



# **Seller Impersonation Fraud in the Real Estate Industry**

What it is and how to best prevent it



**ENTRUST**

SECURING A WORLD IN MOTION

# Introduction

In March of 1950, the Federal Bureau of Investigation (FBI) added Willie “The Actor” Sutton to their list of Ten Most Wanted Fugitives. During his tenure as an American bank robber, Sutton stole an estimated \$2 million and was known for using disguises. Police officer, maintenance worker, postal carrier, and telegraph messenger are a few of the roles the fraudster assumed to execute his heists.

When asked why he robbed banks, he replied, “because that’s where the money is.”

For a modern Willie Sutton, real estate seller impersonation might be considered the latest fraud method of choice. Fraudsters are focusing on compromising the identity of property owners to sell real estate they don’t own. Their goal is to collect the funds a buyer intends to use for purchasing the property before other transaction participants realize the fraudster is not the legal owner.

The issue is trending and has quickly become problematic for the title and real estate industry in the U.S. According to a survey from the American Land Title Association, title professionals reported cybercriminals attempted to deceive employees into wiring funds to a fraudulent account in a third of all transactions.<sup>1</sup> And according to FBI victim complaint data, business email compromise (BEC) scams targeting the real estate sector have risen 72% over a two-year span – with 2022 losses totaling over \$446 million.<sup>2</sup>

BEC scams targeting the real estate sector have risen

# 72%

over a two-year span with 2022 losses totaling over \$446 million.<sup>2</sup>

1. American Land Title Association: Survey: Title Professionals Targeted for Wire Fraud in a Third of all Transactions – April, 2021

2. FBI Internet Crime Complaint Center: Business Email Compromise: The \$50 Billion Scam – June 2023

# What Is Seller Impersonation Fraud?

The goal of a seller impersonation scammer is to convince real estate agents, title companies, and closing attorneys that they are the owner of a property. Because seller impersonation fraud is predicated on a weak identity verification process, the bad actor will attempt to avoid any in-person interaction and insist on closing the transaction via email and online.

First, the bad actor searches public record data to identify real estate free of a mortgage or other liens. Targets typically include vacant land tracts, second homes, and investment properties. Commercial properties are also targets given their high values. Once properties are identified, the bad actor will note the legal property owner's identity as indicated in publicly recorded data.

Once a property is identified, the bad actor will assume the actual property owner's identity and contact a real estate agent to list the property for sale. They will indicate a preference for a cash buyer and instruct the agent to list the property below market value to encourage a quick sale.

To close quickly, bad actors typically accept the first offer submitted by a potential buyer. For the identity verification step during the closing phase, they'll submit photos of a fraudulent ID or other falsified documents to the title agency. And they often mention travel, illness, or other family emergencies as reasons why they're unable to meet in person to sign closing documents or use multi-factor authentication. Then, of course, the bad actors will use fraudulent or compromised notary credentials to complete the process.

At closing, the title agent or attorney initiates a wire transfer of the buyer's purchase funds to a fraudulent account set up by the bad actor. In some instances, the buyer may also be tricked into wiring funds directly to the bad actor's account.

While the burden of verification is on the real estate and title companies, it can be especially damaging for the buyer victim as funds are difficult to recover once the transaction closes. Even if flagged by the title company prior to closing, the buyer may still incur costs for other items such as an appraisal or inspection report.

# Industry Challenges

Each case of seller impersonation fraud carries a high cost, and each party to the transaction may be subject to legal action from the rightful property owner – and potentially the buyer as well.

For example, a Fairfield, Connecticut, landowner discovered a new \$1.5 million home was being built on property he acquired in 1991. In October of 2022, a bad actor impersonated the landowner, and the property was sold to a developer for \$350,000 without the landowner's knowledge. The landowner is now suing the company on nine counts including trespass, statutory theft, and unfair trade practices – seeking damages and compensation of up to \$2 million.<sup>3</sup>

The number of properties and real estate agents, as well as the high value of these transactions, make this segment of the market a lucrative target for bad actors. Consider that in the United States alone:

- There are over 157 million land parcel records<sup>4</sup>
- There are over 3 million active real estate licensees<sup>5</sup>
- During December of 2023, there were 1.3 million homes for sale with a median sale price of \$402,045<sup>6</sup> (That's over \$522 billion worth of real estate on the market for just one month of the year)

Although each party to a transaction shares a role in the due diligence process, the responsibility of mitigating fraud risk can easily be misunderstood among participants. A buyer or real estate agent may assume a title company or closing attorney has conducted all appropriate identity verifications; and a title company may assume the real estate agent has appropriately checked a seller's information. Participants eager to close the deal can inadvertently increase the likelihood of successful fraud attempts. Bad actors know this and are capitalizing on current market conditions to commit fraud.

Further complicating the issue is how wire transfer fraud resolution is handled. The Truth in Lending Act and Electronic Fund Transfer Act protect certain types of money transfers. For example, if a consumer disputes a credit card transaction, the bank or creditor is required to investigate. If they determine an unauthorized transaction was made, the consumer may be compensated. Unfortunately, wire transfers are excluded from those same protections. The party initiating the wire transfer request is typically liable, even if deceived by a scammer.

[3. Business Insider – August 2023](#)

[4. The Regrid Data Store](#)

[5. National Association of Realtors®: Quick Real Estate Statistics – October 2023](#)

[6. Redfin: U.S. Housing Market – December 2023](#)

# Best Practices

Some real estate agents and title company employees are taking precautions to mitigate risk. They may contact the seller directly at an independently discovered and validated phone number. To verify identity, they may also mail the seller at the address on tax records, property address, and grantee address.

While these are worthwhile precautionary steps for mitigating the risk of seller impersonation fraud, researching online databases and sending printed mail can add inefficiencies to the closing process. Plus, these essential verification checks are often performed too late in the transaction workflow. While the potential for a quick closing may be appealing, lax or missing verification standards early in the process present greater risk of fraud.

If you're looking to reduce the risk of seller impersonation fraud, business email compromise (BEC), and wire transfer fraud, you should consider reviewing your entire sales process with the following three key priorities in mind:

1. Incorporating a secure onboarding process for both the seller and buyer, with options for remote ID verification when physical appointments are not possible
2. Ensuring strong authentication is used by all parties involved in a transaction to fight against any risk of phishing, account takeover, or even BEC attack
3. Upgrading contract and agreement e-signature processes to incorporate:
  - Identity verification (if it couldn't be done previously)
  - Multi-factor authentication options for signers
  - Document integrity and authenticity features
  - Secure delivery

These precautions will not only ensure a safer experience and mitigate fraud risks but also improve the seller's and buyer's experience and their trust in your business.

# Working With Entrust

Entrust has a well-documented history of expertise in identity-first solutions for secure transactions and agreements. We can help you strengthen your real estate workflows to meet your business expectations around security, reliability, and trust.

## Secure Onboarding Solutions

Our solutions can help you provide anywhere-anytime onboarding workflows with automated identity verification processes to foster trust in your brand while helping to reduce fraud.

Key features include:

- Biometric identity verification
- Document proofing
- eKYC and device reputation
- Regulatory compliance support
- For banking customers, an option to issue digital and physical payment cards minutes after onboarding

[Learn more](#)

## Phishing-Resistant Identity and Access Management Solutions

Ensure the onboarded sellers' and buyers' identities and devices are verified and authenticated using digital certificates to help protect against business email compromise (BEC) and account takeover (ATO) attacks.

Key features include:

- Multi-factor authentication (MFA)
- Identity orchestration
- Adaptive risk-based access and authentication
- High assurance credential-based access
- Single sign-on (SSO)
- Passwordless access
- Fraud detection

[Learn more](#)

## Did You Know ...

Entrust was named a Challenger in the 2023 Gartner® Magic Quadrant™ for Access Management, recognized for our ability to execute and completeness of vision.

[Get the Report](#)

## Verified Signing Solutions

Integrate seamless, secure, and trusted electronic signature workflows into your existing environment to provide a greater level of assurance for high-value transactions and agreements. The Entrust Verified Signing Solution helps throughout each step of the signing process and enables your team to focus on closing the transaction instead of performing manual checks to verify identities and signatures.

Key features include:

- Web portal, API, and mobile app
- Multiple signature types, including eIDAS advanced and qualified signatures
- Document sealing and timestamping
- Integration with other Entrust solutions for a full end-to-end user experience from onboarding to closure

[Learn more](#)

## Other Fraud-Prevention Solutions

These solutions can help you strengthen your own communication channels to further increase buyer and seller trust in your organization.

- **Verified Mark Certificates (VMCs):**  
Enables you to display your registered trademark logo in the avatar slot alongside outgoing emails. In addition to reducing the risk of seller impersonation fraud, VMCs help prevent wire transfer fraud and BEC. Real estate brokerages, lenders, and title agencies can prove to their recipients that emails received are indeed from the sending organization, while also improving employee phishing-awareness training results.
- **Secure/Multipurpose Internet Mail Extension (S/MIME) Certificates:**  
Allows users to encrypt and send documents securely in real time without the need for zip files or passwords. Real estate agents, title companies, and lenders can prove where and when the message originated as well as demonstrate that documents have not been tampered with in delivery. By retroactively protecting email, Entrust S/MIME certificates also help organizations mitigate the risk of data breaches.

For more information on how your organization can leverage Entrust solutions to reduce seller impersonation and other fraud, [contact us](#).

For more information

**888.690.2424**

**+1 952 933 1223**

**sales@entrust.com**

**entrust.com**

## **ABOUT ENTRUST CORPORATION**

Entrust keeps the world moving safely by enabling strong identities, secure payments, and protected data. We offer an unmatched breadth of solutions that are critical to the future of secure enterprises, governments, the people they serve, and the data and transactions associated with them. With our experts serving customers in more than 150 countries and a network of global partners, it's no wonder the world's most trusted organizations trust us.

Learn more at  
**entrust.com**



Global Headquarters  
1187 Park Place, Minneapolis, MN 55379  
U.S. Toll-Free Phone: 888 690 2424  
International Phone: +1 952 933 1223

Entrust and the hexagon logo are trademarks, registered trademarks, and/or service marks of Entrust Corporation in the U.S. and/or other countries. All other brand or product names are the property of their respective owners. Because we are continuously improving our products and services, Entrust Corporation reserves the right to change specifications without prior notice. Entrust is an equal opportunity employer. ©2024 Entrust Corporation. All rights reserved. SL24Q4-real-estate-seller-impersonation-fraud-wp