Cyber Crime in the Real Estate Industry

Protecting Your Business From Hackers

C.A.R. LEGAL TOOLS

Technology Has Changed Real Estate

- Today, consumers have access to vast troves of information that enable them to make decisions faster than ever before
- Real estate professionals all benefit from faster and more efficient communication via email, mobile devices and other technologies
- Both groups generally agree that technology has brought greater convenience to the real estate transaction

C.A.R. LEGAL TOOLS

Technology Opens Door to Cyber Thieves, Hackers and Scammers

- Cyber criminals have discovered numerous ways to gain access to confidential real estate information
- In 2016, the FBI reported business e-mail compromise as a 3.1 billion dollar scam
- 1,300% increase in identified exposed losses since January 2015 with 22,143 victims

C.A.R. LEGAL TOOLS

The Latest Scam: Stealing Earnest Money, Down Payment or Seller's Proceeds

How it Works:

- Cyber criminal obtains an agent's personal information and breaches an email or other online account
- With access to the agent's emails, transaction files and other information, the hacker creates fake emails that appear to be legitimate
- At the appropriate time, the scammer diverts the client's earnest money deposit or down payment to his account, or alters escrow instructions initiating a fraudulent wire transfer
- Funds stolen using these scam communications often are deposited into an offshore account

C.A.R. LEGAL TOOLS

If You Have Been Scammed…

- Immediately contact the bank and escrow holder to stop payment of funds
- If the funds have been distributed, call the FBI immediately (310-477-6565). Funds may be recoverable if the loss is reported within 24 hours
- Banks should file a complaint with the F.B.I.'s IC3 unit at www.ic3.gov or contact the nearest Secret Service office at www.secretservice.gov/field_offices.shtml
- Notify all affected parties, change your passwords, talk to your attorney and be sure to determine whether any of your own personal or business accounts have been compromised

C.A.R. LEGAL TOOLS

Avoid Becoming a Victim of a Scam: Verify

- Avoid sending and receiving sensitive information by email
- Never wire funds prior to calling your escrow officer to confirm instructions. Use only the verified telephone number specified at the beginning of the transaction. Advise clients to do the same
- Voice verify that the wire transfer instructions are legitimate, and that the bank routing and account numbers are accurate

C.A.R. LEGAL TOOLS

Avoid Becoming a Victim of a Scam: Educate

- Educate clients about wire fraud risks:
  - Use C.A.R.'s Wire Fraud Advisory (form WFA)
  - Share C.A.R.'s brochure: Tips to Avoid Cybercrime in Real Estate
  - Share C.A.R.'s video short on cybercrime

C.A.R. LEGAL TOOLS

Avoid Becoming a Victim of a Scam: Email

- If you must send sensitive information via email, encrypt the message using an email encryption service
- When using a free email account (Yahoo, Gmail, etc.), use two-factor encryption
- Don't use free email without a Virtual Private Network (VPN)

C.A.R. LEGAL TOOLS

Avoid Becoming a Victim of a Scam: Passwords

- Use a strong password that combines upper and lower case letters, numbers, symbols, etc. Better yet, use passphrases
- Change passwords often, and don't share passwords
- Don't write down your password or post it in or around your desk

C.A.R. LEGAL TOOLS

Real Estate Scam Red Flags

- Misspelled words, poor grammar and unprofessional-looking communications are a sure red flag. Delete these emails immediately (and don't click on any links!)

- Today's scammers are much more sophisticated. Communications will be more professional. The scammer is likely to know something about you and will use that information to build trust

- Pay attention to email addresses. Scammers may use an email address that is slightly different from the *real* agent. For example, jsmith@realtyworld.com may appear as jsmith@realtyworlds.com

C.A.R. LEGAL TOOLS

Handling Sensitive Documents

What documents are considered “sensitive?”

- The FIRPTA Form AS – Contains social security number and name
- Preapproval letters that contain bank information
- Verification of down payment. (Delete or black out account numbers on bank statements)

Handling Sensitive Documents

- Bank account and social security numbers on closing statements. (Best practice is for the buyer to deliver these encrypted)

- Personal checks given as earnest money should be delivered directly to escrow (This is a default option in the RPA-CA)

TIP!

zipForm® encrypts documents in transit and at rest on zipForm®. Use a zipLogix Community account with your client to video, audio or text sensitive information in a secure environment.

C.A.R. LEGAL TOOLS

Summing it up…

- Technology has brought convenience to the real estate transaction – and hackers/scammers
- The most recent scam involves stealing client's earnest money, down payment or sale proceeds by diverting funds to the scammer's account using a fraudulent wire transfer
- If you or a client have been scammed, immediately contact the bank and escrow holder to stop payment and notify the F.B.I. and/or Secret Service
- If you must use email, avoid becoming a victim by securing your email system and encrypting sensitive documents
- Use C.A.R.'s Wire Fraud Advisory (Form WFA) and other Legal Tools to educate your clients about fraud risk

C.A.R. LEGAL TOOLS

Additional Resources

- C.A.R. Legal Q & A: Protect Your Brokerage from Cybercrime
- C.A.R. Form WFA, Wire Fraud Advisory (available within zipForm®)
- C.A.R. Brochure: Tips to Avoid Cybercrime in Real Estate (available within zipForm® in the epubs library and on www.car.org in the Legal Tools section)
- C.A.R. Cybercrime Video Short (available on www.car.org in the Legal Tools section)

C.A.R. LEGAL TOOLS