WIRE FRAUD—WHAT IS IT AND HOW TO RESPOND

By: Michael P. Lafayette, Esquire[1]
October 16, 2018

A. Wire Fraud In Real Estate Transactions:

1. Hackers uses electronic communications (mostly email) to steal funds based upon fake communications by posing as clients, real estate agents, lawyers, settlement agents, etc.

2. A typical scenario: someone's email is hacked. The hacker monitors the email account (sometimes for days or weeks!) for a transaction. Once a transaction is ready to close, the hacker sends fraudulent wire instructions by email to a client or the attorney/settlement agent directing funds to the hacker's bank account instead of the proper recipient's account (it can be for the seller's proceeds or the purchaser's funds needed for closing).

3. Another scenario: Fake but authenticate appearing (lender) payoff instructions are sent to the attorney/settlement agent from a hacker with fraudulent wire instructions (to the hacker's account).

4. Risk Management/Office Policy Recommendations:

a. Don't use free public domain email accounts—most are easy to hack.

b. Activate two-factor authentication for email account.

c. Use a company domain name/exchange server and install a firewall to minimize the chance of hacking. Retain an IT consultant to increase your computer security.

d. Carefully examine the email address from which you receive information.

e. **Watch out for phishing emails with embedded links or attachments even when they appear to come from a trusted source. Do not click on link or attachment—delete email.**

f. Do not encourage a client to send wiring instructions by unsecured email.

g. Encourage buyers and sellers to confirm wiring instructions with their attorney/settlement agent before wiring money to their attorney/settlement agent.

---

[1] Michael P. Lafayette is legal counsel to RAR/CVRMLS and is a partner in the law firm of Lafayette, Ayers & Whitlock, PLC, 10160 Staples Mill Road, Suite 105, Glen Allen, Virginia 23060, tel. (804) 545-6250.

B. **Wire Fraud – How to Respond**

1. If you or your client are the victim of wire fraud, immediate action is needed to stop the wire or recall/return the wire if it has been sent.

2. The following is a step-by-step response plan for anyone who suspects wire fraud.

EMERGENCY RESPONSE PLAN
Wire Fraud

1. **Call the Sender's Bank**. Sender must immediately call the bank who originated the wire for the sender and request that it be canceled or recalled (whichever is applicable) due to wire fraud. Speak to the fraud or wire department or someone in authority to deal with wire transfers. If the bank is able to cancel the wire (and the funds are safe), then skip to item #4 below.

If the wire was sent to the hacker, ask the sending bank to immediately notify the recipient bank to return the wire or place a hold on the funds due to wire fraud. Obtain the wire number, recipient bank routing and account nos., and name on account where wire was sent.

2. **Call the Recipient's Bank**. Sender should also call the bank who is receiving the wire and ask for its return or place a hold on the funds due to wire fraud.

3. **Call the FBI**. Call the local FBI office and report a "wire fraud". For the 5 counties of Northern Virginia, call the Washington Field Office at (202)278-2000; for the Tidwater region, call the Norfolk Field Office at (757)455-0100; and for the rest of Virginia, call the Richmond Field Office at (804)261-1044. Though you are calling a local number, your call may be routed to an out-of-state FBI service center. Tell the FBI dispatcher that you "need assistance from the local field office to reverse a bank wire due to fraud." Be ready to provide all of the wiring information. Request the FBI institute a "financial fraud kill chain" with the recipient bank.

4. **Call buyer, seller, real estate agents/brokers and settlement agents**. Call (do not email) everyone connected with the transaction to inform them of the fraudulent wire instructions and hacked email. Avoid email because hacker could still be monitoring it. Advise everyone to rely upon established phone numbers—not a number on an email.

5. **Call the Sender and recipient's banks again**. Call the banks back to confirm your request has been processed.

6. **Call your insurance company**. If applicable, advise your liability/E&O insurer.

7. **Call other important resources**. Advise your IT consultant, lawyer, title company, etc.

8. **Foreign wire sent**. If the wire was sent overseas, sender should hire an attorney in that country to help recover funds.

9. **Report the fraud to IC3.Gov**. Report the wire fraud to the FBI website called "ic3.gov" (Internet Crime Complaint Center) at **https://www.ic3.gov**. IC3 now has an Asset Recovery Team that watches for reports of business email compromise wire fraud activity and immediately contacts the originating and recipient banks to notify them of the suspected fraudulent transactions. This information is also used in aggregate too for Federal agencies to uncover patterns or trends in internet enabled criminal activity.