out the forms, paying the county fee, and boom, we no longer own the property. Worse yet, it can take 1-3 months before we would even know, and the bad guy is long gone." Read "DEED theft"* for details about these services.

Historically, escrow losses caused by payoff errors have negatively impacted the industry. They are problematic because of the monetary losses, the additional work created after the file has closed and, at worst, the payoff error may negatively impact a customer's credit rating. In recent years, a new risk of monetary loss relating to payoffs has emerged and it involves wires for payoffs being diverted to cybercriminals. The story titled "EVERYDAY heroes" describes how to protect the Company and borrowers from becoming victims.

In the simplest of terms, ransomware is computer software created by cybercriminals used to infect a computer or server. It encrypts the computer or the server's contents, so it cannot be accessed or used. Once the server is infected, the criminals demand a ransom be paid in exchange for the decryption key. The data is all still on the server, it is simply encrypted preventing the victim from accessing it unless a ransom is paid to restore access. This month's featured article is titled "WHAT is ransomware?"

IN THIS ISSUE

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

volume 17 issue 2
February 2022

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

TRENDING scams

A trending telephone scam is on the horizon and is similar to the extended warranty scams being perpetrated on car owners. In the first version of this scam, fraudsters will leave a voicemail saying there has been some type of issue with your online Amazon purchase — this could include anything from a delay in shipping to a payment processing issue.

In another version of this scam, fraudsters will claim there is suspicious activity on your Apple® iCloud® account, or your Apple® account has been compromised.

In either case, do not return the call and do not contact any phone number that was left on the message. Instead, it is recommended that you disregard and delete the recorded voice message as soon as possible.

Additionally, if you ever receive a call on this subject that you have accidentally answered, do not give out any personal information. Instead, hang up immediately. Through this scam, victims are tricked into giving out personal information, leading to unauthorized credit card purchases and even identity theft.

To prevent becoming a victim of this and other scams, take extra precaution by educating yourself on trending scams so you are alert and diligent in avoiding them. Watch out for some of the most common red flags:

- You never initiated the contact
- They bring up an issue with your account that you are not previously aware of
- They ask for personal information
- They stress urgency or severity of the situation

It is crucial to remain diligent online and on the phone, when receiving unsolicited notifications for financial information.

For additional information on trending scams visit the following web pages:

www.usa.gov/scams-and-frauds

www.fbi.gov/scams-and-safety

DEED theft

The term deed or title theft can be deceiving. With the circulation of inaccurate information, homeowners may believe that thieves can steal title to their home simply by forging a deed and recording it in the county records. Homeowners may also believe that the deed to their home can be stolen and pledged as collateral to obtain a loan and strip all the equity from the home without the true homeowner's knowledge.

Recently, companies have formed a new type of service which offers deed monitoring services where they purport to regularly check the county records to identify any fraudulent activity involving the title to a homeowner's property.

The companies describe a very rare criminal act. Through an elaborate and carefully worded marketing campaign, these companies prey on the fear that someone is going to "steal" a homeowner's deed or title to their home.

These providers charge a monthly or annual service fee and simply notify the homeowner if anything pops up. This all occurs AFTER someone has recorded a forged deed. It does not prevent a scammer fraudulently transferring your title. Their service is not an insurance product and does not fix the fraudulent recording.

Although it is true that anyone can forge someone's name and record documents, such as a deed, it does not make the thief the rightful owner of that property. Here are a few items to consider when contemplating a subscription to this type of service:

- First, there is no way to "lock" a title or deed.
- Second, anyone can monitor the county records at any time by either visiting the county office in person or checking online. In most cases, monitoring the county records online is free of charge and some counties offer an automated option.

[Continued on pg 3]

STOP

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

[DEED theft — continued]

- Third, this type of service is not a replacement for title insurance. A home title lock cannot replace title insurance. Their services do not help cover any financial burden of title issues or mortgage fraud.
- Last, even if a forged deed is recorded in the county — the homeowner does still own their home. Even if the fraudster does take out a loan secured by the stolen property the homeowner is not the victim; the lender is, since the scammer never legally owned the property a lender has no legal claim and would be unable to foreclose when the fraudster fails to repay the loan.

Lenders protect themselves by requiring the borrower to purchase a lender's title policy as a part of the loan closing process. When a lender suffers a loss due to a forgery in the chain of title, they file a claim under their title insurance policy. This is why it is important to understand these title lock services are nothing like title insurance.

Title insurance is purchased once, at the time a buyer purchases the property, and it provides the insured or their heirs protection against fraud or forgery that occurred prior to the time the insured purchased the property. Title insurance companies protect the integrity of the county records in this country since they examine the chain of title for any potential discrepancies. It is the best way for homebuyers to protect their investment.

MORAL OF THE STORY

Always purchase title insurance when purchasing real property. Learn how to monitor the county records for free. If a forged document is recorded, affecting title to your home, notify the county and law enforcement.

If the forged document is a mortgage or deed of trust, contact the beneficiary to notify them it is a forgery and ask them to release their lien. If you prefer, contact an attorney.

Finally, keep in mind someone cannot simply steal your property out from under you by forging your name. Although it may be a nuisance to clear it up, it is still your home.

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

EVERYDAY *heroes*

Sheri Pickard and Brianna Ray, with Fidelity National Title of California, work in the Roseville Branch. They were working on a refinance transaction. They ordered and received the payoff demand for the borrowers' existing loan. They emailed a copy to the loan officer.

Shortly thereafter, they received an email from the loan officer which included an updated payoff demand. His email said:

"Please do not use the previously submitted payoff statement. I have attached an amended payoff statement to this email. Can you please acknowledge receipt?"

Sheri and Brianna replied:

"Looks like the figures are the same as the one we have. Is there something different that I am not seeing? Let me know and WE can order an update"

Next, they compared the two demands side-by-side. They noticed the amount due was still $804,027.39, but the wire instructions had been changed. They compared the known email address of the loan broker against the email they just received and noticed it had an additional "p" in it. They immediately stopped all email communication with the fraudsters.

Sheri and Brianna called the loan officer and borrower at a known, trusted phone number to notify them that someone's email account had been compromised and explained all communications going forward must be by phone. They reported the incident to wirefraud@fnf.com and followed their instructions.

The hackers continued to send emails to Sheri and Brianna asking for a status. They noticed the emails did not contain any hints of a fraudster, such as broken English or improper grammar. They did not respond and deleted the incoming emails.

Sheri and Brianna were concerned the fraudster may have sent altered wire instructions to the funding lender, so they contacted the funding lender to verbally confirm the company's wire instructions.

[Continued on pg 4]

[EVERYDAY heroes — continued]

Last, they called the payoff lender at a known, trusted number — instead of the number appearing on the demand — to confirm their wire instructions. The transaction successfully closed, and all funds were wired to the intended recipient. Great Job Sheri and Brianna! For their incredible teamwork and stopping the hackers in their tracks, they are splitting the $1,500 reward.

Best Practices
In an effort to prevent losses, it is considered an industry standard to rely only on payoff demands ordered by and addressed to the settlement agent's company. A payoff statement addressed to the settlement agent's company represents a binding agreement in case of a shortage, misappropriation or claim if all of the instructions set forth in that statement are followed.

Some states even provide statutory protections for an entitled person, such as a settlement agent who orders the payoff statement and remits payment pursuant to said demand. The protections allow a settlement agent to rely on the statement as accurate and ensure release of lien will be filed upon receipt of the payment.

This is why payoffs ordered and provided by a mortgage broker, real estate agent or borrower are not relied on. The rise in wire fraud has only demonstrated how important this practice is. Payoffs are the most recent target of cybercriminals. Fortunately, our Company's escrow staff has everyday heroes just like Sheri and Brianna who understand all the risks surrounding payoff demands.

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

WHAT *is ransomware?*

Ransomware is a computer program or malware created by cybercriminals. It is used to infect a computer or server. It is often designed to spread across a network and target database and file servers; thus, it can quickly paralyze an entire organization. It is a form of extortion and a growing threat. Ransomware generates billions of dollars for criminals and their syndicates.

Ransomware is not new. It has existed for more than two decades. Since many online criminals succeed in obtaining the ransom they demand, they find this type of cybercrime is more and more appealing.

Criminals always go where the money is. They go after big targets such as businesses and municipalities in hope of earning more. They often use the same handful of techniques and common tactics, including:

» Deploying wide-scale phishing and targeted spear-phishing campaigns that induce victims to download a malicious file or go to a malicious site

» Exploiting remote desktop protocol endpoints and software vulnerabilities

» Deploying "drive-by" malware attacks that host malicious code on legitimate websites

Although ransomware is pretty simple and straightforward, recovering from an attack is complicated. Knowing and understanding what types of ransomware exist — along with the preventative measures — goes a long way toward helping protect yourself from becoming a victim of ransomware. This will all be discussed in the coming months.

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