FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

TRAINING is key to identifying fraud

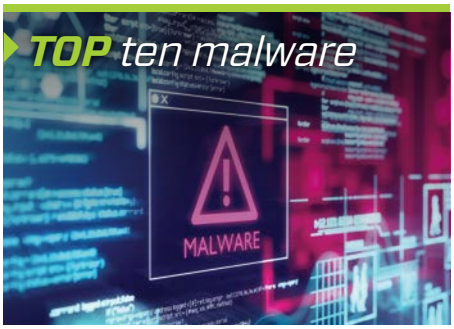
By Lisa A. Tyler
National Escrow Administrator

The Disbursement Solutions Group (DSG) operates as a national back office tasked with clearing up files with funds remaining. The file in the story entitled "DSG = doing some good" had funds on deposit in question between a developer and homeowners' association. The Disbursement Solutions Group is comprised of some of the unsung heroes at FNTG; until now. Read about one of these heroes.

"ANOTHER weird 2020 story" contains a unique mobile signing story that is somewhat entertaining, but mostly just disturbing. Give it a quick read.

Ransomware continues to make headlines across all industries and continues to cost millions of dollars. However, did you know that there are many other types of malware looking to steal your information? We look at the top 10 types of malware from 2019 in the last **cyber buzz** article of the year entitled "TOP ten malware."

IN THIS ISSUE



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

volume 15 issue 12
December 2020

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

DSG = doing some good

Clearing out dormant funds can be quite challenging. In most instances, the parties to the escrow have not made contact with us for some time. To complicate things further, at times, there is minimal information in the file to indicate why the funds remain on deposit or who they belong to. The Disbursement Specialist must familiarize oneself with the details in the file, then track down the parties and obtain written instructions to disburse the funds to the rightful owner.

Kathy Barriball, Disbursement Specialist, was assigned a file wherein the funds had been on deposit for several years. Kathy began working on the file in 2019. The funds represented a security deposit for the completion of improvements related to a subdivision. The agreement was between the developer and the homeowners' association (HOA).

Based on the information available, Kathy determined the funds should be released back to the developer. The public report had been finalized and filed many years earlier indicating the improvements had been completed. Kathy tracked down the authorized signer for the developer and the management company for the HOA.

The developer signed the mutual release instruction authorizing the return of the funds to his company. The HOA's management company said they would present the request to sign the mutual release instruction to their board of directors at their next meeting, which was scheduled for two months later. Kathy notified the developer.

Kathy marked her calendar accordingly and followed up with the management company to ensure the mutual release instruction was on the agenda for their next meeting. The meeting ended up being delayed by two weeks, but the management company confirmed the topic was on the agenda. She contacted the management company the day after the meeting to follow-up. The board elected to forward the documents to legal counsel to review.

Kathy followed up at the end of the month only to receive a response from the HOA's attorney. The board did not feel they had sufficient information to release the funds back to the developer.

However, the HOA was more than happy to bring up another dispute they had with the developer for construction defects and underfunding of the HOA's reserves. Kathy pointed to the written agreement stating it did not provide security to them for these items — it only provided for the completion of specific improvements to the subdivision. The HOA's attorney asked Kathy to notify the developer the HOA was requesting a portion of the funds for construction defects and underfunding of the HOA's reserves.

Kathy responded by asking the HOA to remit a demand pursuant to the security agreement. The HOA simply demanded $54,000 but provided no documentation to support the demand. She passed their request on to the developer; they reached out directly to the HOA and negotiated a settlement.

After months of negotiation, an agreement had been reached. The HOA signed mutual instructions to accept $12,000 as settlement of their grievance and release the balance of $110,915 to the developer. The developer provided a post office box to mail the check to. He asked for an estimated time of arrival so he could plan his next trip to the post office; due to COVID-19, he was not making regular trips to collect his mail.

Kathy was preparing the checks when she received an email. The developer asked her to wire the funds and reply as soon as possible so he could email the wire instructions. The email read:

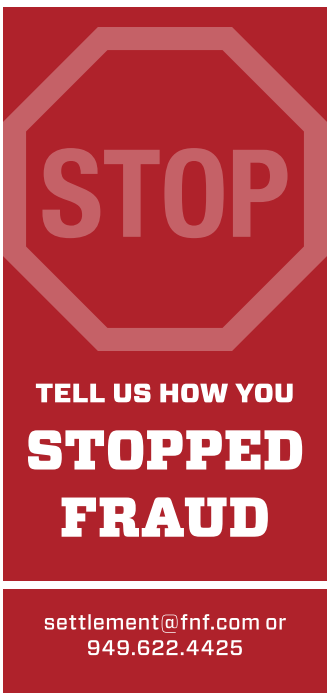
> "This is to let you know that I won't be able to receive check payment for some reasons due to the high rate Covid 19 pandemic our PO is currently closed until further notice, Covid is really getting in the way of business. I would suggest payment sent by ACH/Wire Transfer. Keep in touch as soon as possible so that I can have my banking information forwarded to you as soon as possible.
>
> Thank you.
>
> JOHN DOE"

Kathy immediately noticed many discrepancies:

- John always opened his messages with "Hi," and had the best spelling and grammar.
- Kathy exchanged emails just one day earlier where John indicated he goes to the post office once a week. That contradicted the new message.
- Based on Kathy's email with him from the previous day, she knew the post office was open.
- John always closed his emails with, "… John." This email ended with, "Thank you," with a period and his full name.

It did not add up at all.

[Continued on pg 3]



settlement@fnf.com or
949.622.4425

Kathy did not reply to the email. Instead, she called John at a known, trusted number. She asked if he had just sent her an email. He had not. He stated he suspected his secretary's computer had been hacked just last week. Kathy reported the incident to her manager, National Escrow Administration, and Cyber and Wire Fraud Strategies, and sent the developer a check.

Kathy could have easily fell for this common crime and sent $110,915 to the fraudster's account; but she did not. The Disbursement Specialists with DSG are required to maintain 10 hours of settlement training, along with specialized training provided by DSG's team trainers.

Kathy's training kicked into high gear when she noticed red flag warnings contained in the email. She adhered to the Company policies and procedures and is being rewarded $1,500. Great job!

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

ANOTHER *weird 2020 story*

A husband and wife were signing their loan closing documents with a mobile signing agent at their home. The mobile signing agent assigned to the task could not be bothered to travel to the borrowers' home, so he sent his wife. He planned on his wife obtaining the signatures and then returning the documents to him to notarize.

While at the borrowers' home, the notary's wife saw hot dog buns on the kitchen counter and asked the borrowers to make her a hot dog. The borrowers made her the hotdog. She ate it while they continued signing their loan documents. After she was done with the first hot dog, she asked for another one. The signers obliged and prepared her another and then continued to sign their documents.

When the wife of the mobile signing agent left, the borrowers immediately called their settlement agent to make her aware of what had transpired. The settlement agent knew the commissioned notary could not legally notarize the documents without the physical presence of the signers.

The settlement agent cancelled the signing, obtained the original documents from the signing agent and scheduled a new signing appointment for the borrowers. This story is just another weird sign of the times.

Our Company has a code of conduct mobile signing agents must agree and adhere to. Clearly, this signing agent did anything but adhere to it. The signing agent will no longer be permitted to handle signings for any of the FNTG Family of Companies. Neither will his wife. Our Company and customers expect a higher standard of conduct.

FRAUD Insights

TOP ten malware

Remember the "RANSOMWARE" article in the September 2019 issue of *Fraud Insights*? The cost from the attack to the city of Baltimore was estimated at $18.2 million — with the city transferring $6.5 million from a fund for parks and recreation to help pay for it.

That was just one example of many local governments being recently targeted and attacked. Ransomware remains an issue for not only governments but private businesses as well.

The Center for Information Security published a list of the top 10 malware types in 2019. Here they are:

1. TrickBot: Designed to steal financial login information; usually distributed via email asking a user to click or login through the email.
2. Emotet: Designed to steal financial login information through spam emails asking recipients to click to view, "Your Invoice" or "Payment Details." This malware can spread through systems and infect other computers.
3. ZeuS: Yet another variant designed to steal financial information. This incorporates key-logging malware. It was extremely successful in 2009 when it compromised more than 74,000 FTP website accounts. It is still around to this day.
4. Dridex: Again, designed to steal banking information via a system that utilizes macros in Microsoft® Word®. Be careful if you receive a Word file from an untrusted source asking to use macros.
5. Kovter: Is a file-less malware. Typically infiltrates a computer system through phishing emails, clicking on unsecure internet links or fake program updates.
6. CryptoWall: A ransomware distributed via spam emails with ZIP attachments. Remember, always look at the file type you are opening, as ZIP files may contain malicious PDF files.
7. Gh0st: A remote access Trojan (RAT) used to control infected endpoints. Gh0st is dropped by other malware to create a backdoor into a device that allows an attacker to fully control the infected device.
8. NanoCore: A Remote Access Trojan (RAT) sent via spam emails containing a Microsoft® Excel® spreadsheet. The malware can allow remote access by a cybercriminal and take full control of the infected computer.
9. Tinba (aka Tiny Banker): A type of Trojan malware designed to be a "man-in-the-middle" attack. The malware inserts itself between the user and the website they are accessing. The malware can see and steal the login information of the user.
10. Cerber: A ransomware Trojan on Microsoft® Windows® that can encrypt a user's files from a .docx file that is sent via email. Currently, a decryptor tool is only available for unencrypting the files.

Most of these malwares require a user to interact with an email or malicious file. It is important to remember to always look at who is sending you the file. Never open any file unless it is from a trusted source and you know that person is sending you a valid file.

Cybercriminals work hard to disguise malwares. They incorporate verbiage in emails they know will tempt us to click, "Your payment is past due," "Invoice," "Your SSN has been stolen," and so on. Their goal is to get you to click the link or download an attachment that launches the malware.

Another important reminder is to always update your computer and virus protection software. There is a constant battle between criminals and security companies. Criminals introduce new malware, then security companies provide an update or a patch to stop it, then criminals update their malware to avoid detection, then security companies provide an update to detect it — and on and on. Having the latest version of security updates and patches is a must to protect against many of the known attacks.

In 2018, an Allentown, Pennsylvania city employee took his laptop while traveling and missed several software updates while not on the city's network. During his travels, the employee clicked on a phishing email and infected his computer. When he returned to the office, the infection spread to other computers.

The cleanup cost Allentown more than $1 million. If the updates or patches had been timely deployed, even though the employee clicked on the email, the virus protection software could have detected the attack before it spread.

We hope you enjoyed this year's **cyber buzz** articles concerning all things cyber related. Hopefully, you learned a bit about the cyber world and learned tips to keep safe while at home, work and even when traveling.

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