FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

ADDRESS on tax bill prevents a theft

By Lisa A. Tyler
National Escrow Administrator

Coronavirus may be new, but the fraudulent real estate scams are not. We have shared many stories about how fraudsters target properties which are free and clear and not owner occupied. In the "COVID criminals" story, the property was vacant and undergoing a remodel. The fraudsters swooped in and agreed to sell the property to a real estate investor. Fortunately, the escrow officer, Stacy Heintz, Assistant Vice President, paid close attention to the many discrepancies which all added up to an imposter. Read the article to learn the details.

"*Real Estate Fraud, Mortgage Fraud, Illegal Practice of Law, Performing Real Estate Agent Services without a License.*" This was the subject line of a cease and desist letter issued to a fraudster by the attorney of the sellers. What kind of deal was this? How did the attorney come to this conclusion? Do not miss the story entitled "FORGERY, theft and robbery."

"Hacker," carries a connotation of a malicious person seeking to infiltrate and cause pain for anyone trying to secure data or information on a computer. However, not all hackers are out to do harm; many want to help companies, for a fee. Learn the different types of hackers — and the color of hats they wear — in this month's **cyber buzz** article entitled "NOT all hackers wear the same color hat."

IN THIS ISSUE

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

volume 15 issue 10
October 2020

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

COVID criminals

The buyer agreed to purchase the property "as-is," which indicated the property needed an update. The cash sale was scheduled to close in 10 days. The buyer, a real estate investor, offered a purchase price of $175,000 — far below fair market value — to perform needed repairs.

The property was in Arizona, but the seller's "agent" was from Illinois. To find out which real estate brokerage he worked for, the escrow officer, Stacy Heintz, Assistant Vice President, searched his name on the internet. She found nothing.

Apparently, the seller's "agent" was not a real estate agent — just an "agent." He also waited until three days prior to closing to provide Stacy with an email address and cell phone number for the seller.

Stacy called the seller several times; he never answered or returned her calls. He finally replied to one of her texts. The seller claimed he contracted COVID-19 and, therefore, was not ready to close. He wanted Stacy to just send the closing documents and he would sign them alone.

Stacy explained the Company requires an approved notary to acknowledge his signature. He replied with this text: "I am in no rush to put myself or anyone else in harm's way due to this virus. It will just have to wait until I'm available but that gives me time to review the documents so can you please email me everything I'll be signing so I'm not just signing a bunch of papers I haven't read?"

The closing date came and went, and the seller did not close. The buyer patiently waited. Nearly a month later, the seller called to say he was ready to sign his closing documents. Oddly enough, he called from a new cell phone number.

The phone number the seller originally provided Stacy began with a Florida area code. The new number had a Massachusetts area code.

Stacy asked the seller where he would like to meet the notary for the signing appointment. He told her he needed to call her back. Another week went by before he returned the call. He set up a time and location that afternoon in Florida.

The next morning, the notary contacted Stacy since the middle name of the grantor on the deed did not match the middle name on the seller's identification. Stacy asked the notary to provide the social security number from the Substitute 1099-S.

The notary said the seller could not remember his social security number and had left that line blank. He also entered the property address as his forwarding address, with instructions for Stacy to mail his proceeds to that location. Her gut told her something was wrong.

First, what 44-year old man does not know his social security number from memory? Second, if he is in Florida — why would he want his proceeds check mailed to the property he was selling in Arizona?

Additionally, the U.S. Postal Service will not deliver mail to a vacant property. Stacy checked the tax bill, which indicated the taxes were paid, and found an address in California.

None of the signatures on the documents matched. The signature on the purchase agreement was different than the signature on the Seller's Information and Authorization to Escrow form. Neither of those signatures matched the signatures found on documents in the chain of title.

When Stacy received the second set of closing documents, NOT ONE of the signatures matched, including the seller's signature on both his driver's license and the deed.

Stacy alerted the buyer regarding her concerns and escalated the file for review by National Escrow Administration and her local escrow administrator. An internet search of the phone number for the seller's "agent" revealed the number was for a massage parlor in Illinois.

Although the buyer wanted the property, he realized the value an escrow officer and title insurance brought to his investment. The buyer appreciated Stacy's caution and patiently waited.

The buyer also had some suspicions since his dealings with the seller's "agent" were never in person — only by text message. The "agent" even instructed the buyer to let himself into the property and change the locks; the "agent" told the buyer to take the cost out of his proceeds at closing. Very cavalier!

National Escrow Administration instructed Stacy to send a letter via overnight delivery to the address on the tax bill, asking the owner to contact her regarding the sale of the property. While waiting for a response, Stacy's manager asked her to order an inspection on the property. The inspector found a construction crew already working on the remodel.

The next day, Stacy received a call from the real property owner. The real owner thanked her for contacting him and confirmed his property was not for sale.

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

[COVID criminals — continued]

Stacy resigned from the transaction. The buyer was certainly disappointed, but relieved that Stacy had saved him from buying a property from someone who did not really own it. For Stacy's watchful eye she is being rewarded $1,500. Great job!

MORAL OF THE STORY

Adhering to the Company's procedures helped draw attention to the imposter. First, Stacy did not honor the seller's request to send the closing documents to him. She stuck by the Document Execution Guidelines and insisted he meet with a Bancserv notary. Second, she followed the requirements to send a notice to the address on the tax bill. The notice simply stated:

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 Commitment for Title Insurance for the sale of the properly listed above.

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

These policies and procedures are in place to protect transaction participants from fraud and forgery.

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

FORGERY, *theft and robbery*

The transaction was very unusual. The owners had leased their commercial property and the tenants were operating a successful business.

The buyer offered to purchase the property for $1.5 million dollars, and recommended the owners add the proposed buyer to the title; rather than divest all of the interest in the property — both the buyer and the seller would each hold 50% fee title ownership interest.

The buyer would obtain a new loan for $1 million to purchase a 50% interest in the property, pay off the seller's liens and rehab the property. The sellers would net $123,000 from this first sale.

The rehab was scheduled to take three months. After that, the buyer would refinance the property to buyout the remaining 50% ownership interest. The sellers would net $750,000 from this second (and remaining) sale and the buyer would be reimbursed the cost of rehabbing the property. Title to the property would be transferred to the buyer's limited liability company at that time.

The buyer memorialized these terms in a non-binding Letter of Intent to Purchase Real Estate. The buyer also presented a Commitment for Title Insurance to the seller, issued by a competitor title company; it was attached to a Conditional Loan Quote, from an unlicensed lender, to prove he fully investigated the property and had a lender ready and willing to provide a loan — using the property as collateral.

The order was placed by the lender with Crystal S. Robinson, Commercial Escrow Officer with Fidelity National Title in the National Commercial Services division. Crystal was not familiar with any of the parties to the transaction — this was her first red flag. She was also alerted by an email wherein the loan officer stated Fidelity is the, "…go-to title company, and they understand their funding process."

The title officer prepared the Commitment for Title Insurance, which revealed some title issues to be addressed prior to closing. As soon as the Commitment was issued, the lender rushed to close.

Crystal kept asking for title curative information to clear the title issues. Each person involved in the transaction passed her question to the next person. She searched for contact information for one of the lien holders listed on Schedule C of the Commitment and contacted them to request a payoff demand.

The buyer's lender knew the sellers and found the status of title confusing. The lender put Crystal in contact with the seller's family attorney. Crystal contacted the seller to obtain approval to discuss the details of the transaction with their attorney.

The attorney also contacted her clients to find out what was going on. The attorney reviewed the title commitment and discovered various deeds in the chain of title were forged.

After reviewing all the paperwork and discussing the transaction with her client, the attorney advised her clients not to proceed. They agreed with her advice and authorized her to issue a cease and desist letter to the buyer and his counsel.

Simultaneously, Crystal, realizing the title to the property was not insurable, resigned as escrow holder from the transaction.

The letter from the attorney described that the parties were not licensed to conduct business in the state where the property was located, and the forms did not conform to state law.

The attorney proved the Commitment for Title Insurance (prepared by another title insurer) that was provided to the seller to legitimize the transaction — was bogus.

The attorney concluded her letter, "Based on my review of the Transaction Documents and my preliminary due diligence on you and ABC Holdings, it is my belief the transaction you are attempting to perpetrate is unfair, deceptive and fraudulent and unenforceable."

Crystal Robinson did a great job. She did not wait for the parties to present documents to her to clear up the title issues, as they most likely would have been fraudulent. She took the bull by the horns and researched the title clearance matters herself, an action all good escrow officers do. She pushed until she received sensible answers.

[Continued on pg 4]

[FORGERY, theft and robbery — continued]

Due to her persistence Crystal was able to confirm many of her suspicions were true. The chain of title was clouded. The buyer was attempting to strip the equity from the property and, most likely, leave the sellers without any improvements to the property and with supplemental debt.

Way to go Crystal! For your efforts and protecting the Company by contacting the seller's attorney and getting her to review the transaction, you are being rewarded $1,500. Thank you for protecting the Company from a potential title claim and for protecting the public we serve.

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

NOT all hackers wear the same color hat

"Hacker," to a non-technical or computer-savvy person, generally has a horrible meaning. News outlets report crimes — such as identity theft, data breaches and credit card theft — as perpetrated by the evil hackers.

The ways in which hackers commit the theft or generally cause mayhem is many times ingenious, such as loading malicious software onto credit card point of sale machines to lift credit card data and send it to a cybercriminal or breaking into one of the largest credit companies. Often, the victims are unaware they are being victimized.

The impressive heists beg the question, "What if hackers used their abilities for good?" In fact, many hackers do apply their abilities for the greater good and it is the reason "hacker," within the tech industry, does not always refer to a criminal. Instead, it depends on the color of the hat they wear.

To differentiate hackers, good and bad, they are lumped into categories of hat color: black hat, white hat and grey hat. This is a throwback to the spaghetti westerns where the good guy wore a pristine white hat and his adversary, the "baddie," wore a black hat.

Black Hat Hackers
Black hat hackers, or "black hats," widely called "threat actors," are the most notable variety of hackers. These are the criminals making the news by illegally hacking into credit card data bases or obtaining personal information to sell. Many also look for system vulnerabilities, which they sell to other black hats. The news today is filled with stories such as these, but black hats are not just in it for the profit.

Many black hats hack to send a political or social message by shutting down or modifying websites. Others do it for no purpose — just to cause mayhem and disruption.

The motivations behind the black hats can widely vary. Whatever their intentions are, they do have commonality in that the actions are illegal and not done with the purpose of benefiting the victims.

News and media most often just refer to them generally as "hackers" and do not differentiate. Hackers are portrayed as the common stereotype of the nefarious criminal victimizing innocent companies and persons. We have all seen some version of the person in the black ski mask at a computer.

White Hat Hackers
All hackers, however, are not motivated to cause harm and disruption. Many hackers look to improve and protect our security on the internet. These are referred to as white hat hackers, or "white hats." Their intentions are not to exploit vulnerabilities, but instead to find and fix them. These types of hackers may also be referred to as "vulnerability or penetration actors."

Many times, white hats are employed by companies to act as if they were black hats and gain access to or disrupt a computer system. Then, if issues are found, create fixes or security patches to prevent a black hat from using it for harm.

The intentions of white hats are to use their talents for good instead of evil. White hats are hired and given express permission to try and compromise an organization's system or data. The ability of white hats to carry out preemptive attacks helps to assess an organization's ability to protect themselves from more unscrupulous characters.

Grey Hat Hackers
Unlike in the spaghetti westerns where we know who will win the fight, good and evil in today's world are not as clearly defined. This third color of hat covers the shaded areas between black and white: grey hat hackers or "grey hats." You will sometimes hear these referred to as "security researchers."

Grey hat hackers may be looking to help a company but may not have the permissions that white hats are granted. Often, grey hats look for a company's vulnerabilities — without their consent. When found, the grey hat generally reaches out to the company offering either the information or a fix to the vulnerability — usually for a fee, or "bug bounty."

If a fee is refused, some grey hats may do nothing; others may take a step in the black hat direction. The requested fee may be more along the lines of extortion. If the grey hat hackers are not paid — they may threaten to sell the information to a black hat or even victimize the company themselves.

It is important to note the differences, as not all hackers are the bad guys. Instead, many are on the lookout to make our growing online presence a secure one. Hopefully in the future, more hackers will decide to don the white hat and not the black hat, but until then the high-noon showdowns on Main Street will continue.

Article provided by contributing author:
Scott Cummins, Advisory Director
Fidelity National Title Group
National Escrow Administration