



By Lisa A. Tyler
National Escrow Administrator

The seller came in person to the Chicago Title office to pick up his proceeds check. He was asked for identification; he said he did not have it with him. Chicago Title would not give him his check without proper I.D., so he left. This concerned the escrow officer and prompted her to look closer at her file to ensure the seller really was the owner of the property. Unfortunately, her suspicions were correct. She successfully tracked down the real property owner and confirmed he did not sell his rental property. Read "THE jig was up" to find out how the imposter almost succeeded and find out how this could have been prevented.

Some things you just cannot make up! Read "STING operation" to learn how Alamo Title worked with a local detective to uncover

a crime; the perpetrator was arrested when she showed up to sign closing documents at a competitor title company.

Criminal organizations are realizing more benefits of ransomware attacks from increased revenue streams of these syndicates. Simultaneously, ransomware variants have grown. Reports from government agencies indicate there are as many as 100 variants. Many variations have been used over and over again. Some variants may be more harmful than others, but they all demand a ransom. In the February 2022 issue, we described ransomware as a program that encrypts data found on a computer and/or a network. This is referred to as a crypto malware and is the most commonly used definition of ransomware. Read about other types in "RANSOMWARE types."

IN THIS ISSUE



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



volume 17 issue 6
June 2022

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator



THE jig was up

Courtney Duke, Escrow Officer with Chicago Title, conducted a search online and found the real property owner of the rental property. She called him immediately to verify if he was selling his property.

The owner was shocked. He knew nothing about the sale of his rental property. He asked her what he could have done to protect himself from being a victim. Courtney explained the best way is to have the tax bill go to his mailing address.

The mailing address notifies a title company the property is not owner occupied and gives the title company a method to contact him and confirm he was selling his property. Had his address been correct, she would have sent him a notice at the opening of escrow similar to this:

Dear Owner(s)

Thank you for choosing Chicago Title Company. We are delighted to be of service to you. We are in the process of preparing a preliminary report or title commitment for the sale of the property listed above.

Should you have any questions or be unaware of this transaction, please contact the undersigned immediately.

This simple, but effective, step would have prevented the imposter (who turned out to be the tenant of the property) from almost succeeding.

SPOILER ALERT! The escrow officer was able to successfully unwind this deal. However, this could have all been avoided. "How?" you ask? We will start at the beginning.

The buyer was an investor who simply knocked on the door of the property and negotiated the sale with the person who answered. The investor was led to believe the man who answered the door was the owner of the property.

The buyer wrote up an offer and the seller accepted it; escrow was opened. The investor was a cash purchaser, so the sale was scheduled for a quick close. As soon as escrow had everything she needed, they were ready to close.

The seller was a busy man, so the escrow officer booked the signing with an approved signing agent. The signer gave the notary the runaround having her go to a couple of different work locations to track him down.

The notary finally caught up with the seller at a gas station where he claimed to work. When she asked him for his driver's license, he told her he was just dropped off and did not have it with him.

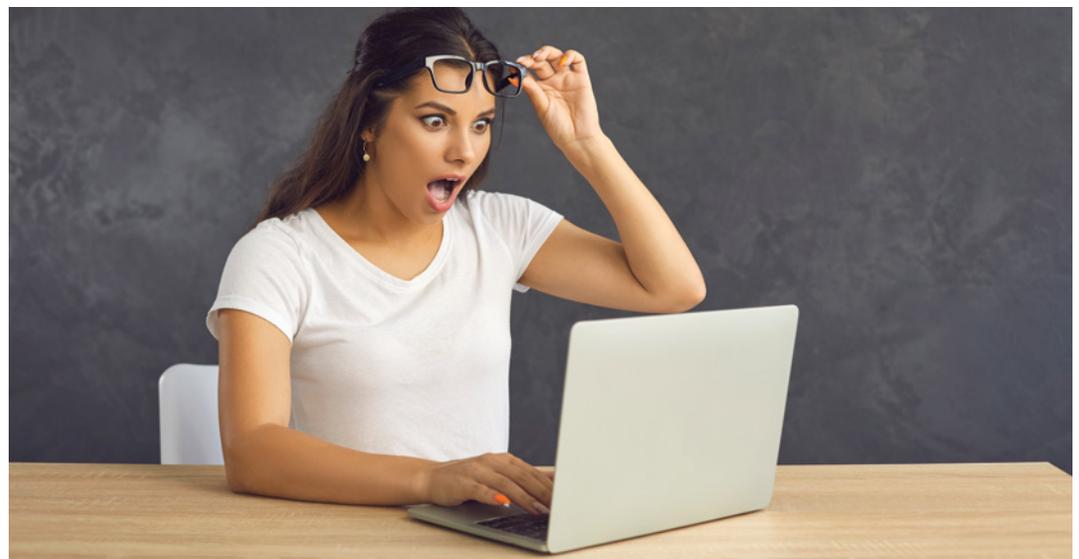
The seller convinced the notary to let him sign. He said he would send her a picture of his I.D. later; she agreed. He signed her journal and the deed, and she left.

The notary placed her notarial seal on the deed and delivered it to Chicago Title. The seller never sent the notary his I.D. She never told the escrow officer what occurred, and the deal closed.

When the seller was unable to present I.D. to pick up his proceeds check, Courtney discovered the seller was an imposter. She immediately reached out to National Escrow Administration. The escrow administrator gave Courtney directions on how to unwind the deal. Courtney immediately jumped into action.

First, Courtney contacted the payoff lender, explained what happened and asked them to send the payoff back. Next, she filed an escrow loss.

Courtney then sent the check register to her corporate escrow administrator who contacted the taxing authorities and utility companies to explain what occurred and request a refund. All of the payees were cooperative in returning the payments.



[Continued on pg 3]



STOP

TELL US HOW YOU
**STOPPED
FRAUD**

settlement@fnf.com or
949.622.4425

[THE jig was up - continued]

After that, Courtney advised the buyer the deal was being unwound and explained why. She wanted to be sure the investor knew as soon as possible so he did not incur additional costs by beginning the demolition of the property.

Finally, she contacted the buyer's hard money lender and advised them. She let the lender know she would need a reconveyance in exchange for a return of the loan proceeds.

Why would the notary do what she did? She did not feel safe. There were a lot of other men at the gas station who were making her feel uncomfortable. She was focused on getting his signature and leaving as soon as possible.

The safety of our employees and approved notaries is of utmost importance to us. No one faults the notary for acting quickly to get out of an unsafe situation. However, the notary failed to follow Company policy in allowing the purported seller to sign without requiring I.D.

Thus, it was the notary's obligation to immediately report to the escrow officer that the purported seller had not produced his I.D. at the signing. Had she explained to the escrow officer what occurred, the escrow officer would have never closed without ensuring the seller was properly identified. It was a very unfortunate, but critical, lapse in judgment.

As a result of the notary's lapse in sound judgement, she will never be authorized to conduct signings on behalf of the Company in the future.

STING operation

Amanda Clower, Escrow Operations Director for Alamo Title in Grapevine, Texas, received a contract on a small, dilapidated trailer that was basically being treated as vacant land, selling for only \$15,000. She personally knew the buyer for more than eight years; she had a transaction coordinator that would help find buyers/sellers and then handle most of the communication.

Amanda spoke to the seller, utilizing the contact information (phone number and email address) provided on the contract. It seemed like a slam dunk. Title came back clear except for delinquent taxes, and those were being paid through closing. The transaction closed and funded.

Fast forward to a month after closing when Amanda received a call from the seller saying she went to pay her delinquent taxes and the tax office told her the property was sold. The seller stated Amanda would be receiving a call from a Johnson County detective.

Based on the call it seemed the seller realized she could sell her property for more than \$15,000 and was having seller's remorse. NOPE. That was not the case!

Amanda received a voicemail from a Johnson County detective. They played phone tag throughout the day. They finally connected around 7:00 p.m. and talked for FOUR HOURS!

It turns out the seller was a fraudster who had presented fake identification, and the actual owner was in the hospital having surgery at the time of the closing. After peeling back layers and discussing the situation, Amanda and the detective were able to unfold two other transactions, currently open in the office, that might also be fraudulent.

Courtney did everything in her direct power to follow Company policy. She booked the signing with an approved signing agent. She took added precautions by requiring I.D. before giving the seller the proceeds check.

Courtney knows the Company policy regarding absentee owners. Had the owner used the correct mailing address (instead of the property address) on his tax bill, she would have sent him a notice as soon as escrow was opened.

The deal took a twist. The "seller" kept calling Courtney wanting to know where his proceeds were. She told him she could not give it to him since he never presented proper I.D. — either to the notary or to her in the office.

The "seller" was so bold he did send over a copy of his I.D. His last name was the same as the real owner of the property, but his first name was different. Fortunately, he did not call back — indicating he knew the jig was up.

Because Courtney immediately jumped into action and was able to unwind the deal by getting all the disbursements back, she was recognized for her efforts. The Company has rewarded her with \$1,500 for following the Company policies.

Article provided by contributing author:

Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration



The detective set up a time to get a statement from the buyer (who closed and was insured), to clear any ties to the fraud. The meeting was successful, as the buyer was not involved in the fraud.

During the meeting, they called Amanda on speaker phone to discuss the other two files currently in escrow. It was determined the other two transactions were also fraudulent. As a result, Amanda and her team resigned as escrow agent and refused to close and insure either transaction.

According to the detective, real estate fraud was only the beginning; the woman perpetrating the fraud had committed

[Continued on pg 4]

[STING operation – continued]

identity theft, forgery and elder abuse. She even snapped inappropriate pictures of the true owner to use as blackmail against the property owner.

The fraudulent grantee on two deeds took pictures that were intended to show a relationship with the prior owner. It was an attempt to claim they were in love, and the real owner wanted her to have the properties. The prior owner passed away in November 2021; the deeds were filed in January 2022. These inappropriate pictures were taken as his health was failing.

During the next few weeks, a real estate agent listed the two properties. The listings were withdrawn after three days when the

detective connected with the real estate agent and filled her in on the situation.

That did not stop the fraudster, she negotiated a sale to a common investor in the area. Amanda connected the detective with the escrow officer and manager at the investor's office.

This is where it gets good. The detective showed up MID-CLOSING and arrested her! She is being held on a \$450,000 bond. Additional charges against her are forthcoming.

RANSOMWARE types

Let us discuss some of the other elements and methods of ransomware.

Malware which contains lockers, locks a computer or device's operating system so the user cannot access it (in addition to encrypting the data on it). It is commonly deployed on Android™-based systems.

Scareware is a type of software which behaves like an antivirus shield or cleaning program. It may enable pop-ups or other alerts to appear claiming to have found an issue and demand money to clear it up. In some cases, it may include a locker.

Syndicates use doxware, leakware or extortionware to threaten their victims to pay the ransom demanded or they will publish all the stolen data publicly. They target entities who deal in highly sensitive data (such as law firms) and would likely pay the ransom rather than suffer the public relations issues if the data was published publicly.

Creators sell user-friendly ransomware-as-a-service RaaS kits on the Dark Web or may lease their malware to other criminals in exchange for a percentage of any ransom the purchaser receives for launching a successful attack. Ransomware-as-a-service has

resulted in an increase in ransomware attacks since this service lowers the technical expertise needed to carry out an attack.

Even Apple's Macintosh® Operating System was successfully hacked through an app called Transmission in 2016. The malicious software encrypted the victim's computer.

Mobile devices are a target too. The most common way into a mobile device is through an application which enables a message stating the device has been locked due to illegal activity. It is often just Scareware but may include a locker.

As you can see, no one is immune to these types of attacks. However, being aware of these types of attacks, using virus scanners and email content filters is the best defense.

Next month, we will share tips for those who are attacked.

Article provided by contributing author:

Diana Hoffman, Corporate Escrow Administrator
Fidelity National Title Group
National Escrow Administration

