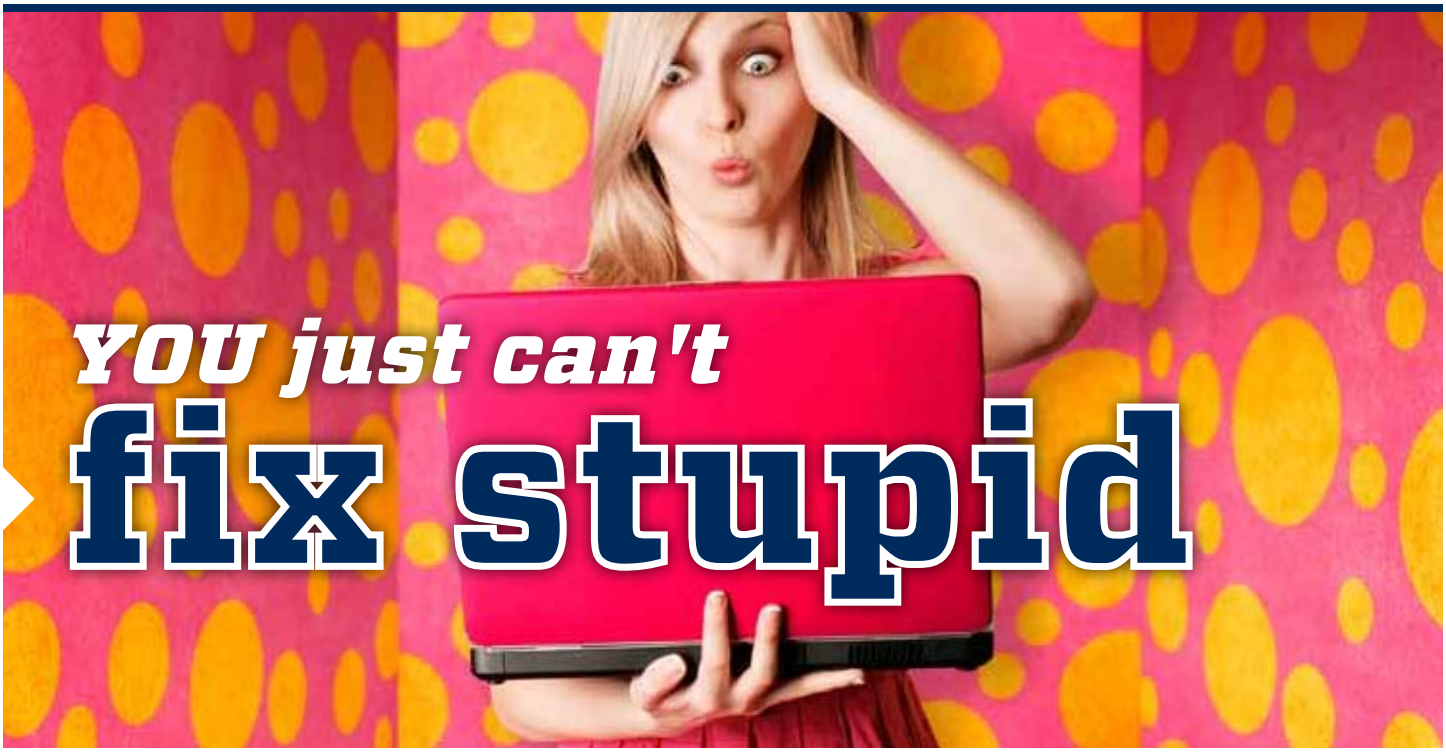
FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL



YOU just can't fix stupid

By Lisa A. Tyler
National Escrow Administrator

In the December edition we reported a crime involving the diversion of a real estate agent's commission in a story titled "CYBER-CROOKS." Believe it or not, we have become the victim of the same crime a second time – and this time we actually sent the money to the crook's accomplice. "ONLINE fiancé" is a story you must read in order to avoid becoming a victim of this type of cybercrime in one of your own transactions.

What would you do if someone walked into your office with 100 money orders as their earnest money deposit? I mean after picking yourself up off the floor! Find out how Fidelity's Fresno, Calif. office handled that exact incident by reading "100 MONEY orders."

This newsletter concentrates on fraud, but there are many other crimes which can affect our readers. Therefore we are introducing "THE SAFETY CORNER," a section featuring tips on personal safety. We launch this new section, with the article "OFFICE and personal safety" to raise awareness of crimes our readers are exposed to and provide tips on how to avoid becoming a victim.

IN THIS ISSUE

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

volume 8 issue 2
February 2013

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

ONLINE fiancé

An Escrow Officer from the Chicago Title Company's Alameda County, Calif. operation was working with an agent named Lynn Lee at Jay Dee Real Estate in San Jose, Calif. on a short sale transaction. On Friday, November 9, 2012 an email was sent from the selling agent to the escrow officer, directing her to wire transfer her portion of the broker's commission in the amount of $5,702.50 to ABC Bank in West Point, Neb. to the account of Beth Black.

On the same day the escrow officer emailed the broker at Jay Dee Real Estate, to confirm the wire transfer of funds direct to the agent was approved. The broker confirmed the wire transfer without actually seeing the wire transfer details.

On Saturday, November 10th, an email sent from the agent to the escrow officer read as follows: "You sent a message to my broker regarding closing...I am confused about the wire instructions?? I did not send you any wire instructions. Please let me know what is going on?? Regards, Lynn." (sic) Thereafter, the escrow officer received a message saying the previous message was a mistake, and to please send the wire as directed.

On Monday, November 12th, an email went out from the escrow officer that read: "Hi Lynn, Sorry the message was a mistakes. I check very well now as it for other client. Inform how we send your commission." (sic)

Later that same day, Lynn responded: "Please let me know when the check and the broker's package will be delivered." The escrow officer responded: "Hi Lynn. I will inform you when the check and the package mail out."

On Tuesday, November 13th, the escrow officer initiated the wire transfer to ABC Bank in the amount of $5,702.50. On Tuesday afternoon Lynn indicated she still had not received her commission check. She forwarded the previous emails to the escrow officer and asked if she had sent them. She became suspicious when she noticed the escrow officer's email address was @ctt.com. The emails were coming from @cttt.biz!

The escrow officer in turn forwarded the wire instruction email to the agent. The emails from the agent were not coming from the agent's actual email address - they were originating from a similar email account. Now there were both fake escrow officer and fake agent email addresses.

The agent never requested a wire transfer of her commission. The escrow officer contacted the accounting center with the details and asked them to recall the wire.

On Wednesday, November 14th, the accounting centers attempted to recall the wire, but were unsuccessful as the receiving bank told them the account had been drained to a zero balance. The Chicago Title escrow branch opened a claim to take a loss for the $5,702.50 to pay the agent her commission.

On Thursday, November 15th, the branch notified their IT Director, since the escrow officer's emails had been intercepted and it appeared her account had been hacked. At 5:15 p.m., the IT Director reported the incident to National Escrow Administration and Lisa Tyler immediately got involved in recovering the funds.

She contacted the account holder, Beth Black in Nebraska, and left a message stating the funds were diverted to her account illegally, the police had been contacted, it was urgent she return the funds and call immediately. Much to Lisa's surprise Beth called back!

Beth claimed the funds were taken to a Western Union® and sent to her fiancé. She promised to get the funds back from the Western Union office, because she had not transmitted them to him yet.

Lisa asked her why she was sending funds to her fiancé. Beth said her fiancé told her the money would be coming to her account and that she was to take it immediately to a Western Union and forward it to him. She claims she did not know he was doing anything illegal and that she had never really met him.

Lisa asked, "How could you be engaged to someone you never met? How did you come in contact with this man?" She said they met using an online dating service. She said his name was Tito and he had sent all the emails directing people to send funds to her account.

Beth said she almost sent the money to him in the Philippines, but finally figured out what she was doing might be illegal. She promised to return the funds to her bank the following day and direct them to send the funds back to Chicago Title Company.

On Friday, November 16th, Lisa contacted the receiving bank in Nebraska and shared with Gerald, a bank representative, the details of the crime. Gerald was shocked and blurted out, "You just can't fix stupid!" He went on to tell Lisa the bank had received a $6,000 wire on the same day from Title Agency, Inc. in West Palm Beach, Fla. to that very same account.

During the conversation, Beth walked into the bank with the cash – $5,702.50 from Chicago Title plus $6,000 from Title Agency, Inc., minus $120 in Western Union Fees. After the cash was counted and deposited, Gerald sent the $5,702.50 back. He then said he would attempt to contact Title Agency, Inc., since they had not tried to recall their wire.

Luckily within two hours, Chicago Title was made whole and received their $5,702.50. In the meantime, Lisa found out Title Agency, Inc. was an agent of Fidelity National Title and she reached out to them to let them know their wire had been illegally diverted. They received their $6,000 back minus the $120 in Western Union fees.

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

MORAL OF THE STORY

Do not act on emailed wire transfer instructions. If you receive emailed wire transfer instructions, put them in an instruction and send them to the principal to review and approve. Do not respond to the sending email account. Initiate a new email to the recipient. And, since the email contains someone else's bank account information, be sure to encrypt the message by using the "Send Secure" feature in Microsoft® Outlook®. If the instructions are for the wire transfer of real estate commission, the instruction should be physically signed by the designated broker.

When wire instructions are changed, closely examine the email address, do not "Reply" but rather call a known-good telephone number (not the one in the email with changed wiring instructions), and make sure the broker or agent knows exactly WHY you are confirming.

Most importantly, if you fall victim to a crime do not wait to get others involved. Your first point of contact should be your immediate supervisor and the second should be National Escrow Administration. The quicker we act, the better our chances for full recovery.

100 MONEY orders

The Financial Crimes Enforcement Network (FinCEN) recently published their findings of a study they conducted assessing Suspicious Activity Reports (SARS) and Suspicious Form 8300 Filings Related to Real Estate Title and Escrow Businesses 2003–2011. The study confirmed the importance of Title and Escrow Companies filing of IRS Form 8300 – Report of Cash Payments Over $10,000 Received in a Trade or Business. Read on for the details of a transaction in which cash was received and reported.

An escrow officer for Fidelity National Title Company in Fresno, Calif. contacted the National Escrow Administrators via email at settlement@fnf.com for assistance. She had just opened a new sale transaction. It was the purchase of a REO property with a sales price of $1.3 million. According to the Purchase and Sale Agreement the buyer agreed to deposit $50,000 in earnest money with the escrow company and the sale was scheduled to close in less than a week. So far so good, right?

Along with a copy of the Purchase and Sale Agreement, the real estate agent delivered an envelope to the escrow officer. Inside the envelope was the earnest money deposit of 100 money orders, in increments of $500. After she picked her jaw up from her desk, she informed the agent she would have to file some additional forms and needed some information from the buyer. She explained she would look into exactly what information she needed and get back with him. This is when she contacted her Escrow Administrators.

She was correct to do so. The receipt of the money orders triggered an obligation to file IRS Form 8300. Pursuant to the IRS Regulations, businesses who receive "cash" payments in excess of $10,000 need to report the funds received. "Cash" as defined by the IRS is:

1. Coin and currency
2. Cashier's checks, official checks, bank drafts, traveler checks and money orders if they have a face value of $10,000 or LESS.

Settlement agents must file Form 8300 upon receipt of multiple "cash" items received in one transaction. The multiple payments may have been made at one time or over the course of the transaction. A settlement agent must report upon receipt of the final "cash" item which puts the total of all "cash" received more than $10,000. Obviously this was the case in this deal.

The National Escrow Administration sent the escrow officer a copy of Tech Memo 153-2012 Reporting Cash Payments over $10,000 using IRS Form 8300 and called her, as there was more than one issue to discuss. First, the escrow officer needed to obtain a signed W-9 - Request for Taxpayer Identification Number and Certification, as well as a copy of the buyer's driver's license. Next, she was reminded the form had to be filed within 15 days. Lastly, they discussed the timeframes for clearance of the funds.

The money orders were issued by Western Union® and MoneyGram®. Money orders may clear as soon as seven to ten business days but they could take longer depending on which Federal Reserves they were drawn on. Additionally, money orders are often counterfeited. If a money order is counterfeit, it could take weeks before it is discovered and the Company is notified. When this occurs, the funds previously credited to the trust account are immediately debited from the account. This poses a risk to the Company if the file closes and is disbursed without allowing sufficient time to pass to ensure they are not fraudulent.

The escrow officer contacted the selling agent to let him know what she needed from the buyer and informed him the closing date would have to be delayed. The agent made arrangements for the buyer to come see the escrow officer by the end of the week. Fortunately, both the buyer and seller understood the need for an extension to the closing and the buyer assured the escrow officer he would wire the balance of the closing funds.

The buyer was cooperative, so she asked why the earnest money came to her in this manner. Turned out he is a real estate investor. He regularly attends auctions. At an auction the successful bidder has to pay right then and there with either cash or certified funds which is why he had money orders in that denomination. Since, at an auction he does not know what the sales price will be he regularly purchases money orders in small amounts so he can pay for his purchases. This explained why he seemed unfazed by the request for his Social Security Number and driver's license - he was familiar with this process.

MORAL OF THE STORY

Real estate transactions are often a target for illegal activity including a means to launder funds. Money laundering involves disguising financial assets so they can be used without detection of the illegal activity that produced them. This is true, unless the funds are reported. Settlement agents have a duty to monitor and report "cash" payments to the IRS. Failure to do so can result in hefty fines.

Although the escrow officer did not believe this buyer was up to anything illegal, she still identified she had a responsibility to report the "cash" received, eliminating the Company's risk of being fined. In order to ensure she did this properly she did not hesitate to contact National Escrow Administration for assistance.

FRAUD Insights

OFFICE *and personal safety*

I had the opportunity to attend a day of training. The topic was safety. Since I so rarely get the opportunity to be the student, I was excited about the chance to learn something new. The speaker was engaging, pleasant and most of all informative. Not only did I gain some great ideas for our offices but for me personally as well.

– Diana Williams, FNF Corporate Escrow Administrator

The most disturbing statistics were the top three real estate crimes: data theft, stalking and assaults. It is no secret identity theft, also referred to as data theft, is on the rise. Although the Company has installed firewalls, invested in anti-virus software and restricted access to unsafe websites on our computer systems, our business still requires us to have non-public sensitive information in file folders in our offices. On a daily basis we have people in and out of our offices with access to all of this information.

What part can settlement agents play in keeping this information safe? Here are a few tips:

» **Make sure if you walk away from your computer (even for a minute) you hit "ctrl+alt+delete" to lock your computer. It takes only seconds for a thief to download information from your computer or load a virus on your system using a USB drive.**

SAFETY CORNER

» **Do not leave back doors unlocked. Only allow customers to enter through the front door.**

» **Have a bell on the front door if it is unattended.**

» **Do not leave someone unattended in your personal office where they have access to your files.**

» **Never allow a visitor to freely wander through the office. If someone needs to use the restroom ask a colleague to escort them.**

» **Scale down. It is not necessary to keep a copy of everything, especially a copy of the entire loan package in your files.**

» **Encrypt emails which contain non-public personal information.**

» **Consider having visitors sign in or be sure the receptionist has a list of appointments scheduled for the day.**

Most of all, plan ahead by having a process. Discuss office safety together, come up with a plan and follow it. Our Company has an entire website dedicated to Information Security which can be accessed through the Company's intranet at home.fnf.com. You can learn about our policies and procedures.

Although the class provided the great office safety tips I was much more inspired by the personal safety tips. Having been in this business for 20 years I have seen many settlement agents put themselves in harm's way. Truthfully, I have even put myself in harm's way. All of these tips are common sense but serve as an excellent reminder of the simple steps you can take to protect yourself.

» **Do not put your vacation schedule on Facebook® or Twitter®. Make sure your out of office message does not say you are leaving.**

» **Lock up or keep your purse out of sight at their office and in your car.**

» **When leaving the office after hours, call to let someone know you are leaving. Talk on your cell phone while walking to your car or ask the security guard to escort you if there is one available to you.**

» **The same is true if you attend a local event or meeting outside of the office. Be sure someone knows where you are and when you are leaving.**

» **Slow down, take a look around. Take just one second to look around before leaving the office, getting in or out of your car.**

» **Do not park near shrubs or something a perpetrator could hide behind.**

I learned all of these tips from Andrew Wooten, C.P.P. and President of Safety Awareness Firearms Education (S.A.F.E.). The website is full of tips for living a safer life including an option to sign up for their monthly newsletter (www.justbesafe.com). The newsletter offers quick and easy tips on how to live a safer life. Take advantage of these free tools to be safe.