Tips to Protect Payoffs from Wire Fraud

February 26, 2019

Traditional mortgage wire fraud scams usually began with a fraudster deceiving a buyer or key party to the transaction into believing the imposter was a legit participant in the deal. Once inserted into the email chain, the criminal changes already established wiring instructions.

In a recent twist, fraudsters are deceiving title companies by issuing counterfeit mortgage payoffs and wire instructions from the start.

"Fraudsters now understand that it's not that hard to 'spoof' or imitate an authentic payoff statement—and that statement is the ultimate authority for title or escrow companies awaiting official wire instructions," said Thomas Cronkright, CEO and co-founder of CertifID. "As a result, the agent's guard is down and, once the fraudulent payoff statements are received by fax or email, the funds are quickly and mistakenly wired directly to the criminals."

According to Cronkright, emerging examples of payoff fraud include:

1. Spoofed lender payoff portals
2. Lender payoff statements received directly from the lender
3. Payoff received from current borrower
4. Land contract payoffs, seller-held mortgages and other third-party payments
5. Payoff trolling

In one instance, the California Land Title Association reported an altered payoff statement appeared to come from a loan servicer on behalf of a private party loan. However, the payoff really came from a spoof email account created to impersonate an employee of the loan servicing company. In

another instance, a nationally recognized bank sent a loan payoff statement. Then two days later, an unsolicited, updated statement came from whom the settlement agent thought was the lender modifying only the bank wire information. The statement and all other information contained was identical. In other instances, payoff statements appear to come from a related third party. When in fact a fraudster compromised the email account of the third party and sent a modified payoff statement. Third parties have included the seller's attorney or real estate agent and other interested parties.

How do the criminals find out about the transactions? In some cases, the fraudsters monitor properties on the Multiple Listing Service (MLS). When the property status updates to pending, the fraudsters watch the transaction by infiltrating one or more of the parties' email accounts. They watch the email traffic looking for payoff statements generated by a lender to the seller's attorney, seller's real estate agent or to the settlement agent directly. At that point, the fraudster intercepts and alters the statement then forwards it on with bank wire information for a money mule instead of the actual lender.

Tips to Avoid Falling Victim

1. Set up a repetitive wire transfer feature in your production system. Include the bank wire transfer information of the entities you repeatedly wire to the most, then lock down the wire information for that entity. If an employee receives a payoff statement containing bank wire information differing from the account information in your system, you will know they received fraudulent account information to illegally divert funds.
2. Disbursement should always make sense. If a nationally recognized bank supplies a loan payoff, the payoff should not direct the funds to another banking institution. In other words, BB&T loan payoffs are not sent to Chase Bank; that makes no sense.
3. Pay attention to details of each payoff statement. The account name on the wire instructions should be that of the payee or corresponding bank and no one else.
4. Verbally verify all bank wire information on payoff statements received from outside third parties. Only use a known, trusted telephone number and not the number reflected on the payoff statement. Statements with differing contact information are a red flag of fraud.
5. Verbally verify every non-institutional payoff every time, since the bank wire information is typically not available from previous successful wires.

"There is no silver bullet that will keep anyone safe at all times," Cronkright said. "A commitment to training, infrastructure, policies and procedures around data security will create a multi-layered approach to combat the ever-growing and evolving cyber threat."

Contact ALTA at 202-296-3671 or ***communications@alta.org****.*

109858