FRAUD ALERT

In our ongoing efforts to keep our approved providers, agents, and other partners informed of potential threats to their business, we distribute Fraud Alerts so that you are aware of potential threats and can take any steps you feel necessary to guard against them.

We have sent out numerous alerts, newsletters, and other communications regarding the rampant epidemic of wire fraud in our industry. While we know that you are actively involved in combating this ever-growing problem, the fraudsters' techniques have continued to evolve in response to the industry's diligent efforts to frustrate their schemes. The latest in a long string of "Social Engineering Fraud" schemes is called "SPOOFING."

First, let's have a refresher on "Social Engineering Fraud." This is a fraud scheme where the fraudster gains information about a transaction and uses this information to gain the confidence of a person involved in a real estate transaction. (The fraudster might possibly intercept an unencrypted email, gain information through social media, or search through the trash.) This information, however acquired, is then used to impersonate a person in the transaction and defraud the disbursing party into wiring money to the fraudster – instead of the legitimate party. These fraudsters are now using technology to enhance their scheme and trick well-meaning and innocent victims.

"SPOOFING" Legitimate Parties

There are four primary ways to spoof a legitimate person in a transaction; to wit: (1) SPOOFED Email Addresses, (2) SPOOFED Web Links, (3) SPOOFED Fax Machines, and (4) SPOOFED Caller IDs. In each instance, the fraudster uses technology to impersonate a legitimate party – could be a seller, buyer, realtor, banker, or settlement agent, etc. **Each type of SPOOFING is very easily detected, if the proper steps are taken and the time is taken to verbally confirm certain sensitive communications – *such as wiring instructions*.**

(1) SPOOFED Email Addresses

We have already alerted you to the fact that many times the fraudsters make a slight change to the email address to gain your confidence or hoping that you will not notice (e.g. using JonTDoe@email.com instead of JonDoe@email.com). This simply required people to notice the different email address (an additional "T" in this example or some other different addition or deletion). As the word got around, more people were catching this fraud attempt, so the fraudsters have gotten more crafty.

Every email address has three ways that it can be viewed: (1) Screen Name (e.g. John Doe), (2) Actual Address (e.g. JohnDoe@email.com), and (3) IP Address (e.g. contains a string of 4 numbers JonDoe@[196.168.0.1] in the address). One way that the fraudsters conceal their true identity is to use the screen name to cover the actual address. If you tried to send an email with the address formatted "John Doe" and not JohnDoe@email.com, it would not go anywhere, but your address book may show the screen name and know what the actual email address is.

If you are sending or receiving an email, if you "hover" over the screen name, you will see the true concealed identity. You will see something that looks like:

John Doe <IWanna@TakeYourMoney.com>

If you read that you were communicating with someone you did not know (or with someone at TakeYourMoney.com) you certainly would not trust the communication. Additionally, just because the email came in an encrypted format, does not mean it is legitimate. **ALWAYS CALL INDEPENDENTLY KNOWN PHONE NUMBERS AND CONFIRM WIRING INSTRUCTIONS.**

(2) SPOOFED Web Links

The fraudsters will use this same technology to SPOOF a website. You see this a great deal on phishing emails that are pretending to be someone with whom you do business – an internet service provider, bank, store, or other legitimate business. The email bearing the logo of your bank may say something alarming like:

> *"Our fraud investigation team has determined that your account may have been hacked. Please click on the link below to log in and change your password."*

Previously, the link might look like this http://iaosdngkdis.com or http://MyBank.TakeYourMoney.com. The first one is unrecognizable and should not be clicked, but the second one has the name of my bank in it and you may wonder if it is legitimate. It is not.

Today, they are SPOOFING the web address hiding it beneath "CLICK HERE" or by using a legitimate looking character string and hiding the true destination by saying click here: My Bank. You can detect a SPOOFED web address by hovering over the link to see what truly lies beneath the link. You would see something that looks like this:

CLICK HERE <"http://IAmABadGuy.com/YourBank">

IF YOU NEED TO VISIT SOMEONE'S WEBSITE, VERIFY THE URL OR TYPE THE NAME OF THE WEBSITE INTO THE ADDRESS BAR ON YOUR BROWSER.

(3) SPOOFED Fax Machines

Some of you have said to yourselves, "I have had enough; I am going back to my fax machine." Once you get it out of the closet, you may have to set it up. The first thing that you will do is put in the "Sender's/Your" number into the memory so it will show up on faxes that you send. Then it hits you, the fraudster can do that too – thereby impersonating or SPOOFING the legitimate sender.

Fax machines are still a very useful tool, but remember that the fraudsters know how they work too. The same thing is true for regular mail. The fraudsters can impersonate legitimate parties just as easily as you can send a letter or a fax.

ALWAYS CALL INDEPENDENTLY KNOWN PHONE NUMBERS AND CONFIRM WIRING INSTRUCTIONS.

(4) SPOOFED Caller ID

Fraudsters have taken their deviousness to new lows. So you have read the alerts and other communications and you would never send a wire without verbally confirming wiring instructions at a safe, known, and independently verified phone number. You are almost ready to send the wire, so you look for a safe contact number. About that time, you receive a phone call from the fraudster pretending to be the recipient of your wire. You have caller ID and you check the caller ID on your phone to your safe number in your file. You asked the imposter/fraudster questions about the transaction and they seem to know what they are talking about. Now you feel comfortable – DO NOT!

Fraudsters and thieves are utilizing prepaid "burner" phones and applications that will "SPOOF" the caller ID of any phone number the caller chooses – even valid phone numbers of actual businesses. A pre-paid "burner" phone can be purchased at a convenience store and then discarded when the minutes are used. Fraudsters are combining this low cost phone with a phone application designed to prank your friends; however, they are using this insidious combination to SPOOF parties to a transaction, realtors, banks, tax offices – and the list goes continues to grow.

Fraudsters have quickly learned that our responsible title and settlement professionals have begun utilizing call-back procedures to validate and verify emails regarding wiring of funds. The fraudsters continue to adapt their scheme in an attempt to circumvent our protective practices and procedures by SPOOFING the caller ID.

DON'T GET SPOOFED! AN INCOMING PHONE CALL NEVER TAKES THE PLACE OF AN OUTGOING CONFIRMATORY CALL BEFORE WIRING FUNDS.

HOW CAN YOU PROTECT YOURSELF OR YOUR FIRM AGAINST THESE SCAMS?

1) Encrypt emails or use other secure methods of delivery of any communication containing wiring instructions, details of the transaction, or other sensitive financial information (such as a settlement statement).

2) Exercise a high degree of suspicion for any wiring instructions you receive that do not come through encrypted email from a trusted source, especially if they replace existing wiring instructions.

3) Prior to wiring any funds, confirm by telephone that the intended recipient of the funds did in fact send or change its wiring instructions.

4) When confirming by phone, do not rely on phone numbers or web addresses in those emails, as they would be fraudulent as well.

5) Always look closely at an email address prior to hitting "reply" to see if it is SPOOFED.

6) Educate parties to the transaction to only use encrypted email or other secure methods to deliver sensitive transaction information. Further educate them that you will only use encrypted or secure technology to communicate with them.

7) Visit http://InvTitle.com/Wire for more resources on protecting your clients and yourself from fraudsters and their SPOOF schemes.

8) Contact your Insurance Agent about purchasing cyber-fraud insurance. Please make sure that the coverage includes recovery for a cyber-breach (loss of information), cyber-crime (loss of money), and cyber social engineering fraud (as detailed hereinabove).

We are interested in alerting our approved providers, agents, and other partners in the real estate business of any and all external and internal threats and fraud scams. In the event that you become the target of a fraud scam, please share that with us so that we may alert others. You may email the facts about the attempted fraud scam to riskmanagement@invtitle.com.

This Fraud Alert is a service of Investors Title. If you have any questions about this Fraud Alert or the contents hereof, please feel free to contact Jonathan Biggs, Vice President of Risk Management and Education, at riskmanagement@invtitle.com.

Investors Title
121 N. Columbia Street, Chapel Hill, NC 27514
800.326.4842
invtitle.com