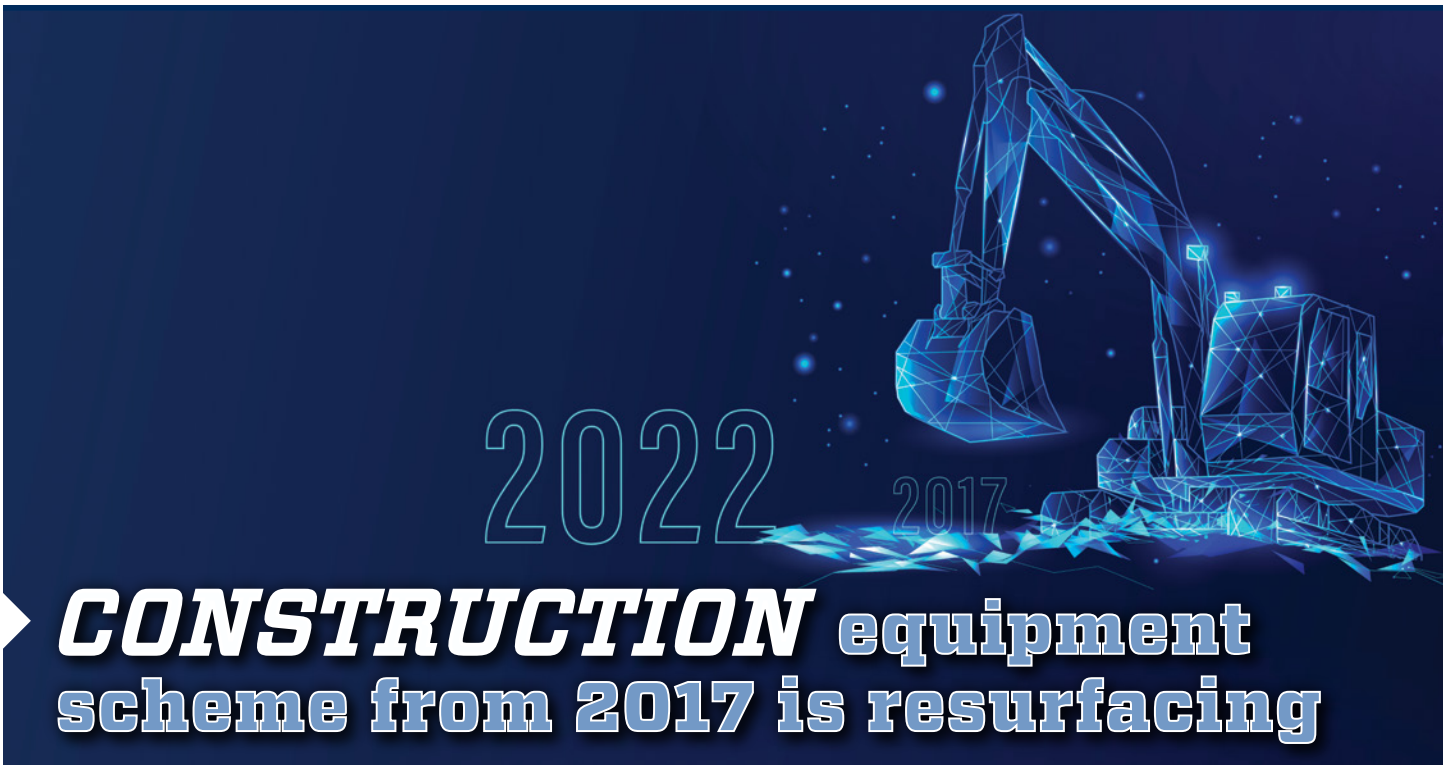
FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL



CONSTRUCTION equipment scheme from 2017 is resurfacing

By Lisa A. Tyler
National Escrow Administrator

On November 29, 2021, an 87-year-old buyer from Pittsburgh, sent a wire transfer in the amount of $342,838.03 to purchase a home in a retirement community in Arizona. The funds were intended to reach Security Title Agency in Glendale, Arizona, but they never arrived. We have all heard of the diverted wire transfer scam perpetrated on real estate buyers, but in this story the funds were not illegally diverted to a fraudster's account, instead they were illegally diverted to another title company! See how this story unfolds in "A days head start," which reveals the construction equipment scheme from 2017 has resurfaced in the real estate industry.

The Federal Bureau of Investigation (FBI) published a Public Service Announcement (PSA) on December 3, 2021, entitled "MONEY mules: a financial crisis," which is reprinted in this edition of *Fraud Insights*. One of the most interesting parts of the announcement is the consequence an individual suffers as a result of acting as a money mule.

Cybercrime occurs when a person uses an online network and a computer to commit fraud. In most cases the computer is used to commit the criminal act and another computer is the target. It threatens the public's safety. Each month in 2022, *Fraud insights* will contain a new cybercrime article; this month read "RANSOMWARE."

IN THIS ISSUE

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

volume 17 issue 1
January 2022

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

A day's head start

Nattalie Moore, an escrow officer with Security Title Agency in Glendale, Arizona, was closing an all-cash purchase of a home for an 87-year-old buyer. Nearing the closing date, the buyer started receiving emails from someone who appeared to be his real estate agent, instructing him to send funds to close right away. The emails created a sense of urgency and read as follows:

> *Due to back to back closing, the title company advised you to prepare to have your cash to close wired tomorrow morning as this well expedite the process of recording with the city and have the title work finalized prior to closing and also prevent any funding delays as they can only disburse on fully collected funds. You will be getting the final amount due at closing from your escrow officer along with wire instructions to complete your wire request. Please acknowledge the receipt of this email.*

The next email the buyer received was sent from a spoof email account meant to look like it came from Nattalie; it read as follows:

> *Our office is fully booked for the next coming weeks so we advise all buyers closing this month and next month to get their funds in earlier. I will send you your closing statement showing the amount due and the wire instructions to have your funds wired tomorrow morning.*

Finally, the message below came from the same spoof account:

> *Please find attached your closing statement showing the final amount due at closing and wiring instructions to complete your wire request this morning. Kindly confirm receipt and send me wire confirmation slip or an email stating wire transfer is done once your transfer is completed for your records and for our file.*

On November 30, 2021, the file was ready to close, but the buyer's funds had still not arrived. Nattalie called the buyer to check the status of his wire transfer of closing funds. He told her he sent the wire the day before, on November 29, 2021. He said he sent the wire after 3:00 pm, so Nattalie did not expect to receive it until sometime the next morning.

When the closing funds did not show up Nattalie called the buyer again. She asked him to confirm the wire instructions used. That is when he told her he sent $342,838.03 to a bank located in Fargo, North Dakota — but the account listed a different title company.

In the meantime, Rhonda Gaul, Nattalie's manager, received a call from the president of the title company in Fargo. She indicated she received a wire in the amount of $342,838.03 on November 29, 2021, that originated from Nattalie's buyer.

Rhonda was puzzled how the wire ended up at another title company. She performed some research to make sure the person she was talking to did indeed work for the title company in Fargo. She then asked the title company president to reject the wire. The title company president called her bank and was told the funds were already credited to her company trust account so the wire could not be rejected.

When Rhonda hung up the phone, she immediately shared the strange events with Nattalie, and acted swiftly to try to save the buyer's funds.

Rhonda sent wire instructions to the title company president in Fargo, and then verbally confirmed them with her, so she could send the funds to the Security Title Agency. Luckily, later that day the $342,838.03 was received by Security Title Agency, less a $25 wire transfer fee.

The buyer, who was buying his forever home in a retirement community in Arizona, cried tears of relief. Everyone involved felt the return of the funds was a miracle. Nattalie completed the closing on time.

However, the story does not end there. On December 1, 2021, the vice president of the title company in Fargo, unexpectedly called Rhonda regarding the wire transfer and left her a voicemail message.

Rhonda reached out to Lisa Tyler, the national escrow administrator, and asked her to join in a conference call returning the message. During the conference call, the title company vice president stated the wire transfer in the amount of $342,838.03 was sent in connection with a valid transaction they were handling and should not have been forwarded to Security Title Agency.

The title company vice president stated the funds came from the buyer's broker in his Fargo transaction — who had the exact same name as the buyer in Nattalie's transaction. What a coincidence!

The title company vice president also stated his company was handling an escrow for the sale of construction equipment — specifically five (5) 2013 Caterpillar 14m Motor Graders at $380,000 each — for a total purchase price of $1.9 million. He said the $342,838.03 wire transfer represented the initial deposit in the purchase agreement.

Lisa pointed out title companies do not handle escrow transactions for the transfer of construction equipment, such as graders or excavators, and it appears that his company is the victim of a scam, which has been perpetrated against title companies since 2017. He argued the

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or 949.622.4425

[A day's head start — continued]

transaction had been opened by an attorney in Fargo that was, "… a good customer."

Lisa explained that the scam would have unfolded as follows: the fraudsters would have cancelled the transaction and signed mutual instructions to have the $342,838.03 refunded to the buyer named in the purchase agreement (not the depositor), less any escrow fees or charges the title company wanted to deduct.

When the depositor finally discovered the funds were illegally diverted to the title company's account, they would sue the title company for disbursing their money without their authorization. And by then, the fraudsters would be long gone with the funds.

The title company vice president called the attorney who told him he, "… thought something was up …," with the buyer and seller. The attorney stated the buyer was not very communicative throughout the transaction that should have closed three months' prior. But once the wire transfer took place, the attorney received twenty-two calls regarding the wire in one day — demanding cancellation and disbursement.

Luckily, the buyer in Nattalie's transaction sent the wire on November 29, 2021, and not November 30, 2021, when it was expected by the fraudster. That provided both the title company in Fargo, and Nattalie and Rhonda, one day's head start to figure out the scam and prevent it from occurring.

Had the funds arrived on November 30, 2021, the title company in Fargo would already have signed the cancellation and disbursement instructions to send the funds to the fraudster. A quick internet search confirmed suspicions that the buyer and seller in the purported construction equipment transaction were not real people residing in the United States.

Nattalie's and Rhonda's quick reactions prevented the 87-year-old buyer from losing his life savings, allowed the transaction to close and prevented the title company in Fargo from a possible loss of $342,838.03. For their efforts, Nattalie and Rhonda will each receive a $750 reward from the Company, as well as letters of recognition.

MONEY *mules: a financial crisis*

A public service announcement from the FBI
Originally published on December 3, 2021

WHAT IS A MONEY MULE?

Any individual who transfers funds, on behalf of, or at the direction of another. Money mules are recruited to assist criminals with laundering proceeds from illegal activity and are often promised easy money for their participation in moving funds by various methods, including:

- Cryptocurrency
- Physical currency (cash)
- Bank transfers (wires, ACH, EFT)
- Money services businesses
- Pre-paid cards

WAYS MONEY MULES ARE RECRUITED

- Unsolicited emails or other communications requesting to open a bank account, cryptocurrency wallet or business in their name
- Romance/confidence scams
- Employment scams promising easy money
- Non-payment/non-delivery scams
- Lottery scams where personal information is collected

WHO IS AT RISK?

Anyone can be recruited to be a money mule; however, targeted populations include the elderly, college-aged students and newly immigrated individuals. Cyber-expertise or knowledge is not required; the money mule will be directed how to open accounts and process various transactions.

RECENT TRENDS

In 2020 into 2021, the FBI's Internet Crime Complaint Center (IC3) received an increase in complaints relating to COVID-19 fraud and online scams involving cryptocurrency, such as business email compromises, extortion, employment scams and confidence/romance scams.

MONEY MULE: COMPLICITY

Unwitting or unknowing mules: Not aware that they are involved in a bigger criminal scheme. These individuals are typically recruited via scams such as romance scams or more recently, employment scams due to COVID-19 pandemic. Generally, these individuals genuinely believe they are helping someone who is acting as their romantic partner or employer.

Witting mules: Ignore warning signs of criminal activity or are willfully blind to the financial activity they are participating in. They may have received warnings from bank personnel but continue to open multiple accounts. These individuals generally begin as an unwitting mule.

Complicit mules: Aware of their role as a money mule and complicit in the larger criminal scheme. They might regularly open bank accounts at various institutions with the intention of receiving illicit funds or openly advertise their services as a money mule and actively recruit others.

The increases in these scams could be the result of isolation due to COVID-19 quarantine restrictions, the loss of employment due to COVID-19, and increases in remote work, which allowed criminals to instruct money mules to provide copies of their personal information online.

Money mules were also asked to provide copies of their personal information or to directly open cryptocurrency accounts and wallets as part of online scams such as romance fraud, extortion, non-payment/non-delivery or investment scams. These accounts, opened in the money mule's name, could then be later used in other scams to target victims of business email compromises, tech support and other online scams.

[Continued on pg 4]

[MONEY mules: a financial crisis — continued]

CONSEQUENCES FOR ACTING AS A MONEY MULE

Individuals acting as money mules are putting themselves at risk for identity theft, personal liability, negative impacts on credit scores and the inability to open bank accounts in the future. Furthermore, they and their families could be threatened by criminals with violence if they do not continue to work as a money mule.

In addition, these individuals face prison sentences, a fine or community service, even if unwitting. Particularly in the United States, potential Federal charges include: Mail Fraud, Wire Fraud, Bank Fraud, Money Laundering, Transactional Money Laundering, Prohibition of Unlicensed Money Transmitting Business and Aggravated Identity Theft. These charges come with fines reaching $1,000,000 and up to 30 years in prison.

TIPS FOR PROTECTION

If you believe you are being used as a money mule:

- STOP communicating with the suspected criminal
- STOP transferring funds or items of value
- Maintain receipts, contact information and communications (emails, text messages, voicemails) so the information may be passed to law enforcement
- Notify your bank or payment provider
- Notify Law Enforcement. Report suspicious activity to the IC3 at www.ic3.gov and contact your local FBI field office

To prevent yourself from being recruited as a money mule:

- Do not accept job offers that ask you to receive company funds into your personal account or ask you to open a business bank account
- Be suspicious if a romantic partner asks you to receive or transfer funds from your account
- Do not provide your financial details to anyone (e.g., bank account information, logins, passwords)
- Do not provide copies of your identification documents to anyone (e.g., driver's license, social security number)
- Conduct online searches to corroborate any information provided to you
- Reach out to your financial institution with banking questions or concerns about financial transactions in your account

For additional information on Money Mules, please view:

FBI Scams and Safety: Don't Be a Mule: Awareness Can Prevent Crime
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules

RANSOMWARE

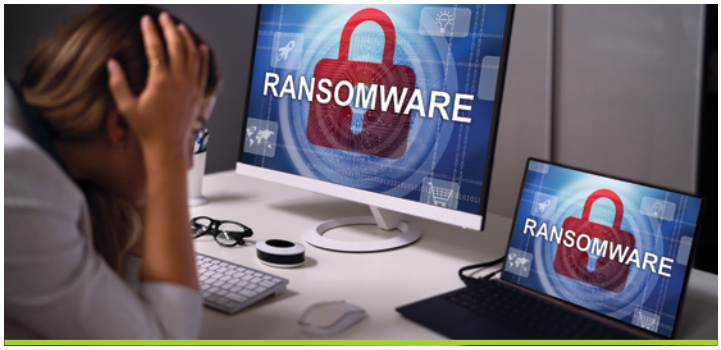
There are many different types of cybercrime. One of these schemes is ransomware, which has impacted both public and private companies who have fallen victim to these attacks. Ransomware attacks can cripple their victims for hours, days, weeks — and even months.

This year, each month will feature an article focused on ransomware. The articles will cover:

- ✔ What is Ransomware
- ✔ Defined Terms
- ✔ How is Ransomware Delivered
- ✔ Why and Who do they Attack
- ✔ Ransomware Types
- ✔ What to do if you are Attacked
- ✔ Why Cryptocurrency?
- ✔ Prevention
- ✔ Resources
- ✔ What's next? Watering Hole Attacks

Criminals who launch ransomware attacks intend to restrict access to the victim's computers by encrypting their data. Then, the criminals demand a ransom to restore the victim's systems and regain access to their data. You can imagine all the pitfalls!

A panel of cyber experts recently reported that more than 90% of all successful attacks occur because of the actions of a person. Humans are the biggest factor in preventing an attack.



SPOILER ALERT: The articles in 2022 will inform readers about this crime and how to reduce your risk of becoming a victim. Three preventative measures you can take are:

1. Use strong and unique passwords
2. Enable multi-factor authentication (MFA)
3. Install all security patches and software updates in a timely manner

Next month's article will describe what ransomware is. Do not miss it.

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