FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

SOCIAL engineering

By Lisa A. Tyler
National Escrow Administrator

Social engineering, as it is known within the telecommunications industry, is the art of utilizing conversational skills to convince unsuspecting victims into forwarding telephone calls through corporate America's telephone systems. The fraudulent schemes which have been in use by telephone service thieves for years have, in recent months, shown a drastic increase among corporate customers. The social engineers can be hackers, prison inmates or telephone solicitors. This edition contains three of the most popular schemes, read about them in "DO not call me!"

Do not stop there…the next story "STOLEN lot" is a fascinating story involving the attempted theft of a vacant lot. The thief stole the identity of the real owner and tried to sell his property out from under him. Luckily for the real owner, the transaction landed in the offices of one of our best and brightest escrow officers. She became suspicious of the seller and proceeded to uncover the crime.

I know I am starting to sound like a broken record, but this edition contains yet another FIRPTA withholding nightmare article, nightmare #6. That is right, the story in this edition is our sixth in the series and it involves another "super helpful" closer, who decided she would complete the IRS Forms 8288 and 8288-A on behalf of her customers - only to cause them more harm than good.

We love hearing from our readers that these stories are opening the eyes of our settlement agents and forcing them to implement changes when it comes to FIRPTA processing. We have also seen an increase in requests from settlement agents to review the forms prior to close, which has been helpful in identifying mistakes. That has allowed us to correct the forms prior to close, ultimately saving our reputation with our customers and preventing escrow losses. Keep reading…six more to go!

IN THIS ISSUE

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

volume 9 issue 6
June 2014

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

DO not call me!

Scams come to us from all different angles: the Internet, emails, package deliveries, stolen identifications, fake account numbers, altered wire instructions, straw/fake buyers, notary mishaps and even bullies. Sadly, we always have to be on high alert. Like most things in life there are new twists. This time it involves your office phone.

Phone fraud seems like the kind of thing that is easy to identify. The phone rings and the person on the other end wants to give a special offer or maybe even purports they are with the police, a credit card company or even a debt collector needing some personal information. With the new twist, unbeknownst to you, you could be helping criminals commit their crimes. In other instances, the scammers are trying to bully and take advantage of you!

Learn the three new social engineering schemes that have occurred in our offices, as well as our title issuing agents:

SCHEME #1:

The thieves target companies typically closed on nights and weekends. They call the company and then access each employee's voice mail. They program the employee's direct line to dial a number outside the U.S. - charging the business each time the number is called.

Hundreds and even thousands of calls are made. How did the scammers get access? The phones either do not have a passcode set to access voicemail or the passcode set is a generic number.

Unfortunately, getting out of paying the fraudulent phone charges is not always easy. Some phone companies will hold customers responsible for all or a portion of the charges and note the customer's equipment was not secure - therefore putting the onus on the victim.

One of our title agents in Indiana recently fell victim to this crime. In one weekend, the fraudsters racked up $50,000 in long distance charges on the agent's phone bill. Another business (not a title agency) in the same city, had charges over the weekend in excess of half a million dollars. The scammers made thousands of overseas calls to phone numbers with a set charge to the business each time the number was called – in this particular case the charge was $34.83 per call. The scammers were paid a percentage from each call.

LESSON LEARNED:
Avoid generic voicemail passcodes like 1111, 2222, 1234. Change your voicemail passcode when you change your Internet password.

SCHEME #2

Working in the front office or at the receptionist desk can be stressful with lots of phone calls to handle, people coming in and out, and assisting in the office tasks. A phone call comes in, the person on the line says they are with the phone company and they are testing the lines. The person states in order to test the lines they need to be transferred to extension 90. Transferring the person to a 90 or 90xx number allows the criminal to connect to an outside long distance operator through the office phone system and call foreign phone numbers that rack up the phone bill. The phone calls are made during normal business

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

[DO not call me! – continued]

hours making it impossible to dispute the charges since there is no way to know who made the calls. The telephone hackers then receive payment as a percentage of each charge.

LESSON LEARNED:
Never transfer a caller to extension 90, 900 or any form of extension 90xx.

SCHEME #3

The caller states they are with a collection agency, such as a "payday loan" company. They are calling to collect payment for a debt from an employee of the Company. The caller knows personal information about the employee, which makes the call seem legitimate. They are relentless in the amount of times they call. The calls become more frequent and the caller becomes more belligerent.

The Caller ID will typically display an invalid phone number, for example 503.210.5366, 397.560.2365, 521.203.0230 or no number at all. They might even call the employee directly, threatening legal action if the debt is not paid. Specifics about the debt are never provided. The intent of the call is to disrupt the business, create frustration, leaving the employee feeling embarrassed and so desperate they send payment to make them stop calling.

LESSON LEARNED:
If the caller knows your personal information it is likely your identity has been compromised. Do not provide them with payment information or any additional personal information. Contact the three major credit bureaus, notify your banking institution and file a complaint via www.ic3.gov/default.aspx. The office should also file a complaint, report the incident to the phone company and ask if it is possible for the phone numbers to be blocked.

The only way to stop this type of fraud is having well-educated employees who are familiar with these types of fraud schemes and refuse to be manipulated by these criminals. Discuss this article with all employees who answer incoming calls.

STOLEN lot

Vacant land or homes are easy targets for criminals. Vacant homes are often vandalized. In some cases squatters move in and refuse to leave, even though they do not pay rent. Vacant lots are used as dumping grounds for trash and debris. Some more brazen thieves are bold enough to even try to steal the property all together. Read on to find out how one such thief was caught!

Tracy Debban-Friberg, escrow officer with Fidelity National Title of New Mexico, opened an order for the sale of a vacant lot. The buyer was a real estate agent and she was one of Tracy's best customers. The sellers were husband and wife. The sales price was $180,000. The order was processed and title began preparing the title report.

When title ran the General Index search in the sellers' names they discovered several judgments which would have to be investigated to determine whether they belonged to the seller, specifically the wife.

Tracy called and reached the husband, she explained there were some judgments which needed to be cleared up and she needed his wife's social security number. The husband stated they were her debts. Tracy asked for the wife's social security number again so she could work on obtaining payoff statements from the creditors.

The husband started back pedaling. Now he said the debts were not his wife's and started asking questions about who the creditors were. He clearly did not want to provide his wife's social security number to Tracy.

Tracy asked him if he knew his wife's social security number and he replied no. She asked him to have his wife call her. He responded she did not speak English. She asked him what language his wife did speak. He stated she spoke Spanish.

Tracy explained her assistant speaks Spanish, she gave the husband her name and phone number, and asked him to have his wife call her assistant. The wife never called.

The buyer was anxious to close. The property was free and clear, and the only items which needed to be cleared up were the judgments title found in the General Index search. The seller was unresponsive.

It was at this point Tracy decided to look closer at the file. Tracy worked with her title department to find a recorded document with the sellers' signatures on it. Since they owned the property free and clear, they had to go back in the chain of title where they found a real estate contract the vendee defaulted on.

Tracy compared the signatures on the recorded document to the signatures on the purchase contract. They were not even close. Next, she noticed the seller made a few mistakes on the purchase contract. He misspelled the city in his mailing address. He claimed to live in Lompoc, New Mexico but he spelled the city Lompac. He also wrote in the wrong zip code. Tracy thought it was odd he made so many mistakes on his address.

Tracy shared her concerns with her colleagues. One of them decided to Google™ the names of the sellers. It is a good thing she did. The search revealed the wife had passed away on April 2, 2014. Her obituary said she fought a long battle with cancer and was in hospice during her last days. Interesting, since she supposedly signed the purchase contract just a few days earlier on March 28, 2014. The obituary also stated the wife was fluent in Japanese, not Spanish as her husband stated.

[Continued on pg 4]

FRAUD Insights

[STOLEN lot – continued]

Tracy resigned from the transaction and refunded the earnest money to the buyer. The phone number for the man impersonating the seller is now disconnected. He has vanished into thin air. The listing agents cannot locate him either. They have cancelled their listing agreement too.

The buyer managed to track down the real owner of the property. She called the real owner and asked him if he entered into a purchase contract with her to sell his lot. He said no. He asked her what the sales price was and she told him it was $180,000. He laughed and said if it seems too good to be true, it probably is. The lot is worth much more than $180,000.

MORAL OF THE STORY

Time and time again escrow officers, closers and settlement agents stop a fraudulent transaction by trusting their escrow gut. Tracy slowed down, looked over her file with a more careful eye and was able to stop this fraudulent sale from going through. She probably deepened her professional relationship with her customer as well. Tracy is being rewarded $1,000 for her hard work.

FIRPTA *withholding #6*

The closer decided parts of her duties were to prepare IRS Forms 8288 and 8288-A on behalf of the buyer and seller. The transaction involved two buyers. She listed both buyers as the withholding agent (each on their own Form 8288-A). She sent the payment along with the forms to the IRS.

The IRS received the payment and credited the payment to one of the buyers listed as a withholding agent, then promptly issued a penalty notice to the other in the amount of $34,717.42. The buyer contacted the closer demanding she fix it.

She had no idea what she had done wrong or how to fix it. She contacted the IRS on several occasions (holding on the phone for as long as an hour) and finally contacted National Escrow Administration. An escrow administrator asked her to send over copies of what had been sent to the IRS.

The administrator explained there should never be more than one withholding agent. Listing two names on the forms always results in a penalty notice. The national escrow administration team could not intervene to straighten the matter out because the closer failed to obtain a completed 8821 Tax Authorization Form from the buyers at closing (authorizing the company to work on their behalf if their remittance had been applied incorrectly).

Eventually the buyers signed and sent the 8821 to the closer. The national escrow administrator contacted the FIRPTA Processing Unit in Philadelphia and they are processing the request to remove the penalties based on the proof of timely payment and a written explanation that the forms were completed incorrectly.

Because we do not know what we do not know, it is imperative the buyers and sellers take responsibility for completing and remitting the forms. Had the buyers completed the forms incorrectly, they would have no one to be mad at except themselves.

As settlement agents we are not expected to know tax law; certified public accountants are expected to know the tax law. Make sure the principals seek advice from their income tax preparer when completing the IRS Forms 8288 and 8288-A.