
July 2, 2026

**Re: Seller Impersonation Fraud and Wire Fraud Diversion – Risk Management Reminders**

Real estate practitioners and title insurers have noticed an increase in the number of attempted and successfully executed seller impersonation scams and wire fraud diversions in recent months. It is always a good time for everyone to review the red flags surrounding common fraudulent schemes.

**Seller Impersonation Scams:**
These scams often involve a remote fraudster listing a property for sale online or with an agent. Most often the property will be vacant land without any mortgages of record, but we have seen second homes and other non-owner-occupied properties targeted on occasion, as well as property with recently deceased owners, and we have seen instances where a fraudster targets properties that are mortgaged because of the expectation of equity payout at closing. These properties will often be listed below market value to entice potential buyers into making contact and get them invested in what seems like a great deal.

While not always the case, often the fraudster will conduct all facets of the transaction by email or telephone and will be unavailable to attend the closing. The fraudster often will present some kind of time pressure to close and will submit all seller documents through the mail, UPS, Fed-Ex or other delivery service.

Fraudsters generally will shy away from in-person or even video appearances because their real appearance generally will not match their false identification. It is likely that notarial signatures and stamps of an actual notary will be forged on the deed. Often there is something unusual about the appearance and execution of the documents and signatures will likely not match the signature of the real owner, as compared to previously recorded documents.

As the fraudster is generally operating from a remote place, the fraudster's telephone number may not correspond to the real owner's location (of course, phone numbers can be spoofed). The executed documents may arrive from an unrelated location. It is not unusual to see a transaction where the real owner lives in one state, the fraudster provides a phone number with an area code corresponding to another state, and the seller documents or Notary can be tracked to a third state (many times Texas or California).

If a party refuses to or has excuses why he or she cannot participate in an identification verification service, the transaction should be treated with heightened scrutiny. Other attempts have been foiled by agents taking time to observe that the IDs presented do not appear quite right or that the person they have been talking to does not seem to fit the appearance of the person on the ID. If you receive an ID that appears suspicious you can contact your local law enforcement department to see if they can confirm the ID as fraudulent or accurate. As many of the schemes involve forged Notary signatures, they may also be spotted by contacting the notary listed on the document through contact information found from the state online notary database where the notary is registered.

These are just some of the red flags associated with these transactions. We recommend that you review the Secret Service's list of red flags, and the 6/16/26 FBI factsheet about Seller Impersonation Fraud. ALTA's identify verification guidance includes creating and implementing a fraud prevention program, creating protocols for your office on what to do when they suspect fraud, and providing training and tools to help your staff verify common identification documents. ALTA's resources on seller impersonation scams can be found here.

These fraud schemes may be foiled by using identification verification services. As our valued Chicago Title customer, we have access to multiple Solution Partners available to you for discounted prices, which can help you attain compliance and provide real solutions to save you and your clients time and money.

Make sure your staff understand the dangers of identity theft and seller scams so they can help protect your office from seller impersonation scams.

**Wire Diversions:**

Wire diversions continue to be a major source of losses in the real estate industry. Most commonly, wire diversions occur when one of the parties to the transaction has a compromised email account. Once the fraudster has access to the compromised email, they will monitor the account until a major transaction is upcoming. Using that knowledge of the upcoming transaction the fraudster will provide a fake set of wiring instructions that will direct funds to their own bank account. The fraudster may attempt to divert seller proceeds or loan payoffs.

The best and most effective way of preventing wire diversions is to institute internal policies to verify every single wire. Verifications should be conducted using known and trusted points of contact or points of contact that can be identified from safe sources. The verifications should never be done over email and should never rely upon contact information provided in payoff letters or obtained through email. We also recommend that you maintain a list of common bank ABA routing numbers to check against wire instructions.

Any change or alteration in wiring instructions should be viewed as a potential red flag. While false payoff letters may contain misspellings or just not look right, increasingly the letters appear legitimate on their face. There is no substitute for having a vigorous process in place for verifying wires. Additionally, you can issue checks in lieu of wiring funds at closing.

There are third-party vendors that offer wire verification services and payoff confirmations. These services can help confirm identities and bank details, secure your wire instructions, and confirm payoffs. If you are interested in wire protection services, look for companies that offer direct coverage over any error that results in wire fraud, as well as wire fraud recovery services. Several of these are included in the services available to you through our discounted Solution Partners as a valued Chicago Title customer.

In the event of a discovered wire diversion, time is absolutely of the essence. You should notify your bank and the receiving bank immediately of the attempted fraud and request that the bank initiate the FBI Financial Fraud Kill Chain. We recommend that you also contact the Secret Service immediately as we have found that agency has often acted very quickly when notified to freeze the funds before they are moved from the initial fraudulent account.

ALTA has also created a Rapid Response for Wire Fraud Incidents flyer with a step-by-step best practice instruction, which can be found here.