SECTION FOUR

PROTECTING CONSUMERS' CONFIDENTIAL INFORMATION

1. What security measures do you have in place in your office to protect your clients' confidential information? _____
   _____
2. What are some of the common real estate scams occurring on websites like Craigslist? _____
3. A buyer sends an email to her buyer's agent with a copy of the buyer's recent paycheck and a credit report attached. Is the email secure? _____

Learning Objectives

Upon completing this Section, you should be able to:

- describe common real estate scams and how to safeguard against them; and
- explain methods for protecting confidential consumer information.

Real Estate Scams

Craigslist

Tandon School of Engineering Research Study

A research team at the Tandon School of Engineering at New York University recently conducted a study of 2 million Craigslist advertisements for rental properties over a five month period. The researchers discovered a total of 29,000 false listings in 20 major cities, more than half of which had not been detected by Craigslist.

NYU's study uncovered that Craigslist rental property scams typically fall into one of the following three (3) categories:

1) The prospective tenant is told to first order a credit report even though there is no property to show, and the scammer receives a commission from the credit reporting site the prospective tenant used.

2) The scammer copies a property listing from one site, whether for sale or lease, and posts the duplicate information on another site, usually offering the property at a rental rate at or below market value to stimulate immediate interest.

3) A "Realtor® Service" company, usually unlicensed and having no connection to the advertised properties, for a fee offers consumers access to listings of pre-foreclosure rentals or rent-to-own properties.

To read Tandon's article regarding the study, which includes a link to the full study report, go to: http://engineering.nyu.edu/press-releases/2016/03/01/renter-beware-study-finds-craigslist-catches-barely-half-scam-rental-listi

Common North Carolina Craigslist Scam

Of the three categories identified in NYU's study, NC real estate brokers seem to encounter and report the second type most often. Several listing brokers in the state have reported that properties listed for sale by their firms have "appeared" on Craigslist as being available for rent. Generally, the brokers have discovered the fraudulent advertisements when prospective renters have appeared at the homes, often having already paid security deposits or rent in advance. Contact information for the supposed property managers typically turns out to be false, and the prospective renters' money is never recovered.

How might a listing broker or property manager guard against clients' properties being falsely advertised on sites such as Craigslist?

- Discuss the issues with your property owner-clients to make them aware of the risks.
- Set up a *Google Alert* with the property address to monitor new activity related to the property address. Go to https://www.google.com/alerts for information.
- Ask the owner to search and monitor Internet sites for new listings related to the property address.

If a listing broker or property manager discovers that a client's property is being falsely advertised on a site such as Craigslist, what steps should the broker take?

- Tell the owner immediately.
- Report to the police.
- Contact the website to report the false advertisement.
- File a report with the Attorney General's Consumer Protection Division office within North Carolina at 1-877-5-NO-SCAM (1-877-566-7226) or 919-716-6000. Go to http://www.ncdoj.gov/Consumer.aspx for more information.

Wire Fraud

You attend a settlement meeting on behalf of your seller-clients who are unable to attend, but who previously signed both the General Warranty Deed as well as written wire instructions for the sale proceeds. Present at the meeting are the buyer, the buyer's agent, and the closing attorney. During the meeting, you and the attorney receive an email from the sellers stating they would prefer that the attorney wire the funds to a different bank account than previously authorized by the sellers. What should you and the attorney do in this situation? _____
_____

On January 2, 2016, Peter Bolac, the Trust Account Compliance Counsel for the North Carolina State Bar, released an email fraud alert to all licensed attorneys in North Carolina. It read in part: [emphasis added]

> Last week the Bar received multiple reports of fraudulent activity relating to wired funds in real estate transactions, with losses as high as $200,000. Here is a redacted sample of what we have received:
>
> "On a closing that took place on Friday morning, before we disbursed, we received an email and a phone call from a lady purporting to be our out-of-state seller asking us to wire funds to her bank account. On Monday we learned that the seller's email was compromised and bad actors had inserted themselves in her place. We attempted to retract the wire and we learned late yesterday that the bank did not retract the wire and will not communicate further without a subpoena."
>
> This firm had two-level authentication practices in place to protect against fraudulent wires, but the hackers emailed and called the firm to confirm the wiring instructions as was required. The hackers gained access to the email account of one of the parties to the transaction and learned the necessary information in order to assume the identity of one of the parties and initiate the fraudulent transaction. Another defrauded firm noticed after the fact that the email address of the hacker was different from the actual seller's email address by one letter.

Similarly, the *Wake Bar Flyer*, Oct-Dec 2016 edition, contained an article from Lawyers Mutual, a malpractice insurer for attorneys, titled "Wire Instruction Fraud Plagues NC Lawyers." It began:

> Over the last few weeks, Lawyers Mutual has received multiple reports of North Carolina attorneys who were targeted by scammers attempting to divert seller closing proceeds following real estate transactions. Unfortunately, several of these attacks were successful and hundreds of thousands of dollars were stolen and are very unlikely to be recovered. ….
> What went wrong and how can we prevent it? …It appears hackers first became aware of the closing by compromising email accounts of differing parties. Sometimes the attorney account was compromised, sometimes the Seller's account was compromised but the most common scenario was the Realtor's account was being monitored by international crime organizations.

Broker Best Practice: Verify Source of Wiring Instructions

If the seller wants to have sale proceeds wired to an account, then any wiring instructions provided by the seller should be signed by the seller, preferably manually, *as should any changes in those instructions!* If the seller doesn't plan to attend the settlement meeting, then the wiring instructions should be sent with the deed to be signed by all sellers.

Any notice received, particularly via email, changing previously approved wiring instructions should not be obeyed until the party receiving the funds has been personally contacted and the new instructions at least orally confirmed. Most importantly, ***the telephone call to the payee should be initiated by the broker or closing attorney***, neither of whom should rely on telephone confirmation initiated by the alleged payee or telephone numbers provided in the email.

REMEMBER: Monies sent via wire transfer are extremely difficult to recover.

Alerts may be found on the Office of the Controller of the Currency (OCC), Department of Treasury, at www.occ.treas.gov in addition to the NC Attorney General's website, http://www.ncdoj.gov/ .

Counterfeit Checks

A broker/escrow agent receives an earnest money check for $15,000 from buyers who are under contract to purchase a property. The broker promptly deposits the check into his company's escrow account. Three days later the buyers change their minds and deliver written notice of termination of contract to the seller/listing agent. Since the buyers terminated the contract prior to the Due Diligence date, they demand that the broker-escrow agent return their earnest money deposit. The buyers want the check to be returned immediately. What should the broker/escrow agent do? _____

Brokers in many states, including North Carolina, have reported situations similar to the example presented in "For Discussion." Another common scam is when an individual overpays [using a counterfeit check] for an item offered for sale and asks the seller to remit the difference.

Scammers are counting on brokers/firms to remit "refunds" before the banks have time to verify funds. In other words, the brokers/firms pay the scammers back before the original checks have cleared so there is no indication that the scammers have given them counterfeit checks.

These types of scams are especially dangerous for brokers/firms. If a broker/firm remits a refund for an earnest money deposit (or other trust money) before allowing the bank enough time to verify funds, and a deposit is later deemed to be counterfeit, the broker/firm will have spent other clients' monies.

The fake checks may look very real, even to banks. According to a September 2011 article in the *NC Bar Journal* "…Scammers are now counterfeiting certified bank checks from nearly every major and minor bank." According to the NC Department of Justice website:

> …advances in printing technology mean that crooks can now make very convincing counterfeit checks. Even banks have a hard time spotting these checks as fake because scammers often use the name and account number of a real company. It can take weeks for the check to be discovered as a fraud.

The bank may not be liable if an escrow agent chooses to release funds that are only provisionally credited. In a 2015 court case in which a real estate company sued its bank for a $30,000 loss from the real estate company's trust account due to a counterfeit check, the Texas appellate court held that the bank was not liable, particularly given the real estate company's failure to identify numerous "red flags" indicating that the proposed transaction was a scam. A summary of the case as published in the October 2015 edition of ARELLO's *Boundaries* is reprinted at the end of this section.

Broker Best Practice: Verify that funds have been collected by your bank before refunding them or wiring them to another account.

BIC ALERT: **NEVER** deposit a check and send the difference or overpayment back to the payor until you know the payor's check has been honored.

Only disburse funds after you know the deposit has been honored. This may take 7-14 days or more, as scammers may use false routing numbers on the checks to delay processing.

Protecting Consumers' Personal Information

List types of personal client information that brokers often have in their files. _____
_____
_____

Within the cyber world, hacking, malware attacks, and other attempts to steal personal information are becoming increasingly common. Examples from 2016-2017 include:

- February 29, 2016: The *Internal Revenue Service* announced that a May 2015 data breach compromised more than 700,000 taxpayer accounts, rather than 100,000 as previously reported.

- March 10, 2016: Premier Healthcare reported that a laptop was stolen from its billing department. While the laptop was password-protected, the data was not encrypted and personal information concerning 200,000 patients was compromised.

- March 25, 2016: *Verizon Enterprise Solutions* acknowledged that hackers stole information about 1.5 million customers after a cybersecurity journalist found the data for sale in an underground cybercrime forum. Ironically, the victimized company provides information technology and data breach assistance to businesses and governmental agencies globally.

- September 22, 2016: *Yahoo* discovered that a hacker stole information from at least 500 million accounts in late 2014, including email addresses, passwords, user names, birth dates, and in some instances, security questions and answers. However, this news paled when compared to Yahoo's December 14, 2016 announcement that a 2013 breach compromised personal information of *one billion* accounts.

- Four scams were reported in the April 2017 edition of Boundaries, published by ARELLO. One involved broker-Realtor members in Florida who received a letter from a bogus "Florida Board of Realtors" threatening to terminate their listing privileges unless the recipient sent $225 to an address. (The legitimate trade association is officially known as the Florida Realtors®.) The letter contained a working URL that appeared legitimate, but the links either didn't work or lead nowhere. In Colorado, cybercriminals sent emails targeting appraisers, real estate brokers, attorneys, and members of other regulated professions informing the recipient that a complaint had been filed against them. When the recipient clicked on the link to open the attached complaint, it unleashed a malicious code that created an "open lane" to the person's computer.

- May 2017: DocuSign announced that a third party had gained access to a "non-core" system used to communicate service-related announcements to users and stolen perhaps more than 100 million email addresses. According to DocuSign, only email addresses were stolen from the non-core system, but no names, physical addresses, passwords, social security numbers, or credit card information. Its core eSignature service, envelopes, and customer documents were not accessed and remain secure.

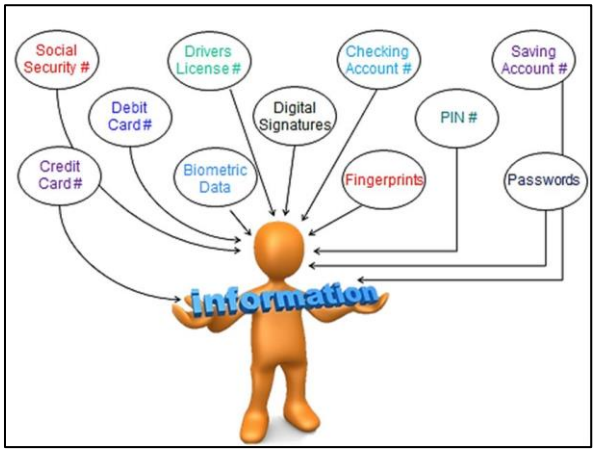
Brokers must safeguard and protect the personal information they collect from their clients or customers as well as information they electronically transmit to others whether by phone, email, text, etc. The transportability and utility of tablets, smart phones, laptops or other electronic media also presents one of the biggest inherent dangers; *these small, portable devices with incredible memory capacity can be easily stolen or lost*. Virtually all federal agencies now require all data on government laptops and portable devices to be encrypted unless the data is classified as "non-sensitive." Some GPS applications may help locate lost or stolen devices.

What is "Personal Information?"

North Carolina's Identity Theft Protection Act [NCGS §75-60, *et. seq.*] says:

> "Personal information" includes a person's first name or first initial and last name in combination with any of the following information:
>
> 1) Social security or employer taxpayer identification numbers.
> 2) Driver's license, State identification card, or passport numbers.
> 3) Checking account numbers.
> 4) Savings account numbers.
> 5) Credit card numbers.
> 6) Debit card numbers.
> 7) Personal Identification (PIN) Code …
> 8) Digital signatures.
> 9) Any other numbers or information that can be used to access a person's financial resources.
> 10) Biometric data.
> 11) Fingerprints.
> 12) Passwords.
>
> [See G.S. 75-66(c).]

Personal information may also include electronic identification numbers, electronic mail names or addresses, Internet account numbers or Internet identification names, and possibly a parent's surname prior to marriage. [See G.S. 75-61(10) incorporating G.S. 14-113.20(b).]



Client and Transaction Files

The Commission's record retention rule dictates what records must be kept and for how long, but it doesn't address the *manner* of retaining those records, other than to require that they "...shall be made available for inspection *and reproduction* by the Commission or its authorized representatives without prior notice." [Rule 58A.0108(c).] Thus, brokers/firms may choose to retain records:

1) in paper form and store them either on or off-site, depending on space; or

2) in an electronic or digital form and save them on a hard drive or thumb drive or other device within the control of the broker or upload them to the cloud.

   NOTE: There are numerous electronic document management and storage providers. For recommendations as to how to assess providers' suitability, please review the Commission's "Electronic Signatures and Documents" section of the *2014-15 General Update* course. To view the article, go to Commission's website (www.ncrec.gov), click on Publications, and select "Update, BICAR Topics."

Typically, the broker-in-charge formulates office policy including, among other issues, how the company/office will maintain and store both its transaction files and trust account records. A broker-in-charge should train all affiliated agents and any unlicensed administrative staff and assistants regarding the record keeping and retention procedures for that office. Similarly, affiliated agents have an affirmative obligation to inquire about and be familiar with office policies and procedures on all issues, including record maintenance and retention.

Whatever retention method is chosen, the company/broker should take whatever steps are necessary to ensure that consumers' personal information is protected. Following are a few examples.

What may a broker do to safeguard copies of earnest money deposit checks, due diligence fee checks, and tenant security deposit checks?

Commission Rule 58A .0117, Accounting for Trust Money, requires a broker to maintain or retain copies of earnest money checks, due diligence fee checks, and tenant security deposit checks. Thus, a broker who accepts possession of a consumer's check for any of these three (3) purposes should make a copy of that check and retain it as part of the transaction file. To safeguard paper copies of such documents, a broker might store them in a locked file cabinet or room and restrict access to the storage area. If documents are stored electronically, a broker should use strong passwords and limit access to the files. On paper or electronic copies, a broker may choose to redact confidential information such as account and routing numbers.

 ***A broker has 10 unlicensed salaried employees who assist her in showing and leasing various properties, collecting rents, and responding to repair and maintenance requests. The broker's policy requires every prospective tenant to provide with the rental application a copy of a recent paycheck stub (or other evidence of income) and authorization for the broker to obtain a credit report. Does the broker have any duty to protect the prospective tenant's information?***

YES. A broker who receives such information must safeguard and protect the consumer's personal information so long as it is in the broker's possession/transaction file, subject to the record retention requirements of Commission Rule A.0108.

The Broker should also consider:

- Who receives and reviews prospective tenants' applications and paycheck stubs?
- Who receives the credit reports?
- Who reviews the documents and decides whether to rent to tenant-applicants?
- Should all 10 salaried employees have access to personal tenant information?
- Where is application and tenant information stored once it is received?

Brokers clearly have a duty to safeguard and protect all personal consumer information that comes into their possession, whether the information belongs to a client or a customer, and should incorporate their procedures and best practices into their written office policies. The more people allowed to have access to personal information, the greater the possibility of theft or misuse with more possible suspects.

 **BIC ALERT**: If you employ accountants, bookkeepers, assistants, or others to assist you in handling finances or confidential client information, it is vital that you vet the individuals before hiring them. Suggestions include requiring a pre-employment background report and requiring employees to be bonded.

Electronic Communications

A broker uses a free email account (e.g., Gmail, Yahoo, Hotmail, etc.) to send and receive emails for both business and personal purposes. The broker has a password-protected secure internet connection both at home and at the office and her laptop is password-protected. The broker believes that all information she receives or sends is secure, as are all emails and information on her laptop.
Is the broker correct? _____ Why or why not? _____
_____

Security DO'S for Electronic Communications

- DO maintain multiple email accounts for your various purposes, e.g., one for online shopping, a separate account for personal emails, and a third account for business purposes.

- DO enable **Two Factor Authentication** (**2FA**); this process requires both a password and a second identifier.

- DO install firewalls, and use anti-virus and anti-malware/spyware applications.

- DO choose ***strong passwords*** and change all passwords periodically.

  The more unique the password is to you, the harder it is to crack. A "strong" password should be at least 12 characters, including upper and lower case letters, numbers and permissible symbols, or alternately, three random words (that you can remember) containing the foregoing features.

- DO choose tough security questions.

  If you can't create your own question and must select from a menu of questions, consider providing a false answer (but remember what the false answer is!). For example, if the question asks for a town where you were born or raised, name a town in which you never lived or a school you never attended, etc.

- DO encrypt your server, devices, and messages.

  Encryption is a process to protect data by converting readable data (called *plaintext*) into unreadable data (called *cipher text*) by using an algorithm (called a *cipher*). Decryption is the reverse process to convert unreadable text into readable text. The conversion is accomplished with ***paired keys***. So long as the decryption key is protected, the data is safe.

There are various encryption software products available for protection of data on networks, desktop computers, laptops, and other portable devices. Brokers and firms should consult with an IT specialist to determine the products that will best protect their data and devices.

- DO monitor your account for suspicious activity.

- DO turn your electronic devices off when you leave your office or aren't using them.

Security DON'TS for Electronic Communications

- DON'T use unsecured public Wi-Fi sites or public computers to check your email, financial accounts, or transaction files, as none of it is private or protected.

  If you must check email or a document, either use a mobile data service, e.g., 4G, or if you must use a public computer or Wi-Fi, use Virtual Private Network (VPN) which will encrypt the data passing through the VPN.

- DON'T open messages from unknown senders or click on links within or attachments to a message, particularly if there is no subject specified or the subject is generic.

- DON'T use the same password for all your online accounts.

  Since most people don't use multiple passwords or change them that frequently, hackers will use passwords found in one account to break into other accounts of the same user.

Office Common Areas

You are a BIC of an office with 50 brokers, some of whom are "full" brokers and others are provisional. The office has a work area equipped with six computers, a printer, and a copy machine that any broker may use. Often, brokers use the computers while meeting with buyer and seller clients. You scroll through the documents on one of the common computers and find drafts of multiple offers, copies of credit reports, buyers' loan estimates, and other documents received by various brokers during their transactions. *What should you do?*_____
_____

Having confidential information readily available on computers in common areas is not safeguarding the consumers' personal information. Further, maintaining information in this manner would likely destroy the company's ability to practice designated dual agency. Firms should have clear policies regarding the use of public or common access computers.

Public Meeting Locations

 **BIC ALERT**: Are brokers meeting consumers at public places, e.g., coffee shops, to discuss brokerage matters? If so, remember to keep conversations private and to be careful about using public wireless internet services.

Disposal of Personal Information

North Carolina's Identity Theft Protection Act also requires all "businesses" (broadly defined to include all entities, sole proprietorships, associations, or other groups however organized, whether for profit or non-profit), that conduct business in North Carolina:

> "… that maintains or otherwise possesses personal information of a resident of North Carolina must take reasonable measures to protect against unauthorized access to or use of the information in connection with or after its disposal..."
> [G.S. 75-64(a).]

This statute [G.S. 75-64] says **businesses should have written policies concerning the proper destruction or disposal of documents** containing personal information; reasonable disposal methods might include:

- "… the burning, pulverizing, or shredding of papers containing personal information so that information cannot be practicably read or reconstructed.

- …the destruction or erasure of electronic media and other nonpaper media containing personal information so that the information cannot be read or reconstructed."

Alternatively, a business may enter into a written contract with a record disposal company to destroy the business's records in accordance with state law.

Resources

Federal Trade Commission's Website

The Federal Trade Commission's website has a wealth of information and recommendations, such as an article, *Protecting Personal Information: A Guide for Business*, summarizing the FTC's recommendations for protecting personal consumer information. Within the article is a link that allows you to download a 36 page brochure explaining in greater detail the FTC's advice.
https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business

ARELLO Article: *Texas Appellate Court: Bank Not Liable for Brokerage's Counterfeit Check Loss*

[Reprint from the Association of Real Estate License Law Officials (ARELLO) *Boundaries* publication, October 2015, p. 13-14.]

A Texas appellate court recently held that a bank was not responsible for a $30,000 loss from a real estate brokerage escrow account that resulted from a successful counterfeit check scheme. In doing so the court relied, in part, on the failure of the brokerage to identify numerous "red flags" indicating that the proposed transaction was a scam.

The case, Am. Dream Team v. Citizens State Bank, involved a real estate brokerage ("ADT") that received emails from a purported Chinese buyer, "Mr. Yang Hua Lopez," who represented that he was the chief financial officer of a Chinese company. "Lopez" wrote that he wanted to buy a home "in your city and state," and would have his stock broker in America send money "to keep in a trust account." An ADT agent responded by sending information about prospective properties. Ninety minutes later Lopez chose one, which he described as his "dream home." Lopez then sent an email stating, "...my stock broker has sent you a payment of $105,000.00 USD ($500,000.00USD) will be down payment of the property the rest will be completed upon my arrival and $98,000.00 (USD) will be for the purchacse [sic] of Chinese home style [furnishings]." In a third email Lopez wrote that his stock broker had sent "...a new payment of $35,000 via UPS ($5000.00USD) will be the down payment of the property the balance will be completed upon my arrival and ($30,000.00USD) will be for the purchacse [sic] of Chinese home style [furnishings] in China." On the same day ADT received a check, purportedly from an individual named "Mr. Green Sound" who identified himself as Lopez' "account manager." The numerals on the check stated "$35,000.00USD", and, in writing, "THIRTY THOUSAND AND 00/100 USDOLLARS." The check's purported drawer was AXA Insurance Company of Canada and the purported payer bank was the Bank of Montreal in Toronto, Ontario. Lopez never executed a buyer representation agreement as requested by ADT, or a signed earnest money contract to purchase the property.

An ADT corporate officer deposited the check into its escrow account at Citizens State Bank, in the amount of $35,000. Instead of paying a fee to have the check sent for collection, ADT opted to receive a provisional credit that would make the funds available immediately, subject to the bank's deposit agreement with its customers. Bank employees told ADT officials that "the funds were here," "it looks like they're good," the check had cleared and the funds could be disbursed. ADT then, at Lopez' request, caused the bank to wire $30,000 to a Tokyo bank. The check was later identified as counterfeit and the wired funds were never recovered. The bank then charged-back the $30,000 provisional credit against the brokerage escrow account.

ADT sued the bank alleging, among other claims, misrepresentation and fraud. In large part, it based those claims on the statements made by the bank employees regarding the status of the funds. A trial court entered summary judgment in the bank's favor. ADT appealed.

The Court of Appeals of Texas affirmed the trial court judgment. The court ruled that the employees' statements were, in fact, true; reasoning that, pursuant to the bank's deposit agreement, it is not responsible for deposits beyond the exercise of ordinary care and check deposits are subject to receipt of final payment. And, the bank's policy is to make funds available on the first business day after a deposit. Thus, the employees' statements were true because, in accordance with the bank's deposit agreement and policy, the funds were there, were good, and ADT could disburse them. The court also found that the conversations between ADT and the bank employees regarding whether the check had "cleared" were ambiguous and did not support the claims of fraud and misrepresentation.

The court also examined the issue of "justifiable reliance," a necessary element of civil fraud and misrepresentation that cannot be established if there are "red flags" indicating that reliance is unjustified. The court found that "The red flags for ADT appeared in the first communication with Lopez and never stopped" and that ADT "...appeared to accept all of the implausible names, conflicting messages, inconsistent numbers, contradictory instructions, unusual circumstances, and absence of key documents at face value, rather than probing further into these red flags to determine if this was a legitimate transaction." The court thus held that the bank was not responsible for the $30,000 escrow account loss because ADT could not justifiably rely on the employees' statements when, at Lopez' request, it directed the bank to wire the funds to a bank in Tokyo for the purchase of furnishings in China for the Texas property.

The Court of Appeals also ruled that, pursuant to its customer deposit agreement, the Uniform Commercial Code, and corresponding state statutes, the bank properly charged-back the provisional escrow account credit after the check was determined to be counterfeit. The appellate court also affirmed that ADT is responsible for the Bank's $72,938.00 trial-level attorneys fees, plus appellate costs.

[*Am. Dream Team, Inc. v. Citizens State Bank*, 2015, Tex. App. LEXIS 9683 (Tex. App. Sept. 16, 2015).]

ANSWERS TO DISCUSSION QUESTIONS

For Discussion on page 55

1. What security measures do you have in place in your office to protect your clients' confidential information?

   Possible answers: locked storage area, password security, limited access to files, etc.

2. What are some of the common real estate scams occurring on websites like Craigslist?

   Possible answers: false rental listings, requiring prospective tenants to run false credit reports, etc.

3. A buyer sends an email to her buyer's agent with a copy of the buyer's recent paycheck and a credit report attached. Is the email secure?

   Answer: It depends. Are both the buyer and broker using secure servers to send and receive the email? Are the attachments encrypted? If either server is not secure, the emailed information is at greater risk of being hacked.

   If the broker's email server is secure and his/her laptop automatically encrypts all files when the broker logs off, then the client's personal information is protected on the broker's laptop. If the laptop doesn't encrypt files, then the attachments should be removed from the email and stored securely elsewhere.

For Discussion on page 57

You attend a settlement meeting on behalf of your seller-clients who are unable to attend, but who previously signed both the General Warranty Deed as well as written wire instructions for the sale proceeds. Present at the meeting are the buyer, the buyer's agent, and the closing attorney. During the meeting, you and the attorney receive an email from the sellers stating they would prefer that the attorney wire the funds to a different bank account than previously authorized by the sellers. What should you and the attorney do in this situation? _____

Answer: The settlement agent/closing attorney controls the settlement meeting and the monies are in his/her trust account. While it is unlikely that the attorney will accept the wiring instruction change without additional confirmation, the attorney and/or you should immediately contact the sellers by calling or texting numbers you know to be theirs to verify whether they issued the change in wiring instructions. No funds should be released until wiring instructions have been verified.
Also: No funds should be disbursed to anyone until the attorney has completed the last-minute title search and recorded the deed, which may be an hour or more after the settlement meeting.

For Discussion on page 58

A broker/escrow agent receives an earnest money check for $15,000 from buyers who are under contract to purchase a property. The broker promptly deposits the check into his company's escrow account. Three days later the buyers change their minds and deliver written notice of termination of contract to the seller/listing agent. Since the buyers terminated the contract prior to the Due Diligence

date, they demand that the broker-escrow agent return their earnest money deposit. The buyers want the check to be returned immediately. What should the broker/escrow agent do?

Answer: The broker should inform the buyer that the buyer's earnest money deposit will be returned once the broker confirms that:

1. *the seller doesn't dispute the earnest money refund to the buyer; AND*
2. *the bank notifies the broker that the funds are now "collected."*

For Discussion on page 60

List types of personal client information that brokers often have in their files.

Possible Answers:

- *Tax returns*
- *Social Security Numbers*
- *Driver's Licenses*
- *Credit History*
- *Paychecks*
- *Monthly Expense Documents*
- *Credit card and bank account numbers*
- *Alimony and child support payment history*

For Discussion on page 64

A broker uses a free email account (e.g., Gmail, Yahoo, Hotmail, etc.) to send and receive emails for both business and personal purposes. The broker has a password-protected secure internet connection both at home and at the office and her laptop is password-protected. The broker believes that all information she receives or sends is secure, as are all emails and information on her laptop. Is the broker correct? Why or why not?

Answer: No. The emails she sends and receives are secure only as long as both the sender and recipient are using secured internet connections; if either is using an unsecured connection, then that email no longer is protected. Additionally, none of the documents or emails on the broker's laptop are secure unless they are encrypted. The moment someone discovers her laptop password, that individual has access to anything and everything on her computer. One solution is to purchase a computer that automatically encrypts all documents. Absent that, she should avoid storing any documents with personal information on an unprotected device; instead, she should copy the sensitive document to a flash drive or other external hard-drive for safe-keeping and delete the document from her unsecure device.

UNDERSTAND that even if your network is secure, if the recipient retrieves the communication using an unsecured network, the communication no longer is secure on their end. In other words, the emails you send are only as safe as the recipient's inbox. One option is to put all confidential content in a password-protected encrypted attachment, rather than the body of the email (and obviously don't include the password in the same email). The email itself is not protected, but the attachment is.

For Discussion on page 65

You are a BIC of an office with 50 brokers, some of whom are "full" brokers and others are provisional. The office has a work area equipped with six computers, a printer, and a copy machine that any broker may use. Often, brokers use the computers while meeting with buyer and seller clients. You scroll through the documents on one of the common computers and find drafts of multiple offers, copies of credit reports, buyers' loan estimates, and other documents received by the brokers during their transactions. What should you do?

Answer: You should regularly inspect all the common use computers and remove all documents containing personal consumer information, saving those documents in some other secure manner. Software programs are available that will erase all information on the public-use computers at a pre-set time (e.g., daily at midnight).

THIS PAGE INTENTIONALLY LEFT BLANK.