FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

By Lisa A. Tyler
National Escrow Administrator

A woman represented by a real estate agent made an offer to purchase a home, signing both her name and her husband's name to the contract. Once the offer was accepted, she dropped off her earnest money deposit at an escrow branch near the home she was purchasing, not at the office in which her escrow officer was located. The escrow officer reviewed the documents and raised some concerns regarding a power of attorney and a doctor's letter stating the husband had dementia. Read the story entitled "ABUSE of veteran's benefits" for all the crazy details.

Nicole Andrews, an escrow officer with Chicago Title Company of Washington, in Tacoma, opened a sale transaction on April 3, 2020, with an anticipated closing date of May 15, 2020. The sale price was $369,000. The buyer deposited $1,000 earnest money at the time of opening by using what looked like a counter check, meaning the check appeared to be a personal check given over the counter at the bank. There was no remitter information at the top of the check and showed the check number of 0100. The buyer in this transaction was a limited liability company, purchasing jointly with its managing member as an individual. Read "DELAYS turn into dismay" to find out what happened next.

Think your password is up to par? Many of us use simple tricks to try and create a memorable password that meets security requirements. However, many of these add no real strength or security. Read this month's **cyber buzz** article "PASSWORD1?" as we review some password best practices.

IN THIS ISSUE

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

volume 15 issue 9
September 2020

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

ABUSE of veteran's benefits

Chris Champion, an escrow officer with Lawyers Title of Arizona, opened a sale escrow for $465,000. The buyers were a married couple supposedly moving from Colorado. The property was in Goodyear, Arizona. The wife signed the purchase agreement for herself as well as her husband, using her signature for both parties.

The wife had a cashier's check in the amount of $5,000, representing the earnest money deposit. However, she dropped it off at the Surprise, Arizona branch, even though the transaction was being handled at the Scottsdale branch.

The balance of the purchase funds was coming from a Veterans Affairs Loan (VA Loan). The wife stated the veteran was her elderly husband, but she was entitled to his VA benefits. She produced a power of attorney for the transaction because her husband was mentally incapacitated.

When Chris told the wife she would like to speak to her husband to verify that the power of attorney was still in good standing and not revoked, she produced a letter from a doctor stating the husband was suffering from dementia. Chris studied the letter. She was concerned the doctor wrote his assessment of the husband's mental condition six months before the power of attorney was signed and that the power of attorney may not be valid since he may have been in a diminished mental state upon signing the POA.

During the discussions between Chris and the wife, she disclosed she also had a fiancé who was going to be moving into the home with her. Supposedly, she would still be the caretaker of her mentally deficient husband. At this point, Chris decided to escalate her concerns about the transaction to her manager, Mark Walker.

Chris and Mark decided that the best course of action was to resign as escrow agent due to the wife using a potentially invalid POA and obtaining another person's VA benefits — possibly without his knowledge — to house herself and her fiancé.

Mark contacted the buyer and informed her the Company would not handle the closing and insuring of the home purchase. At that point, the wife became belligerent. She claimed Mark was saying she was committing fraud; she accused him of denying her VA rights and demanded an explanation. Mark politely responded that the Company had every right to refuse to close the transaction and provided no further explanation.

In what may have been a last ditch effort to salvage something from this scheme, the buyer then wanted Mark to deposit the $5,000 cashier's check (since it was payable to Lawyers Title Company), that represented the earnest money deposit. She wanted Mark to send her a check payable in her name only. He politely declined this request as well.

Chris could have ignored the red flags — but she did not. She brought her concerns to her manager and together they made the decision to resign.

Chris and Mark felt protecting the rights of the incapacitated person and preventing potential fraud against an agency of the U.S. Government, as well as a potential claim against the Company, was far more important than any revenue the transaction would have produced for the Company. As a result, the Company has rewarded Chris $1,500.

P.S. Chris is a double reward winner. A story in the January 2020 issue, described how she received a reward for protecting the Company from a potential loss. There is no limit to the appreciation the Company has for her experience and expertise.

If you have previously received a reward, please know you are still eligible to earn future rewards.

STOP

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

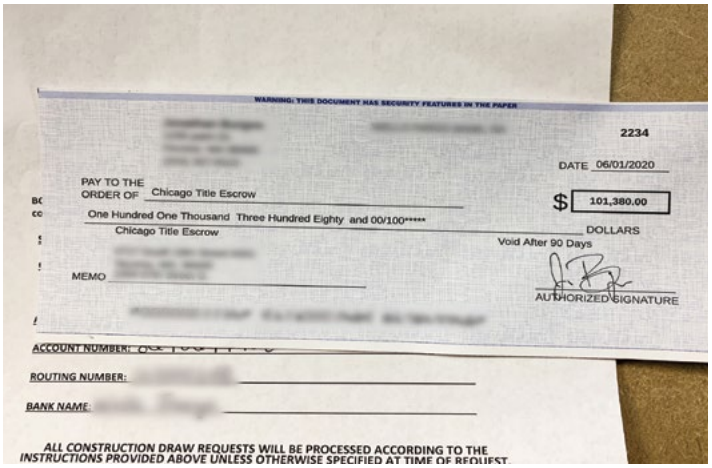
DELAYS *turn into dismay*

Nicole Andrews, an escrow officer with Chicago Title Company of Washington, in Tacoma, opened a sale transaction on April 3, 2020, with an anticipated closing date of May 15, 2020. The earnest money check in the amount of $1,000 was deposited and cleared the bank.

The buyer kept negotiating contract extensions past the May 15th closing date with the seller. The buyer and seller had signed all the closing documents; the escrow officer was waiting on the buyer's funds to close, as well as loan funding from a private hard money lender.

The buyer told his agent, the escrow officer and the lender that the down payment and closing funds were in his account on hold and a wire would be sent as soon as, "…they were clear." On June 1, 2020, an unexpected "test wire" appeared in the escrow trust account in the amount of $49.54. The incoming wire referenced the escrow number for the file; the funds, however, came from an entity called "Right on Shine" — which was not a party to the transaction.

The next day, the buyer appeared at Chicago Title Company and gave Alex Tarin, escrow assistant extraordinaire, what looked like a business check with the individual buyer as the remitter. The check was in the amount of $101,380.



Alex thought the check looked odd because it did not contain issuing bank information, such as the city, state or routing number or other identifying bank information that would normally appear on the check. Alex stepped away with the check and showed it to the escrow officer, Nicole Andrews, who quickly captured a picture with her phone. Alex returned to the buyer and handed the check back to him. Alex let him know it was not acceptable for closing and he would either need to provide a cashier's check or to wire transfer the funds.

The buyer left with the check and Nicole sent the picture to the issuing bank to verify if the check was valid. The representative at the bank quickly confirmed the check was not valid. They asked Chicago Title to turn the check over to them, but Nicole told the representative the buyer left the office with the check in his hand. The banking representative stated they would monitor the account (which was a valid account — but did not belong to the buyer) to see if the check was deposited elsewhere.

Nicole and Alex resigned from the transaction, letting the listing agent, selling agent, lender and title officer know the buyer had attempted to deposit a counterfeit check. The title officer performed further research and verified the organizational documents the managing member had presented for the purchasing entity were altered and forged. Nicole requested the accounting center reject the $49.54 wire transfer; the $1,000 earnest money deposit was returned to the depositor.

Due to their instincts and high degree of professionalism, Alex and Nicole saved the Company from depositing a counterfeit check and refused to do any further business with the buyer. For their efforts and expertise, the Company has rewarded them $750 each.

MORAL OF THE STORY

Checks deposited into escrow should always be examined for irregularities. The moment an escrow officer discovers funds deposited into escrow are counterfeit or returned for non-sufficient funds, everyone involved in the transaction needs to be notified.

It is disheartening that due to the buyer's action the seller had taken the property off the market during the most valuable market time of the year, but Alex and Nicole acted swiftly to make sure everyone was aware of the scam the buyer was perpetrating. By notifying all parties through a resignation as escrow holder, they enabled the seller to terminate the contract and put the property back on the market. Bottomline: The Company does not tolerate criminal activity of any kind.

PASSWORD1?

Passwords are frustrating. Many times the requirements placed on them make their creation — and more importantly remembering them — difficult. The most frustrating situation is when your password is not being accepted, then resetting your password and then having your new password rejected because it matches what you originally typed.

If you are accessing a managed system, in many instances, passwords must be changed approximately every 90 days, be a certain length and contain certain special characters.

The reasoning behind this is to prevent users from using generic passwords such as "Password," as a way of securing their account.

The Company indeed has requirements in place that you must follow when creating a password. However, even with these policies, everyone can improve their awareness and hopefully limit risk to the Company. In addition, if you regularly access personal email or online banking or log in to any online system, these guidelines may help to protect your personal accounts and information from unwanted access.

[Continued on pg 4]

[PASSWORD1? — continued]

The National Institute of Standards and Technology (NIST) is a non-regulatory agency of the U.S. Department of Commerce. Their mission is, "…to promote U.S. innovation and industrial competitiveness by advancing measurement science, standards, and technology in ways that enhance economic security and improve our quality of life."

The NIST regularly releases publications on many important topics. The publication, "Digital Identity Guidelines," lays out best practices for password creation.

Surprisingly, some of the NIST suggestions go against what we have been taught about strong, secure passwords. It recommends new password guidelines that will impact website password framework and you. They suggest the following practices be put in place:

1. Eight (8) character minimum (when it is set by a human, instead of a system generated password)
2. Support at least 64 characters maximum length
3. All ASCII (pronounced ask-ee) characters (including a space) should be supported (ASCII codes represent 128 English characters as numbers, with a letter assigned as a number. For example, the ASCII code for an uppercase M is 77.)
4. Truncation of the secret (password) shall not be performed when processed
5. Check chosen password with known password dictionaries
6. Allow at least 10 password attempts before lockout
7. No complexity requirements
8. No password expiration period
9. No password hints
10. No knowledge-based authentication (e.g., What is the name of your first pet?)
11. No SMS for a one-time password

In the past, it had been taught to complicate shorter passwords with special characters and changes to case letters. For instance, if your password is "Password," you would have changed it to "P@55w0rd," and supposedly achieved a higher degree of security.

Per the new guidelines, however, the NIST found length is more important than complexity. Setting a longer password means more time for a computer to cycle through potential passwords and find one that works.

According to howsecureismypassword.net, "P@55w0rd," would take a computer approximately nine hours to crack. The password "National Escrow Administration," solely based on length, would take approximately 27 undecillion years (yes, that is a long, long time). Many systems have limits in place on the number of password tries. Not all of these best practices, however, are a complete fail safe from this type of password attack.

Length of a password is not the only factor to consider when setting a password. In the above example, common words were used as passwords. It is likely that common words or phrases would not be any faster to crack than suggested, since cybercriminals use password dictionaries in attempting to crack passwords.

Password dictionaries are lists of passwords that are built on previously used passwords (released through prior cyber-attacks) and commonly used words or phrases. The length and size of these lists are staggering. If you are still using a password that was exposed in a cyber-attack — even if it is for a different login — there is a good chance it appears in a password dictionary.

Another important best practice to satisfy password requirements is avoid simple, common changes. For instance, if you chose "Password," but you still need to include a number, you change it to "Password1." You still need a special character, so now it becomes "Password1?." It is not a very unique or secure password. NIST recognizes this within their best practice of, "No complexity requirements."

NIST also acknowledges the limited ability of humans to remember complex passwords and how the requirements, while met, often do not add security — as the example above illustrates. When you are simply meeting the requirements of a password, make sure to follow the spirit of the requirement and not just the requirement itself. If you use common words or phrases and merely add "1?," your password would probably make the dictionary list or would be much easier to guess.

Many user portals also provide a secondary way to gain access through security questions. Many of these involve basic knowledge and history, which goes against the NIST "No knowledge-based authentication" best practice. For instance, following your social media feed may reveal, "What is your favorite color?" Instead, be cautious when answering those questions.

Do not use common knowledge answers, as an IT professional did when working at a large credit card data processing facility. Cybercriminals created a dossier on the victim by following him on social media, and learning his favorite food, color and other pertinent information. Then, they called the victim's company and reset the password by answering the security questions with the information they had collected. Criminals gained access to the victim's account and reams of credit card data.

For increased security, use longer passwords and avoid common phrases, words or substitutions. If you have trouble remembering passwords, start with a sentence you can remember and then make uncommon changes.

Alternately, sign up for a password storage program that maintains and creates strong passwords for you. Avoid using duplicate passwords. If you are aware of your account being breached, change your password, and never use that one again. After all, no one likes getting spam from your compromised email account.

Note: Not all hackers are out to do harm and many look to help companies, for a fee. Learn the different types of hackers and the color of hats they wear in next month's **cyber buzz** article "NOT all hackers wear the same hat."

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