FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

HEALTHY skepticism

By Lisa A. Tyler
National Escrow Administrator

Never discredit your gut instinct. If something deep inside of you indicates something is not right about a person or situation, trust it. Michele Smiley and Simone Clacher, both Escrow Officers at Fidelity National Title of Florida, always do their best to protect the Company from potential claims, regardless of the dollar amount. They read *Fraud Insights*, they follow Company Policy and have developed a healthy sense of skepticism which proved to be beneficial when they were asked to handle a sale of a vacant lot for $18,000. Read "SPIDEY senses" for the details.

Fraudsters continue to divert money away from real estate transactions. Multiple safeguards and checks and balances help keep the best of us from making a mistake. In the story "ATTENTION to detail," Sandee Dhanowa double checked the account number before processing a payoff to reveal the payoff statement had been altered.

Do you subscribe to a credit monitoring company or identity theft protection service? Diana Hoffman, Fidelity's Corporate Escrow Administrator, does. She was alarmed one morning when she woke up to an email that read, "**Information about you may have been exposed on the dark web**." Read this month's **cyber buzz** article entitled "WHAT is the dark web?" for more information.

IN THIS ISSUE

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

volume 15 issue 11
November 2020

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

SPIDEY senses

The listing agent was contacted by the seller online. The seller explained he was French but working in Spain and unable to travel due to the pandemic. He asked the real estate agent to list his vacant lot for sale.

They agreed on a price and the real estate agent processed the paperwork. She also recommended a Certified Public Accountant (CPA) firm to assist him with the Foreign Investment Real Property Tax Act (FIRPTA) withholding paperwork. He contacted the CPA by email.

The lot sold quickly for $18,000 and escrow was opened at Fidelity National Title of Florida with Michele Smiley and Simone Clacher. The listing agent let them know the seller was the citizen of a foreign nation and already working with a CPA to put the FIRPTA Withholding paperwork together. The real estate agent told Michele and Simone the seller was working in Spain and provided them with his email address. This prompted Simone to ask more questions.

Simone wanted to know if the listing agent ever met or spoke on the phone with the seller. The real estate agent said no; she only communicated with him via email. Simone explained to her she would not close the transaction unless she spoke directly to the seller via phone or by some type of video conference.

Simone offered several options. They could meet via Microsoft® Teams, using Facebook® WhatsApp, Microsoft® Skype or another virtual method. The real estate agent said she would convey the information to the seller.

The CPA firm contacted Fidelity for information about the sale. Michele asked them if they had spoken with the seller yet and whether they had a signed release from the seller authorizing her to discuss the transaction with them. The CPA firm stated that it had not and that he had yet to respond to any of its emails.

Michele advised the CPA firm contact to let their client know she needed his authorization and he should contact her or Simone by phone. The CPA firm understood and assured Michelle that she would be kept in the loop.

Everyone knew Simone and Michele would not close without meeting the seller over video conference and receiving a copy of his passport. They wanted to be able to compare the picture of the seller from the passport to the video when they met virtually.

The real estate agent advised her client in order to proceed with the title search for closing, the title company had requested a copy of his passport, phone number and the contact information for the CPA firm — along with his authorization to speak with them.

The seller emailed a copy of his passport to the listing agent, which only confused the situation further. He told her he was French, but the passport was issued by Switzerland. The signature appeared to be an eSignature rather than a live signature and it generally appeared suspicious.

Keep in mind it was only a black and white scanned copy, but that was what made it so suspicious. The picture was crystal clear and other parts of it appeared blurry.

The listing agent dug in, did some additional research and found a U.S. mailing address for the property owner. She sent the property owner a certified letter to which the property owner replied by email. The message read:

> *This is to refer to your June 17, 2020 letter enclosing a signed copy of an alleged listing contract. I am afraid that there is a major misunderstanding on your side.*
>
> *As a matter of fact, I don't recall having ever signed with your Company any "Vacant Land Listing Agreement."*
>
> *I am especially disturbed to note that the contract sent to me bears a signature which is not mine. It appears to me that you are trying to force me to entrust your Company to sell a piece of land which is my property in Cape Coral, Florida.*
>
> *You are therefore kindly requested to confirm that you have never been entrusted by me at any time to sell any piece of property I owe in Florida on my behalf.*

The listing agent discussed the response with her broker. They both reached out to the real property owner to explain the situation and assure him they were trying to protect him.

The broker contacted Fidelity and advised them to stop all communication with the fake seller. The broker instructed escrow to refund the earnest money to the buyer.

Michele and Simone immediately resigned from the transaction. The earnest money was refunded to the buyer and the title officer was notified so they could add a note to the title plant in case the imposter tried to sell the property to someone else.

Stacey Barker, V.P. and Escrow Administrator, nominated Michele and Simone for this award.

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

[SPIDEY senses — continued]

She said, "I thought you would like to see a transaction where the closer's due diligence and attention to detail revealed a fake seller. The fake passport and his unwillingness to contact the closer for a conversation were dead giveaways."

Stacey was proud of Michele and Simone. We are too, which is why they are splitting the $1,500 reward. Their healthy skepticism proved to be useful in avoiding a potential claim.

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

ATTENTION to detail

Fraudsters work hard to conceal their identity and have found ways to insert themselves into every step of the real estate process. They make last minute changes to keep the victim or settlement agent unaware that wiring instructions have been tampered.

Our employees, however, have become more vigilant and aware of the fraud. Sandee Dhanowa, a processor for Lawyers Title Company, works in the payoff department. She performed a second review of wiring instructions before processing a payoff wire, partially shown below:

Wiring Instruction - *You must include the "Reference" information listed below if wiring funds*		
Bank Name:	Receiving Bank	
ABA Number:	123456789	
Account Number:	1231231231	
Account Name:	Mortgage Servicing Company	
Reference:	1234567890 / Buyer Name	
PO1.rpt – Email		fraudster@gmail.com
5/11/2020	20	1

Comparing these instructions to any other demand from the same company would reveal nothing suspicious. The letter format, text, font and appearance were identical. The remainder of the payoff statement was completely unmodified.

However, Sandee never strayed from Company policy. She compared the account number to the known and verified mortgage servicer instructions and discovered the account number was not a verified account number for payoffs.

The escrow was being handled by an independent escrow agent. Sandee requested they obtain another demand from the mortgage servicing company. Comparing her first documents to the new, unaltered payoff statement seen below, there was little to distinguish them apart — except for two items. The first exception was the account number.

Wiring Instruction - *You must include the "Reference" Information listed below if wiring funds*	
Bank Name:	Receiving Bank
ABA Number:	123456789
Account Number:	2342342342
Account Name:	Mortgage Servicing Company
Reference:	1234567890 / Buyer Name

The second exception was the email address that was added to the altered instructions. All the other information appears in the same order as the valid, unaltered payoff. The account name and routing number are all the same.

Realizing the instructions had been modified Sandee alerted the independent escrow agent, providing advice on how to communicate moving forward. Her actions ultimately saved the Company and our customers from a major headache and a potential loss of $346,714.47.

Fraudsters continue to try and lull our busy industry to sleep by making the least amount of changes possible. Double checking our work will only strengthen our defense against fraudsters. Moreover, remaining on red alert for all wired funds is a must, no matter how trivial the wiring instructions may seem.

Sandee prevented a potential loss by spotting a small change only recognizable by a watchful and attentive approach. For her efforts, the Company is awarding her $1,500.

Article provided by contributing author: Scott Cummins, Advisory Director • Fidelity National Title Group • National Escrow Administration

WHAT is the dark web?

When I received an email that read, "Information about you may have been exposed on the dark web," I had so many questions. What does this mean? What do I do? How do I protect myself? I logged on to my identity theft protection service to find the answers to my questions.

The website clearly and concisely explained what they found and what I should do. It read:

What is this notification and why are you receiving this?
The exposed information is potentially associated with the website/service sharethis.com. In the past you may have signed up for sharethis.com or provided the information to a service that is in some way associated with sharethis.com.

It may be difficult for you to remember — or you simply may not know — other services are associated with sharethis.com. What is important to know is that information belonging to you appears as if it is being shared improperly on the dark web.

Exposed information from data breaches, hacking incidents or leaked information, can be bought and sold on the dark web as "lists." The buying and selling activity by identity thieves may occur months to years after it was actually exposed in a security incident.

Even though you may have stopped using sharethis.com, or perhaps deactivated the account, or maybe unsubscribed, the information could still be available in their systems.

Description
The site sharethis.com had been reported in February 2019 to possibly have suffered a data exposure that could include names, usernames, emails and passwords.

Exposed Information
Any personally identifiable information that has been taken during a breach, hacking incident or leaked information is referred to as exposed. This data may show up on the dark web where

[Continued on pg 4]

[WHAT is the dark web? — continued]

cybercriminals look to sell this information to make money. Exposed information does not yet necessarily mean that it has been used to hack into your account or to commit identity theft.

The following information has been exposed on the dark web; even though you have not provided this information to us, it may be associated with your identity. Note that stolen data on the dark web can often be outdated or unrelated to you.

Email
*h*******@fnf.com
Additional Exposed Information
Password, Full name

What can you do next?
Being proactive with best practices and next steps, such as the following, can help:

- Change the password associated with the affected website or any other site that uses that password.
- If you do not remember your password, perform a password reset on the site.

Review your credit report, watch for new credit inquiry alerts or suspicious activity, and consider freezing your credit file.

The good news, I have never used that website before. My personal information was not exposed, but this was a great reminder to change passwords and ensure the sites I do use are secure. Additionally, there was no evidence that FNF was the source of the exposure of my email and password.

However, I still had so many other questions starting with, "What is the dark web?" I found out the world wide web has three different levels and the content is based on the access available and common purposes.

Public Web
Information you readily find on public search engines such as Google™ or Microsoft® Bing. Most internet users spend their time at this level shopping, searching for information, and sharing photos and videos on social media.

The Deep Web
The deep web is the next level. These sites are not indexed by search engines, meaning they will not show up in search results using Google or other publicly available search engines. Examples of deep web content includes:

- Internal company sites
- School intranets
- Online databases
- Member-only websites or pages which require a subscription or payment to access

These sites are found in the deep web level because the sites are only intended for member-access — such as those behind paywalls or which require authentication. While the name may sound menacing, most deep web sites are legitimate and lawful, just hidden from or not indexed by any public browsers on purpose. Sometimes the deep web is referred to as a "bad" place only because it is being confused with the dark web.

The Dark Web
Below the deep web lies the dark web. The dark web is a hidden network of websites which are inaccessible through standard browsers or methods. Accessing it often requires special resources or browsers.

Those who do access the dark web do so with a high degree of anonymity since the browsers they use mask their true identities by hiding their IP address. This is contrary to what occurs on the public web.

Visitors of a website on the public web records or reveals the users IP addresses, then tracks online activity. On the dark web, masking software installed on the computer routes the connection through a randomized path to its destination, bouncing around a number of encrypted connections. Ultimately, the process masks both the location and identity of the person searching or accessing the dark web.

Since users and their locations are hidden, it is no surprise the dark web can be a haven for all kinds of illicit activity; including the tracking of stolen personal information captured through means such as data breaches or hacks. Reams of personal information is often posted on the dark web for sale to criminals up to no good.

On the dark web, people looking for this information can get access to records referred to as "fullz" because they include the full package for fraudsters to wreak havoc on someone's credit or worse. The "fullz" includes their full name, Social Security Number, birth date, account numbers and other sensitive data. These criminals can make a decent living by selling, buying and using other people's personal information.

How Can You Protect Yourself from the Dark Web?
People often are not worried about the dark web until something like a data breach happens and they are notified their information was stolen. There is no absolute way to keep your information off the dark web because hackers are always trying the latest scheme to get your information and sell it to those looking to pay for it. You can be vigilant about looking for red flags:

- Monitor your accounts and statements for any charges or changes you did not make
- Check your credit report regularly for new accounts or activity you did not authorize
- Use strong passwords
- Consider an online product to help you protect your identity and monitor your credit
- Know how to respond immediately to suspicious activity
- Do not reuse passwords across multiple sites
- Enable multi-factor authentication if websites offer that as an option

At Fidelity, the Security Operations Center monitors the dark web for accounts that use the .fnf domain email address. By staying on top of potential issues, you can help minimize the impact if your personal information falls into the wrong hands.

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