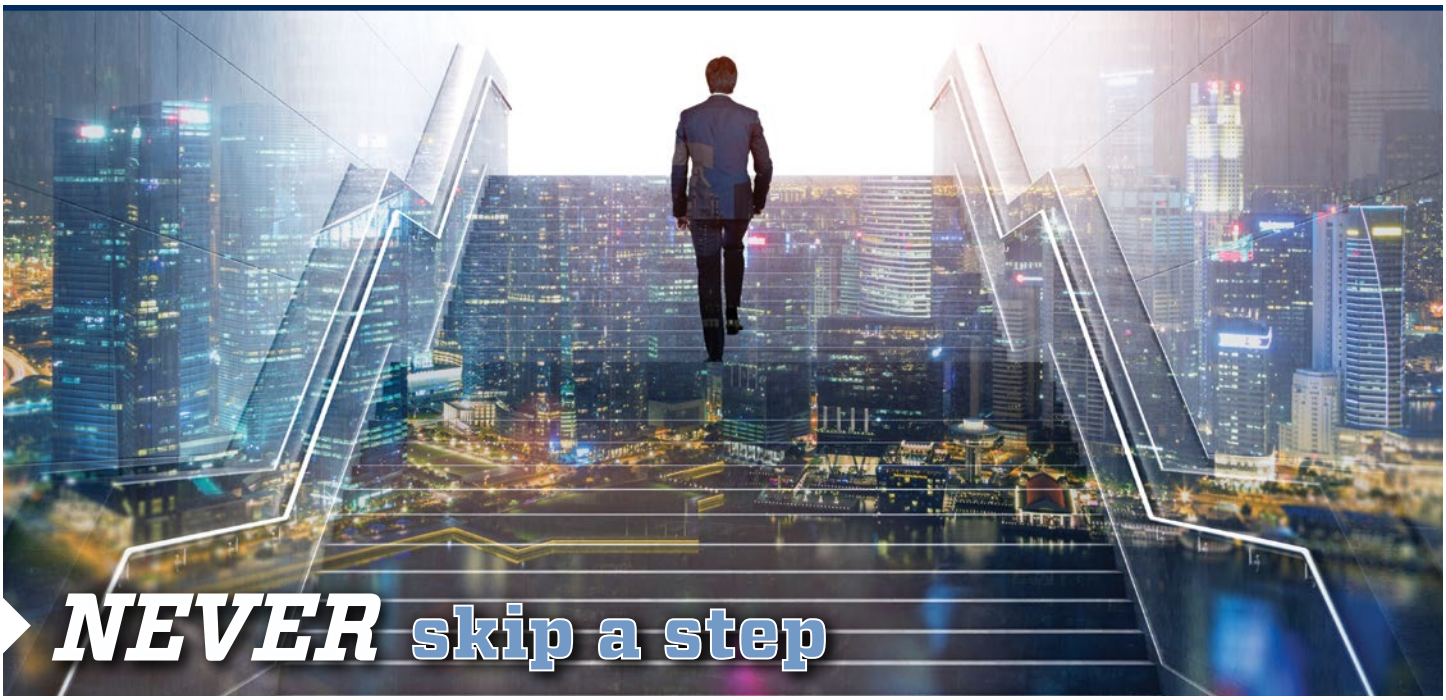
FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL



By Lisa A. Tyler
National Escrow Administrator

The Company is traded on the New York Stock Exchange (NYSE). Being traded on the stock exchange means the Company is held to the highest standards and must ensure we have proper measures in place to protect Company funds and those on deposit in our trust accounts. The Sarbanes-Oxley Financial Modernization Act was put in place to help protect investors from fraudulent financial reporting by corporations describes minimum standards traded companies must adhere to, to avoid the mismanagement of accounts controlled by the Company. Our Company has had procedures in place for several years to help fight wire fraud. Read more about it in article titled "STEPS to prevent wire fraud."

Absentee owners of real property are often the target of criminals who pose as the owner offering the home or property for sale or as collateral for a new loan. These imposters sell the property and abscond with the sale proceeds or strip any equity in the property with a new loan. The real property owner has no idea their property is the subject of a real estate transaction. The scam is typically perpetrated on owners of vacant land. Find out how one escrow assistant prevented a landowner from becoming victim to the scam in the article titled "VACANT lot in austin."

"WHAT to do in a ransomware cyberattack" is this month's article on the topic of ransomware. Entities who are held ransom must first determine which computers and systems have been hacked and disconnect them from their network and power them off. Next, consult with the appropriate departments within their organization to determine what data has been compromised and whether it can be restored.

IN THIS ISSUE

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

volume 17 issue 7
July 2022

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

STEPS to prevent wire fraud

All out-going wires sent from the Company's escrow trust accounts must be approved by two authorized bank signers before they are sent to the Operational Accounting Center (OAC). The OAC requires two more approvers to review the wire for accuracy against the source document before sending it out.

Here is how the process works: The person sending a payoff wire verbally verifies the wire instructions at a known, trusted phone number and documents when and who they spoke to so anyone looking at the file knows the wire was verified. If the wire instructions appear on the repetitive wire list documentation is noted.

Next, the demand is read thoroughly to ensure the full amount necessary to pay the loan is being sent. Then they ensure the file is fully funded and will not be overdrawn by the disbursement. Finally, the wire up is set-up in the system. Once the wire has been set up a second bank signer is required to verify all the same items and confirm the information entered is correct. They must ensure the routing number and account number are correct. They must make certain the correct loan number and borrower name is referenced before approving the wire to be released to the OAC.

The payoff demand must be uploaded to *smartview*. Once the approved out-going wire request is received by the OAC, they too will verify the wire instructions against the repetitive wire list. If it does not appear on the repetitive wire list, they look for evidence the wire instructions were verified. Next, they read through the demand to ensure the wire will pay off the loan per the written demand or estoppel. The OAC verifies the routing number and account number are correct against the demand. They check the correct loan number and borrower name is referenced. When each person does their part, the process protects the Company and ultimately our customers.

Recently, one of our offices ordered a payoff demand from a mortgage company. The demand was ordered on April 25, 2022. It was received on April 27, 2022, via email. This payoff included wire instructions to a bank in New York. On May 2, 2022, an amended demand was received which included an increase to the amount of trust funds advanced by the mortgage company. The original demand reflected an increase in advanced funds in the amount $103.72, and the new amount was for $207.72. No other amounts on the demand changed. On May 4, 2022, the office received an "updated" demand by eFax. Unknown to the office, this "updated" payoff had altered banking information to send funds to a bank in California rather than the bank in New York.

The file closed and the wire was set up and approved at the branch and sent to the OAC for processing. The wire transfer was in the amount of $149,546.13. DeeDee Kelly, an amazing member of the OAC team, reviewed the wire. She compared the wire instructions against the payoff demand and the Company's repetitive wire list. She did not find a match, so she combed the escrow branch file looking for evidence the wire instructions were verified at a known trusted number. She did not find it. The wire request was returned to the branch. The branch contacted the mortgage company who confirmed the payoff demand had been altered. They had no record of that payoff demand having been set by their office on May 4, 2022.

DeeDee is our hero! She followed the Company's standard operating procedure which proved once again to be our best defense against wire fraud. Great job DeeDee. She is being rewarded $1,500 for her efforts. Never skip a step and be sure to completely review each demand for discrepancies. Any changes should be verified before proceeding.

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

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

VACANT lot in austin

Chicago Title Company opened a sale transaction involving a tract of vacant land not far from downtown Austin. The tract is located in a desirable part of Austin where there are very few vacant tracts of land. The purchase contract was brought in by the buyer, who is a real estate investor and previous customer. There were no brokers or real estate agents involved. The contract price for the sale was $316,427 all cash.

The order was opened by Tabitha Jacobs, an extraordinary escrow assistant. She talked to the seller, Davin Rain, on the telephone to confirm the order was opened. He said he lived in Georgia; his phone number was a Nevada area code. Tabitha said Mr. Rain was not forth coming with information and acted very suspicious on the phone. When she explained the closing documents would need to be signed with a mobile signing agent in Georgia, he flat out refused using a Company approved signing agent.

Then, one of the other Chicago Title offices in Austin received another contract on the same property. The system notified the office of an existing open order with Tabitha's office. The other escrow officer contacted Tabitha, and both were confused about receiving two separate contracts with two different buyers and two different sale prices for the same property. Tabitha looked at the appraisal district information and saw the address where the property tax bills were being mailed was located in Austin, which did not match up with the seller residing in Georgia.

Tabitha drove to the address where the property tax bills were being mailed and asked to speak with Mr. Rain. He was an elderly gentleman who confirmed his property was not for sale. He urged Tabitha not to continue with the present transaction and not to close on the sale of his property, as it was not for sale.

When Tabitha returned to the office, she notified her title officer, and an alert was sent to all operations in Texas. She and her escrow officer resigned from the transaction, returning all funds and documents on deposit to their original remitter. The other branch office did the same. Both contract buyers were disappointed; they did not know anything about being involved with a fraudulent seller. They said they saw a good deal on a property, and both jumped on it.

After that, the individual masquerading as Mr. Rain continued trying to sell the property to other buyers, each time opening the escrow with a different escrow branch for a different sale price. Through the offices being diligent and the internal system flagging files, the Company rejected six additional contracts from this individual attempting to sell the property.

In one of the six transactions, the buyer was represented by a broker who was adamant about going forward with the deal even after the Company resigned and informed him the property seller was an imposter. The broker said they were going to move the transaction to a competitor and still close under the contract. Unbelievable! Thankfully, the property has not been illegally transferred.

For Tabitha's due diligence in ferreting out the absentee owner and protecting the Company from a potential loss of $316,427, she has been rewarded $1,500 and a letter of recognition.

MORAL OF THE STORY

Although the Company would have preferred Tabitha send a notice to the address of the owner where the property tax bills were being mailed, rather than appear in person, she still acted on her gut reaction to the seller and the inconsistencies in the overall transaction.

Settlement agents can take steps to prevent this crime from happening. Begin by comparing the mailing address provided by the seller or borrower to the address on the tax bill, where available. If the address is different than the address provided to you, or no address was provided send a letter to the address on the tax bill.

FRAUD Insights

WHAT to do in a ransomware cyberattack

The Cybersecurity and Infrastructure Security Agency (CISA) has put together a comprehensive website which contains tools for victims. One of these tools is a Ransomware Guide which includes a comprehensive checklist for victims. It is available on their website https://www.cisa.gov/stopransomware/ransomware-guide. (Important: FNF employees should report any cyberattacks to our Security Operations Center for handling.)

Management also needs to consider whether they should enlist assistance from outside cybersecurity resources and/or report the attack to law enforcement. There are plenty of private firms who offer forensic, incident response and recovery services. In addition, the Federal Government has set up resources that companies can contact voluntarily for assistance. These resources offer two types of assistance.

1. The first type of assistance is technical in nature. CISA and the Multi-State Information Sharing and Analysis Center (MS-ISAC) are agencies which have extensive knowledge of the tactics and variants criminals use to infiltrate their victims' computers and networks. They may be able to provide technical details on the attack and recommend mitigation strategies and actions. The agencies can be contacted directly for assistance.
2. The FBI and U.S. Secret Service are the agencies to contact to initiate a criminal investigation. They will investigate with the goal to bring the perpetrators to justice, but their investigation will include efforts to investigate links to other attacks and threats to our national security. Ransomware complaints can be filed directly with the FBI at https://www.ic3.gov/Home/Ransomware or with the Secret Service https://www.secretservice.gov/contact/field-offices/.

Last, the victim must decide whether they should pay the ransom or not. The federal government does not support the payment of ransom in response to a ransomware attack. Paying the ransom does not guarantee the criminal will deliver the decryption software/keys or restore the stolen data. Paying the ransom can also encourage the criminals to carry out more attacks and can attract new criminals looking to make a quick buck. It can also fund illicit activities or parties, in violation of the law. If the victim does not remediate the original vulnerability, the criminal may carry out the same ransomware attack again. More recently, in a twist on the typical ransomware scheme, criminals have exfiltrated sensitive data, threatening to sell or release the data on the black market unless a ransom is paid.

Whether a victim pays a ransom or not, the government still encourages victims to report the attack. This enables the government to track ransomware activity and link possible syndicates to other successful attacks. It also allows the government agencies to share the information with the private sector that may be helpful to prevent future attacks. Next month's article will discuss the type of payment the criminals demand and why. Tune in.

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