Fannie Mae®

Mortgage-Related Wire Transfer Fraud

On Aug. 27, 2015, the FBI released a public service announcement that advised businesses of the increasing prevalence of business email compromise (BEC) schemes. BEC tactics can target businesses that regularly perform wire transfer payments. This scam is carried out by compromising legitimate business email accounts via social engineering or computer intrusion techniques (i.e., hacking) to conduct unauthorized wire transfers. BEC scams continue to grow, targeting businesses of all sizes. FBI data shows a 270% increase in identified victims and exposed loss between January 2015 and January 2017. Exposure to U.S. victims since October 2013 exceeds $748 million. Fannie Mae's Mortgage Fraud Program (MFP) has received multiple referrals related to such wire transfer frauds. Preventing wire fraud begins with understanding how it is perpetrated and the many options fraudsters have for initiating fraudulent wire requests.

What is wire transfer fraud? Wire transfer fraud occurs when transfer instructions are altered, causing funds to be diverted from the intended recipient and delivered to another account.

How does mortgage-related wire transfer fraud happen? MFP has had several tips involving BEC. One particular action involved a Fannie Mae REO sale in New Jersey. The perpetrator sent an email to the buyer (using an email address that was similar to the settlement agent's email address) indicating that a "wiring change" had taken place and providing changed wire transfer instructions. The buyer complied with the instructions in the email and wired the proceeds as directed. When funds were not received in the timeframe anticipated, the buyer was contacted. Upon investigation, it was determined that the actual settlement agent had not changed the wire instructions, and the money went to a staged bank account in Dallas. Ultimately, the funds were absconded by the perpetrator. Per the FBI, in some cases such ill-gotten gains are sent overseas.

What are the methods of compromise? No two attacks are alike. Fraudsters use a variety of tactics to commit wire fraud using malware, social engineering, phishing, and email compromise, just to name a few. In the example above, the compromised email address may have been different by as little as one letter, making it nearly impossible to detect the difference.

Opportunity attracts fraud! Within the mortgage industry, millions of dollars are sent via wire transfer on a daily basis. This creates a prime opportunity for offenders to orchestrate BEC-type frauds. Detecting and preventing wire fraud is everyone's responsibility.

- Confirm that email addresses are legitimate − perpetrators make minor changes that mimic legitimate email addresses.
- Always follow your applicable business unit procedures for confirming the validity of changes to wire instructions.

Wire Fraud Costs

Did you know that the wire amount is only a subset of potential losses incurred during a fraudulent wire transfer?

Additional costs and expenses suffered by the victimized financial institution could include:

- Investigation – it takes at least 100 person hours to complete an investigation into a fraud attack
- Litigation fees

Preventing Wire Transfer Fraud

How can you prevent wire transfer fraud?

- Use a confirmation process. This can include verbal communication using a telephone number known by both parties.
- Know your customer. Be aware of your client's typical transfer activity and question any variations.