Mortgage Payoff Fraud Is Rising; Here's How to Protect Your Business

CERTIFID

Introduction

Stop a moment and think about this scenario: After months of hard work preparing to sell their house, going through the stress of finding a new home to purchase, and diligently completing back-to-back closings, your seller receives a late payment notice from the mortgage lender of the home they recently sold.

How could that have happened? Did the lender fail to apply the mortgage payoff to the proper loan? Was there another loan that was missed during the title search?

After some investigation, your team discovers that the mortgage payoff that was sent after closing was intercepted by a criminal.

The average mortgage balance in the United States reached $229,242 in 2021, making mortgage payoffs a top target for wire transfer fraud.

The average mortgage balance in the United States reached $229,242 in 2021, making mortgage payoffs a top target for wire transfer fraud. Title companies across the country are feeling the impact of this growing threat as an increasing number of fraudulent mortgage payoff statements find their way into active real estate transactions. When a fraud of this type occurs, not only could the entire transaction be voided, but the title company responsible for the mortgage payoff transfer of funds is on the hook.

So how does a cybercriminal operating from other parts of the world pull off this type of heist? And, more importantly, how can title companies protect themselves and their customers from this risk?

This guide will not only answer these questions but also outline the steps each party involved in a real estate transaction can take to prevent and, if needed recover from, this form of wire fraud.

What exactly is mortgage payoff fraud?

Mortgage payoff fraud is a financial crime where a fraudster impersonates a mortgage lender in a purchase or refinance transaction and manipulates bank account information on a mortgage payoff statement for the purpose of influencing a title or escrow company into sending a mortgage payoff payment to the fraudster's bank account.

While the exact path that criminals follow to perform a mortgage payoff fraud can vary, it generally includes the following steps:

- Sending phishing emails to real estate professionals such as title companies, real estate agents, or even buyers and sellers to gain unauthorized access to their email accounts
- Collecting information about active and upcoming real estate transactions, including the mortgage payoff details such as account numbers, banking institutions, payoff amounts, parties to the transaction, and key dates
- Intercepting the genuine mortgage payoff statement and changing the bank account details for the purpose of directing the payment to a criminal's bank account
- Impersonating the mortgage company and sending the fraudulent payoff statement to the title company
- Receiving and redirecting the payoff funds to alternative bank accounts to reduce the chance of recovery

While these steps seem complicated and hard to pull off, this form of fraud is becoming more and more common. In fact, according to Hugh Sprowson, Senior Underwriter at Argenta, mortgage payoff fraud "is the biggest payment risk facing title agents and a growing source of wire fraud-related insurance claims."

With the average mortgage payoff amount topping $229,000, this presents a significant risk to title companies because most of their insurance policies do not adequately cover incidents of wire fraud. This means that title companies are essentially self-insuring all or a portion of the risk if a payoff wire is stolen.

"Mortgage payoff fraud is the biggest payment risk facing title agents and a growing source of wire fraud-related insurance claims."

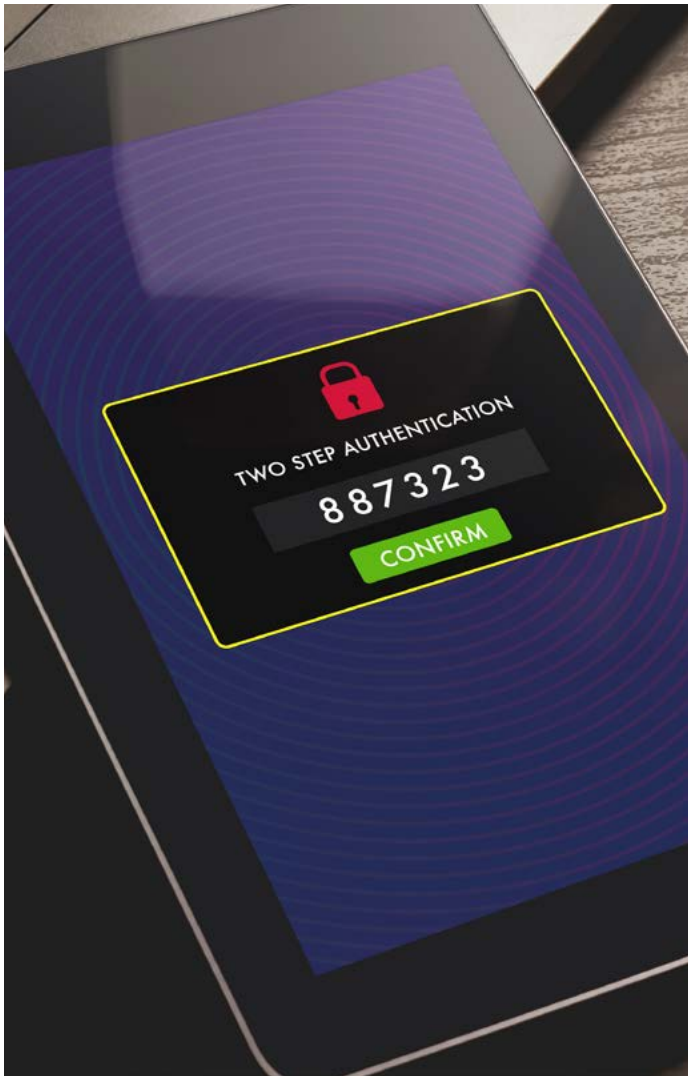
– Hugh Sprowson, Senior Underwriter at Argenta

What are other common tactics criminals use to pull off mortgage payoff scams?

Given the high returns cyber perpetrators gain from their efforts, they continue to invest in the technology and social engineering strategies that will place them inside the trusted communications shared between transaction participants. This includes text messaging, spoofed web portals, facsimile service breaches, and artificial intelligence used to deploy phishing attacks on a nationwide scale.

In addition to bolstering security around email, including the adoption of complex passwords, email monitoring, and multifactor authentication, businesses must be mindful that cyber risks come in many forms, and steps must be taken to mitigate risks along the following attack vectors:

- Electronic facsimile accounts where, if breached, fraudulent mortgage payoff statements are sent directly to your employees
- Web portals that spoof, or mimic, the identity of lenders or mortgage companies to gain loan and closing date details from parties to a transaction
- Social engineering geared toward tricking your staff into accepting and acting upon "updated" or "revised" mortgage payoff statements without proper verification of authenticity
- Impersonating trusted parties, such as a seller or listing agent, to distribute fraudulent wiring instructions to the title or escrow company



Timing and stress play a critical role when it comes to preventing mortgage payoff fraud. Cybercriminals understand the natural rhythm of a title or escrow company where stress and pressure build up to the last few days of the month. Often, employees feel the pressure to close out transactions and finalize mortgage payoff wire transfers during these periods, which can cause them to overlook otherwise obvious signs of fraud.

How can title companies and other real estate professionals help prevent fraud?

Despite the prolific rise of mortgage payoff fraud in recent months, there is a path to reduce this risk by leveraging the right tools, technology, and processes on each mortgage payoff.

Look out for the warning signs.

Like the neighborhood criminal looking for signs of homeowners out of town or cars left unlocked, cyberthieves are also looking for the easiest route to pull off their crime.

Here are some of the key warning signs to have your team watch out for:

- **Out-of-date or a lack of cybersecurity controls**, especially failing to have antivirus and malware protection, multifactor authentication, and strong password management in place
- **Suspicious or unexpected updates** or requests for changes to mortgage payoff statements
- **Unusual communications** (i.e., emails, faxes, or text messages) from unfamiliar accounts or sources claiming to be existing, trusted partners
- **The tendency to overlook or skip steps** to confirm key data when faced with the pressure of deadlines, especially independently verifying the payoff information and account numbers before sending a wire transfer
- **Requests to use contact information** for parties to the transaction or financial institution not verifiable through trusted sources

Ultimately, taking the extra time to verify the account information is worth the opportunity to avoid the risk of falling victim to wire fraud. In some cases, if the title company is unable to verify the bank account information supplied for the wire transfer, they choose to add per diem interest to the payoff amount and send a check via overnight courier to the mortgage lender.

Securely collect key data with end-to-end encryption.

Title companies also now have a powerful tool that they can use to add an additional layer of security for their customers and business: a data collection platform that offers end-to-end encryption.

Solutions such as CertifID easily integrate with existing title production platforms, allowing for the seamless and secure collection of wire transfer account information. CertifID works by verifying the authenticity of each user, enabling end-to-end encryption, and then allowing users to put in their required information.

For extra peace of mind, each transaction facilitated by CertifID is insured by Lloyd's by up to $1 million per wire transfer, and every customer has access to CertifID's experienced support team if they have a question or concern.

To date, CertifID has helped secure hundreds of thousands of transactions and can help to spot—and stop—suspicious activity before it can affect yours.

For extra peace of mind, each transaction facilitated by CertifID is insured by Lloyd's by up to $1 million per wire transfer.

What options do victims have in the wake of mortgage payoff fraud?

When it comes to attempting to recover from wire fraud, every minute counts. This is especially true because criminals usually work to move the stolen funds multiple times—and usually out of the country—to make it difficult to recover, let alone track. In recent months, the use of cryptocurrency wallets has made it even harder to recover funds that land in the hands of a fraudster.

While no one wants to face such a daunting financial situation, there are some key steps you and others can take to help potentially recover from falling victim to wire fraud.

To recover from wire fraud, every minute counts.

Here are some key steps to take as soon as possible:

- **Contact your financial institution** and request that they notify the financial institution that received your funds of the fraudulent transfer.
- **Contact the FBI** at www.ic3.gov and file a complaint; they may be able to assist with coordinating with the banks involved.
- **Contact your local law enforcement** office and/or the United States Secret Service's local office.
- **Contact** CertifID's Fraud Recovery Services to engage a team of professional fraud recovery experts.
- **Notify your insurance carrier** if you have protection for identity, cyber, or funds transfer loss.
- **Contact your IT department or third-party IT provider** to determine the initial tactic that the criminal took to grant them the access needed to perform the fraud, and contain any company systems that may have been breached.

After you contact the relevant financial institutions, law enforcement agencies, and your other service providers, check in with them regularly to provide any information they need and to ensure they do not lose sight of your case.

Although none of these steps can guarantee that your funds will be recovered, acting quickly and in a coordinated manner can dramatically increase your chances of at least recovering part of the money.

Take your wire fraud prevention to the next level.

Unfortunately, the risk of mortgage payoff fraud is only continuing to grow.

As a key part of the real estate industry, title companies and other real estate professionals like you need to make sure that they are doing their part to protect their customers, their brand, and their bottom lines. This is especially true since most title companies do not have adequate insurance in place to cover them in the event of wire fraud, leaving them to shoulder the risk and the fallout alone.

However, taking the necessary steps to bolster your organization's cybersecurity practices and increase the security of your mortgage payoff workflow with a platform such as CertifID can deliver your customers the security, reliability, and privacy that they deserve.

Want to add an additional layer of protection? Then take a look at PayoffProtect, which leverages one-of-a-kind technology to validate and secure payoff instructions. With the combined security of PayoffProtect and the CertifID platform, you will have the peace of mind of knowing that your mortgage payoff transactions are safe from constant threats by cybercriminals.