Avoid being a wire fraud victim

4 min read T- T+

Follow the tips below to prevent email wire transfer scams.

Be vigilant and when it comes to wire transfers and to verify the information from trusted sources. If you receive an email, you need to make sure it's from a trusted source. If you receive a text, you must make sure it's from a trusted source. If you receive a call, you need to make sure it's from a trusted source.

- **In these situations, the seller should sign the wiring instructions, and the signature should be notarized, if possible.** Even then, the seller should verify the closing instructions over a phone call initiated by the law office, using contact information received prior to any discussion of proceeds and wires. Confirming a phone call verification via email is a good practice and a great way to document the file, but an email verification alone is inadequate.
- **Verify Every Wire Request:** The more personal the verification, the better. Have the seller sign wiring instructions at the closing ceremony in the presence of an attorney. If the seller cannot attend the ceremony, the wiring instructions should be included in the deed package.
- **Review Emails and Verify Instructions:** If wire instructions are received via email, mail or phone, you should always verify you are speaking with the right party by meeting in person or following a call back procedure using a phone number from a third-party source. This practice will ensure you are confirming with the correct individual. If wiring instructions are ever changed, you should presume the change to be fraudulent. Review the modified instructions in detail for any inconsistencies and always follow a call back procedure.
- **Advise Buyers to Not Accept Wiring Instruction Changes:** Hackers target emails with wiring instructions. Then, they use this information to send a modified email with updated directions for wiring money into their personal account. This type of scam is not covered by E&O insurance, so it is extremely important for real estate professionals to protect themselves and their clients in this situation.
- **Verify the Authenticity of Wiring Instructions Sent from a Free Email Service:** If wiring instructions are attached to an email from a free service like Gmail, Yahoo, or aol.com, you should assume they are fraudulent. Sometimes, hackers set up an alias account with a very similar name to send modified instructions. Examining the account name in detail is a good idea. Because the hacker already has access to the original account, he or she may use the same account in all other correspondence.
- **Don't Use Free Email Accounts:** These accounts have major security issues, and they are likely being mined for data by their providers. Plus, they may be in violation of the Rules of Professional Conduct. If you are currently using a free service, find a more secure and professional alternative.
- **Beware of Unusual Activity:** Be wary of wires going to any account that is not in the name of the seller. Also, be suspicious of any account with a geographic location different than the seller. There are possible explanations for different names and odd locations, but these red flags should be explored in detail, not via email.
- **Don't Send Wires Overseas:** Once money leaves the United States, it is likely gone forever.
- **Regularly Change Your Passwords:** Updating your password on a regular basis ensures someone can't acquire your password and use it to access your private accounts.

How to avoid losing your home settlement funds in a wire fraud

- Never wire funds to anybody or any institution unless you have checked the wire instructions independently with your title company, settlement or closing agent.
- If you can't or won't confirm the information over the phone, most title companies, settlement companies and closing agents post their wire instructions online, so be sure you check their official websites. If they do, you can compare those instructions with the instructions you received.
- Some agents will confirm the instructions you received over the phone if you give them the information you received. Just make sure you are talking to the right person at the right place.
- You need to have a good working relationship with your settlement agent to make sure that you know that "trusted" source.
- The safest way is to go to see the closing or settlement agent in person and then go to the bank to initiate the wire transfer. That way, you have face-to-face information with your trusted source.

How to stop a wire transfer to Western Union or Money Gram

Sometimes a payment needs to be stopped. For example: in case of fraud, or when a duplicate payment has been erroneously sent. Criminals launder billions of dollars overseas through financial fraud schemes like wire transfer fraud, corporate account takeovers, business e-mail compromise scams and other financially motivated crimes. Detecting that you sent money to the wrong account within 24 hours is the best chance of recovering your money.

What to do immediately: Call your financial institution and ask to issue a recall notice for your wire.

How to stop a wire transfer to Western Union or Money Gram

Western Union: Call the Customer Service number at 1-800-448-1492 (select option 5 to speak to a representative) or its Consumer Fraud number at 1-800-325-6000 (say "no," say "consumer Fraud," select 1 "protect me"). Western Union will need the individual's name and phone number(s), including any variations in the spelling of the name (such as nicknames, abbreviations or misspellings). Western Union will ask for the tracking number (MTCN), the name of the at-risk individual and the telephone number on the transaction.

MoneyGram: Call the Customer Service number at 1-800-666-3947 (select 5 "more options," then select 5 "fraud"). Non-family members should call MoneyGram's general Customer Care Center at 1-800-926-9400 (select 5 "more options," then select 5 "fraud"). MoneyGram will need the individual's name and phone number(s), including any variations in the spelling of the name (nicknames, abbreviations, or misspellings).

Large international wire transfers

For international wire transfers over $50,000, call your regional FBI office (https://www.fbi.gov/contact-us/field-offices (https://www.fbi.gov/contact-us/field-offices)) and local police. The FBI offers a Financial Fraud Kill Chain (FFKC) process to help recover large international wire transfers stolen from the United States. The FFKC is intended to be utilized as another potential avenue for U.S. financial institutions to get victim funds returned.

The FFKC can only be implemented if the fraudulent wire transfer meets the following criteria:

- the wire transfer is $50,000 or above
- the wire transfer is international
- a SWIFT recall notice has been initiated by your financial institution
- the wire transfer has occurred within the last 72 hours.

If this criteria is met, the following information will be needed:

- Summary of the incident
- Name of victim
- Location of victim (City and state)
- Originating bank name
- Originating bank account number
- Beneficiary name
- Beneficiary bank
- Beneficiary account number
- Beneficiary bank location (if known)
- Intermediary bank name (if known)
- SWIFT number
- Date
- Amount of transaction
- Any additional information that may be available, such as "for further credit," or "in favor of"

Any wire transfers that occur outside of these thresholds should still be reported to law enforcement (**http://www.ic3.gov/ (https://www.ic3.gov/)**) but the FFKC cannot be utilized to return the fraudulent funds.