FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

REALTOR® safety month

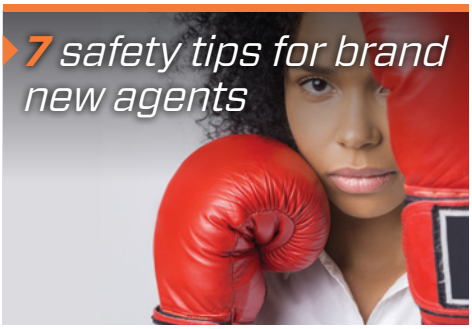
By Lisa A. Tyler
National Escrow Administrator

This newsletter is regularly shared with FNF's customers who are, in large part, real estate agents. The National Association of REALTORS® has designated September as safety awareness month. In light of that, we are sharing our "7 safety tips for brand new agents" story. We hope this month's edition makes it into the hands of new real estate agents — or even seasoned real estate agents — to provide them with tips to make sure they make it home safely every day to their friends and family.

Providing for your children in the event you die prematurely takes more than picking someone to raise them. Parents should also consider what will happen to any money or property their children inherit. Often, that planning includes the creation of a life estate. A life estate gives the ownership of the estate to someone else in the future. The owner retains the right to live and use the property as long as they are alive. In short, they have given away the future ownership. In a case where the kids have the future ownership, then they own that remainder interest. Unlike a will, this cannot be changed by the parents in the future without a court proceeding. Read about a fake court proceeding detected by a closing coordinator in the story titled, "LIFE estate."

Ransomware can be difficult to stop and is clearly on the rise due to the opportunity of large profits to cybercriminals. Organizations must invest in detection and mitigation measures. It is essential to have systems in place to prevent and detect any potentially malicious activity. Organizations must also regularly educate their staff on detecting and avoiding potential ransomware threats and attacks. Read this month's latest ransomware article titled, "RANSOMWARE prevention," to discover tips to protect against a ransomware attack.

IN THIS ISSUE



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

volume 17 issue 9
September 2022

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

7 safety tips for brand new agents

While you have probably thought about many of the aspects of practicing real estate, the one you should start with is your personal safety. Here is how to stay safer as you go about your daily activities.

You've made it through hours of, let's face it, often mind-numbingly boring real estate classes. You've passed your state and national exams. You've found the perfect real estate brokerage to hang your license with. You've set your credit card on fire buying supplies and association and MLS memberships. Now you're ready to set the world on fire and become a wildly successful real estate agent.

How much have you thought about your safety? Here are a few tips that can help you be safer in your daily activities as a real estate agent.

Don't do it alone

While it's virtually impossible to always have someone with you, there are many times when you can. And it not only helps you be safer, but it can also help your business.

Take a partner to an open house (a good lender, home inspector, or contractor – for example). Does the listing have a pool? Tap a local pool store for an expert in pool care.

Ask a fellow agent to accompany you on showings. As a new agent, it's an opportunity for you to learn from an experienced agent.

Never meet a new client alone. Bring them into your office or meet them at a public coffee shop or café.

Practice good situational awareness

Every safety expert agrees that proactively preventing a safety issue before it occurs is far superior to reacting to a live safety event. The single best way to avoid a serious situation is to practice good situational awareness.

Situational awareness is simply being cognizant and aware of your situation and surroundings. Trust your gut. If something feels wrong, it probably is. There has never been a commission check cut that is worth compromising your safety.

Screen your contacts and clients

You have to show your driver's license to rent a car, stay in a hotel, buy a beer, donate blood, or get on an airplane. Yet the real estate industry is reluctant to ask a total stranger to show ID before meeting them, alone, in a vacant house. Yes, IDs can be faked. But asking for an ID is a simple step that can prevent many potential safety issues.

Take classes and practice self-defense

The problem with any method of self-defense is that if the techniques and tools are not regularly practiced, they swiftly lose their effectiveness. There is a reason law enforcement regularly practices – it's to build muscle memory. No one knows how they will react in a situation, and the more you practice, the better chance you have of remembering your self-defense tactics and employing them correctly.

This brings up the often-discussed topic whenever safety conversations arise of whether to carry a weapon. That's a deeply personal choice, and much of the decision is governed by state and local law and regulations. If you choose to arm yourself, you must frequently practice using your weapon. Always remember that carrying a weapon does not guarantee your personal safety.

Use a safety app

Technology can be both a blessing and a curse. In the case of safety, it's much more of a blessing. There are numerous safety apps out there that can be valuable tools in the safety toolbox. But simply installing an app on your phone doesn't help. You have to use it, every time.

It's not just violent crime

Often forgotten are other safety-related things an agent should be aware of. Be prepared for a breakdown. Make sure your spare tire isn't flat and know how to change a tire. Keep a car safety kit in your trunk with basic tools, flares, and cones.

Know what to do if someone suspicious starts following you (drive to a police station or public place). Being alert and aware of your

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or 949.622.4425

surroundings goes for while you're driving too. Don't drive when you're exhausted.

Another thing agents do is send a lot of email and texts, some involving client financials. Be aware of cybercrime and understand basic preventative tactics.

Sadly, nothing eliminates the safety threat

None of these tips will eliminate the safety threat. They can, however, reduce that threat. Be vigilant, be aware, and never take your safety for granted.

This article was originally published through *Inman News*.

Article provided by contributing author:
Jay Thompson
Director for the Beverly Carter Foundation
Former brokerage owner and Zillow Group employee and all-around great human

LIFE estate

Lisa Williams, closing coordinator for ServiceLink in Moon Township, Pennsylvania, was processing a cash-out loan. The property being used as collateral for the loan is in North Carolina and held in a life estate for two minor children. A deed taking the property out of the life estate had been recorded.

Lisa noted per ServiceLink's underwriting counsel, the deed that recorded in July 2022 (taking the property out of the life estate) was not valid without a special proceeding under North Carolina law NCGS 35A — with a superior court judge allowing and confirming the sale.

The underwriting counsel stated the borrower would need to hire a North Carolina attorney to petition the court. Lisa informed the borrower of the underwriting requirement via email.

Miraculously, the next day, the borrower responded with a document entitled, "Special Proceeding with Superior Court." His email read, "Good morning, please see attached document. Wow. We were able to get a signature quickly. They must be tired of us harassing them. :-) "

Lisa noticed the Special Proceeding with Superior Court document was missing the court case information and the formal submission pages that should have been included. She sent the document to the ServiceLink title curative team for review. They denied it for insuring purposes for the same reasons.

Lisa took it upon herself to contact the court directly to obtain a full copy of the proceedings. The court coordinator who answered the phone requested a copy of the document Lisa had received from the borrower. The court coordinator said she would research the proceedings and call back.

Lisa received a call back from the court coordinator letting her know the document was fraudulent and the court did not have a proceeding on August 15, 2022, the date indicated on the Special Proceeding with Superior Court.

The court coordinator then sent a copy of an email message to Lisa that read, in part:

Good Afternoon Sheriff,

We have an issue.

Beginning of this month, I received a telephone call from a xxxx xxxx. He was asking me to have a judge send an email to his title company stating that the elimination of a life estate and the deed filed in July was good. He is trying to refinance. I told him that a judge would not send an arbitrary email clearing title. He said that his brother is an attorney and is helping him. He was advised that he needed to open a case in the County, file a petition and have a hearing. I asked Mr. xxxx for the telephone number of his title company so I could explain all to them. I have spoken with Lisa Williams, Closing Coordinator with Servicelink in Moon Township, PA. She told Mr. xxxx the same thing.

Mr. xxxx also went to the County Clerk's office. They advised that they need a petition so a special proceeding could be opened.

Today, I receive a call from Lisa Williams advising that she has an order signed by the Judge but was missing information.

I have confirmed the following:

1. No special proceeding action has been open
2. No hearing took place on Monday, August 15th before the Clerk or Judge
3. Judge has been out of the County all week
4. Judge did not sign the Special Proceeding with Superior Court document. I have an email confirming that.

The Judge instructed me to contact you.

I alerted the title company that they should not rely on the attached document.

In a search of the County deeds, I found possible contact information for Mr. xxxx for your reference.

Please let me know if you need any additional information from me.

Lisa's contact with the court led to the verification that the document was indeed fraudulent. She saved the Company from closing and insuring a $100,000 cash-out loan with a deed in the chain of title that had not been properly approved by the courts.

The deed represented a cloud on the title to the subject property. The borrower cannot use the property as collateral with the life estate still intact.

For her detection and prevention of a possible claim Lisa has received a letter of recognition from the Company, as well as a $1,500 reward.

FRAUD Insights

RANSOMWARE prevention

Here are a few tips to protect against a ransomware attack. Keep in mind this list only scratches the surface:

Always back up data. Backups should be protected and — if possible — segregated from the network. Data backup files should be encrypted to add an additional layer of protection. Backup files allow for restoring files if a computer infection occurs. Periodically, test backups by restoring critical systems to ensure the backups will work if needed.

When a person has backups, the cybercriminal loses some leverage. Backup files allow victims to restore their files once the malware has been removed.

Stay updated. Operating systems, programs and security software must be updated with the latest versions and security patches. Enable automatic patches and updates to ensure they are promptly installed.

Use a trusted security software that offers more than just antivirus features. Some security software can help detect and protect against threats to an individual's identity and their devices, including your mobile phones.

Be cautious with email attachments or links. Email phishing, which contains a link or has an attachment, may contain malware. Only open email messages, attachments or click on links from a trusted source. Emails from an unknown or unfamiliar source should be deleted.

Surfing the world wide web. Be sure to use a secure internet connection. If the connection is not secure, such as public WiFi, use a virtual private network (VPN) to protect your connection and information.

Always use caution when surfing the internet. Pop-up ads or websites may contain malware. Just as with emails, only visit websites or open pop-ups from a known, trusted source.

Use Multi-Factor Authentication (MFA). MFA requires a user to present two forms of credentials when logging in to an account or secure network. The credentials are typically something the user knows, such as their password, and something they have, such as a token or code texted to their cell phone.

This type of authentication enhances security because the user has to prove they are who they say they are. Since the process requires two types of credentials it helps to prevent hackers from gaining access to a network or blocks them from escalating privileges.

Employee Training. Cybersecurity awareness and anti-phishing training should be implemented for all employees. Employees should be taught how to identify, avoid and report phishing attempts.

Periodic phishing exercises should be run to determine whether employees realize the risks associated with email attachments and embedded links in fake emails. Information Technology should monitor emails in order to set up filters to block spam and emails that contain malicious attachments or links from reaching employees.

Password Management. Organizations should ensure users establish strong, unique passwords — with a mix of letters, numbers and symbols. Passwords should be changed regularly and not be reused.

Removable media. Use of removable media or external storage devices, such as USB sticks, should be carefully considered and possibly restricted as users may unknowingly install malware if the source of the removable device is unknown to them.

Implement an incident response plan. All organizations must put an incident response plan in place. Test and review the plan, at least annually. Ensure senior leadership is involved and aware of the plan so it can be leveraged during an actual incident.

With new ransomware variants appearing, it is imperative to take all measures to minimize exposure. Knowing what ransomware is, understanding how it works and taking precautions can help protect computer data and personal information from becoming a ransomware target.

Remember, this list only scratches the surface. Proactive prevention through effective cyber training and security controls is often the best defense. Anyone who is in charge of cybersecurity or who wants to put a policy or procedure in place should be sure to consult with a cyber expert or the various government sources for more details.

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