FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

REMOTE notarization

By Lisa A. Tyler
National Escrow Administrator

Shannon Havens, Escrow Officer in Whitefish, Montana, was the latest target of a fraudster behind a Business Email Compromise (BEC) scam. While wrapping up a transaction for another successful closing, the fraudster stepped in to perpetrate his crime. He was not successful because Shannon identified all the red flags and stopped the scammer right in his tracks. Read "IT could happen to you" for all the details.

Leanne Shufelt, Branch Manager, Assistant Vice President of Fidelity National Title of Florida, Inc., wrote to us saying, "You always hear about wire fraud and Susan West has been excellent in keeping us informed at the weekly conference calls our managers have with us, but you always think this will never happen to me. Well let me tell you it does." Read "LAST minute change" for all the details.

The death certificate says he died of a heart attack and other complications; he was just 64 years old. One year earlier he purchased a condo in Oxnard, California, to live out his remaining years. He obtained a new loan to purchase the condo which was insured by the Department of Veteran Affairs. He proudly served his country in the Vietnam War as a sergeant in the United States Marine Corps and had two sons. If only he could tell us in person what happened in the last years of his life. "MARY a. richman" reveals the story the documents tell us.

In 2011, the State of Virginia passed a change to their notary laws. The change allows Virginia notaries to notarize documents electronically. There are many states that have provisions in their statutes for electronic notarization, but this one also allows the signer to appear in front of the notary electronically. The signer can be anywhere in the world and a Virginia notary can notarize the documents by using audio-visual conference technology. Find out more about it in the story entitled "WEBCAM notarization."

IN THIS ISSUE

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

volume 12 issue 11
November 2017

FRAUD Insights

IT could happen to you

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

Shannon Havens, Escrow Officer in Whitefish, Montana, received a few emails from someone who was impersonating her seller. As she reviewed them she was able to identify the following red flags she had previously read about in *Fraud Insights:*

- The seller sent her an email with new wire instructions for his proceeds.
- The email had poor punctuation, grammar and run on sentences, including "advise" spelled as "advice."
- The account name was not the name of the seller in her transaction.
- The seller indicated the bank account was under review and needed to change wire instructions at the last minute.
- The Canadian seller directed her to wire his proceeds to a U.S. Bank in South Carolina.

Other than the last minute emails, the transaction was seemingly normal. Shannon spoke to the seller and his real estate agent by phone and kept in regular communication with them by email. The seller was very responsive to any of her requests and followed her instructions in a timely manner.

A week prior to the scheduled closing date, the seller sent her wire instructions for his proceeds, which she confirmed with him on the phone. On the day the transaction was scheduled to close she received the following correspondence:

> "Hi, Shannon, what time we expect to be recorded and when should I expect the Disbursement of Sales proceeds."

Shannon replied she did not know the exact time she would be able to record and would let him know as soon as she received the buyer's closing funds.

> "You should email me once you have the buyer's funds, I have a pending transaction on my account which I thought would have cleared before now and the account is presently under review. I am not sure if the problem will be resolve today, Can I provide a trust account for the wire of sales proceeds to enhance a smooth transaction. Please advice."

Shannon stated that would be fine, but asked him to confirm he did not want her to wire his proceeds to the account he previously supplied.

> "I don't want it wired to the RBC account again, the account is still under review. I will forward the new account details shortly."

The hair on the back of Shannon's neck stood up as she had a feeling of what was going on. Next, she received an email with different wire instructions. The account name on the instructions was for an LLC with further instructions to reference the seller's name.

The buyer's funds came in and the transaction closed with no other hiccups. When it came time to disburse funds, Shannon picked up the phone and called the seller at a known phone number and left him a voicemail to call her right away.

She also emailed the seller's real estate agent to let her know she had received an email from the purported seller with new wiring instructions for a different account. She informed the agent she would not release the wire until she was able to speak with the seller direct to verify his wire instructions. Not five minutes later the seller replied to her email.

> "I got your calls and voice note. I can't receive or call out for now because I am in a conference. You should go ahead with the wire of my sales proceeds to the new account details provided earlier."

The real estate agent called Shannon to find out if the transaction was recorded. Shannon asked if she received her email. The real estate agent said no, she had not received any emails from Shannon. Shannon did confirm the file was recorded and they hung up the phone.

As soon as their call ended, Shannon received an email from the real estate agent.

> "You should go ahead with the wire, He informed me about the changing of account and also said he will be in a conference."

It was signed exactly as she would sign all her emails. Shannon felt a little suspicious and wondered why the real estate agent did not tell her this over the phone.

Shannon replied stating she had to talk to the seller. The agent replied.

> "Yes I spoke with him earlier today, He can't pick up if you call him right now, He should be in a conference. You can go ahead with the wire, I am sure he will give you a call later."

Shannon called the real estate agent back to confirm whether she had been emailing her. The real estate agent confirmed she did not. Shannon stopped communicating via email with everyone in the transaction and reported the incident by hitting the "Report Phishing" button on her Microsoft® Outlook® toolbar.

The seller called her back and confirmed he did not send her revised wire instruction. Shannon explained the situation to him, and he was very grateful she did not act on the revised instructions. Turns out, the real estate agent's email had been compromised. The agent found out any email from her would automatically defer to the hacker.

Everyone — including the seller, real estate agent and Shannon's colleagues — was amazed by how tricky the fraudsters were. The emails supposedly came from two different people, but in reality it was the one hacker responding. Shannon said, "It made me sick to think what could have happened. For this, I am very grateful to Fidelity National Title to advise me of this scheme and constantly remind me to VERIFY WIRE INSTRUCTIONS!"

We are grateful to you Shannon for identifying the scam, and taking the steps necessary to protect and save the Company from a $210,818.60 loss. She is being rewarded $1,500.

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

LAST *minute change*

Leanne Shufelt, Branch Manager, Assistant Vice President of Fidelity National Title of Florida, Inc., had a closing at 10:00 a.m. The buyer was obtaining a new loan to purchase the home. The buyer had not yet wired in the closing funds so she could not disburse the proceeds to the sellers.

Leanne made arrangements with the sellers at the closing to pick up the proceeds check later that day. The sellers indicated they were going to use the funds to pay off the home equity loan on their primary residence with Navy Federal Credit Union®.

Within 10 minutes after the buyer and sellers left her office she received the following email,

> "Hi Leanne,
>
> Thank you so much for assisting with the closing. But regarding our disbursement can you assist with changing disbursing to our Sun Trust bank account. Please note that this is very important. Kindly get back to me so I can send you wire instructions.
>
> Thanks
>
> Mr. and Mrs. Marty Graw"

Leanne was confused. She just spoke to the sellers about the fact they bank at Navy Federal Credit Union. They never mentioned anything about SunTrust being their bank. Plus, Marty was very specific about picking up his check.

Leanne replied to the email explaining she would not be able to accommodate his request unless he came back to her office to complete and sign her wire out instructions, and provide a copy of a voided check from his SunTrust account. She never received a reply to her email and Marty confirmed he never sent that email.

Leanne was confident she knew the email was a scam. She spoke in detail to the sellers about when their proceeds would be available, she knew their plans for the money and where they banked.

Leanne was particularly unnerved about the fact the hacker seemed to know exactly when the closing was scheduled and when the sellers had left her office. It is scary how savvy the hackers were.

The proceeds were in excess of $355,000. Had Leanne not paid attention to the details, she could have fallen for the scheme. Instead, she is being rewarded $1,500 which far outweighs the loss the Company could have suffered.

MARY *a. richman*

Kari Allegro, Escrow Officer for Ticor Title with the Woodland Hills office in California, opened a sale transaction. The sellers, Mary A. Richman and a company we will call "RE Holdings," were selling a condo for $335,000. She sent the order to her title department, where her co-workers did a search and found two uninsured deeds in the chain of title.

In April of 2011, Darren Deeds, a Vietnam Veteran, purchased the condo. On November 29, 2012, a deed was recorded transferring the property to Darren Deeds, Mary A. Richman and RE Holdings. On February 12, 2016, another deed was recorded where Deeds transferred his interest in the property to Richman.

These deeds were cause for alarm because neither of them were recorded as a part of an insured transaction. They were also held onto for a long time after they were executed. The first deed was executed on February 28, 2012 and the second on March 16, 2012.

Even more concerning was the fact Darren passed away on March 22, 2012. Kari had no way of confirming with Darren if he did, in fact, sign the deeds, and she was concerned whether he was of sound mind or not. She dug in further.

Kari pulled a copy of the deed of trust signed by Darren when he purchased the property in 2011. She compared his signature to the two deeds and discovered they did not match. In May 2012, a deed of trust dated September 12, 2011, was recorded against the property — also not part of an insured transaction. Kari compared the signature on this document and was unable to confirm or deny whether it was Darren's signature. Both of these loans were now in default.

As if the uninsured deeds, deceased former owner and mismatched signatures were not enough to stop the transaction dead in its tracks, Kari searched the California Secretary of State's website for a status for RE Holdings, but the search came back with no legal entities under that name.

Kari asked the listing agent to obtain copies of the organizational documents and noticed a man named Tom Morrow signed the purchase and sale agreement on behalf of RE Holdings. According to the Statement of Information provided by Richman, her husband's name was Tom Morrow. Perhaps Richman really did marry a rich man.

Was it a case of elder abuse? We will probably never know. Kari never spoke to Richman, but Richman did indicate to the listing agent that Darren was her uncle. Kari shared her concerns with her Chief Title Administrator, Chris Akin, who chose not to insure the sale, since he could not be certain the deeds in the chain of title were validly executed.

Chris submitted this story for nomination so Kari would receive her well-deserved reward of $1,500. We agree with Chris. Thank you for your hard work Kari.

FRAUD Insights

WEBCAM notarization

When a webcam is used to witness a signature, the document is uploaded into a secure online system the notary provides and ensures it is in compliance with their state law. Both the signer and the notary log in and view the document simultaneously on their respective computer monitors.

The signer electronically signs the document by clicking a "Sign Here" button or similar button, and the signer verbally acknowledges his intent to sign the document to the notary.

Next, the notary countersigns the document by clicking a similar "Notarize Here" button. When the notary clicks the button, the notary's commission information, including the notary's full name, date of commission expiration and commission number, is affixed to the document along with the notary's electronic signature.

The electronic signature of the notary and the signer would appear as a "script font," much like this example: *John Q. Doe*.

The law requires both the signer's signature and the notary's signature and commission information be affixed to the electronic document using tamper-evident technology. Any attempt to modify the document after notarization would be detectable to anyone viewing the document. This tamper-evident technology would prevent fraudulent alteration of the document.

The notary must maintain a copy of the recording of the video and audio conference and a notation of the type of any other identification used for five years.

To ensure remote electronic signing is more reliable and resistant to fraud and manipulation than traditional notarization, the remote notary must confirm the identity of the signer by using one of three methods:

1. Personal knowledge;
2. Reliance on prior in-person identity proofing by a trusted third party which is confirmed electronically with independent database checks; or,
3. Reliance on the signer's use of a digital certificate authenticated either by a biometric or a high-security Personal Identity Verification (PIV) card (used by government employees and contractors).

In October, 2015, Montana began permitting its notaries to perform webcam notarizations under specifically defined circumstances. Florida also authorized webcam notarizations, but is limiting the practice to certain law enforcement and correctional officers who are authorized to administer oaths and affirmations.

Although this process may be legal in Florida, Montana and Virginia, it does not mean the Company must insure transactions — which include documents — notarized in this manner. Transactions where the documents have been notarized in this manner or where the principals have asked if they can use a notary via webcam should be referred to Underwriting or National Escrow Administration at settlement@fnf.com for assistance.