CHAPTER

07 SECURITY ISSUES

Learning Objectives

After this chapter, you will be able to

→ Discuss how to advise clients regarding in-home surveillance whether they are buying or selling a home.
→ Recognize types of cyber fraud and how to protect yourself and your clients.

In-Home Surveillance

Both state and federal laws cover surveillance. Chapter 16.02 of the Texas Penal Code and federal law Electronic Communications Privacy Act (ECPA) prohibit audio monitoring or recording without the consent of at least one individual who is part of the conversation. Neither Texas law nor federal law allow audio monitoring or recording during a showing without the seller being present and participating in the conversation, even if the monitoring or recording was done inside the seller's own home. Every seller with the capability of having audio monitoring or recording of persons in their home should seek the advice of competent legal counsel before performing any type of audio monitoring or recording.

Silent video is not prohibited by federal law except in places where an individual would have a reasonable expectation of privacy (for instance, a bathroom). Again, every seller with monitoring capability should seek competent legal counsel before videotaping persons in the home.

The fines are significant. Illegal recording is a felony offense in Texas and anyone who has been recorded could bring a civil suit against the seller, which could result in fines up to $10,000 per occurrence and other damages, court costs and attorney fees.

What should the license holder do when listing or showing a home where there might be in-home surveillance?

Sellers should be advised to seek the advice of an attorney before recording audio or video of the showings of their home.

Buyers should be advised to never make comments that could impact their negotiating position inside the home OR on the premises, AND should be advised to contact the security company after closing to make sure all the devices are either disabled or removed from the seller's name and access.

See Appendix G for the article "Is Your Seller's Surveillance Putting them at Risk" from *Texas Realtor®* magazine, November 2017.

Cyber Fraud

In recent years, fraudsters have increasingly targeted real estate transactions, and they have been so successful that wire fraud is now a multi-billion dollar industry. The perpetrators use various methods to deceive parties into wiring funds to fraudulent accounts, and they do not even need to hack into or gain unauthorized access to email accounts. Rather, they are able to intercept information sent over the internet. They are able to gather enough information about a transaction (such as the property address, the names of the parties, agents, and escrow officer, and the date and time of closing), to be able to effectively impersonate others involved in the transaction.

For example, the scam may look like this: a fraudster creates an email address that, on first glance, looks like it belongs to the escrow officer (e.g. janesmith@tit1e-company.com). The buyer receives an email that purports to be from their escrow officer, Jane Smith, but the buyer does not notice that there is a "1" instead of an "l" in the word "tit1e" in the email address. The fraudster's email provides bogus wiring instructions for the closing, and the buyer wires their closing funds to the fraudulent account, thinking they have been sent to the title company. By the time the buyers realize the error, the funds may be overseas with no ability to get the funds back.

The more information the scammer has about the transaction, the more believable it is to the unsuspecting victim, so it is essential for real estate agents to be aware of how information sent over the internet can be used. Many title companies have policies that require the settlement statement/closing disclosure (amongst other documents) to be sent to the parties using special encryption software. Encryption programs allow information to be sent over the internet without being accessible by those that would intercept it. However, if the agent receives an encrypted attachment from the title company, but then forwards the document to the client unencrypted, the information is then exposed. If a fraudster has a settlement statement, they can craft a more specific email that also contains the exact amount of the funds the buyer needs to wire for closing.

It is in the best interest of all involved in a real estate transaction to be cautious about the details of a transaction that are sent over email. Real estate agents should inform their clients about the prevalence of wire fraud and ensure that they know to verify all wire instructions via known phone numbers. (It does not do any good to call the phone number found in the signature block of the "escrow officer" in the fraudulent email! The fraudsters are more than happy to confirm their intended destination!)

Wiring Funds or Cashier's Checks

Real estate agents and their clients need to be aware of the potential of wire fraud and be cautious; however, wire transfer is a popular and legitimate form of transferring funds in a real estate transaction. With the potential of wire fraud, the client may prefer to use a cashier's check to transfer funds. Ultimately, the client needs to follow the actual title company or escrow agent's directions. Always double check any wiring instructions directly with the escrow agent by phone or in person.

Case Study 2

Follow the Rules

Capcor at KirbyMain LLC v. Moody National Kirby Houston, LLC, Court of Appeals, Texas, Houston (1st District) 509 S.W. 3d 379

Moody National Kirby Houston, L.L.P. (Moody Kirby) owned a vacant lot near the Texas Medical Center. Capcor agreed to purchase the land from Moody Kirby using a standard "Unimproved Property Contract" promulgated by the Texas Real Estate Commission. The contract specified a definite date for closing and provided that Buyer pay the Sales Price in good funds acceptable to the escrow agent. If a party failed to close the sale by the closing date, the other party was entitled to exercise its contractual remedies, which included terminating the contract and receiving the earnest money as liquidated damages.

The parties agreed to use Moody National Title

(case study continued)

Company, L.P. (Moody Title), a company wholly owned by Moody Kirby's sole owner, Brett Moody, as the title company. The day prior to closing, the Moody Title escrow agent informed Capcor's lawyer that Moody Title needed to receive the purchase funds in the form of a wire transfer. She informed Capcor's principal of the same requirement when he arrived at Moody Title's office the next morning to sign the closing documents, noting that the wired funds must be received by 3:30 p.m. Sometime after 5:00 p.m. on the day of closing, Capcor's principal showed up with a cashier's check for the balance due for closing. The title company informed Capcor that it could not accept the check because it was against their underwriter's policies. The seller terminated the contract the next morning for failure of the buyer to close. Capcor refused to sign a release of earnest money and sued Moody Kirby and Moody Title.

The appellate court affirmed the trial court who found that Capcor had defaulted and that the title company had not breached its fiduciary duty. While the Texas Department of Insurance says a cashier's check is good funds, it does not require a title company to accept a cashier's check. The TREC form specifies, "Buyer shall pay the Sales Price in good funds acceptable to the escrow agent." (Paragraph 9.B.2.) The title company during trial testified that a cashier's check is subject to a three-day hold, and it is their policy not to accept them as good funds. The contract affirmatively bestowed upon Moody Kirby the right to terminate if Capcor defaulted by failing to timely deliver good funds acceptable to the escrow agent. Escrow funds and attorney fees were awarded to Moody Kirby.

Avoiding Cyber Fraud

Just when you think you have learned everything you can to protect yourself and your clients, another scam appears. License holders should be aware of the types of cyber fraud and how to protect themselves and their clients.

Definitions

Cybercrime - criminal activities carried out by means of computers or the internet.

Spoofing - imitate something, a technique used to gain unauthorized access to computers where the intruder sends a message to a computer with an IP address indicating that the message is coming from a trusted source.

Wire Fraud - (man-in-the-middle attack) a hacker hijacks (spoofs) information between a trusted person and a network server and uses the information to replace the client's IP address with its own IP address. The hacker then continues to communicate with the client (buyer or seller) and the communication still appears to be from a trusted source (real estate agent, title, mortgage, etc…). The FBI estimates from June 2016 to May 2018, there was a loss of more than $1.6 BILLION in the US alone.

Phishing - the fraudulent practice of sending emails purporting to be from a reputable company in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

Social Engineering - the use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes.

Malware - software that is intended to damage or disable computers and computer systems.

Ransomware - a type of malicious software designed to block access to a computer system until a sum of money is paid.

Typo Squatting - the purchase of misspelled versions of a popular domain names for the purpose of attracting visitors who make typographical errors when entering web addresses, so that hackers can introduce malware into the user's computer.

Spyware - unwanted software that infiltrates your computer, stealing your internet usage data and sensitive information. It is a type of malware.

HOW do you protect yourself?

- ✓ THINK before you click on anything!
- ✓ Have MULTIPLE step authentications on all your accounts.
- ✓ Challenge telemarketers.
- ✓ If anyone initiates contact with you without your invitation, consider it a scam.
- ✓ Never sign into a public WIFI system.
- ✓ Be very careful when you type in website addresses.
- ✓ Do not download anything you were not expecting.
- ✓ Hover your cursor over the "from" email before you open it. Hover your cursor over any "click here" to be sure this is what you were expecting, if not, do NOT "click here".
- ✓ Know that nothing is free.
- ✓ Back up your data.

- ✓ Install antivirus/anti-malware software.
- ✓ Keep your software updated.
- ✓ Make your passwords HARD and illogical. Change them often. Consider using a password manager.

In Closing…

At the closing table on a $450,000 cash transaction, when the title officer asks for the cashier's check, you do not want to hear your buyer say, "I wired the funds to the title company 3 days ago, like your email said."

The FBI will now begin a relationship with you and your client!