FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

ARIZONA is being targeted

By Lisa A. Tyler
National Escrow Administrator

In Arizona, the title department works with all operations and brands across the state as a central processing facility. The Company has very talented title professionals searching titles and ensuring the Company's underwriting policies are adhered to. They work closely with escrow to successfully close real estate transactions. Recently, Chris Ziegler, Chief Title Officer, gathered examples of a trending fraud in Arizona. His close attention to detail has resulted in the Company halting the closings of eight transactions within just a few months, preventing millions of dollars in potential claims. Read "PROPERTY owners under attack" for all the details.

Offices are asked on a regular basis to take money orders. Money orders are supposed to be a more trusted method of payment than a personal check because the purchaser of a money order must present the cash and pre-pay for the amount shown on the face of the instrument at the time of purchase. Money orders can be purchased at United States Postal Service offices (USPS), banks and other non-bank issuers. In general, money orders are not issued for more than $1,000. Unfortunately, money orders are also the target of fraudsters who may create fake ones. The Fidelity Family of Companies does accept money orders but only if there is sufficient time for the money order to be collected by the bank and its issuer. Read the story titled "MONEY orders" to find out how to process money orders for closing.

Ransomware affects us all, including the settlement and title industry. The September 2019 issue of *Fraud Insights* included an article about the attack on the city of Baltimore and how it impacted their recorder's office. The city and most of the services they provide were disabled for weeks while they worked with outside experts to restore their systems. This meant real estate closings were delayed. Transactions ready to close were delayed since the deed and/or deed of trust or mortgage could not be recorded. New transactions were delayed since the chain of title could not be examined. Learn how ransomware attacks continue to impact the title industry, and how you can ready your business to mitigate ransomware risks, in the article titled "RANSOMWARE attacks pose threats to the industry."

IN THIS ISSUE

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

volume 17 issue 10
October 2022

FRAUD Insights

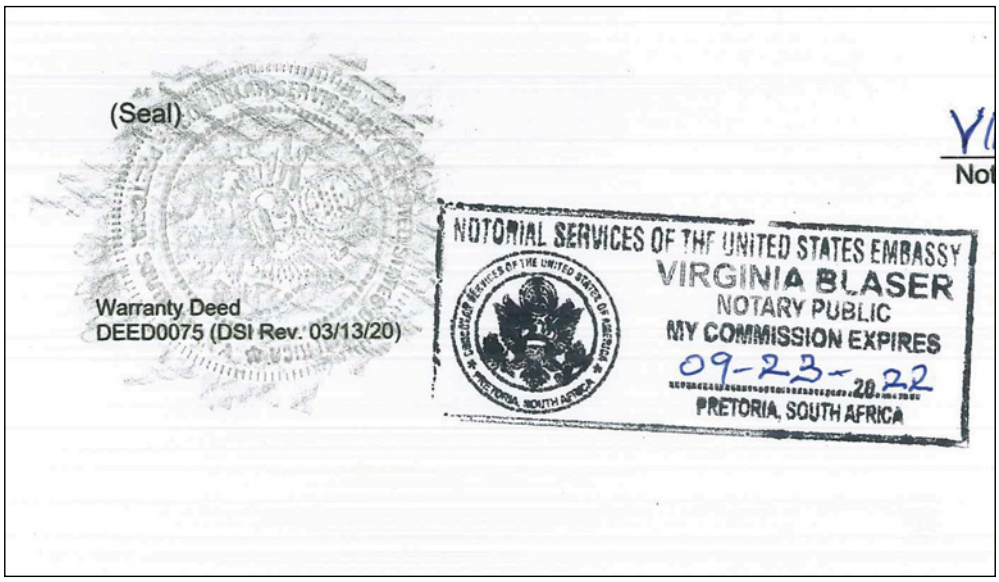
Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

PROPERTY owners under attack

Eight sale transactions were opened at different closing locations throughout the state of Arizona, so none of the offices knew of the other transactions being processed. The documents were supposedly signed in South Africa in front of a duly authorized notary.

Luckily, the returned signed documents were reviewed thoroughly by Chief Title Officer Chris Ziegler, with the Southwest Title Group. He noticed "notorial" was misspelled in the notary's seal. Here is what the notary seal looked like. Notice the spelling of notarial with an "O" instead of an "A":



Chris then performed an internet search of the notary's name, Virginia Blaser, which confirmed the documents were forged, since the notary was no longer in South Africa. This is what he found online:

> *A FAREWELL MESSAGE FROM U.S. CONSUL GENERAL IN CAPE TOWN VIRIGINA BLASER*
>
> *OCTOBER 29, 2020*
>
> *It has been an honor and privilege to serve both the United States and South Africa in this special role. I am humbled by the many wonderful friendships offered to me, thankful for the many chances to grow as a diplomat and as a person during this posting and comforted by the enduring presence the Cape now has in my heart.*
>
> *Signing off, one last time, as the U.S. Consul General to Cape Town… a fond farewell to you all. May we meet again…*
>
> *U.S. Consul General in Cape Town*
> *Virginia Blaser*

Then he found this announcement:

> *We're excited to announce that U.S. Consul General Virginia Blaser is headed to East London next week! ... · Sep 12, 2020*

The first deed reviewed by Chris was supposedly notarized on March 23, 2022, in South Africa, by U.S. Consul General Blaser. Clearly it was a forgery since the notary was no longer located in South Africa.

All of the property files Chris reviewed were non-owner-occupied vacant lots. The sellers were all in South Africa. The properties were all listed for sale by licensed real estate agents.

The sellers reached out to the real estate agents via email to list the lots for sale. The real estate agents only method of communication with the sellers was by email. They never met the seller by any other means. The lots were priced competitively for a quick sale attracting investors who had cash in hand to purchase the lots resulting in a quick escrow.

Chris immediately notified underwriting of his findings. Underwriting sent out communications to all of the Company's operations which said:

> URGENT! Anytime the property is vacant or non-owner occupied send a notice out to the owner immediately. Although there are other ways to identify this scam, the best defense is to reach out directly to the owner at the address their tax bill is sent to. In addition, this alerts them so they can keep tabs on their property.

Real estate agents and title companies can take steps to prevent this crime from happening. One way is to compare the mailing address provided by the seller to the address on the tax bill. If the tax bill address is different than the seller provided mailing address, send a letter to the address on the tax bill notifying the seller of the pending transaction.

[Continued on pg 3]

STOP

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

At our Company we send a notice via overnight delivery that reads:

Notice of Pending Real Estate Transaction

Date:

To: Record Owner @ address on tax bill

Re: Property Address Order Number:

Dear Owner(s)

Thank you for choosing [insert Company name]. We are delighted to be of service to you. We are in the process of preparing a [insert preliminary report or title commitment] for the [insert sale or loan] of the properly listed above. Should you have any questions or be unaware of this transaction, please contact the undersigned immediately.

Sincerely,
Escrow Officer
Title Officer
Settlement Agent

While waiting for the owner to reply, set up a virtual meeting. Ask the potential seller simple questions such as:

- ☐ When did they acquire the property?
  - ○ For how much?
- ☐ Why are they selling?
- ☐ Where do they reside?
- ☐ Why is the tax bill sent to a different address?
  - ○ What is that address?
- ☐ Who did they buy the property from?
- ☐ Ask them to show you I.D. by having them hold it up to the camera

These are only suggested questions. Other questions or actions may be appropriate depending on the specifics of the transaction.

The intent of the questions is not necessarily to require or obtain perfectly accurate answers. The intent is to determine whether or not the sellers are the legitimate owners.

The true owner may not remember exact details that could be read from a recorded instrument, though they will likely remember context or be able to provide information that a fraudster with access to public records would not know.

These questions should only be asked when speaking to the seller on the phone or virtually. The questions should never be emailed or provided in advance, as that would give an imposter the opportunity to research the answers.

These imposters are part of criminal syndicates. They do not work alone, are very smart and know how to use the internet to find the answers. If the seller declines to talk by phone or virtually, or gives an excuse why they cannot, proceed with caution.

This scam is being perpetrated all over the country. Pay close attention to the spelling of the seller's name on all documents, including purchase and sale contracts, a passport or a driver's license. Be sure to send a letter to the property owner at the address where the tax bill is sent. This is the quickest and best way to avoid becoming a victim.

Many other operations have identified transactions with the same or similar red flags; the hero in this story is Chief Title Officer Chris Ziegler, who was rewarded $1,500. Thank you, Chris!

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

MONEY orders

Money orders issued by the United States Postal Service (USPS) are considered good funds the day after they have been deposited, unless they are fraudulent. Settlement agents who receive a USPS issued money order must review each instrument carefully. The USPS has provided these steps for verifying a money order:

Before accepting a money order, make sure it's real. There are several key things to look at to spot a counterfeit money order.

Examine the Paper
Real USPS money orders have specific marks and designs to prevent fraud. If you hold the money order up to the light, you should see:

- » Watermarks of Ben Franklin on the left side repeat top to bottom (circle 1 on image).
- » On the right of the Franklin watermark, a vertical, multicolored thread with the letters "USPS" weaves in and out of the paper (circle 2 on image).

Check the Dollar Amounts

- » If the dollar amount is discolored, it may have been erased, indicating fraud (circle 3 on image).
- » Make sure the dollar amount is imprinted twice (circle 4 on image).
- » See if the dollar value is too large.
  - Domestic money orders cannot be more than $1,000.
  - International money orders cannot be more than $700 ($500 for El Salvador or Guyana).

Suspect a Fake?

- » If you suspect fraud, call the U.S. Postal Inspection Service at 1.877.876.2455.

[Continued on pg 4]

[MONEY orders — continued]

If it appears to be valid, then check the status of the money order by calling the money order verification system at 1.866.459.7822. Keep in mind, the USPS can only verify a money order 48 hours after it has been issued. This is the safest form of money order to accept.

Money orders issued by anyone else should be verified by contacting the issuer to verify it is valid and then wait 14 business banking days before disbursing against it, to ensure it has been unconditionally collected. If the money order represents closing funds, it may be necessary for the customer to remit the funds by wire transfer instead.

RANSOMWARE attacks pose threats to the industry

Even when title companies are not the direct targets of ransomware, these attacks can have significant downstream impacts on our industry. Last year, Cloudstar — a provider of IT security solutions and cloud hosting services — was one of many companies that fell victim to a ransomware attack.

Many of Cloudstar's customers were settlement agents and title companies, who used Cloudstar's encrypted cloud storage service to host their production systems and data. When the ransomware attack took Cloudstar's systems offline, the settlement agents and title companies had no ability to access their production systems or data. This caused a disruption to their business by delaying closings.

Other providers, such as SoftPro, quickly offered their expertise, products and services to the settlement agents and title companies affected by the attack, which helped to minimize the disruption to the industry. Many Cloudstar customers, however, had to start from the beginning and re-build their data because it was all encrypted in Cloudstar's systems, which were inaccessible with no ETA on restoration.

More recently, Suffolk County, New York, was struck last month by a ransomware attack that targeted many of the county's computer systems, including the systems that house the county's legal and land records.

Without the ability to access these records, the title industry could not conduct title searches, creating delays in real estate transactions and closings. Three weeks after the attack, Suffolk County announced a plan to restore its systems, with priority given to restoration of its emergency call systems.

The criminals behind these attacks are becoming smarter and, since so many have been successful, they have attracted more perpetrators — resulting in more attacks. The element of cyber espionage made the ransomware risk even greater than before. In the Suffolk County attack, the hackers claimed to have extracted more than four terabytes of data (four terabytes is 4,000,000,000,000 bytes of data or equivalent to 2,000 hours worth of movies) and threatened to publish that data if the county was unwilling to communicate with them.

These attacks demonstrate how a single attack within the supply chain or business process can have a large impact on one industry. The title industry must account for these risks when assessing vendors, as well as when developing business resiliency and continuity plans and processes.

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