ELECTRONIC SIGNATURES AND DOCUMENTS

2014-2015 GENERAL UPDATE

Outline:

Learning Objective: To enhance a broker's understanding of:

1) what constitutes a legally enforceable electronic signature,
2) when an electronic signature may be used,
3) required disclosures in consumer transactions to authorize use of electronic means, and
4) security considerations both as to creating an electronic signature and maintaining records in an electronic format.

INTRODUCTION

Change is the primary constant in today's real estate brokerage practices. Now a decade into the 21st century, more and more business transactions are being handled electronically. Communication occurs via cell phones, texting, skyping, video-conferencing, and electronic mail (hereafter "email"), including the exchange of documents that often are stored in "the cloud."

As commerce leaves the tangible paper-driven world behind in favor of a more immediate, expedient paperless society, many brokers are wondering: what *is* an "electronic signature" or, more likely, what is an *enforceable* electronic signature? Are offers signed and exchanged electronically legally binding once "signed" by all parties? When are electronic documents received? Must I retain a hard paper copy of every transaction file? What security matters should I consider if I choose to transmit information electronically? This Section will provide some answers to these questions, understanding however that technology's advances often occur far more rapidly than the law's ability to keep pace.

APPLICABLE LAWS

By the dawn of this century, various legislative bodies were enacting laws to address novel issues created by the emerging technology revolution. The National Conference of Commissioners on Uniform State Laws (NCCUSL) is a non-profit unincorporated association that has worked since 1892 to propose laws in certain subject areas for enactment by each state to make those laws uniform in every adopting state. One example of their work is the *Uniform Commercial Code* proposed in 1952 to facilitate interstate commerce by making the laws relating to the sale of goods similar, if not identical, in each enacting State. This Code has been enacted, with some local variation, by all fifty states, the District of Columbia, Puerto Rico, and the Virgin Islands. Generally, states may enact any uniform or model law verbatim, modify certain sections as needed, or decline to adopt it.

In 1999, the NCCUSL completed its proposed draft of the **Uniform Electronic Transactions Act (UETA)**. UETA has now been enacted in 47 states, the District of Columbia and the Commonwealth of Puerto Rico. *North Carolina* enacted its version of *UETA effective October 1, 2000*. It is found in Article 40 of Chapter 66 of the North Carolina General Statutes. Congress enacted a corresponding federal law, **Electronic Signatures in Global and National Commerce Act (ESIGN)**, effective June 30, 2000. [See 15 United States Code Section 7001, *et. seq*.] Many of the provisions and definitions in both UETA and ESIGN are similar, but ESIGN regulates ***interstate or foreign commerce***, *i.e.*, commerce across state lines, rather than *intra*state commerce, *i.e.*, commerce within a state. Further, states that either have enacted UETA or have state laws similar to ESIGN generally are exempt from the typical preemption of federal law. In other words, state e-commerce laws generally will apply, rather than the federal law.

The trend towards electronic commerce seems undeniable. Even before adopting UETA, North Carolina enacted the *Electronic Commerce Act* in 1998 to "...facilitate electronic commerce with public agencies and regulate the application of electronic signatures when used in commerce with public agencies...." (G.S. 66-58.1 *et. seq.*) In 2005, the General Assembly enacted another "uniform" law, the *Uniform Real Property Electronic Recording Act* (GS 47-16.1 *et. seq.*). This law allows the recording of electronic documents, *i.e.*, documents received by a Register of Deeds in an electronic form. Likewise, the Federal Housing Administration (FHA) recently announced that it will accept electronic signatures on "authorized documents" for single family mortgages and home equity conversion mortgages **if** the lender complies with ESIGN requirements. However, the FHA won't accept as an electronic signature a "sound" that is voice or audio only and it won't accept an electronic signature on the promissory note. Previously, it had permitted electronic signatures only on third party (non-lender) generated documents.

KEY: *The primary thrust of all these laws appears to be that **IF** parties consent to use electronic means in effectuating their transaction, **they cannot later deny the validity of those transactions by arguing that other laws required certain documents to be "in writing."***

North Carolina's Uniform Electronic Transactions Act ("UETA")

The law that will govern most North Carolina real estate brokerage transactions is North Carolina's Uniform Electronic Transactions Act (hereafter "UETA" or "the Act"). We will first discuss certain definitions and provisions of UETA (found at NCGS §§ 66-311 *et. seq.*), apply the Act to brokerage practice, and then address security considerations.

UETA Scope and Definitions

Subject to a few specific exceptions, UETA applies to "***electronic records and electronic signatures relating to a transaction***." Pursuant to G.S. 66-314, the law "…applies to ***any*** electronic record *or* electronic signature *created, generated, sent, communicated, received or stored* on or after the effective date of this Article," October 1, 2000. The purpose of the law is to provide a legal framework for the use of electronic signatures and records in business transactions. UETA makes electronic records and signatures as legal as manually signed paper documents ***so long as*** the parties agreed to use electronic means.

Definitions

The statute defines ***electronic*** as "... relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities."

A "***record***" is information in a tangible medium or stored electronically so long as it is "retrievable in perceivable form."

"***Information***" is broadly defined to include "... data, text, images, sounds, codes, computer programs, software, databases, or the like."

What is an *"electronic signature"*? UETA defines it as an *electronic*:

1) sound, symbol or process,
2) attached to, or logically associated with, a record,
3) executed or adopted by a person with the *intent* to sign the record.

All three elements must be present to constitute a valid electronic signature under the Act. An electronic signature may resemble a person's actual handwritten signature or it may not look like a traditional signature at all. It may be *any sound, symbol or process the person has selected as his or her electronic signature.*

What is an *"electronic record"*? It is any record that is:

- created
- generated
- sent
- communicated
- received or
- stored by electronic means.

*Note how **broad** this definition is.*

"Transaction" and "Consumer Transaction"

"***Transaction***" is defined as "*an action or set of actions occurring between **two or more persons** relating to the **conduct of consumer, business, commercial, or governmental affairs***."

"***Consumer transaction***" is defined as "*... a transaction involving a **natural person** with respect to or **affecting primarily personal, household or family purposes.**"*
[G.S. §66-312(4) and (17).]

The definition of "consumer transaction" is unique to North Carolina's version of UETA. The definition mirrors the federal ESIGN.

"Person" versus "Natural Person"

Note the difference in the definitions of "transaction" as between two or more "*persons*" versus "consumer transaction" involving a "***natural*** *person.*" The statutory definition of "person" includes individuals, governmental agencies, or "any other legal or commercial entity," e.g., corporation, limited liability company, partnership, business trust, estate, joint venture, etc.. On the other hand, a "*natural* person" can only be a *human being*.

If the parties to a transaction are entities, for example an LLC owner selling to a corporation, then under UETA, it would be a "transaction" but not a "consumer transaction." No natural person (human being) is a *party*. (Although the entities are negotiating and communicating through their human principals or employees, this is not enough to create a consumer transaction as the *party* is still the entity, not the human beings.) However, if an individual is purchasing a personal residence that is owned by an entity (LLC, corporation, LLP, etc.), then that would be a *consumer transaction* since one of the parties is a "natural person" and is purchasing property primarily for "personal, household or family purposes."

Required Notice in Consumer Transactions per NCGS § 66-327

Question: What does it matter if a transaction falls within the legal definition of "consumer transaction?

Answer: *Consumer transactions trigger other disclosures and requirements* ***before*** *soliciting the consumer's consent to engage in the transaction electronically.*

If the transaction *is* a consumer transaction, then *prior to consenting to use electronic means,* the consumer must be provided with a ***clear and conspicuous statement*** informing him or her of the following:

- the right to have any record provided in paper or non-electronic form;
- the right to revoke consent to deal electronically at any time and the consequences of the withdrawal of consent which may include termination of the relationship but can't include the imposition of any fees due to the consumer's decision to withdraw consent;
- the scope of the consumer's consent, i.e., this transaction only or a series of transactions;
- the procedures to follow to withdraw consent and to update the consumer's information;
- how the consumer may request and obtain a paper copy of an electronic record.

Additionally, the consumer must be told *what hardware and software will be required* to access and retain electronic records and ***the consumer should confirm his/her consent electronically to demonstrate the consumer's ability to access the information.*** All of the foregoing disclosures must be provided to the consumer ***before*** the consumer is asked to consent to using electronic means in the transaction.

NC UETA Exemptions

As with ESIGN, there are certain subjects and notices to which UETA doesn't apply because those subjects are governed by other laws. Exceptions outside the area of real estate include: 1) laws governing the creation and execution of wills, codicils and testamentary trusts, 2) Uniform Commercial Code sections governing the purchase or lease of "goods" (*not* real property), and 3) North Carolina's Electronic Commerce in Government Act. The relevant law in these three areas will supersede UETA's provisions.

UETA also doesn't apply to the following *notices – some affecting real estate* - that still must be given in a tangible form:

- any notice to cancel or terminate utility services, including heat, power and water;
- any notice of foreclosure, eviction, repossession, default, acceleration and right to cure relating to the primary residence of an individual;
- any notice to cancel or terminate health or life insurance or benefits, excluding annuities;
- any notice recalling a product that risks endangering health or safety;
- any document required to accompany the transport or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

Other than the foregoing exclusions, *virtually any transaction* related to consumer, business, commercial, or governmental affairs *may be conducted electronically* ***with the consent of all parties***. So long as the record or signature or contract is created or stored electronically *in compliance with UETA*, then it is legally valid and enforceable, despite the use of electronic means. Under UETA, a transaction may be totally paperless, with parties electronically signing documents created and exchanged electronically.

Must the parties agree to use electronic means?

No. The law expressly states that UETA doesn't compel parties to use electronic means, it merely permits it where all parties agree to conduct the transaction electronically.

How do you prove the parties agreed to use electronic means?

There are many possibilities, depending upon the transaction. One method would be written acknowledgment of receipt of the required disclosure (if the subject is a consumer transaction) and consent to the use of electronic means signed by all parties to the transaction. Another would be the use of electronic signature or transaction software that maintains records of the parties' consent.

Isn't the parties' use of electronic means to communicate enough to prove consent?

G.S. 66-315(b) states:

> ...Whether the parties agree to conduct a transaction by electronic means is *determined from the context and surrounding circumstances, including the parties' conduct*.
> [Italics added.]

Thus, *in non-consumer transactions*, where brokers and parties exchange information and records via email or other electronic means without objection, their consent to communicate electronically may be inferred from their actions. ***However****, in "consumer transactions," a party's* ***consent*** *to use electronic means* ***may be evidenced by conduct*** *under G.S. 66-315(b)* ***"only when accomplished in compliance with …" the consumer disclosures required under G.S. 66-327(c)(1)-(4)***.

Applicability to Real Estate Brokerage Practices

While North Carolina's UETA has been in effect since October, 2000, there has been minimal caselaw created to interpret it – perhaps because there has been little controversy over the increasing use of technology in real estate brokerage or elsewhere. Brokers and consumers routinely email information, disclosures, and contracts, and rarely does this cause a dispute over the legal validity of the documents. It seems clear that the use of electronic communication will only increase over time. Because UETA imposes particular disclosure requirements in certain situations, brokers should be mindful of the disclosure requirements when using electronic means to conduct certain consumer transactions, as discussed in more detail here.

In a purchase transaction, what property the buyer is purchasing, what they intend to do with it, and who the buyer is may influence whether the parties are engaged in a "consumer transaction." ***When handled electronically***, the following real estate transactions appear to meet the definition of a "consumer transaction," namely:

1. the sale or purchase by a natural person of an owner-occupied residence along with the related agency disclosure and agreements;

2. the lease of a vacation rental to a natural person; and

3. the lease of a residential property built before 1978 to a tenant.

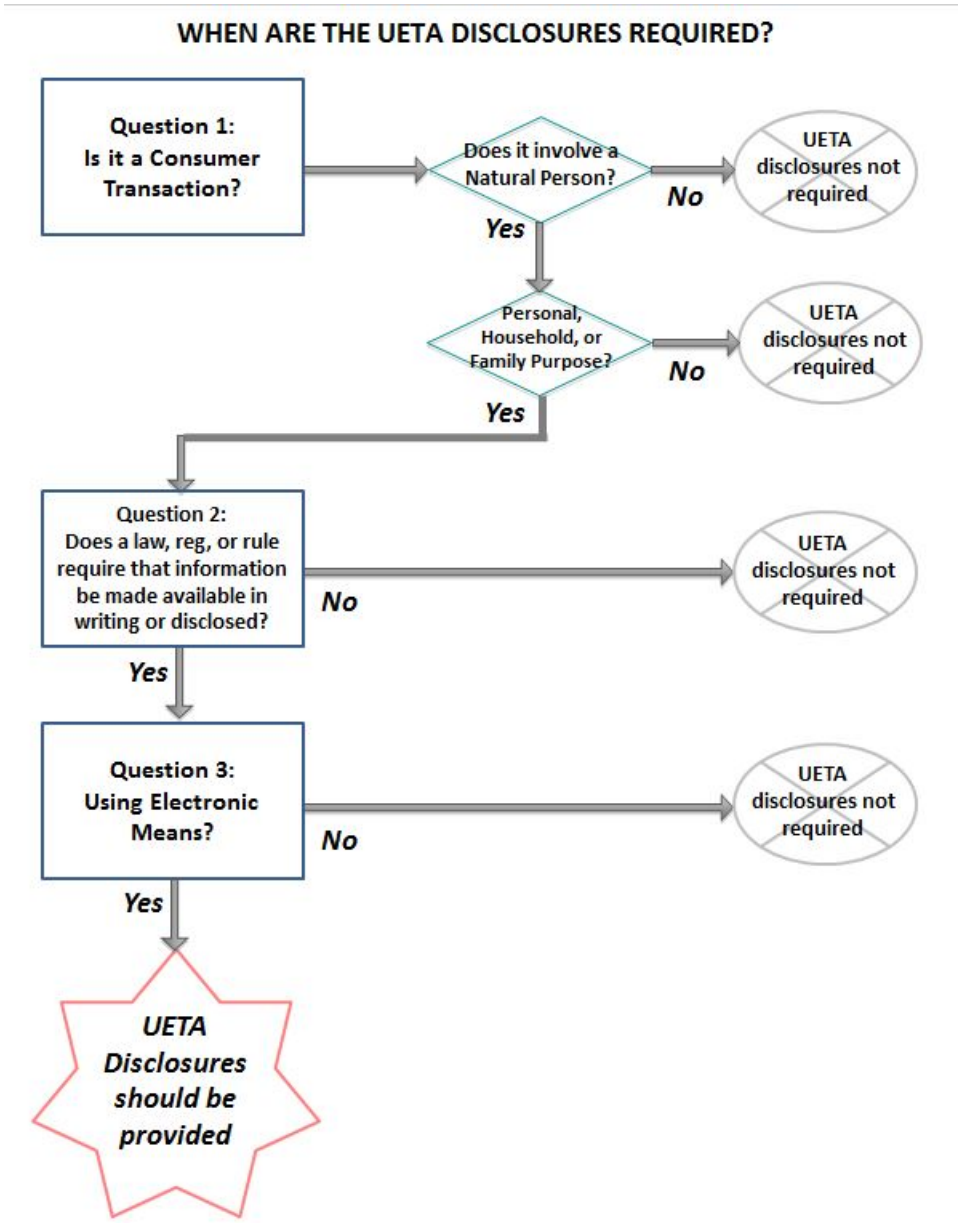
What makes the foregoing three situations "consumer transactions"? Remember that under UETA, a "consumer transaction" involves a natural person with respect to or affecting primarily a personal, household or family purpose. Further, UETA provides that in a consumer transaction where a statute, regulation, or rule requires that information be disclosed to the consumer or provided in writing, the consumer must be given the required disclosures for the transaction to be legally valid. Consider the following questions:

1. Does the transaction involve a natural person/human being?

2. Does the subject matter primarily affect a personal, family or household purpose?

3. Is any disclosure in that transaction required, or is the transaction required to be in writing?

If the answer to each of the foregoing three questions is yes, *and the parties elect to use electronic means* in the transaction, then it is safest to assume that it is a consumer transaction and the disclosures required by G.S. 66-327(c) must be provided.



1) <u>Purchase or Sale of Owner-Occupied Residential Property</u>

What could be more personal, family, or household related than the sale or purchase of a primary residence that is or will be owner-occupied? The nature of a traditional residential sales transaction seems to place it squarely in the definition of "consumer transaction." Moreover, the Statute of Frauds (state law) requires any contract for the sale of property to be in writing to be legally enforceable. Thus, if a natural person is selling the residence in which s/he lives OR if a natural person is buying property to use as his/her primary residence, that transaction likely will be considered a consumer transaction as defined in UETA. Remember, in residential sales transactions state law (and Commission rule) requires the *sales contract* to be *in writing*, and in most cases, requires the seller to provide the buyer with the *written Residential Property and Owner Association Disclosure Statement*.

Additionally, in all sales transactions, Commission *Rule A.0104* requires that the *Working with Real Estate Agents* brochure be provided to prospective buyers and sellers at first substantial contact *prior* to determining the working relationship and entering into a *written agency agreement*. Because both the disclosure and agency agreement are required by *rule* to be in writing, when a broker is hired to help with the sale or purchase of an owner-occupied residential property, *the formation of the agency relationship itself may be subject to the UETA consumer transaction disclosure requirements* ***when the agency disclosures and/or agreements are provided to natural persons using electronic means***.

However, if a natural person is either A) selling residential *investment* property or B) purchasing residential investment property (i.e., non-owner occupied property in each case), then that sales transaction might not be a "consumer transaction" under UETA because it doesn't relate to or primarily affect a personal, family or household purpose.

2) <u>Leasing Vacation Rentals to Tenants</u>

When leasing *vacation rental property,* North Carolina law requires the agreement with the tenant to be in writing, to contain a specific disclosure, and to address certain provisions. [See G.S. 42A-11.] Typically, the tenants are human beings, rather than entities, and vacations generally are for personal, family and household purposes. Thus, if the vacation rental agreement is sent to the prospective tenant electronically, the broker should also provide the required UETA consumer transaction disclosures.

What about creating the agency relationship? The *Working with Real Estate Agents* brochure is not required to be given in lease transactions. While the vacation rental management agreement must be in writing from the outset pursuant to Commission rule, the owner most likely views the vacation rental as an income-generating business opportunity. Because the management of the vacation rental isn't related to a personal, family or household purpose of the owner, the broker would not be required to provide the UETA consumer disclosures to the owner when creating the management agreement. Typically, brokers don't attempt to represent tenants in vacation rentals, so that issue is moot.

3) <u>Long-term residential leasing</u>

Generally, brokers who engage in long-term residential leasing on behalf of owners *will not be required* to provide the UETA consumer disclosure notices to either the owner-client or the tenant-customer. From the owner's perspective, the leasing of the property relates to a business purpose, rather than personal, family or household, and the UETA consumer disclosures need not be provided to the owner, even if the property management agreement is formed electronically.

The primary exception would be if the property was built prior to 1978 *and* the broker conducts the lease transaction electronically. Because the Lead-Based Paint Disclosure is required by both law and regulation to be given in writing, and because the tenant's lease of a personal residence clearly is for personal, family or household purposes, *the broker would have to provide the UETA consumer disclosures to the tenant when transmitting the Lead-Based Paint Disclosure*.

If the transaction is not conducted electronically in any other respect, and the rental manager faxes or emails the lead-based paint disclosure, it is not clear under the law whether the UETA consumer disclosures are required. This may not be enough to rise to the level of a "transaction." But because the legal definition of "transaction" is broad ("an action …between two or more persons relating to the conduct of consumer, business, commercial, or governmental affairs"), the safest course is either to:

1) provide the only disclosure document that may be required by law to the tenant in person or by U.S. mail, *or*
2) include the required UETA consumer disclosures if providing the lead-based paint disclosure to the tenant in an electronic communication.

UNDERSTAND that this issue only arises in residential leases of property that were built prior to 1978, or for other long-term rentals or leases where the initial term of the lease is three years or more and therefore required by the Statute of Frauds to be in writing. *If the leased property was built after 1978 and the residential lease is for less than three years at the outset, then a broker does not need to provide the special UETA consumer transaction disclosures to the tenant even if the transaction utilizes electronic means, as there is no document required to be in writing by law, rule or regulation.*

Other transactions

It does not appear that the lease, sale or purchase of commercial property or vacant land or the sale or purchase of non-owner occupied residential property (investment property) is a "consumer transaction," as it does not "primarily affect personal, family or household purposes."

When to Give Additional "Consumer" Disclosures?

If brokers are uncertain about whether to provide the consumer disclosures required by G.S. §66-327 when using electronic means to conduct transactions, the safest course is to ***provide the disclosures***. There are few, if any, consequences in providing a disclosure when it is not required, but there may be consequences if one fails to provide a disclosure when it is required. It is interesting to note that UETA doesn't impose any specific consequences for violating the Act. However, it is possible that a party trying to avoid a contract entered into using electronic means might argue that his or her performance should be excused because required disclosures weren't given. Giving the disclosures helps assure the validity of the underlying agreement, whether an agency agreement, sales contract or vacation rental lease.

Thus, whenever a transaction involves a natural person (human being) *and* the purpose relates to the purchase or sale of a primary residence or the lease to a tenant of a vacation rental, a *broker would be well advised to provide the required G.S. §66-327 consumer disclosures:*

1) *contemporaneously with the Working with Real Estate Agents disclosure in a sales transaction, and*

2) *at first contact with a prospective vacation tenant*

IF *either the formation of the agency relationship in the sales transaction or the leasing of the vacation rental to a tenant is being effected through the use of electronic means.*

A table summarizing the foregoing discussion is reprinted on the final pages of this article after General Statute Section 66-327.

How Can the UETA Disclosures Be Provided?

In many cases, there may be no need for a free-standing disclosure form. An electronic signature service provider may generate the required notice when establishing an account with the consumer. A broker who intends to use electronic signatures should invite the consumer to establish an account at the outset using an electronic signature provider that includes all the required consumer disclosures. This alleviates the burden on the broker and assures compliance with the UETA disclosure requirements from the beginning of the transaction. In vetting electronic service providers, brokers should ask what disclosures the provider gives in transactions involving "natural persons" in a "consumer transaction." ***Often, however, it is the* broker's responsibility *to notify the electronic signature provider that the consumer disclosures must be given in any particular transaction.*** Frequently, this is accomplished by the broker checking a particular box when asking the service provider to contact the consumer and invite the consumer to create an account. ***Brokers should therefore familiarize themselves with the documents provided to the consumer by the electronic signature provider, and make sure the provider gives the necessary disclosures.***

The law doesn't clearly address whether the occasional use of email or facsimile transmissions to deliver documents physically signed by the consumer (e.g. faxed or scanned after signing) trigger the consumer transaction disclosure requirements under NC UETA. Arguably, however, given the very broad definition of "electronic record" (see p 3), an offer or disclosure that was emailed or faxed to a natural person, printed by them and signed, and then faxed or scanned and emailed back to the broker would be an electronic record. If the purpose of that transaction related to personal, household, or family purposes, then the consumer disclosures should also have been provided. However, the NC Act doesn't specify the consequences for failing to provide the consumer disclosures, if required in a particular transaction. *The safest course is to give the UETA consumer disclosures at the beginning of any transaction involving a natural person and the sale/purchase of an owner-occupied dwelling or lease of a vacation rental where electronic means are anticipated to be used in conducting the transaction.*

Delivery and Record Retention under UETA

If the parties agree to use electronic means in their transaction, then information required to be provided, sent, or delivered may be provided, sent or delivered electronically ***so long as it is in an electronic record capable of retention by the recipient***. A recipient can't retain an electronic record if the sender's information processing system inhibits the recipient's ability to print and store the record **or** if the electronic record can't be accurately reproduced later by all parties or persons entitled to retain the record. *If a sender inhibits a recipient's ability to store or print an electronic record, then the electronic record is not enforceable against the recipient.*

When Sent?

An electronic record is deemed "sent" when it:

1) is properly addressed or directed to an information processing system designated by the recipient from which the recipient may retrieve the electronic record;
2) is in a form the system can process; and
3) is sent to a system under the recipient's control and outside of the sender's control.

When Received?

An electronic record is received when it:

1) enters an information processing system designated by the recipient from which the recipient can retrieve the information, and
2) is in a form that can be processed by the recipient's system.

The presumption of receipt upon the electronic communication entering the recipient's information processing system applies even if the system is not at the person's place of business or home. The law further states that a record is deemed received "*...even if no individual is aware of its receipt ....*" ***except*** that in a consumer transaction it's only deemed received if the sender had a reasonable basis to believe that the record could be opened and read by the recipient. **NOTE TOO** that under UETA an electronic acknowledgment from an information processing system may establish that the record was received by the system, but *doesn't by itself establish that the content sent corresponds to the content received.*

How Long to Retain?

UETA doesn't specify any minimum length of time to retain electronic records, but it recognizes that other laws or rules may establish time limits for regulated occupations, such as real estate brokerage. UETA states that record retention requirements imposed by other laws will be satisfied by retaining an electronic record so long as it:

1) accurately reflects the information set forth in the record at the time it was generated as an electronic document; and
2) remains accessible for later reference.

Checks may also be retained electronically ***so long as*** the electronic record contains the information on the **front *and back* of the check**. Documents may also be notarized electronically.

Whatever record retention methods licensees choose to utilize, whether paper or electronic, they must comply with **Commission Rule 58A.0108** and retain all required records for at least three years following:

1) the successful or unsuccessful conclusion of the transaction, or
2) termination of the broker's agency relationship, and
3) disbursement of all trust monies related to that transaction held by the broker

*whichever of these three triggers **last occurs**.*

Licensees are referred to the article "*Record Retention Requirements*" from the 2012-2013 BICAR Course materials available on the Commission's website under "Publications" for a comprehensive discussion of the Commission's record retention requirements and other considerations. [www.ncrec.gov/pdfs/bicar/records.pdf.]

ELECTRONIC SIGNATURES & RECORD RETENTION

Electronic vs. Digital Signatures

While some may view "electronic" and "digital" as synonymous terms, are they? In reality, they are not. *All digital signatures are "electronic signatures" under the Act, but* ***not all electronic signatures are digital***. Because the term "electronic signature" encompasses both electronic and digital signatures, that term will be used hereafter to refer to both types of electronic signature.

Non-digital electronic signatures are easy to use, involving the click of a mouse or using a finger to "write" one's name, but they lack many security features that digital signatures possess. The differences between the two forms are summarized in the table below.

Non-Digital Electronic Signatures	**Digital Electronic Signatures**
• Vendors may create own standards so long as meet legal minimum requirements. • Signature is *an uncoded image affixed to a document,* but doesn't "tamper seal" the document.*	• More uniform technical standards. • Accepted internationally. • Secure coding *permanently linking document to signature & vice-versa at time of signing,* i.e., document is "tamper sealed," so signature is always secure.

*Comment: Some electronic signature providers may not offer digital signatures as a method of signing a document, but they may apply digital signature technology to the document after signing to tamper seal the document.

Where to Store?

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, a real estate company may choose to retain records:

1) in paper form and store them either on or off-site, depending on space; or
2) scan any tangible documents into 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
3) scan tangible documents into an electronic or digital form and upload them to the cloud.

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 both his/her 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.*

Confidential Client Information

Whatever method is chosen, the company/broker should take whatever steps are necessary to *ensure that clients' confidential information is protected* to the extent that it is retained. For example, if a broker obtains copies of his/her client's income tax returns for two years (with the SSN), as well as a credit report, and a copy of the client's driver license, the broker needs to keep those documents in a secure area of his/her transaction file.

Back-up / Disaster Recovery Plans

The broker must also have back-up plans for preserving all records and their data. Storing the original paper records is fine, but what is the disaster control plan if there is a fire or water damage in the facility housing the records? If there are no duplicate copies or the original records weren't also scanned into a system, the broker has no back-up and may have violated the Commission's records retention rule.

Records saved in electronic form on a hard drive in the office should also be backed-up on a thumb-drive or on a second hard drive, preferably at a different location. Alternately, the broker may store records on his/her hard drive, but also hire an outside service to back up the broker's hard drive on a regular basis.

The Cloud

What about "the ***cloud***?" What *is* it? Cloud computing or storage refers to *uploading documents or files from a hard drive to an offsite facility via the internet where data is stored in a large data center operated by a hosting company. Documents and files are stored in such a way that they can be accessed anytime, anywhere, with either a personal computer or a Mac by any person who has access* — and therein lies the ***key – who has authorized access***? It is similar to sending or receiving an email with an attachment; once it is transmitted, that email and attachment may be accessed by the sender or recipient from any location where either has access to the internet, and thus their email server.

Security Considerations in Electronic Communications

Brokers must always be mindful of the confidential information they collect from their clients or customers and information they convey to others whether by phone, email, text, etc. Who else may overhear or who may view that email or text other than the intended recipient? Are you using a secure network to communicate? Are you encrypting your messages? The transportability and facility of tablets, smart phones, laptops or other electronic media also presents one of the biggest inherent dangers - that 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 **encryption**? 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. Encryption has become a standard security measure for protecting laptops and other portable devices and brokers should seriously consider using it, depending upon what documents or information they store on thumb-drives, laptops, other devices, or the cloud.

Encryption Options

There are two main approaches to protecting data on hard drives:

1) *full disk encryption* protects the entire hard drive and automatically encrypts all information and allows decrypted access when an authorized user logs in.

2) *limited encryption* protects only specified files or folders and the user must elect to encrypt, rather than it being automatic as with the full disk protection.

There are also three kinds of encryption: 1) hardware full disk encryption, 2) encryption in operating systems, and 3) encryption software. Most laptop and hard drive manufacturers today offer full disk encryption built into the hard drive, which may be easier to use than encryption software. The contents of the drive are automatically encrypted when an authorized user logs off the computer and it is automatically decrypted when an authorized user logs into the system. ***Strong passwords*** *are critical and most experts recommend an* ***automatic logoff*** *after a certain period of time of non-use to prevent unencrypted data from being exposed if the user forgets to turn off the device*. Recommendations for a "strong" password are that it have at least 12 characters and include upper and lower case letters, numbers and permissible symbols.

Business versions of certain operating programs such as Windows and Apple OS-X, have built in encryption ability, but some question how effective it is in defeating attempts to crack the system. A third alternative is to use third party encryption software products for hard drives, USBs or portable devices.

Encryption devices also exist for Smartphones and tablets as well, since they essentially are mini-computers. Blackberry devices have been touted for their secure cell phone communications, using the Blackberry Enterprise Server to automatically encrypt communications. However most smartphones now offer built-in encryption in their more recent models and there are third party encryption applications that can be used with earlier phone models. Follow the manufacturer's instructions to set up the encryption, set a strong passcode, and activate the automatic logoff function after a certain period of non-use.

Wireless networks should be secure, *i.e.*, encrypted, to protect transmissions against interception. There are three wireless encryption schemes:

1) Wire Equivalent Privacy (WEP);
2) Wi-Fi Protected Access (WPA); and
3) WPA 2, which is second generation WPA.

A review of the literature suggests that of the three, WEP is the weakest and can be cracked fairly readily. WPA2 appears to be the most favored network encryption from a security standpoint. Understand as well that *even if your network is secure, if the recipient retrieves the communication using an unsecure network, the communication no longer is secure* on their end.

Many people compare an email to a postcard — it can be read by anyone, even using a secure network, unless the email is encrypted. When applied to email, the term "***encryption****" refers both to encryption of the data to protect its confidentiality,* ***as well as*** *authentication of the sender's identity*. Email encryption usually involves both the sender and the recipient having both a public and private key. As David G. Ries and John W. Simek explain in their article, "*Encryption Made Simple for Lawyers*" (GP Solo magazine, Nov/Dec 2012):

> For protection of confidentiality and authentication, the sender's and recipient's key pairs are used in combination. The sender uses both the Encrypt Message and Attachments command button (that uses the recipient's private key) and the Sign Message command (that uses the sender's private key). At the receiving end, the email program automatically uses the recipient's private key to decrypt the messages and automatically uses the sender's public key to verify the authenticity and integrity. Again, the challenging part is obtaining key pairs, exchanging public keys, and setting them up in the email program for encryption.

As alternatives to paired key email encryption, Mssrs. Ries and Simek mention using a managed messaging service provider when needed; the service provider will encrypt the email without the complexity of obtaining and exchanging keys. Another option is to put all of the confidential message in a password-protected encrypted attachment, rather than the body of the email (and obviously don't include the password in the email). The email itself is not protected, but the attachment is.

FACTORS TO CONSIDER IN SELECTING PRODUCTS & PROVIDERS

There are numerous providers of electronic signatures and document storage and retention. Probably the most widely known and used within many real estate brokerage markets is DocuSign which has entered into a relationship with the National Association of REALTORS® and is a REALTOR Benefits® Partner. However there are numerous players in the market and the Commission generally does not recommend or favor any one provider over another, so long as all satisfy minimum legal requirements. Rather, ***it is the broker's job to do his/her own due diligence to investigate and compare any provider of services the broker may use to assess the attributes, features, competency, and integrity of each before selecting or recommending a service provider***.

No doubt the trend favoring electronic signatures and transaction document management will only increase as we advance through the 21st century. The demands of an active brokerage practice require brokers to become more familiar and comfortable with this new technology. It facilitates communication among numerous individuals and provides ready access to data and documents. However, brokers must be aware of and safeguard against the pitfalls.

> UETA defines "**security procedures**" as:
> ... a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

Recommended Practices

When assessing any provider's suitability to supply electronic signature and document management services, a broker should consider the following matters.

As to electronic signatures:

1. What security measures does the provider employ to verify that the individual creating the signature is in fact the person to whom the signature will be attributed?
2. Does the provider offer a) non-digital signatures, b) digital signatures or c) both?
   Can the system integrate a faxed signature on a document?
3. Where are documents stored once signed, for how long, who has access and how?
4. What happens to existing signatures and documents if the broker changes service providers?
5. How long has the provider been in the business?
   What is their standing/ranking/reputation in the industry?
6. Does the service provider give the disclosures required in consumer transactions under North Carolina law and at what stage of the proceedings?

As to electronic document management and storage:

1. What security features are employed to protect the confidentiality of data?
   Are stored documents encrypted?
   What procedure is used to encrypt and decrypt documents? Who has access and how?
2. What data back-up systems exist, where are they located (i.e., in the United States or a foreign country), and how frequently are back-ups run?
3. What is the provider's disaster recovery plan and how has it been tested?
4. Who owns the data? How long is the data/document retained?
   Whose insurance covers loss of data?
5. What happens to previously stored signatures and/or documents if: a) ownership of the service provider changes, or b) the broker changes vendors/service providers?
6. What is the provider's privacy policy? *Do the service provider's employees have access to stored documents*? What are the provider's terms of service?

Brokers should evaluate providers separately as to each provider's ability to furnish electronic signatures versus the provider's document storage capabilities. While those providing electronic signatures presumably retain all documents signed using their services, a broker might select a different service provider deemed better qualified for document retention and storage. *A broker should always have the ability to download or print a copy of any given document so long as the broker has an account with the service provider*.

If a brokerage company or broker is considering storing all of its required transaction file and trust account records electronically, the ***broker must first confirm that the service provider has the ability to retain all the documents required by Rules A.0108 and A.0117.***

> *Example*: A system that allows a broker to retain copies of all offers received while the transaction is pending, but only allows retention of the contract and purges all other offers upon the successful completion of the transaction would be totally out of compliance with Rule A.0108, thereby exposing the brokerage company and/or broker to disciplinary action.

Similarly, if changing service providers causes the former service provider to discard documents accumulated while the broker had an account, then the broker first must either download or print hard copies to preserve any required records for transactions that are still within the three year record retention window of Rule A.0108. Failure to preserve and retain such records could subject a broker to disciplinary action.

Understand as well that while an office may choose to use electronic means in its transactions and document storage, i.e., be "paperless," ***it must always have the ability to print a hard copy of any document***. It is neither a valid excuse nor defense for a broker to argue that "I can't provide any paper copies because our whole office is electronic." A prudent broker will always be equipped with paper versions of required disclosures and other necessary documents in the event the consumer doesn't wish to use electronic means in the transaction.

Realize too that a client may feel comfortable communicating with his/her broker via email, but not authorize email as an accepted method of communication on the final page of Standard Form 2-T, or may authorize email communications to the client's broker's email, but not the client's personal email by the other party.

§ 66-327. Consumer transactions; alternative procedures for use or acceptance of electronic records or electronic signatures.

(a), (b) Repealed by Session Laws 2001-295, s. 5.

(c) Consent to Electronic Records. – In a consumer transaction in which a statute, regulation, or rule of law of this State requires that information relating to a transaction or transactions in or affecting commerce be made available in writing or be disclosed to a consumer, the consumer's agreement to conduct a transaction by electronic means shall be evidenced as provided in G.S. 66-315, and shall be found only when accomplished in compliance with the following provisions:

(1) The consumer has affirmatively consented to the use of electronic means, and the consumer has not withdrawn consent.

(2) The consumer, prior to consenting to the use of electronic means, is provided with a clear and conspicuous statement:
   a. Informing the consumer of any right or option of the consumer to have the record provided or made available on paper or in non-electronic form.
   b. Informing the consumer of the right to withdraw consent to have the record provided or made available in an electronic form and of any conditions or consequences of such withdrawal. Those consequences may include termination of the parties' relationship but may not include the imposition of fees.
   c. Informing the consumer of whether the consent to have the record provided or made available in an electronic form applies only to the particular transaction which gave rise to the obligation to provide the record, or to identified categories of records that may be provided or made available during the course of the parties' relationship.
   d. Describing the procedures the consumer must use to withdraw consent as provided in sub-subdivision (2)b. of this subsection or to update information needed to contact the consumer electronically.
   e. Informing the consumer how, after the consent to have the record provided or made available in an electronic form, the consumer may request and obtain a paper copy of an electronic record.

(3) The consumer, prior to consenting to the use of electronic means, is provided with a statement of the hardware and software requirements for access to and retention of the electronic records; and the consumer consents electronically, or confirms his or her consent electronically, in a manner that reasonably demonstrates that the consumer can access information in the electronic form that will be used to provide the information that is the subject of the consent.

(4) After the consent of a consumer in accordance with subdivision (1) of this subsection, if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was the subject of the consent, the person providing the electronic record provides the consumer with a statement of the revised hardware and software requirements for access to and retention of the electronic records, provides a statement of the right to withdraw consent without the imposition of any condition or consequence that was not disclosed under sub-subdivision (2)b. of this subsection, and again complies with subdivision (3) of this subsection.

(d) Written Copy Required. – Notwithstanding G.S. 66-315(b), in a consumer transaction in which a statute, regulation, or rule of law of this State requires that information relating to a transaction or transactions be made available in writing or be disclosed to a consumer, where the consumer conducts the transaction on electronic equipment provided by or through the seller, the consumer shall be given a written copy of the contract or disclosure which is not in electronic form. A consumer's consent to receive future notices regarding the transaction in an electronic form is valid only if the consumer confirms electronically, using equipment other than that provided by the seller, that (i) the consumer has the software specified by the seller as necessary to read future notices, and (ii) the consumer agrees to receive the notices in an electronic form.

(e) Oral Communications. – An oral communication or a recording of an oral communication shall not qualify as an electronic record for purposes of this section, except as other provided under applicable law.

(f) Consumer Transaction Entered Into in North Carolina. – If a consumer located in North Carolina enters into a consumer transaction which is created or documented by an electronic record, the transaction shall be deemed to have been entered into in North Carolina for purpose of G.S. 22B-3 which shall apply to the transaction. (2000-152, s. 1; 2001-295, s. 5.)

This table summarizes the discussion on pages 6-10 regarding the applicability of UETA consumer disclosures to real estate brokerage practices.

Type of Agreement	**Consumer Transaction?**	**Law, regulation, or rule requires that information be made available in writing or disclosed?**	**UETA disclosures required?**
Agency Agreement for Purchase or Sale of Owner-Occupied Residential Property	Yes, assuming client is natural person (not entity).	Yes. WWREA brochure and agency agreement required to be in writing by Rule.	YES, if using electronic means.
Purchase or Sale of Owner-Occupied Residential Property	Yes, assuming party is natural person (not entity).	Yes. Sales contract required to be in writing by law. Residential Property & Owners Association Disclosure Statement required in most cases.	YES, if using electronic means.
Lease Agreement for Vacation Rental	Yes.	Yes. Lease agreement required to be in writing by Vacation Rental Act.	YES, if using electronic means.
Lease Agreement for Long-Term Residential Lease	Yes, assuming tenant is natural person (not entity).	ONLY if property built before 1978. (Residential leases only required to be in writing if lease period is more than three years, which is rare.)	ONLY if property built before 1978 <u>AND</u> using electronic means.
Agency Agreement for Purchase or Sale of Residential Property used for Investment	No. Purpose would likely be considered business.	Need not address	No.
Purchase or Sale of Residential Property used for Investment	No. Purpose would likely be considered business.	Need not address	No.
Property Management Agreement for Residential Property	No. Purpose would likely be considered business (as to owner).	Need not address	No.