FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL FAMILY OF COMPANIES

REWARD increased to $1,500

By Lisa A. Tyler
National Escrow Administrator

Great instincts and heroic acts have made our associates renowned crime fighters! Now, those acts can make employees and agents even wealthier! The *Fraud Insights* reward has increased from a cool grand to $1,500!!! If you or someone in your office has thwarted crime, be sure to share the details with us by calling 949.622.4425 or emailing the story to settlement@fnf.com. If the story is published in a future edition, the hero will receive a letter of recognition from the Company and $1,500 as a token of appreciation for protecting the Company from a potential claim or loss.

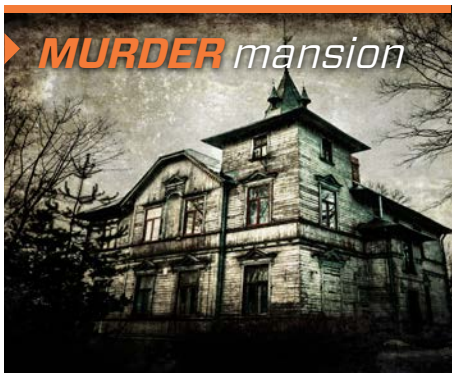
"MURDER mansion" is a story about a landmark property in Los Angeles County which was the subject of a new title order placed with Chicago Title's Oxnard, California office. The title officer received the documents and funds to close the transaction, but stopped just short of recording to investigate the independent escrow company which directed the transaction. During that brief moment the title officer uncovered a forgery and ended up saving the Company from a potential claim of $1.8 million.

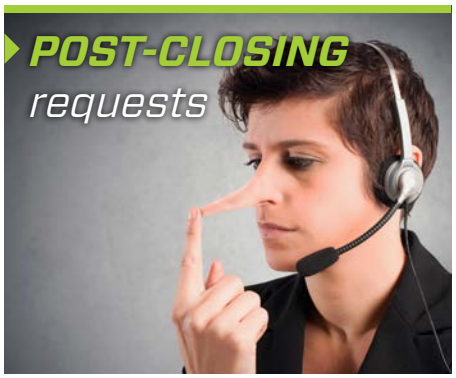
In an effort to prevent their policy holders from further email hacking and cyber theft, an errors and omissions insurance carrier (for closing attorneys and title agents) published a notice sharing recent claims received by their offices. The claims stories they shared are all too familiar to the industry and our Company, and are worth sharing to raise awareness of the danger of accepting emailed wire transfer instructions from anyone. Be sure to read "E & O claims" to discover the types of crimes settlement agents are suffering from nationwide.

The crooks are always finding new ways to steal personal information. Read "POST-CLOSING requests" to discover an email received by a title agent in Northern Virginia from a crook who initially called posing as the original borrower on a transaction, and then sent an email requesting a copy of his loan application and other closing documents.

The Consumer Financial Protection Bureau (CFPB) introduced some new terms contained in the consumer finance laws that changes long-standing industry terms. Find out the newly defined words that will be flying out of our mouths after the new rules take effect on August 1, 2015 by reading "NEW vernaculars."

IN THIS ISSUE





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

volume 10 issue 4
April 2015

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

MURDER mansion

Kim Nelson, a Title Officer from Chicago Title's Oxnard, California office, stopped a transaction from closing that would have been a $1.8 million fraudulent sale. The order for a preliminary report was opened on a rush by an independent escrow company. The subject property was free and clear of any liens. The buyer was financing the purchase with a hard money lender.

As soon as the preliminary report was sent out the lender funded $1.2 million to Chicago Title's trust account. The buyer was pressing to close. Closing documents, including the seller's signed deed and buyer's signed deed of trust, were delivered to Kim by the independent escrow company.

Kim sensed something was wrong as she had never heard of the escrow company or done any business with them. She searched for their website and their license online, and quickly discovered the company did not exist.

Next, Kim carefully reviewed the documents delivered to her as she suspected the deed had been forged. She pulled recorded documents from the chain of title containing the property owner's signature and confirmed the deed had been forged.

The documents had another title company stamped on them so the other title company must have rejected the deal and the crooks took it to Chicago Title. Kim guessed the crooks probably thought they could take the transaction to an out-of-county office, and convince them to record and pull off the crime of stealing someone else's property.

Kim did some more research and found out the property was abandoned, and had become a landmark known as a "murder mansion" after a previous owner, a doctor, went crazy and attacked his family in 1959.

The news article that Kim uncovered said the doctor went after his wife with a hammer, bludgeoning her to death. The doctor later drank a glass of acid, which killed him. The doctor and wife had three kids, who survived the attack and lived to tell the story.

Kim notified her local underwriter who agreed the deed was forged and confirmed the company had other claims with the parties to the transaction, namely the buyer and the lender. Kim canceled her file and returned the lender's funds.

Kim posted an Office Information (OI) to the chain of the title for the subject property, so if the deal is opened at yet another company office, they will be instructed to call Chicago Title before insuring.

As quickly as the order opened and funded, Kim wanted to make sure no company office got burned on this deal. For Kim's recognition of the forgery and for acting swiftly to protect the Company from a future claim, she has been rewarded $1,500 as well as a letter of recognition from the Company.

MORAL OF THE STORY

Had Kim recorded the documents and deposited the funds given to her, and disbursed the loan funds, she would have ended up paying the illegitimate independent escrow company the majority of the proceeds, exceeding $1 million. If the transaction would have closed, the current owner would have lost clear title to their property and the lender would not have a valid lien securing their $1.2 million note. She saved the Company from two potential claims.

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

E&O claims

An errors and omissions insurance carrier published a notice sharing recent claims received by their offices. The stories were shared to alert title agents to a pattern of fraud occurring in escrow transactions.

A summary of some of these claims follows to show the severity of the resulting loss. The carrier urges their policy holders to review communication protocols and to consider using fax communications to process escrow transactions in lieu of using email – which can be hacked.

Claim Received 09/05/2013

Insured served as buyer's closing agent for a transaction in which Claimant seller sold his vacation home to buyer for $225,000. The seller's closing agent's email account was hacked into by a third party who provided "updated" wire instructions via email to the Insured. On the computer screen the email looked legitimate and the fake address was only apparent if printed (which insured did not do until after the fact).

The Insured sent an email to the other closing agent to verify the new wire instructions. The hacker intercepted that email and created a fake reply from the other closing agent, confirming the wire instructions. The insured sent the wire of approximately $225,000 to the fraudster.

We received a claim from the seller who demanded that the Insured repay $225,000 plus his attorney fees of about $15,000. There was no defense to the claim and we settled it before incurring significant litigation expenses after it was apparent the FBI was not going to be able to recover the funds. The paid loss was $240,000 and paid expenses totaled $24,639.

Claim Received 04/16/2014

This is a fraudulent wire transaction of $7,458, which represents the seller's proceeds for the sale of real estate. Insured was the settlement agent for the sale of property. The seller forwarded closing instructions via email for the proceeds of the real estate sale.

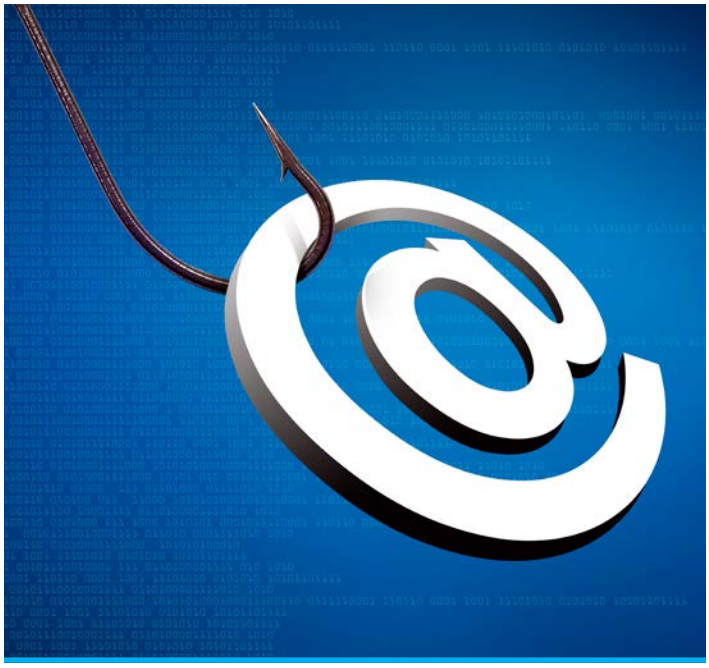
The next day, the Insured received another email requesting a change to a different account. Although Insured did not realize it at this time, the second email instructions were sent from a different but very similar email address. Apparently, an unknown third party hacked into either the Insured's email or the Seller's email account and altered the closing instructions.

Insured wired the funds as per the second email, which turned out to be a fraudulent account. Insured attempted to rescind the wire; however, the funds were withdrawn from the account before the rescission request. The insurance company paid $2,458 but the Insured paid its $5,000 deductible toward the balance of the sustained loss.

Claim Received 06/30/2014

The Insured was the settlement agent for the bank, the seller of the property. The Insured sent the closing funds in the amount of $376,043 to the wrong account after a hacker intercepted emails to and from the Insured, and provided the Insured with fraudulent closing instructions.

The hacker apparently gained access through a breach in seller bank's security and sent the Insured instructions to send the closing proceeds to a different account from which they were subsequently stolen. The Insured later discovered the fraud and attempted to rescind the wire transfer, which appears to have been



partially successful; however, the hacker was able to withdraw approximately $38,000 before the rescission took effect.

Claim Received 09/11/2014

The Insured was the settlement agent for the transaction involving the sale of property. Shortly before the closing, the Insured received a request to change the wire instructions for the sale proceeds by email. A paralegal from the seller's attorney allegedly sent the altered instructions via email. The email was then forwarded to the Insured by a paralegal for the buyer's attorney. The Insured then wired the seller's proceeds for the sale through its escrow account at Bank #1 for deposit in a Bank #2 account.

The Insured became aware of a potential problem and immediately contacted Bank #1 to rescind the wire transfer. The Insured also contacted Bank #2, the receiving bank, in an attempt to freeze the account. It appears the breach of security was from a home computer of the paralegal for the seller's attorney. The rescission was successful and the entire proceeds were recovered but this might have resulted in a significant claim.

Claim Received 09/17/2014

The Insured received fake wiring instructions from a hacker posing as the closing agent for the transaction. Insured wired $135,000 to a false account. The Insured contacted the bank that received the funds and notified them it was an erroneous transfer. They had their fraud unit review the matter, and concluded it was a legitimate transaction for that particular account and that they were not required to return the funds. The Insured also notified police and FBI who are attempting to recover the money. So far, the police have not been able to trace the funds.

Protect Against Wire Transfer and Email Fraud

In their notice, the E & O carrier encouraged their policy holders to take all appropriate steps to secure information, and protect against wire transfer and email fraud. In particular, they asked policy holders to maintain a high level of vigilance to avoid computer hacking incidents.

FRAUD Insights

POST-CLOSING requests

One of our title agents received this puzzling request on a Thursday. A guy called the office purporting to be a borrower of a transaction they recently closed and asked for post-closing contact information for his closer. He then emailed the following message to the closer:

Hello Samantha,

This is Mike Keeny, can you please forward me a copy of my uniform residential loan application. The address of my property is 1212 Summerset Dr. McLean, VA 22101

Thanks,

Mike

This was the settlement agent's response:

Mike,

For security reasons, would you please confirm the other email address we have on file? This is not the email address we have.

Samantha

Fortunately the closer is very wise and protects customers' information dearly. She questioned the email address it was sent from. She then reached out to the REAL borrower to confirm his request. The borrower was unaware of any request for these documents from him or his wife.

This seems to be a new scam, in which identity thieves can obtain the title company's information from the land records, pretend to be the borrower, call the title company and request documents. A lot of new procedures have been set in place in regards to the privacy and protection of customer information, but something tells me, someone might fall victim if they are not alert....

Next, one of our offices reports they had just received a call from "John Doe" looking for a copy of his loan documents. The lucky person who answered the phone asked when he purchased the property. The caller said he did not know, "somewhere around the 29th or 30th of last month."

Our office personnel asked which settlement agent closed his transaction. He did not know what a "settlement agent" was but said he closed with Fidelity. She told him to call his lender and he hung up on her. His number came across the phone screen as anonymous.

Make sure you do not provide private information or documents to an unknown caller or in response to an unknown email address. If you receive a phone call from an unknown caller or an email from a different email address, ALWAYS call the customer at the phone number you have on file to confirm the request before providing documents or information.

NEW vernaculars

Know before you close.™ | CFPB Readiness

The CFPB replaced long-standing terminology used in the real estate industry in their recently published 1,888 pages of rules that govern mortgage home lending in America. The new vernacular used throughout the new rules and on the new disclosures themselves is defined as follows:

Business Day – A day on which the creditor's offices are open to the public for carrying on substantially all of its business functions. For purposes of rescission under TILA, the term means all calendar days except Sundays and the legal public holidays.

Creditor – A loan originator, lender or banker.

Consumer – A borrower in a residential loan transaction.

Consummation – The day the borrower becomes legally obligated to repay the debt, in other words, the date of the signing of the loan documents.

Variances – The new rule contains three tolerance levels, but describes them as variances and expands the charges that cannot increase at closing to include charges for any service the borrower cannot shop for, as well as charges for any service provided by a subsidiary or affiliate of the creditor.

FIDELITY NATIONAL TITLE GROUP® Know before you close.

Your CFPB readiness partner - every step of the way.

www.fnf.com