CERTIFID

WIRE FRAUD STOPS HERE

CLEAR TO CLOSE

The Complete Guide to Understanding and Preventing Real Estate Wire Fraud

Wire fraud is an epidemic in nearly every U.S. industry.

According to information recently obtained from the FBI, from June 2016 through December 2018, roughly $90 billion in attempted wire fraud was reported through the FBI's IC3 division.[1]

Because of this, it is crucial that companies are aware of how these scams work, and—most importantly—what you can do to protect your business and your customers from these types of fraud.

While wire fraud affects nearly every business, this guide will focus on its impact on the real estate sector.

1. Obtained under the Freedom of Information / Privacy Acts (FOIPA) from the Federal Bureau of Investigation; requested as "Wire Transfer Complaints"; December 2018

How Real Estate Wire Fraud Happens

While no two real estate scams are the same, cybercriminals tend to follow a typical playbook that includes the following steps:

1. Fraudsters find publicly available information of anyone involved in the transaction via social media, company websites, and online resources. This could target buyers, sellers, real estate agents, lenders, settlement providers, attorneys, or any other party to a transaction.

2. Known transaction participants are targeted with phishing scams designed to gather email account details. Once the fraudster gains access to one email account, all other parties to the deal are exposed and may be individually targeted or spoofed by the fraudster.

3. Armed with account access, fraudsters wait patiently and obtain intimate details about a transaction and the participants involved; particularly when someone is expected to transfer funds electronically.

4. The fraud begins once the fraudster identifies that funds are to be electronically transferred for a closing (e.g. via Wire or ACH). Using a compromised or spoofed email address, the scammer will send emails containing fake wiring instructions to the victim. This is typically a buyer wiring cash to close to the title company. Or it could be the title company wiring funds to a broker, seller and/or current mortgage holder in connection with the disbursement process.

5. Once the money lands in the fraudsters account, it is quickly wired to other bank accounts or withdrawn in cash, through an elaborate network of money mules that await instructions in real-time.

Parties Affected By Real Estate Wire Fraud

While wire fraud directly affects the party sending funds to the fraudulent account, all other transaction participants stand to lose too.

Buyers

Buyers continue to be the most vulnerable to real estate wire fraud as they are largely unaware that cybercriminals may personally target them. The purchase of a home is typically the largest financial decision the average U.S. consumer makes in their lifetime. For that reason, most people go through the process just a few times in their life. Inexperience with the process makes them susceptible to being tricked.

33%

First-time buyers made up 33 percent of all home buyers in 2018.

Home Buyer and Seller Generational Trends, National Association of REALTORS, April 2019

Sellers

Baby boomers make up a significant portion of sellers. Their lack of sophistication with technology leads to mistakes that could provide fraudsters access to critical transaction details.

If a transaction is compromised, sellers are directly affected when closing funds are diverted to a cybercriminal. If a transaction participant is unable to recover stolen funds quickly, the sale may fail, and the seller will have to go through the whole selling process again.

55

The typical seller was 55 years old, with a median household income of $98,800 in 2018.

Home Buyer and Seller Generational Trends, National Association of REALTORS, April 2019

Title and Escrow Companies

As title and escrow companies themselves often wire money, they are vulnerable to various wire fraud attack vectors.

Once a title and escrow company has received money for a closing, fraudsters will attempt to insert themselves into the stream of communication with the goal of leading unsuspecting title and escrow companies to send money to a fraudulent account during the disbursement process. For example, this could be a seller net proceeds or mortgage payoff that is diverted.

> ***The threat from wire fraud is wide. It's international in nature. It's difficult to track. And, its perpetrators are growing increasingly more sophisticated in their ability to disguise its true nature.***

Joseph Murin

"Sounding the alarm: Mortgage wire fraud is a much bigger threat than you realize." Housingwire, January 2018

Learn more about how mortgage payoff fraud is the fastest growing wire fraud scam sweeping the country in CertifID's Whitepaper "Mortgage Payoffs Under Seige" November 8, 2018.

Real Estate Agents and Brokers

Both their reputation and business are on the line. If a lawsuit is filed after a loss occurs, they may be held responsible for failing to notify their clients about the risks of wire fraud and complying with current industry standards around cybersecurity and secure email communication.

> ***Wire fraud isn't just costing realtors a commission check and a bad client experience; it's causing an overwhelming amount of heartache and legal issues.***

Ashley Cook

"Wire Fraud is Costing Realtors® Way More Than a Paycheck" Colorado Association of Realtors, June 2017

Law Firms

Cyber scammers know that law firms receive and send funds through their escrow accounts for real estate transactions. Scams that divert incoming wires from buyers and redirect disbursement wires after closing are proving successful against law firms and the individual attorneys representing clients in a real estate transaction.

Why Real Estate Wire Fraud Happens

There are three main attributes that make real estate transactions a prime target for wire fraud:

1. The median home listing price is ~$280,000.

2. There is an average of eight parties involved in every transaction.

3. All the information to start a fraud can be found online.

1. Large Wire Transfers Happening Frequently

Fraudsters target real estate transactions because they are incredibly lucrative and happen frequently. In 2018, 5.34 million existing homes[1] and 617,000 newly constructed homes[2] were sold in the United States. This sales volume would equate to over 23,000 closings per day-topping $33.3 trillion in value.[3] This provides ample opportunity and incentive for cyber perpetrators to develop and execute real estate fraud scams.

1. National Association of Realtors®, Quick Real Estate Statistics, May 2019

2. United States Census Bureau, New Residential Sales, May 2019

3. Lloyd, Alcynna, U.S. housing market value climbs to $33.3 trillion in 2018 Housingwire, January 2019

2. Multiple Parties Communicating Electronically

There is an average of eight parties involved in any U.S.-based real estate transaction. While their obligations may differ based on whether they are representing the seller or buyer in a transaction, there is one commonality among them all—they exchange communications and sensitive transaction information electronically. Many times these parties have never met in person and rely solely on the information exchanged over phone calls and emails. Making matters worse, real estate transactions are driven by specific timeframes that are agreed upon by the parties in the buy-sell agreement. Newly introduced parties, short time frames, and the stress of trying to close a home make everyone involved more susceptible to getting tricked or making a mistake.

3. Sensitive Details Easily Accessible Online

Most people in the real estate industry have no idea how easy it is for fraudsters to find sensitive information online. Sources fraudsters use include simple Google searches, social media profiles, MLS listings, and services like Spokeo that provide personal details about an owner of a property. In addition, they can identify the title or escrow company used to close the transaction by profiling the prior sales of a real estate agent. Using public notaries, fraudsters review the recorded deeds to determine whether the same notary public closer was used and identify where the transaction is likely to close. These three real estate transaction attributes create the perfect conditions for cybercriminals to be successful. Without taking further security measures to verify identity and ensure wiring details haven't been compromised, fraudsters will continue to be successful in diverting money from real estate transactions.

Fraud Strategies To Look Out For

Fraudsters use different methods to gain access to communications and manipulate details or share fake wiring instructions. Here are some of the techniques most often used to start a fraud.

Email Phishing

Phishing is when criminals send an email to a fraud target—or pool of targets—designed to get the recipient to enter account credentials or personal information about themselves.

When running a phishing scam, hackers send out an email that claims to be from a trusted organization; such as a bank, email provider, electronic document platform, or other reliable company.

40.9%

Total phishing volume rose 40.9% in 2018.

2019 Phishing Trends and Intelligence Report. PhishLabs. 2019

The email will often look real. Attackers usually send the phishing email from a disguised email address and include the logos and taglines of the company they are spoofing.

The hacker also provides a convincing reason for needing the information. They will then specify the information required, before highlighting a negative consequence for not sending it.

Spear Phishing

Spear phishing is a targeted attack on a specific individual.

The fraudsters send out an email from a cloned email account that's nearly identical to that of a trusted party. They'll likely use the same name, email, job title, and signature of the trusted source. Posing as the buyer, seller, title agent or realtor, fraudsters convince victims to divulge critical information.

Whaling and Business Email Compromise

Whaling is a scam used to target or impersonate business owners and high-level executives to divert wire transfers to fraudulent accounts.

$12.5B

Business Email Compromise losses reached $12.5 Billion in 2018.

FBI Public Service Announcement. Alert Number I-071218-PSA, July 2018

In the case of real estate fraud, hackers can use the access to a title company owner's email account to run a business email compromise scam. In these scams, they use the compromised account to convince employees to wire money to bank accounts they control. If you're a key decision maker in your organization, be wary of personalized emails asking you to verify account details or transfer funds. If you have any doubt, don't act!

Vishing

While most attacks come via email, vishing—voice phishing—is another method used during fraud attempts. Fraudsters know that most companies are requiring phone call verification or "call back" procedures before funds are wire transferred. With this knowledge, they can prepare well crafted and timely vishing attacks.

In these scams, hackers will call the victim or leave a voice message. The call or message will seem like it's coming from a trusted party in the transaction such as the title company, attorney's office, or bank.

The fraudster will often lead with specific transaction details and state that the call is being made to protect the person on the other end from fraud. This builds instant credibility and disarms the victims. The scammer can then move on to the goal of the call—get the victim to trust a new set of fraudulent wiring instructions and convince them to act quickly to execute the transaction.

How To Prevent Wire Fraud

A commitment to education and the adoption of preventative measures will lower your risk profile and protect yourself and your customers from fraud.

Here are some strategies to help you prevent fraudsters from gaining access to transaction-level information required to run a scam.

Limit Publicly Available Information

Running a business requires that certain information be shared about your company. However, there are things you can do to protect some of the more sensitive data about your organization and employees. You can see what is available publicly by merely performing a Google search on your business or employees. If you see anything sensitive, take steps to remove it.

Use Strong Spam Filters

Preventing phishing emails from being seen is the best way to stop employees from falling for them. A strong email filter is one of the best ways to do this. Products like Mimecast and Spam Bully provide solutions that block and filter phishing emails.

Install A Password Manager

Using the same passwords on any of your personal or professional accounts may expose you to security threats. Password managers like LastPass and 1Password provide the ability to create and store complex passwords that are more secure and harder to crack. Services like these are an easy way to lower risk and improve your security hygiene.

Phish Your Employees

People are the weakest link in your security. For that reason, we recommend performing periodic phishing tests on your employees to see how susceptible they are to clicking on fraudulent links and giving out confidential information.

We recommend hiring a third-party company to perform a phishing test or taking advantage of free online tools like the Google Phishing Quiz. It provides a great set of emails meant to educate you and your employees on how to identify phishing versus legitimate emails.

Use Two-Factor Authentication

Usernames and passwords have never been more vulnerable. Accounts that use two-factor authentication (2FA) require an extra piece of information on top of a username and password to log in.

Types of 2FA include:

- A code sent to an app on the user's phone.
- Virtual private networks that are tethered to each company device.
- A physical key like YubiKey.
- An SMS message with a code sent to your phone whenever you try to log on.

One final thing you can do regarding 2FA is to educate your customers and referral partners about the benefits of turning it on. If everyone involved has 2FA turned on, the chances of a hacker being able to access an account is drastically reduced.

Always Verify the Person You're Doing Business With

Wire fraud is a symptom of the lack of proper identity verification at critical points in a transaction. The success rate of wire fraud scams is due to the exploitation of a trusted relationship between two parties. If identities are confirmed properly, that trust is never breached.

Some things you can do to help verify information include:

- Gather and share contact information early in the transaction cycle.
- Have a secure process for sending and receiving wire transfers.
- Educate customers and staff about what a scam looks like.
- Authenticate wiring details and identity before funds are transferred.

To learn more about how to prevent wire fraud, watch CertifID's webinar "Lowering Your Risk Profile Through Technology, Training & Awareness" with special guest Josh Douglas, VP of Threat Intelligence at Mimecast.

How To Recover From Wire Fraud

Understanding Why Recovering Funds is Difficult

Fraudsters move fast when they successfully convince a victim to wire money. When the stolen funds arrive in the fraudster's bank account, they engage a network of money launderers who immediately withdraw funds in cash, wire the money to several different accounts and/or convert it to cryptocurrency.

The longer the trail between the original account—used to receive the transfer—and the money's final destination, the harder it becomes for the victim to recover their money.

Because of this, it is essential that you act quickly when you realize you have become a fraud victim.

The Recovery Roadmap

If you or someone you know falls victim to a wire fraud, the following roadmap may serve as a guide to maximize your chance of recovery.

1. Contact your bank and initiate a "SWIFT recall" on the wire transfer that left your account.
2. File a complaint with the FBI's Internet Crime Complaint Center (IC3).
3. Contact your local FBI field office and provide the IC3 complaint number.
4. Contact all banks that may have also received your funds.

5. Contact local authorities and file a police report.

6. Contact your security team, IT department, or consultant and initiate the information technology kill chain.

For those of you that have not been a victim a fraud but want to be proactive in preparing for the worst, we recommend creating a policy that includes the recovery steps above.

You may also want to consider designating an internal team who will be responsible for responding to a wire fraud incident should one occur. This team should also be responsible for creating and testing the timing and execution of the above protocol before a fraud incident arises.

Understanding Insurance Coverage

Wire fraud may, or may not, be covered in your errors and omissions insurance and/or cyber insurance policy. This is because the wire transfer is often made after a social engineering attack, not as a direct result of cybercrime or a direct breach to your computer network or attack on your personnel.

The fraudster convinces the victim to transfer money voluntarily. Technically, the fraudster does not directly use your computer to steal the money. Often, the claim is made by a third-party such as a buyer who was tricked into wiring their earnest money deposit or "cash to close" to a fraudulent account. Given these claim profiles, the various policies may respond differently–which can lead to finger-pointing by the carriers if a claim is made and delay settlements.

Today, it is worthwhile to check with your insurance agent and underwriter to confirm several things:

1. Identify the policies that cover the type of wire fraud(s) seen in real estate.
2. Review whether the limit of coverage for that exposure is adequate.
3. Review the claim triggers under which a loss will be covered by each policy.
4. Coordinate the various policies so that it is clear what will happen if a claim arises.

Conclusion

The promise of homeownership is the principal goal of many Americans; it's part of the "American Dream." These hopeful buyers approach what is likely the most significant financial decision of their life and are dependent on the experts they hire in the title, legal, real estate, and lending industries to guide and protect them through the process.

We are the custodians; we're the protectors and guardians of the transaction with the unique and lofty position of fighting on the front lines of wire fraud prevention.

Follow this guide and implement a layered approach to security across the hardware, software, people, and process that make up your organization. Those that embark on this journey, make the investment, and create a culture of compliance internally, will be positioned to benefit from lower instances of fraud attacks and will stand out as a leader in their communities. Fighting fraud is a journey, not a destination and we welcome you to come along with us as we strive to educate the community and create a shared culture of curiosity to stay alert and one step ahead of the threats.

About CertifID

CertifID is a real-time identity verification platform that allows parties to transfer wiring information securely. Every transaction protected by CertifID is guaranteed up to $1,000,000 against fraud. The company has protected over $1 billion in wire transactions, nationwide. CertifID was founded in 2017 by Tom Cronkright, Tyler Adams, and Lawrence Duthler.

About the Author

Tom Cronkright is a licensed attorney, large title agency owner, and award-winning business leader. His crusade to prevent wire fraud in the United States began after he and his business partner, Lawrence Duthler, fell victim to wire fraud in 2015 that cost their title company, Sun Title, $180,000. After two years of hunting down the culprits, they realized who they were up against. A sophisticated global network had cracked the code on these transactions and was wreaking havoc on the more than 25,000 title companies in the U.S. through hijacked email, fake phone numbers, and stolen credentials. Through that experience, they identified a need in the marketplace to create a real-time solution to verify identities and documents in financial transactions – CertifID was born.

In 2018, Tom was instrumental in helping the U.S. Department of Justice with the extradition and conviction of a Nigerian, cyber fraud syndicate leader, operating within North America. He is a national speaker on wire fraud and cyber security and author of several nationally-recognized whitepapers on wire fraud.

CERTIFID

1365 PLAINFIELD AVE. NE, GRAND RAPIDS, MI 49505
PHONE NUMBER: (616) 855-0855
WWW.CERTIFID.COM
INFO@CERTIFID.COM