Loan Closing Scams

What is it?

In many credit transactions, it is common for homebuyers, businesses, real estate agents, law firms, and title and settlement companies to exchange information about the transaction and settlement via email. Loan Closing Scams are when a fraudster gains knowledge of a settlement, and impersonates one of the parties to the settlement in order to redirect funds transfers at, or near, the time of the transaction settlement. In many cases, emails purportedly from the settlement agent, real estate lawyer or settlement agent are sent containing "new" payment instructions, and could even demand the down payment be sent just before the closing date. In other cases, the fraudsters pose as the other party and send changes to payment instructions to the real estate lawyer or settlement agent in order to redirect the proceeds of the transaction to an account under their control, probably using a money mule. Some cases also involve phone calls from the fraudsters to "verify" personal information regarding the transaction.

Because participants in settlements commonly use irrevocable wire transfers, funds sent to fraudsters' accounts are redirected or withdrawn quickly and are unrecoverable.

Recent FBI statistics show that approximately 1,137 such schemes are reported each month and create victim losses of over $17 million per month. The FBI says, "Victims most often report a spoofed e-mail being sent or received on behalf of one of these transaction participants with instructions directing the recipient to change the payment type and/or payment location to a fraudulent account. The funds are usually directed to a fraudulent domestic account which quickly disperse through cash or check withdrawals."

Avoid Being a Victim

Financial Institutions:

- ✔ Make real estate industry customers such as real estate brokerages and title and settlement companies aware of this fraud. *Consider establishing code phrases known only to the parties. For example, a phrase that is meaningful to the parties, but uncommon to others.*
- ✔ Through your mortgage division, educate borrowers of this scheme. *Establish procedures that require verification of payment type and bank account information before funds disbursement.*

Consumers & Business Owners:

- ✔ As with all types of email phishing or spoofing schemes, be skeptical of emails containing changes to payment instructions.
- ✔ Verify all emails and phone calls, especially if revised or new payment instructions, or a change of communication method are provided. Use known phone numbers to call and verify the contents of the email or voice request.
- ✔ Avoid clicking links in emails. Check first with a trusted representative such as your real estate agent or settlement agent, to verify that they sent the email. Do not send sensitive information via email.

How It's Done

- Fraudster employs use of malware to gain access to email accounts.
- Email traffic is monitored regarding the transaction, closely following closing/ settlement dates and payment instructions.
- After identifying the target, the fraudster impersonates a party to a settlement transaction.
- The fraudster provides new account information and instructions for a pre-settlement payment, usually by wire transfer.
- Payment instructions direct the funds to an account controlled by the fraudster, or a money mule.