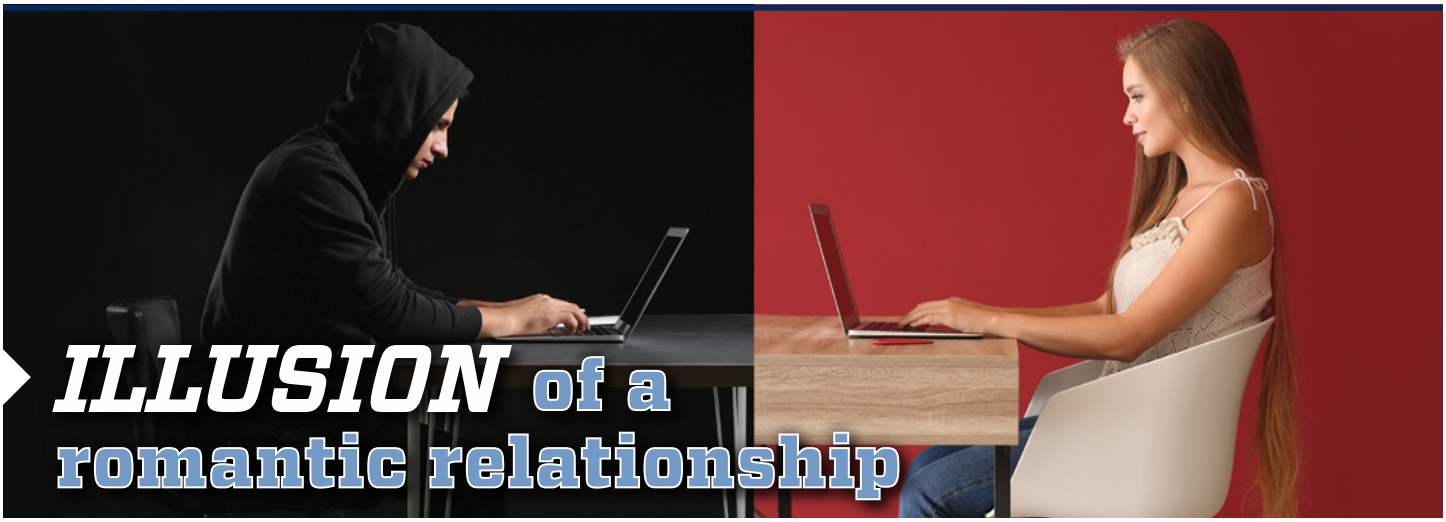
FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL



ILLUSION of a romantic relationship

By Lisa A. Tyler
National Escrow Administrator

Investing in real estate can be a terrific way to build wealth in America. Property values have increased, providing property owners with big returns on their investment. Owners have also found creative ways to sell their property. Some turn to the many online resources to market their property without the benefit of a licensed real estate agent. The competitive, low inventory real estate market has made it difficult for investors and home buyers to identify new properties to buy. Many search online for properties being sold For Sale by Owner (FSBO), but some have discovered that purchasing properties direct from the seller comes with added risks. Read "FSBO" to discover more.

There are a number of programs or companies offering equity participation products geared towards residential owners. These programs include second loans secured by an appreciation in the equity or options, in return for down payment help that look to appreciation in the property for repayment. Fidelity's underwriting counsel has reviewed these programs and decided that our Company is NOT interested in providing either title or closing services to these providers. Read "EQUITY share programs" to find out more.

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim. The criminals who carry out romance scams are experts at what they do and will seem genuine, caring and believable. Unfortunately, con artists are present on most dating and social media sites.

The scammer's intention is to establish a relationship as quickly as possible, endear himself to the victim and gain trust. They may propose marriage and make plans to meet in person, but that will never happen. Eventually, they will ask for money. Discover how this scam affected the real estate industry when an escrow company owner and limited practice officer fell for the scam in "ROMANCE scam."

There are good hackers who work with companies to help develop security measures to prevent a malicious computer or network attack. Unfortunately, there are too many bad hackers who do it for basic bragging rights, curiosity, revenge, boredom, challenge, theft for financial gain, sabotage, vandalism, corporate espionage, blackmail and/or extortion. The intention of some hackers is launching a ransomware attack. They often work with others who are all part of a criminal organization to develop and deploy a digital suite of malware tools used to target businesses and individuals all over the world. Read more about it in this month's article on ransomware, titled "WHO do they attack and why."

IN THIS ISSUE

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

volume 17 issue 5
May 2022

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

FSBO

Kelly Lobeck, escrow officer for Ticor Title in Las Vegas, has more than 20 years of experience in the escrow industry. She has worked hard to develop a great reputation. A real estate agent she knows referred one of his family members to her. He had found a lot for sale on one of the hottest real estate websites. The site allows owners to list their home for sale without the benefit of a real estate agent.

The sales price was $150,000 for a vacant lot. The buyer felt he had found a hidden gem. Escrow was opened and Kelly reached out to the seller who was only available by email because he was currently working overseas.

Kelly sent her opening packages to the buyer and seller to complete and sign electronically, but she took one more step. She reviewed the property tax website which included a mailing address for the seller. She sent an introductory letter to the seller via overnight delivery at the address listed on the property tax website.

Since the buyer had cash on hand, the transaction was moving quickly. Then Kelly received a response to her letter, which stated:

> Hello Kelly,
>
> John and Joan are long time clients and friends of mine. I am assisting them in communicating with you. The Smiths are in receipt of your letter regarding their property. This is a fraudulent transaction. The Smiths have never listed this property for sale. I have copied Mr. Smith in this email.
>
> Please advise what the Smiths should do to protect their property and stop this fraudulent transaction.
>
> My number is listed below. John's number is 555-555-5555. Thank you.
>
> Kind regards,
> Adam Jones / Top Seller Team
> REALTOR®

Kelly called the seller to confirm the letter was accurate. The seller was relieved because the property had an actual value of more than $1,000,000. He thanked her for contacting him.

Kelly called the buyer, who was shocked and said the deal felt too good to be true. He asked Kelly to put him in touch with the seller's real estate agent to see if they could work something out. In the end, she resigned from the transaction, returned the earnest money to the buyer and cancelled her file.

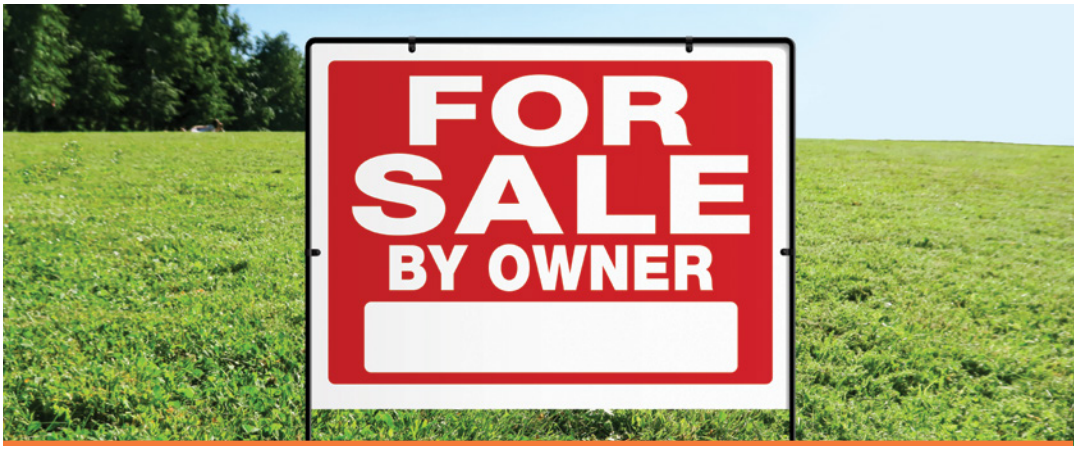
Kelly did not skip a beat. She opened the order, but immediately performed her due diligence in an effort to protect the Company from a potential claim. Her efforts paid off for the Company and as a thank you she will receive a reward of $1,500.

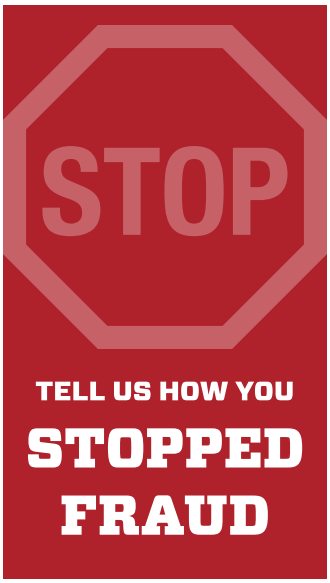
Absentee property owners are under attack. Our industry and our product, title insurance, is more valuable than ever before. Title insurance is an insurance policy, but it works differently than other types of insurance, because the coverage provided is based on items which can be found in public records.

Title companies eliminate risks by a thorough examination of the items of record affecting the property. Title clearance is performed, providing prospective buyers and lenders with information concerning which items may or may not affect the property.

The title report helps determine what must be addressed before the transaction can close. Dollar-for-dollar, title insurance is the best investment a property owner can make to protect their interest.

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





TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

EQUITY share programs

Under an equity share agreement, an organization provides funding under a home buyer program (picture down payment assistance) or a homeowner program in exchange for an option to purchase an interest in the property in the future.

The equity share agreements allow for the organization to exercise its option under certain circumstances, such as the expiration of a 30-year term, eventual sale of the subject property, death of the homeowner or a request from the homeowner for a special termination of the agreement.

In these cases, the organization values its interest and is paid off in lieu of exercising its option to purchase an interest in the property; the agreement can potentially harm the homeowner by taking all their earned equity.

The average down payment assistance for a purchase is $100,000. The average payment under a homeowner program is $115,000. At closing, the home buyer or owner is presented with 80+ pages of documents to review and sign. The documents can include:

1. Option Agreement (sets out the financial terms)
2. Covenant Agreement (outlines the homeowner's rights)
3. Security Agreement (recorded lien on the property)
4. Memorandum (recorded notice of the organization's rights)
5. Mortgage (recorded under the homeowner program)

Every equity sharing transaction must be thoroughly investigated by our underwriting colleagues before determining if we can agree to close and insure. The underwriting counsel will attempt to determine if the program clogs the equity of redemption and could potentially harm the homeowner.

There are some programs for teachers and other first time homebuyers that title companies will close and insure. If you are requested to participate in any transaction that includes this type of "down payment help" please refer the request to your regional counsel.

Despite refusing this business in the past, some of these transactions may have closed with our agents or operations. There are companies that claim they have closed with Fidelity brands; we are concerned that this representation — while it may have been true in an inadvertent situation — will mislead offices and agents to assume that we have somehow approved these processes when we have not.

ROMANCE scam

An escrow company owner who was also a limited practice officer, which is required in her state in order to complete legal documents, maintained an escrow trust account at a national banking institution.

In October 2021, the bank issued two notices of insufficient funds for the account. In September and October 2021, the company owner knowingly made multiple, unauthorized disbursements of customer escrow funds by wire transfers to a payee in Turkey; the disbursements totaled nearly $2 million, causing overdrafts to the payees of other checks.

When the payees discovered their checks were returned by the issuing bank for insufficient funds, they reached out to the escrow company owner who told them the company's escrow trust account had been hacked. She promised she would make the checks good, but she never did.

On November 10, 2021, the escrow company owner emailed two of the check payees admitting to lying about the account hack and informing them she had willfully transferred funds from the trust account to an unknown party; she caused the account shortage but was unable to pay them.

When the state's regulators found out, they issued a cease and desist, ordering the escrow company to immediately stop accepting new escrow transactions; the escrow company could not accept or disburse any funds from the escrow trust account or the operating account.

As a result of the escrow company owner's actions, all existing active transactions had to be transferred to another escrow company to close and her limited practice officer license was surrendered.

The company was not only out the $2 million she wired from the escrow trust account, but she was out another $1.5 million of her own personal funds that she wire transferred to Turkey in a cash-out refinance of her personal residence.

[Continued on pg 4]

FRAUD Insights

[ROMANCE scam — continued]

The 68-year-old woman admitted she had wire transferred $3.5 million to Turkey to assist a friend who was in danger and in fear for his life. As a result of her actions the public interest was irreparably harmed. In addition, she lost her company, her limited practice office license and her life savings.

Below are tips from the FBI on avoiding the romance scam:

- Be careful what you post and make public online. Scammers can use details shared on social media and dating sites to better understand and target you.
- Research the person's photo and profile using online searches to see if the image, name or details have been used elsewhere.
- Go slowly and ask lots of questions.
- Beware if the individual seems too perfect or quickly asks you to leave a dating service or social media site to communicate directly.
- Beware if the individual attempts to isolate you from friends and family, or requests inappropriate photos or financial information that could later be used to extort you.

- Beware if the individual promises to meet in person but then always has an excuse why he or she cannot meet. If you have not met the person after a few months, for whatever reason, you have good reason to be suspicious.
- Never send money to anyone you have only communicated with online or by phone.

WHO *do they attack and why*

Cyber criminals often partner up with other syndicates to share their hacking techniques, malware code and information they have uncovered about technology infrastructure. This helps them to develop new techniques or employ previously used ones for phishing attacks that deliver ransomware.

Hackers post their successes to criminal name-and-shame websites used to embarrass and coerce victims. The gangs also share software flaws referred to as zero-day vulnerabilities.

Cyber criminals use a few different methodologies to pick their targets. In most cases, it comes down to opportunity and reward. Meaning, they may target a specific industry because their security protocols are weak; they may target a company who needs to access their data immediately, therefore being more likely to quickly pay a ransom. Other businesses pay the ransom in order to avoid the attack from being publicized.

Some cyber criminals target various sectors in the U.S. and other countries. The gangs believe healthcare providers and small municipalities make good targets because their security may be weak and/or they may need to quickly pay a ransom because the services they provide are critical.

Utility companies are also prime targets. The attack on the Colonial Pipeline which caused gasoline shortages proved this. The hackers were successful in extorting millions of dollars in order for the pipeline to be put back into service.

Treasury Secretary Janet L. Yellen said, "Ransomware and cyber-attacks are victimizing businesses large and small across America and are a direct threat to our economy."

In recent years, syndicates have implemented new extortion tactics designed to create additional incentives for victims to pay the ransoms, resulting in maximized profits. It is referred to as double extortion or leakware. The hackers threaten to publish the encrypted data if the ransom they demand is not paid.

Cyber criminals focus on infrastructure critical to public safety. This includes emergency service providers, such as hospitals and other first responders or emergency service providers, because they cannot afford to be offline without dire effects which threaten society.

Clearly no one is immune, and everyone must be on high alert. Here at the Fidelity family of Companies our information security teams are constantly putting measures in place to secure our customers' information.

Next month's article will explore in detail some of the different types and methods of ransomware.

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