FRAUD Insights

Fraud Insights is published by: FIDELITY NATIONAL FINANCIAL

MORE than $130 million in ransoms

By Lisa A. Tyler
National Escrow Administrator

We have been discussing real estate scams involving vacant properties for years, including sharing tips and tricks on how to prevent fraud from occurring in transactions insured by the Company. Read about the alert recently issued by the U.S. Secret Service Cybercrime Investigations on the increase of real estate fraud associated with vacant property titled "REAL estate scams – vacant properties."

In other news, the FBI revealed on January 26, 2023, it had secretly hacked and disrupted a ransomware gang called "Hive." The operation allowed the bureau to thwart the gang from collecting more than $130 million in ransomware demands from more than 300 victims. Government hackers broke into Hive's network and put the gang under surveillance, stealthily stealing the digital keys the group used to unlock an organization's data. Find out more about this amazing story by reading "HACKED the hackers."

Mike Merlo, Vice President and Title Operations Manager for Lawyers Title Company in Burbank, California, has an impressive title department that offers sub-escrow services which complements their working relationships with independent escrow companies. Not only does his department search titles, but they also provide disbursement services for title clearance related items which work hand-in-hand with the escrow agent. Therefore, Mike's operation has standard operating procedures in place to ensure the department runs efficiently and protects the Company from losses. Read "HOW to be wire safe" for the details on how Payoff Processor Don Escusa, one of Mike's employees, followed the procedures and discovered two different payoff demands.

There are many different methods money launderers use to "clean" money. To learn the three stages of money laundering read the featured article titled "HOW is money laundered?" It is an interesting read on how law enforcement attempts to counteract this illegal activity.

IN THIS ISSUE

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

volume 18 issue 3
March 2023

FRAUD Insights

Publisher
Fidelity National Financial

Editor
Lisa A. Tyler
National Escrow Administrator

REAL estate scams — vacant properties

The U.S. Secret Service has recently observed a sharp increase in reports of real estate fraud associated with vacant and unencumbered property. Criminals are impersonating real property owners and negotiating the sale of properties that are vacant or lien free.

Specifically, the criminals are using Business Email Compromise (BEC) schemes. Visit the Secret Service website for guides on BECs and other cyber-enabled financial crimes.

How the real estate scheme works. A criminal:

- Searches public records to identify real estate that is free of mortgage or other liens and identifies the property owner. These properties often include vacant lots or rental properties.
- Poses as the property owner, then contacts the real estate agent to list the targeted property for sale and requests it to be listed below current market value to generate immediate interest.
- Demonstrates preference for a cash buyer, and quickly accepts an offer.
- Refuses to sign closing documents in person and requests a remote notary signing.
- Impersonates the notary and provides falsified documents to the title company or closing attorney.
- Receives closing proceeds that the title company or closing attorney has unwittingly transferred to the criminal.
- Communicates electronically, not in person.

The fraud is often discovered when recording the transfer of documents with the relevant county.

This scheme has particularly affected elderly and foreign real property owners, but it is not limited to these groups, because there are no means to automatically notify the legitimate owners. Therefore, the burden of verification is on the real estate and title companies.

How to prevent a vacant land/non-owner-occupied scheme:

- ✔ Independently search for the identity and a recent picture of the property seller.
- ✔ Request an in-person or virtual meeting. Request to see their government issued identification.
- ✔ Be alert when a seller accepts an offer below market value in exchange for receiving the payment in cash and/or closing quickly.
- ✔ Never allow a seller to arrange their own notary closing.
- ✔ Use a trusted title company and/or attorney for the exchange of closing documents and funds.

HACKED the hackers

In January 2023, the FBI revealed it had secretly hacked and disrupted an international ransomware gang called "Hive." Hive was one of the most prolific cybercriminal groups that extorted businesses by encrypting their data and demanded massive cryptocurrency payments in return.

Hive used a ransomware-as-a-service (RaaS) model featuring administrators, sometimes called developers, and affiliates. RaaS is a subscription-based model where the developers or administrators develop a ransomware strain and create an easy-to-use interface with which to operate it and then recruit affiliates to deploy the ransomware against victims. Affiliates identified targets and deployed this readymade malicious software to attack victims and then earned a percentage of each successful ransom payment.

Hive actors employed a double-extortion model of attack. Before encrypting the victim system, the affiliate would exfiltrate or steal sensitive data.

The affiliate then sought a ransom for both the decryption key necessary to decrypt the victim's system and a promise to not publish the stolen data. Hive actors frequently targeted the most sensitive data in a victim's system to increase the pressure to pay.

After a victim pays, affiliates and administrators split the ransom 80%/20%. Hive, however, will publish the data of any victims who do not pay ransom on the Hive Leak Site.

Using lawful means, government hackers broke into Hive's network and put the gang under surveillance, stealthily stealing the 300 digital keys the group used to unlock data from the organizations who were currently under attack.

[Continued on pg 3]

TELL US HOW YOU STOPPED FRAUD

settlement@fnf.com or
949.622.4425

[HACKED the hackers — continued]

Additionally, the FBI distributed more than 1,000 decryption keys to previous Hive victims.

News of the takedown was reported online when Hive's website was replaced with a flashing message that read, "The Federal Bureau of Investigation seized this site as part of coordinated law enforcement action taken against Hive Ransomware."

The takedown was a global initiative requiring cooperation across national borders and continents between the FBI, German Federal Criminal Police and the Dutch National High Tech Crime Unit. The German police and Dutch crime unit seized Hive's servers at the time of the takedown.

This takedown was different than other ransomware cases — there were no monetary seizures because investigators intervened before Hive demanded the payments. The undercover infiltration, which began in July 2022, went completely undetected by the gang until the January 2023 announcement.

It was reported that the FBI's operation helped a wide range of victims, including a Texas school district. The FBI provided decryption keys to the school district, saving it from making a $5 million ransom payment. At the same time a Louisiana hospital was spared a $3 million payment and the loss of important data.

Short of any arrests, Hive's hackers will likely either set up shop soon under a different brand or get recruited into another ransomware-as-a-service group. Either way, the sting operation took down Hive's nefarious activities and saved multiple companies from losing millions of ransom dollars and millions of data bytes.

HOW to be wire safe

Don Escusa, Payoff Processor for Lawyers Title Company in Burbank, California, was preparing to pay off a loan to clear title. The loan servicer on the loan was Freedom Mortgage. He reviewed the demand and verified it was a loan secured against the property which was the subject of the file he was working on. He confirmed the borrower's name matched the principal in his transaction.

Don reviewed the wire instructions. As a payoff processor, he is familiar with many of the loan servicer's wire instructions and noticed right away the bank listed on the demand was not the usual bank nor was the phone number shown on the demand. He compared the wire instructions on the demand against the repetitive wire list. The bank, account number and ABA number did not match.

Next, Don called Freedom Mortgage, at a known, trusted phone number and confirmed the wire instructions were **not** correct.

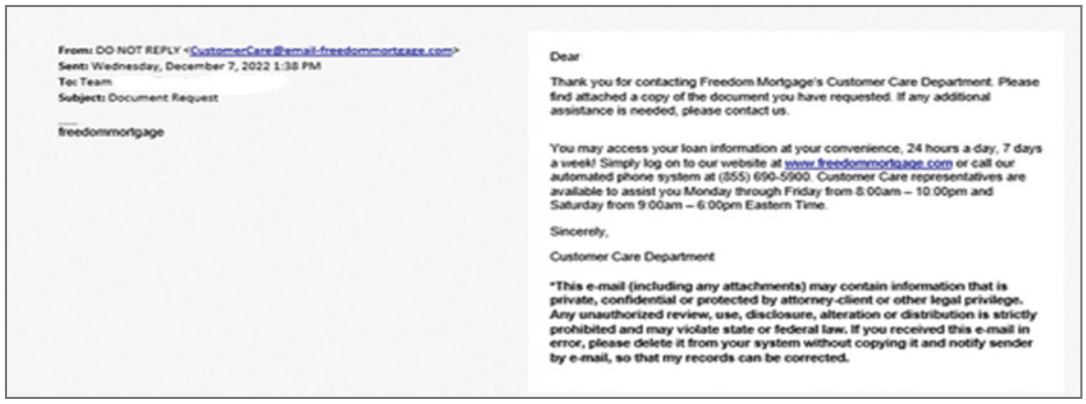
Don escalated the demand to his manager. They reached out to the independent escrow officer for more information. She explained she received two different payoff demands.

The first payoff demand was emailed to the independent escrow officer from Freedom Mortgage. The second one came a month later, but it came by fax. The independent escrow officer forwarded the revised demand to Lawyers Title.

Below are the demands side-by-side:

First Demand *Received December 7, 2022*	**Second Demand** *Received December 29, 2022*
Freedom Mortgage Corporation Reference: Payoff/Payment Department KeyBank, 127 Public Square, Cleveland, OH ABA: 123456789 Bank Account: 987654321 Borrower Name: Lois Price Loan Number: 1029384756	Freedom Mortgage Corporation Reference: Payoff/Payment Department **Truist Bank**, 127 Public Square, Cleveland, OH ABA: **100203098** Bank Account: **439821765** Borrower Name: Lois Price Loan Number: 1029384756

Here is the email which included the initial, valid demand:



From: DO NOT REPLY <CustomerCare@email-freedommortgage.com>
Sent: Wednesday, December 7, 2022 1:38 PM
To: Team
Subject: Document Request

freedommortgage

Dear

Thank you for contacting Freedom Mortgage's Customer Care Department. Please find attached a copy of the document you have requested. If any additional assistance is needed, please contact us.

You may access your loan information at your convenience, 24 hours a day, 7 days a week! Simply log on to our website at www.freedommortgage.com or call our automated phone system at (855) 690-5900. Customer Care representatives are available to assist you Monday through Friday from 8:00am – 10:00pm and Saturday from 9:00am – 6:00pm Eastern Time.

Sincerely,

Customer Care Department

*This e-mail (including any attachments) may contain information that is private, confidential or protected by attorney-client or other legal privilege. Any unauthorized review, use, disclosure, alteration or distribution is strictly prohibited and may violate state or federal law. If you received this e-mail in error, please delete it from your system without copying it and notify sender by e-mail, so that my records can be corrected.

[Continued on pg 4]

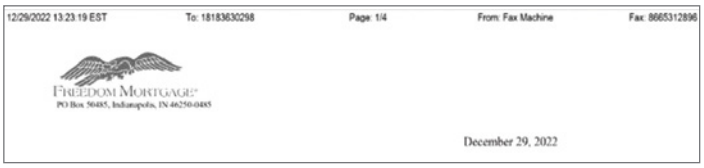
[HOW to be wire safe — continued]

This was the letterhead the demand came on:


FREEDOM MORTGAGE®
PO Box 50485, Indianapolis, IN 46250-0485

November 29, 2022

This is the letterhead of the invalid demand:


12/29/2022 13:23:19 EST To: 18183630298 Page: 1/4 From: Fax Machine Fax: 8665312896

FREEDOM MORTGAGE®
PO Box 50485, Indianapolis, IN 46250-0485

December 29, 2022

Here is the invalid demand, sent by fax:


From: MyFax <NoReply@MyFax.com>
Sent: Thursday, December 29, 2022 10:26 AM
To: Team
Subject: MyFax message from "18665312896" - 4 page(s), Caller-ID: 18665312896

myfax

You have a new fax! Click the attachment to view.

You can also view your faxes in the MyFax mobile app or by logging in to your account online.

Fax Details

Caller ID: 18665312896
Date Received: 2022-12-29 18:25:32 GMT
Type: Attached in pdf
Number of Pages: 4
Reference #: usw2b prod.afc_did12-1672338205-18183630298-380

If you have any questions, please visit our online help center.

Thank you for choosing MyFax!

Sincerely,
The MyFax Team

Get documents signed online with jSign – try it free!

Don did not know two different demands had been received nor did he know anything about how the demands were received by escrow. He simply followed the standard operating procedures which have proved to be tried and true.

Not only did Don protect the Company from a potential loss of nearly $500,000, he also shared his findings so others could be aware of the latest tactics being used. To show the Company's gratitude, he has received $1,500.

The methods the fraudsters use vary from one instance to another, which is why we continue to publish these stories. It is the best way to ensure everyone knows the latest tactics being used.

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

HOW *is money laundered?*

There are many different methods a money launderer may use to clean money but in all instances, there are three steps to the process. Those steps are:

1. Placement
2. Layering
3. Integration

The first step, **placement**, is the riskiest. This is where the launderer introduces the illegally obtained funds into the financial system. The funds are typically divided into smaller amounts and placed in a multitude of different ways, including being deposited into accounts of individuals within their network or by purchasing monetary instruments for a small amount.

Once the funds have been placed into the financial system the professional money launderer moves to the **layering** step. They move the funds around to conceal their origin. Funds are transferred all over the world since there are many countries who assist in concealing the customer's identity.

On paper, the money launderer purchases goods or services from the entities and send funds, even though the business serves no actual legitimate business purpose. Names are concealed by layering entities used to hide the person or person(s) making the purchases. Obviously, more money makes the layering step more complex.

Once the first two steps are complete, the criminal profits move to the **integration** step where they re-enter the legitimate economy.

The launderer might choose to invest the funds in real estate, luxury assets or business ventures. These transactions appear to be legitimate, but there still may be red flags involved with them.

Over the years, as law enforcement has uncovered the many tactics professional money launderers use, regulations have been put in place to identify those who facilitate this crime. The Bank Secrecy Act requires most financial institutions to report cash deposits and even some withdrawals — especially when multiple deposits are made in small increments. This act helps law enforcement prosecute professional money launderers and assists in crippling criminal organizations.

The information provided herein does not, and is not intended to, constitute legal advice; instead, all information, and content, in this article are for general informational purposes only. Information in this article may not constitute the most up-to-date legal or other information.

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