FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

NEW rules, new forms you need to know

By Lisa A. Tyler
National Escrow Administrator

On November 20, 2013, the Consumer Financial Protection Bureau (CFPB) published the Integrated Mortgage Disclosures, combining disclosures consumers receive in connection with applying for and closing on a mortgage loan under the Truth-in-Lending Act (TILA) and the Real Estate Settlement Procedures Act (RESPA).

The final rule includes new forms that will be used in virtually every residential mortgage loan originated and closed after August 1, 2015. The new rules are 1,888 pages long! To find out how they are going to impact settlement agents and title insurers nationwide, join us at a "2014 Ultimate Escrow Training" event.

The new vocabulary used in our world lately is amazing. For example, "blight" is not a new word, but it has a new definition and is currently used in many real estate related news articles. It was originally used to describe a plant disease. Currently it is used in the real estate context to mean, "…the physical decline of a property, neighborhood or city due to a combination of economic downturns, residents and businesses leaving the area and the cost of maintaining the quality of older structures."

In this edition we introduce you to a new term called "iMugging." Read the article "BE careful of iMugging" to discover a new word and its definition.

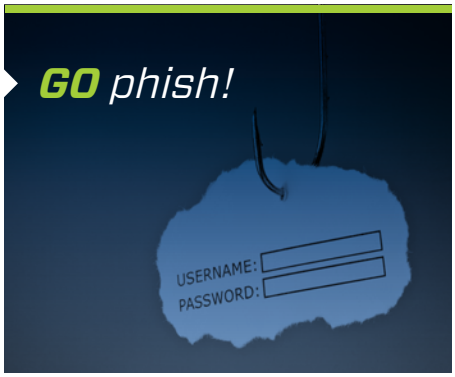
Has the junk email you receive increased significantly? Recent changes to our email accounts have changed the way the spam is filtered by our email servers. The story entitled "GO phish!" reveals the ways hackers are tricking you into clicking on malicious email links.

Is one of your resolutions to be more productive this year? We have the perfect solution to keep you on track with your goal. Read "START the year off right!" to discover 10 tips for making yourself more productive in the coming year. Work smarter, not harder!

Our settlement agents are so HELPFUL! They truly want to help consumers understand everything about the closing process and MORE! We want to prove to you over the next twelve months that there are just some things you do not know and as a result, should not help the customer understand.

For the next 12 editions we will run a story called "FIRPTA nightmare" to convince our readers to stop helping customers attempt to understand federal tax law and instead, to refer them to a tax professional.

IN THIS ISSUE



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

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

2014 ultimate escrow training

Come on safari with us as we guide you through the labyrinth of new industry rules, explore real estate trends and hunt down the answers to all your tail-biting questions. Fidelity National Title Group takes great pride in the "Ultimate Escrow Training" events. You are guaranteed to walk away unscathed with a treasure chest full of new information.

Employees of the Company can register for a live seminar event or a live webcast event, using the following link: http://escrow.fnf.com/

Whether you attend a live seminar event or a live webcast event or both, the escrow training events are absolutely free to our employees. These training events provide the information needed to better service your customers while remaining compliant with Company policy and procedure. Do not delay. Register for a training event today!

BE careful of iMugging

iMugging occurs when someone attacks you to steal your smart phone or tablet. iMugging was first used to describe someone being mugged for their Apple® device, such as an iPod®, iPhone® or iPad®. Due to the popularity of these types of devices iMugging is not just limited to Apple products. Anyone with an MP3 player, smart phone or tablet is at risk.

iMugging is big business and because the stolen items are so expensive iMugging can be categorized as grand theft. It is easy for a robber to iMug someone because the expensive devices visibly distracts users.

In addition, it is simple to identify what type of device you have. Using the white headphones provided with your iPhone makes you an easy target because it can identify what type of phone you have. Being on the phone also makes you less aware of your surroundings.

Since our business requires us to be mobile, many of us use smart phones and tablets in order to stay connected with our customers. Here are a few tips to ensure you can work safely and still be responsive to your customers:

1. **Password protect your device**
   One of the great conveniences of mobile devices is the fact you can stay logged on to your email account. Unfortunately if you are iMugged, this means the thief can also access your email. Be sure to secure the device by locking the screen requiring you to log in to access your phone.

2. **Do not send non-public information from your mobile device**
   Keep in mind emails which are sent within the FNF network are safeguarded, but if you forward an email from your personal mobile device to a customer it might not be sent securely. You might have to wait until you are back in the office to properly encrypt an email before sending it on.

3. **Do not open or click on links in suspicious emails**
   It is not as easy to identify a suspicious email received on a smart phone. Before opening any emails, look at the email address or name of the sender. If you do not recognize it consider waiting until you are at the office and working on your desktop before opening. If you do open the email and it contains a link in the body of the email - stop. Take a second look to confirm if the email has come from a trusted source. Do not click on a link if you do not know who the sender is.

4. **Install anti-virus software**
   Mobile devices are subject to hacking just as desktop computers are. Be sure to protect your tablet or smart phone by installing anti-virus software. Work with your Information Technology (IT) Department to find the best software for your device.

5. **Familiarize yourself with the FNF Web Presence and Social Media Policy**
   Being mobile makes it quick and convenient to update your Facebook® page or send a Tweet with Twitter®. Be sure you have read and understand the Company Policy to ensure compliance.

[Continued on pg 3]

settlement@fnf.com or
949.622.4425

[BE careful of iMugging – continued]

Lastly, be sure to keep your mobile device in your control at all times. Do not leave it unattended. Be aware of your surroundings. Trust your gut instincts and remember your personal safety is of utmost priority.

If you are iMugged be sure to file a police report and notify your IT manager so they can have the device shut off. Following the steps above will help ensure the only thing the robber gets away with is the device itself.

GO phish!

In the last year changes to Microsoft® Outlook® have resulted in an increase of junk emails received. Unfortunately some of these emails are not simply advertisements or junk; they are dangerous and could potentially result in someone hacking into your email account. Once a hacker has access to your email account, emails may be intercepted or sent from your account. Protecting your email account from hackers is actually quite simple. Read on for tips on how to protect your account.

Hackers try to trick (phish) you into clicking on links that may appear to be legitimate, but are actually trying to fool you into providing your login credentials. Phishing emails often have tell-tale signs they are fraudulent. For instance the "To:" line may be blank or grammatical errors may be abundant. Additionally requests that require you to act immediately or urgently are a red flag that should be a warning to think carefully before you click on any links. The subject line of the email can also be a clue to phishing emails; especially if the subject references transactions that do not exist or the context of the email is out of character with your normal correspondence.

Anytime you are asked to click on a link in an email, you should first place the cursor over the link. Do not click on the link. This reveals the true Uniform Resource Locator (URL), which is the address of a Web page. If the URL does not match up with the sender's information, do not click on the link.

Legitimate websites use Secure Sockets Layer (SSL) (Secure Sockets Layer (SSL): A proposed standard method of increasing security on the Internet, by making it difficult to intercept critical information, such as credit card numbers, when those are communicated on the Internet.) or other similar security technology which helps protect their customers' personal information entered on their site. You can verify the site is secure because the Web address will begin with https://. The "s" after http stands for secure (instead of the usual http://).

Be aware of URLs that include the @ sign. Browsers ignore anything in a URL which comes before the @ sign.

Another common technique used by phishers is a URL which displays a reputable company name but on closer scrutiny is slightly altered. For example, www.microsoft.com could appear incorrectly as:

www.micosoft.com

www.verify-microsoft.com

www.mircosoft.com

Other tips include viewing the email headers to see where the message really originated from. If the "From" information does not match the email address of the sender or the company being represented in the email, it usually means the message did not truly come from that individual or company.

Look for **incorrect grammar and spelling. Be suspicious of plain text emails which are absent of logos or graphics**. If an email is all plain text and looks different than what you are used to seeing from that sender, it is best to go with your gut feeling and ignore the message.

Compromised accounts not only pose a threat to a company's IT or security departments, they also lead to a drop in our customers' overall trust and loyalty, affecting marketing, sales and beyond.

START the year off right!

Here are 10 easy ways to get more done in the coming year. Adopt these 10 tips early and use them all year long to become a better, more productive you!

1. **Leave your email address on your voicemail message**
   A voicemail message consumes minutes of your time (more if you have to replay the message) to communicate information you could absorb from an email in seconds. Record your email address in your outgoing voicemail message and encourage callers to send you an email, rather than leave you a voicemail.

2. **Hone your email program's sorting rules**
   It takes time and energy to change gears to sort through (and respond to) a long list of disconnected messages. Microsoft®

[Continued on pg 4]

[START the year off right! – continued]

Outlook® allows you to route different types of messages into folders where you can review and respond en masse rather than piecemeal.

3. **Reward your body with high-quality fuel**
What you eat determines your energy level, and your energy level determines how much you can get accomplished. Sugary treats provide a quick energy boost but then create an even deeper dip. Heavy foods take energy to digest, leaving you with less to use. Instead, eat a small amount of fruit, vegetable and proteins every few hours to stay full and on the top of your game.

4. **Make your decisions more quickly**
Most people waste an extraordinary amount of time obsessing about (and second-guessing) their decision making. However, you are always better off making a good-enough decision quickly rather than waiting for an imaginary best decision.

5. **Get up and move!**
The human body is not designed to sit for hours on end. Attempting to do so inevitably creates aches and pains that steal your energy. Taking a five minute stretch or walking a few times throughout the day will keep your body fit and your mind functioning at a higher level.

6. **Completely disconnect for a while**
If you stop pretending to be productive when you are eating and sleeping, you will be far more productive when you are actually working. Always being available is an unfailing recipe for stress, illness and bad decision making. Give it a rest.

7. **Stop wasting time**
For some people, a day at work means an endless coffee klatch. They wander the halls searching for somebody to discuss business with, but they really just want to chat. Do not let these time-leeches hobble your success. Just say no. If necessary, get rude.

8. **Go paperless**
Going paperless using smartVIEW is the fastest way to attain efficiency. You and your colleagues will stop wasting precious time searching for files when a customer calls or when mail, faxes and emails are received.

9. **Turn off the noise**
When you are working up a complex transaction, the last thing you need is your computer beeping for your attention or your cell phone chirping with text messages. Turn the sound off until you have finished the task. You will finish the work faster and with a higher degree of accuracy.

10. **Do not get distracted**
The biggest impediment to completing tasks throughout the day is social media. Checking Facebook® and Twitter® throughout the day to see what your friends or followers are up to will add minutes onto your already crushing schedule. Set aside time in the morning and evening to be on social media sites.

Best wishes to you for a productive and profitable New Year!

FIRPTA nightmare #1

An escrow officer had a closing where the seller was a foreign national. The buyer and seller instructed her to withhold and remit 10% to the IRS at closing. The escrow officer decided she disagreed with our policy and procedure described in Tech Memo 120-2010. She felt it was good customer service to complete the forms herself. She typed up the forms (8288 and 8288-A, copies a, b and c) and had the buyer sign the 8288.

The escrow officer did not have the seller read and review the forms. She did not proofread her work. She did not have anyone else proofread her work. She closed and sent the forms along with the payment to the IRS.

The file closed in August 2013. In November the seller tried to obtain a refund from the IRS, but the IRS did not show the credit for the payment against the seller's taxpayer I.D. number. After many calls to the IRS, the seller discovered the payment was credited to another taxpayer.

The payment was credited to the number reflected on the 8288-A which contained a typo. The escrow officer inadvertently typed in the incorrect taxpayer I.D. number on the form. Her typo was causing a delay in the seller receiving his refund. The seller was MAD. He demanded she fix her mistake.

She contacted National Escrow Administration. National Escrow Administration asked her to send over copies of the 8288, 8288-A, proof of delivery and the 8821 for the seller. The escrow officer sent over the 8288, 8288-A and proof of delivery. National Escrow Administration asked again for the 8821. She replied she did not obtain one. Great!

This means the IRS will not talk with us to have the error corrected. The seller would not cooperate because he was very angry and unsatisfied with the escrow officer's customer service. He did not trust the Company enough to give us power of attorney.

The seller felt we should simply open a claim, pay him the amount of his refund and deal with the IRS ourselves to recoup our loss - otherwise he threatened to bring legal action against us. The operation had to take a $6,800 loss to pay him.