FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

By Lisa A. Tyler
National Escrow Administrator

The wire fraud schemes have evolved yet again. The latest evolution involves fraudsters spoofing or imitating legitimate FNF email addresses. Email spoofing is the creation of email messages with a forged sender address, making it appear that the email is sent from an email address even when it is not. The fraudsters obtain detailed transaction information by compromising the email account of a party to the transaction, typically the real estate agent's account or buyer's email account – not the FNF employee's email – and sending fraudulent wire instructions through an email account, either using a spoofed email address or using an email address which closely resembles that of an FNF employee's email address.

From there, the fraudsters monitor the transaction, deleting and intercepting legitimate emails containing wire instructions and then sending their spoofed or fraudulent email in an attempt to divert the wired funds at closing to their own account. Read "YOU have hit the Lotto!" to gain more detailed information on this complex scheme.

Next, cyber-thieves have discovered the next big jackpot by hacking the email accounts of parties involved in an exchange. Read "EXCHANGE accommodators" to discover how the thieves are attempting, sometimes successfully, to re-direct exchange funds into their own accounts via altered wire transfer instructions.

As mentioned in "OWNER'S title insurance – part I" from last month, the new CFPB rules require any charge allocated to the buyer for owner's coverage to contain the word "optional" in the description on both the Loan Estimate and the Closing Disclosure. In some markets, if the buyer opted not to purchase an owner's policy at closing, the cost of their loan policy would increase.

The CFPB rules require the full loan policy premium be reflected on the Loan Estimate and Closing Disclosure and not a discounted amount. As a result, the mortgagee's policy charge would not increase at closing. The rule calls for discounts to be mathematically applied in an entirely new way, which do not comport with most states' filed or promulgated title rates, or the contractual or customary payment arrangements between the buyer and seller. Read "OWNER'S title insurance – part II" to discover the correct amounts needed to disclose owner and loan policy premiums on the new forms.

IN THIS ISSUE

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

volume 10 issue 8
August 2015

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

YOU have hit the Lotto!

In a recent sale transaction, a real estate agent had his email account hacked. The hacker was watching emails going to and from the agent and the escrow officer. When the transaction was getting ready to close, the hacker created a fake email account that, upon a cursory glance, looked like the escrow officer's email account but was only slightly different.

Then, the hacker attempted to have the buyers wire their closing funds to an unrelated third party by sending an email to the agent, with a copy to the buyer, purporting to be from the escrow officer, using the faked email account.

The email from the hacker read as follows:

Hi Guadalupe, closing on the 16 June by 4 pm & statement process is progressing and you will get the buyer to wire there fund this week today to enhance smooth closing

The buyers had already signed their closing documents and deposited their closing funds with a cashier's check in the amount of $33,000, and so the buyers responded:

Sorry, I don't understand the request, my personal funds are already in the escrow account? Does this refer to me contacting my bank to get their funds deposited into the account or does that just happen?

The hacker's response:

You are required to get your lender to get fund deposited into the account I will give you the wire instruction if you able to wire funds today so let me know.

The buyer:

Okay will get it done today, please send instructions.

Hacker:

Here you go, attached is the wire instruction kindly send the confirmation of transfer once done for reference purpose.

The buyers dutifully forwarded the emailed wire instructions to their lender, thinking they needed them in order to fund the loan. Much to the loan officer's surprise, when she opened the attachment she discovered wire instructions to an account of an unrelated third party named Jane Doe. The loan officer then forwarded the email to the REAL email account of the escrow officer, who in turn shared the whole chain with FNF's national escrow administrator.

The national escrow administrator sent the email string along with the wire instructions to the bank in Texas where Jane Doe's account was held, informing them their account holder was attempting to divert and steal $33,000 from unsuspecting buyers in a real estate transaction.

The bank in Texas immediately contacted Jane Doe only to discover she was not a criminal at all. Instead, Jane was actually a victim in the foiled crime. The bank representative called FNF's national escrow administrator to share additional details they learned from Jane.

The representative said Jane was an elderly woman who had been notified by email she had won a lottery amounting to millions of dollars. The notification stated she had to pay a fee to a law firm in order to collect her winnings. The notification went on to say the host of the lottery would loan her the money to pay the law firm until she received her winnings. Thereafter the amount of the loan would be deducted from her winnings.

Jane received a separate email notification asking for her bank account information so the loan funds could be wire transferred to her account. She obliged with the request and waited for the funds to arrive. She had every intention of turning around and remitting the funds to the "law firm." Thanks to this particular buyer, however, the funds never arrived. The bank told Jane she was involved in a scam and they are actively helping her change her bank account information.

MORAL OF THE STORY

In most cases, a non-FNF email account of a party to the transaction is compromised with the attacker sending fraudulent emails in each direction during the wire transaction.

a. Attacker compromises an email account of a party to the transaction and monitors emails relating to the transaction. As FNF accounts are protected through a variety of means, it is outside email accounts, like real estate agents, lawyers, buyers and sellers, which are being compromised.

b. Attacker sees emails containing wiring instructions, and intercepts and deletes the email within the compromised account.

c. Attacker sends a fake or spoofed email to a wire remitter (buyer or escrow officer) appearing to come from the party who had sent the legitimate wire instructions; and this faked or spoofed email contains fraudulent wiring instructions.

d. Buyer or escrow officer receives the fake email and unknowingly wires the money to the fraudulent account, then emails the sender that the transaction has been completed.

e. Attacker then intercepts and deletes further emails traveling both ways to create confusion, all the while covering their tracks and escaping with the money.

Customers have no reason to suspect the

[Continued on pg 3]

TELL US HOW YOU
STOPPED FRAUD

settlement@fnf.com or
949.622.4425

MORAL OF THE STORY – CONTINUED

new wire instructions they receive are fraudulent since the email appears to be sent from a legitimate email address. As a result of this fraud, the Company and our customers can potentially be swindled out of large sums of money.

The Company is continuing to emphatically exhort our direct operations to educate their business partners on the latest scheme so that they can make the changes previously recommended by the Company to their internal policies relating to the acceptance of wiring instructions. Recommend any party to the transaction confirm all wiring instructions sent by email with a phone call to a known, good phone number.

Settlement agents sending out wire instructions to customers could include an alert in either their initial communications with customers or in their signature blocks. The alert could read that email recipients of wire instructions should immediately call the escrow settlement agent directly to confirm the legitimacy of the enclosed wire instructions. Here is a sample message added to escrow settlement agent's signature blocks:

*****Be aware! Online banking fraud is on the rise. If you receive an email containing WIRE TRANSFER INSTRUCTIONS call your escrow officer immediately to verify the information prior to sending funds.*****

EXCHANGE accommodators

Other potential targets for a cyber-theft using emailed wire instructions are 1031 exchange accommodators who receive increased reports of attempted diversion of funds in and out of their exchange transactions, through hacked emails and altered wire transfer instructions.

On April 28, 2015, Liz Jameson, an Exchange Coordinator with Investment Property Exchange Services, Inc., (IPX1031®) was sent an email from a current exchanger including instructions for a wire transfer in the amount of $19,340. Below is the content from the email:

Hi Liz,

We need to make a domestic wire transfer in the amount of $19,340. So we need about 19,400. net from the account. Please advice. Do you have to provide us with the letter of Authorization for Dad and mom to sign?

All the best,
Ivan Investor

In her review of the email, Liz picked up on a few subtle warnings that the message might not be legitimate. She noticed the spelling of advice (instead of advise) and the sender requested, "a domestic wire transfer in the amount of $19,340. So we need about 19,400. net […]." Liz realized this was a request for an estimated amount and the real exchangers already knew the exact amount required to close their transactions.

Liz called the exchanger directly rather than respond to the email. The exchanger confirmed he did not send the email and realized his email had been hacked. Liz's proactive measures not only prevented a loss, but also informed the client his email account was compromised. What was particularly scary in this story is that from reviewing Ivan's email account and prior communications, the hacker even knew the file was in the name of Ivan's mom and dad, and that Ivan was only serving as attorney-in-fact!

For Liz's efforts in detecting the hacked email and preventing funds from being wired to a thief's account, she has been rewarded with $1,500 along with a letter of recognition from the Company.

The industry has had a similar incident with quite a different ending. In this case the fraud was perpetrated against a settlement attorney. As a result, the net sale proceeds were sent to the fraudsters instead of an exchange accommodator in the amount of $500,000!

Similar to what we have seen in the last attempt, the fraudster hacked into the actual email account of a party to the transaction. In this case, the email belonged to the paralegal of the settlement attorney. This is significant because emails from the fraudster were sent from the actual email of the individual the parties communicated with during the transaction and thus more difficult to detect.

Once in the account the fraudsters deleted the falsified emails from her "sent" and "deleted" folders, hiding the fraud and making the subsequent investigation more difficult.

In addition, the fraudsters sent an email to the paralegal impersonating the exchange accommodator, changing the wiring instructions.

Wiring Instructions

Bank Name:	XYZ Bank NM1-231-01-01-01 6645 Camino Coors NW Albuquerqu 87120
Routine No.	107000324/026009593
Account Name:	ABC, LLC
Account No.	123456789

Elsie Accommodator, AVP
Exchange Coorinato

What did you notice about the content of these instructions?

1. The spelling of Albuquerque is incorrect.
2. Routing Number is referred to a Routine No.
3. Account name is not the exchange accommodator
4. Coordinator is missing an "r"

[Continued on pg 4]

FRAUD Insights

[EXCHANGE accommodators – continued]

The paralegal apparently failed to notice any of these items and did not call the exchange accommodator to verify the emailed instructions. Instead, the paralegal wired more than $500,000 in exchange funds to the account of ABC, LLC.

Following the redirection of the funds, the exchange coordinator received a number of emails from the paralegal's email account by the fraudsters stating she was waiting for the buyer's funds to clear before the net proceeds could be wired to the exchange accommodator. The significance of this is the fraudsters knew the "good funds requirements" and also delayed detection of the misdirected wire.

In addition to the ignored "red flags" this incident also illustrates the importance of a "Call Back Policy." If the paralegal had followed a "Call Back Policy" and phoned the coordinator to verify the wire instructions the fraud probably would have been averted.

Remember, fraudsters continue to lurk in the shadows, and we need to continue to be vigilant at detecting and preventing their crimes. Your continued attention to detail, dedication and adherence to the Company's policies are the best defenses!

Know before you close.™ | CFPB Readiness

OWNER'S title insurance – part II

If a buyer opts not to purchase an owner's policy, in most states they would not receive the benefit of a simultaneous issue discount applied to the loan policy premium. Currently, in a typical residential transaction, a lender quotes the discounted rate on a Loan Estimate.

However, any increase in this premium would result in a tolerance violation or increased annual percentage rate. Therefore, the CFPB wrote into the new rules any simultaneous issue discount must be applied to the owner's policy premium and not the loan policy premium.

Therefore, when the new CFPB rules are implemented, the lender will need to disclose the full lender's policy premium on the Loan Estimate and the preparer of the Closing Disclosure will charge the full loan premium. The new formula for calculating the owner's premium with the simultaneous issue discount applied is as follows:

Owner's Premium
+ Simultaneous Issue Rate
- Full Loan Premium
= Owner's Rate

The new calculation method applies regardless of which party to the transaction is paying the owner's policy premium. For example, the premiums on the purchase of a $300,000 residence with a $240,000 loan closed simultaneously with actual premiums are as follows:

Owner's Policy Premium	$1,090
Loan Policy Premium (Full Rate)	$928
Loan Policy Premium (Simultaneous Issue Rate)	$469

On a transaction closed prior to the effective date of the new rules the seller would pay $1,090 and the buyer would pay $469. On the same transaction closed after the effective date of the new rules the disclosure would reflect the seller paying the calculated premium of $631 and the buyer paying the full loan premium of $928.

The title provider will still receive all the total premium dollars due to them. However, the seller ends up paying $459 less than obligated and the buyer ends up paying $459 more than obligated.

	Seller's Cost per Contract	Buyer's Cost per Contract	Seller's "Cost" per Disclosure	Buyer's "Cost" per Disclosure	"Cost" Difference – Seller	"Cost" Difference – Buyer
Owner's Policy	$1,090	$0	$631 ($1,090 +$469 - $928)	$0	$459 less ($1,090- $631)	$0
Lender's Policy	$0	$469	$0	$928	$0	$459 more ($928- $469)

The only way the formula works is if one of the parties to the transaction is paying both policy premiums, which in most markets is not customary. As a result, our systems have been designed to provide an off-setting debit to the seller for the balance of the owner's premium and an offsetting credit for the same to the buyer.

The disclosure amounts, and off-setting debits and credits only appear when the Closing Disclosure is printed using the Company's escrow production systems. Any other document, such as a closing statement or fee ticket, will print the premium dollars in the normal fashion.