

SELLER IMPERSONATION FRAUD IN REAL ESTATE



SHIELD
TITLE AGENCY

FRAUDSTERS are impersonating property owners to illegally sell commercial or residential property. Sophisticated fraudsters are using the real property owner's Social Security and driver's license numbers in the transaction, as well as legitimate notary credentials, which may be applied without the notary's knowledge.



Fraudsters prefer to use email and text messages to communicate, allowing them to mask themselves and commit crime from anywhere.

Due to the types of property being targeted, it can take months or years for the actual property owner to discover the fraud. Property monitoring services offered by county recorder's offices are helpful, especially if the fraud is discovered prior to the transfer of money.

Where approved by state regulators, consumers can purchase the American Land Title Association (ALTA) Homeowner's Policy of Title Insurance for additional fraud protection.

WATCH FOR RED FLAGS

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A PROPERTY

- Is vacant or non-owner occupied, such as investment property, vacation property, or rental property
- Has no outstanding mortgage or liens
- Has a different address than the owner's address or tax mailing address
- Is for sale or sold below market value

CONSIDER HEIGHTENED SCRUTINY OR HALT A TRANSACTION WHEN A SELLER

- Wants a quick sale, generally in less than three weeks, and may not negotiate fees
- Demands proceeds be wired
- Wants a cash buyer
- Refuses or is unable to complete multifactor authentication or identity verification
- Is refusing to attend the signing and claims to be out of state or country
- Wants to use their own notary
- Is difficult to reach via phone and only wants to communicate by text or email, or refuses to meet via video call



For more information about real estate fraud, ask a Shield Title agent or visit shieldtitleaz.com

SELLER IMPERSONATION FRAUD IN REAL ESTATE



SHIELD
TITLE AGENCY

TAKE PRECAUTIONS

SOURCES

- Contact the seller directly at an independently discovered and validated phone number
- Mail the seller at the address on tax records, property address, and grantee address (if different)
- Ask the real estate agent if they have personal or verified knowledge of the seller's identity

MANAGE THE NOTARIZATION

- Require the notarization be performed by a vetted and approved remote online notary, if authorized in your state
- If remote online notarization is not available, the title company should select the notary. Examples include arranging for the seller to go to an attorney's office, title agency, or bank that utilizes a credential scanner or multifactor authentication to execute documents

VERIFY THE SELLER'S IDENTITY

- Send the seller a link to go through identity verification using a third-party service provider (credential analysis, KBA, etc.)
- Run the seller's email and phone number through a verification program
- Ask conversational questions to ascertain seller's knowledge of property information not readily available in public records
- Conduct additional due diligence as needed

USE THE PUBLIC RECORD

- Compare the seller's signature to previously recorded documents
- Compare the sales price to the appraisal, historical sales price, or tax appraisal value



CONTROL THE DISBURSEMENT

- Use a wire verification service or confirm wire instructions match account details on seller's disbursement authorization form
- Require a copy of a voided check with a disbursement authorization form
- Require that a check be sent for seller proceeds rather than a wire

FILE FRAUD REPORTS

- IC3.gov
- Local law enforcement
- State law enforcement, including the state bureau of investigation and state attorney general
- Secretary of state for notary violations

FIGHT FRAUD WITH INDUSTRY PARTNERS

- Educate real estate professionals in your community, such as county recorders, real estate agents, real estate listing platforms, banks, and lenders
- Host educational events at the local or state level
- Alert your title insurance underwriter of fraud attempts