Buyer, Seller, Real Estate Agents and Escrow-holders BEWARE: Criminals are targeting your Wire and Electronic Funds Transfers!

Issue Date: October 2018

Real estate transactions in today’s world often involve the wiring or electronic funds transfer (EFT) of money to complete a deal. Previous consumer alerts have referenced or covered wire fraud in timeshare transactions and fraud against seniors.

Wire transfers and EFT’s in real estate purchase transactions have become the targets of criminals who interject themselves into a real estate transaction by posing as a party in the transaction. In these cases, the criminal often takes on the identity of a title or escrow company or real estate agent in the transaction and provides legitimate-looking instructions directing the buyer where to wire or transfer funds. These instructions result in the wiring or transfer of funds to the criminal’s bank account, often overseas, and the immediate loss of thousands, or hundreds of thousands, of dollars to the victim.

These are sophisticated, professional-looking attacks on your real estate transactions, and you need to be on the lookout. Cybercriminals may convincingly take on the identity of legitimate parties to your transaction, using authentic-looking logos and personal details in communications, in order to make you feel comfortable. It is best to be safe in how you respond, and to assume that your transaction is being targeted.

What can you do to avoid such criminal activity?

1. Whenever possible, use alternatives to wire transfers or EFT’s, such as cashier’s checks, and get a receipt. For smaller transactions, make the payment in person by check or credit card and get a receipt, as these payment sources provide you with proof of payment.
2. Obtain phone numbers and account numbers of real estate agents and escrow-holders at the beginning of the real estate transaction, and use those numbers throughout the transaction.
3. Even if it looks or sounds legitimate, do not act on a change of wiring or EFT instructions that you receive electronically (via email) or via phone call. If your real estate transaction will utilize wiring or EFT of funds, and you receive an instruction change about wiring or EFT of funds, call the real estate agent or escrow officer by phone at the known number you obtained at the start of the transaction and verify new instructions before sending money. Better yet, if there is a wiring or EFT instruction change, instead make payment in person using cashier’s check!
4. Do not send personal information (bank account numbers, credit card numbers, social security numbers, and financial details) by personal email or text. Take steps to use a secure, encrypted site to send personal information, or provide this information in person.

If you are victimized, it is critical that you contact your depository institution and the Federal Bureau of Investigations (FBI) immediately in order to have a chance at halting the criminal transfer. You can file a report with the FBI by calling a local FBI office or reporting online at FBI Internet Crime Complaint Center.