

Buyers are sending billions to cyber criminals

Instances of wire fraud are spiking around the globe – be aware and prepare! Hackers monitor email traffic and look for opportunities to send false wiring instructions to home buyers, hoping they'll wire their purchase money to the fraudster's account.

Make smart decisions about transferring funds ...

Here are some best practices for buyers as they prepare to bring funds to closing:

- A cashier's check may be a safer option than a wire transfer, and generally banks have lower service fees for checks than for wires. If the title company receives the cashier's check the day before closing, there's likely no slowdown in the timeline for disbursements.
- If a wire is necessary based on specific logistics, it's vital that the buyer call the title company (using a number from the company's website, NOT from an email) to confirm instructions.

If you're a victim of wire fraud ...

First and foremost, *move quickly* and take these steps:

1. Contact your bank immediately and ask for the wire to be stopped or returned.
2. Ask your bank to contact the bank where the fraudulent wire was sent.
3. Contact your local Federal Bureau of Investigation (FBI) office. The FBI can work with other agencies and might be able to help return or freeze the funds.
4. File a complaint with the Internet Crime Complaint Center using the form found at bec.ic3.gov.

The FBI has published a complete list of information they will need at:

www.ic3.gov/media/2017/170504.aspx

The list includes:

- The name and address of your bank
- Your account number
- Copy of the fraudulent wiring instructions containing the below:
 - The name and address of the bank where funds were sent ("Beneficiary Bank")
 - The beneficiary's name and account number
 - The correspondent bank (if applicable)
 - Dates and amounts transferred
 - IP and/or e-mail address of the fraudulent e-mail



For more information go to IndependenceTitle.com and search "wire fraud," or visit the FBI's website dedicated to internet crimes: www.ic3.gov

Wire transfer hijackings on the rise

Kara McGregor, Senior Vice President of Business Development, Independence Title

Imagine this scenario ... You're finally buying your dream home, and have saved up a large down-payment. You've made it through the obstacle course of loan approvals, negotiations and home inspections. You've worked through the logistics of planning a move involving kids, pets, and a lifetime accumulation of stuff. Your closing is a few days away.

Then, you get an email from your Realtor, title company, or loan officer (with standard logo and signature) that says the following:

"Congratulations, you're almost there! Attached are your wiring instructions for transfer of funds. Please make sure to initiate the wire a few days ahead of your closing. As you may know, instances of wire fraud are becoming more common, so please call your escrow officer Sarah at (512) XXX-XXXX and confirm these instructions before sending your funds. Please don't hesitate to get in touch with any questions."

The only recourse for a wire fraud victim is to contact the bank immediately to see if the wire can be stopped or returned, and to contact the FBI.

You call the number and talk to someone who answers the phone as "Sarah with Brand X Title," and she confirms the wiring instructions. You head to the bank with confidence. And you send all your funds to an account belonging to a cyber-criminal who has been monitoring your email exchanges for weeks, waiting for the right moment to step in and hijack your money. Your funds are gone, you can't buy the house (which has to go back on the market), and everything you have left is in a moving truck.

Don't underestimate how common this scenario has become. Title companies in our market area alone are seeing dozens of wire fraud attempts each month. When funds are misdirected, victims have to act fast. The only recourse is to contact the bank immediately to see if the wire can be stopped or returned, and to contact the FBI.

All parties to real estate transactions need to be aware of this threat and discuss precautions.

Here are two suggestions:

- The best protection at this time is to bring funds to closing via cashier's check. Online security systems currently lag behind cyber fraud schemes, and the old-school paper cashier's check is one way to keep your money safe as you complete your purchase.
- If a wire is the only option, follow strict protocols about verifying wiring instructions exactly. Do not ever confirm an instruction from a phone number given in an e-mail, regardless of how bona-fide the email appears to be. Pick up the phone and call your escrow officer using a number from the company's website, and confirm instructions. Never act from e-mailed instructions without an independent verification.

The old-school paper cashier's check is one way for buyers to keep money safe in a transaction.

Talk to the closing team at your title company about specific best practices. And visit IndependenceTitle.com (search "wire fraud") for some great resources to help you protect your transactions. You'll see details on options for bringing funds to closing, common wire fraud scenarios, and tips on what to do if your money is hijacked.

