So you want to go digital…

Intellectual Property and Technology News

11 APR 2019
By: Margo H. K. Tank | David Whitaker

In the United States, there are two primary laws – we refer to them below as the eSignature Laws – that make it possible to present information and sign agreements and other documents electronically in circumstances where a written document and a "wet" signature would previously have been required.

These two laws bring with them new challenges and, more importantly, potential liability. The design of a system for signing electronic records, or delivering notices or disclosures electronically, requires a detailed understanding of the interaction between electronic processes and legal requirements.

This article assists businesses in identifying the core issues that must be addressed to ensure the legal sufficiency of transactions conducted on eSignature platforms.

We do not attempt to provide a reference to the many other laws that may be applicable to various transactions, or to any given industry sector. Rather, this is a short analysis of key elements of the eSignature laws applicable to all industry sectors, providing key minimum requirements and additional guidance with respect to the following:
Part 1: A brief overview of the US eSignature laws

The following two statutes are the primary sources of law for using "electronic records" and "electronic signatures" in consumer financial services transactions (sometimes collectively referred to as the "eSignature Laws"):

- The Electronic Signatures in Global and National Commerce Act (ESIGN)\(^1\) and
- The Official Text of the Uniform Electronic Transactions Act, as approved and recommended by the Uniform Law Commission (formerly the National Conference of Commissioners on Uniform State Laws) in July 1999 (UETA).\(^2\)

While ESIGN is a federal law, UETA is a uniform law recommended by the Uniform Law Commission for adoption by individual states.

Scope of the eSignature laws

As written, the UETA applies to the use of electronic records and signatures in connection with a "transaction," which is defined as "any action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs."\(^3\) The term "commercial" is meant in its broadest sense, encompassing virtually any transaction, which is related to or connected with trade and traffic or commerce in general. As such, both business-to-business and consumer transactions are covered. ESIGN has an equivalent definition covering business, commercial and consumer affairs.\(^4\)

A transaction requires an interaction between at least two parties – a unilateral act, such as the creation of a "living will," is not included in the definition. Consumer protection laws requiring the delivery of notices and disclosures "in writing" are among the types of laws and regulations covered by ESIGN and UETA.

There are a few specific exceptions, among them:

- Under ESIGN (but not UETA) recordings of oral communications are excluded from the definition of electronic record for purposes of consumer notices and disclosures.\(^5\)
- Under ESIGN (but not UETA), notices of utility termination, default or foreclosure under a mortgage or lease, termination of health or life insurance, and product recalls and safety notices.\(^6\)
- Under ESIGN and UETA, any notices or disclosures required to be provided in writing under the Uniform Commercial Code, other than notices and disclosures under Article 2 (Sales) and 2A (Leases).\(^7\)

While most of the Uniform Commercial Code, other than Article 2 and 2A, is excluded from coverage under both UETA and ESIGN, the UCC Articles governing funds transfers, letters of credit, security interests in personal property and securities all permit the use of electronic records and signatures for most purposes, according to their own terms. As a result, most types of commercial agreements, and related documents, may now be delivered and executed electronically.

Some states have added special exclusions not in the UETA. These exclusions do not necessarily mean the excluded documents cannot be executed electronically; however, the authorization must exist under other law. In addition, some exclusions may be preempted by the ESIGN Act, described further below.

Three states have their own electronic signature laws: Illinois, New York and Washington. In general, these laws support the use of electronic records and signatures, and to the extent they conflict with the ESIGN Act, may be preempted (see below). Documents for use in these states may require additional scrutiny.

Authorization to use electronic signatures and records

For the vast array of laws and transactions within the scope of UETA and ESIGN, the following rules are the pillars...
on which the two statutes are built:

- A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.
- If a law requires a record to be in writing, an electronic record satisfies the law; and
- If a law requires a signature, an electronic signature satisfies the law.\(^8\)

The three pillars, in turn, are built upon three defined terms: **record**, **electronic record** and **electronic signature**.

A **record** is “information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.”\(^9\) This encompasses not only traditional writings, but also anything stored on magnetic or optical media (such as a computer hard drive or CD-ROM).

An **electronic record** is “a record created, generated, sent, communicated, received, or stored by electronic means.”\(^10\) Essentially, the term is intended to cover any type of record generated or stored electronically; as such, it would cover records created on a computer and stored on any type of media.

An **electronic signature** is an “electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.”\(^11\) Included within this definition would be typed names, a click-through on a software program’s dialog box combined with some other identification process, biometric measurements (such as a retinal scan or thumbprint), a digitized picture of a handwritten signature, or a complex, encrypted authentication system. As with traditional ink signatures, the legal consequences of the signature, and the question of whether it may properly be attributed to a particular person, is left to other law and the surrounding factual circumstances.\(^12\)

**Consent to use electronic records and signatures**

The eSignature Laws are opt-in statutes. This means that a set of actions constituting a transaction is covered by the eSignature Laws only if the parties have agreed to conduct the transaction through electronic means. Consent to conduct one transaction electronically does not prevent a party from refusing to conduct another transaction electronically.

Consent may be obtained on a transaction-by-transaction basis, or in the form of a blanket or continuing consent to perform whole classes of transactions electronically. Unless blanket consent is given, the scope of the transaction limits the scope of consent. The eSignature Laws do not prescribe standards for determining what chain of events constitute a single transaction, as opposed to multiple transactions. This should leave the parties free to determine by agreement what constitutes a single “transaction.”

ESIGN includes special consent rules for use in connection with certain consumer transactions (the ESIGN Consumer Consent Process). The special consent procedure applies if a federal statute, regulation, or other rule of law calls for information related to a transaction to be provided to a consumer in writing, and should precede presentation of the material covered by the writing requirement.

The elements of the ESIGN Consumer Consent Process are:

- The consumer must affirmatively consent, or confirm prior consent, electronically;
- The party obtaining the consumer’s consent must provide some specific disclosures prior to consent in clear and conspicuous statement; and
- The consent must “reasonably demonstrate” the consumer’s ability to receive electronic records in the formats that will be used for delivering the required information.\(^13\)

Some states have adopted the ESIGN Consumer Consent Process as part of their state enactment of UETA, so that it also applies to state laws in those states.

**Special rules for electronic records**

While ESIGN and UETA set up no special standards for the use of electronic signatures, they do have a number of special rules for electronic records that are intended to substitute for certain types of writings. These rules include:

- If a person is required by law to provide or deliver information in writing to another person, an electronic record only satisfies that requirement if the recipient may keep a copy of the record for later reference and review. If
the sender deliberately inhibits the recipient's ability to print or store the record, then the record doesn't satisfy the legal requirement.

- If a law or regulation requires that a record be retained, an electronic record satisfies that requirement only if it is accurate and remains accessible for later reference. UETA does not establish for how long the record must be retained or to whom it must remain accessible. ESIGN provides that the record must be accessible to all people entitled by law to access it for the retention period prescribed by law. Neither statute requires that the electronic record necessarily be accessible in a particular place – the parties entitled to access can, by agreement, establish a storage location.

- If a particular writing is required by law to be displayed in a particular format, UETA does not change that requirement. For example, if a law requires a notice to be printed in at least 12-point type and a boldface font, that requirement remains in place under UETA. If the law requires two elements of a document to be placed in a particular physical relationship to each other or some other part of the document, that requirement is not changed by UETA. For example, if the law requires a disclosure to be displayed just above a contracting party's signature, that rule must be observed within the electronic record.

- If a law expressly requires a writing to be delivered by US mail or by hand delivery, UETA does not change those delivery rules.¹⁴

Generally speaking, these rules are not variable by agreement under either ESIGN or UETA; however, under UETA if the underlying statutory requirement that information be delivered in writing, or by a particular delivery method, may be varied by agreement, then the requirement that an equivalent electronic record be capable of storage, or be delivered by the same method as a writing, may also be waived.¹⁵

Permitting electronic records to substitute for writings serves little purpose if the records are not admissible in evidence in the event of a dispute. The rule is simple: a record or signature may not be excluded from evidence solely because it is in electronic form.¹⁶ An electronic record also qualifies as an original, even if that record is not the original form of the document, and satisfies statutory audit and record retention requirements.¹⁷ Beyond that, the ordinary rules of evidence will apply.

**Federal preemption – which law applies?**

ESIGN, as a federal law, governs both federal and state laws governing a transaction affecting interstate commerce. ESIGN gives states limited authority to "modify, limit or supersede" the provisions of section 101 of ESIGN (which contains the act's provisions giving legal recognition to the use of electronic records and signatures).¹⁸ States may "modify, limit or supersede" section 101 of ESIGN¹⁹ by adopting either:

- the official text of UETA or
- any other law that specifies "alternative procedures or requirements for the use or acceptance" of electronic records or signatures, but only if those alternative procedures or requirements are:
  - "consistent" with the substantive provisions of the act and
  - neither require nor accord preferred status to the use of a specific technology or technical specification for electronic records or signatures.²⁰

This generally means that any provisions of state law that are inconsistent with section 101 of ESIGN, other than provisions that are part of the Official Text of UETA, are preempted by ESIGN with respect to any transaction affecting interstate commerce.

**Documents requiring special treatment**

Some documents that are otherwise eligible for electronic records and signatures require special treatment or are subject to special rules. These documents include:

- Documents evidencing debt obligations secured by specific goods or leases of specific goods (e.g., automobile purchase loans, leases, and retail installment sales contracts)²¹
- Documents evidencing a transfer of an interest in real property
- Documents that must be notarized
- Documents filed with a public office
- Powers of attorney
- Negotiable promissory notes²²
Special review with legal counsel is required for documents falling in these categories.

**Part II: Minimum requirements and additional guidance**

*Capitalized terms are defined in the glossary at the end of the table.*

<table>
<thead>
<tr>
<th>Topic</th>
<th>Minimum Requirements</th>
<th>Additional Guidance</th>
</tr>
</thead>
</table>
| Consent  | Each party to the transaction must agree to use electronic records and electronic signatures in place of written documents and manual signatures. This agreement may be express, or implied from the circumstances, except for consumer transactions, where the ESIGN Consumer Consent Process must be followed. | Consent for business-to-business transactions does not need to be written or expressly stated – it can be implied from the circumstances (such as using an online signing process). However, for commercial transactions consent is generally evidenced by:  
- Entering into an express, separate agreement or statement of consent to use electronic records and signatures and/or  
- Including provisions for the use of electronic records and signatures in the transaction documents (See the sample terms attached as Appendix B).  
For most consumer transactions, the ESIGN Consumer Consent Process must be completed. This special consent procedure applies if a statute, regulation, or other rule of law calls for information related to a transaction to be provided to a consumer in writing, and should precede presentation of the material covered by the writing requirement. The elements of the ESIGN Consumer Consent Process are:  
- The consumer must affirmatively consent, or confirm prior consent, electronically  
- The party obtaining the consumer’s consent must provide some specific disclosures prior to consent in clear and conspicuous statement and  
- The consent must “reasonably demonstrate” the consumer’s ability to receive electronic records in the formats that will be used for delivering the required information. |
| Authority | Transaction participants must have authority to engage in the transaction and to make agreements.                                                                                                                     | In most consumer transactions, authority is based on the individual’s competence to contract.  
In commercial transactions, authority is established through processes that are independent of the process used to present electronic records and obtain electronic signatures as part of the transaction. For example, documentation appropriate to show necessary authority to engage in the transaction: |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Minimum Requirements</th>
<th>Additional Guidance</th>
</tr>
</thead>
</table>
| Authentication | Generally, the identity of the transaction participants must be established in some manner. Authentication includes:                                                                 | Initial authentication of participants in a business transaction usually focuses on the participant’s business title or role and authority to act as the representative of a business entity. It is less common for authentication to focus on the participant’s actual identity as an individual. In other words, the process often focuses on whether the individual actually holds the business position/title being asserted, and whether the individual has been authorized to enter into the transaction, and not on whether the individual is actually “Fred Smith.”  
Methods of initial authentication for business transactions, for example, could include:  
- Self-authentication (optionally combined with):  
  - Positive authentication (e.g., obtain the person’s contact information, including business email address and telephone number, and/or  
  - Negative authentication (e.g., confirm that office address is not a known mail drop or temporary office suite) and  
- Positive authentication – certification or verification documents from the represented entity or a trusted third party.  
- Logical authentication – the information provided by the transaction participant is checked to make sure it is logically consistent.  
- Negative authentication – the information provided by the transaction participant is checked to determine if it has previously been associated with fraudulent transactions or identity theft.  
- Knowledge-based authentication – KBA can be used if the actual identity of the transaction participant cannot be confirmed. |  
- Confirming a transaction participant’s actual identity or status as an authorized business representative at the beginning of the transactions ("initial authentication") and  
- Confirming that the same person initially identified as a transaction participant continues to be the person participating in the transaction ("ongoing authentication"). |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Minimum Requirements</th>
<th>Additional Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>participant is also relevant. KBA authentication is a combination of positive, negative and trusted-third party authentication.</td>
<td>Ongoing authentication of the participant also needs to be addressed.</td>
</tr>
<tr>
<td>Delivery and presentation</td>
<td>Electronic records should be presented in a way that is easy to identify, navigate and read. Electronic records should be presented at the appropriate time and sequence in the context of the transaction.</td>
<td>Disclosures, notices and agreement terms should generally be placed by any decision the transaction participant is asked to make by checking a box, clicking a button or creating an electronic signature. Electronic records may be displayed behind properly labeled hyperlinks. When using hyperlinks, always take into account general principles of fairness and state and federal prohibitions against unfair and deceptive practices. As a related matter, whenever possible, businesses often include in their agreements, terms governing sending and receipt of email. These terms usually include a description of the delivery methods, such as attaching the electronic record to an email or making the electronic record available at a particular website. Where delivery is necessary and is provided via email, it is common for the sender to monitor its systems for notice of actual delivery failures and to re-send or send via traditional means in the event of a bounce back or other notice of non-delivery.</td>
</tr>
<tr>
<td>Electronic signature</td>
<td>Examples of electronic signatures include click-through, holographic or digitized signatures, check boxes/radio buttons, process-based (including digital signatures using system-generated digital certificates), oral recordings. The electronic signature, or the process through which the electronic signature is created, should: Establish the signer's intent to create the signature and Attach the electronic signature to, or logically associate the electronic signature with, the record being signed. Confirm that a previously identified transaction participant is the person accessing, reviewing and/or signing the electronic records (&quot;ongoing authentication&quot;).</td>
<td>Intent can be established if, for example, the transaction is structured so that language evidencing the signer's intent to be bound by his electronic signature is presented to the transaction participant on or just prior to the electronic record to be electronically signed. Electronic signatures are often attached or embedded in electronic records as graphic symbols. However, certain types of electronic signatures, such as a click-through signatures, are not usually attached or embedded in the electronic record. Those signatures are often logically associated with the signed electronic record through an audit trail tying the signature to the signed electronic record — this is often part of the same process used to establish attribution of the electronic signature to the signer (see below).</td>
</tr>
<tr>
<td>Topic</td>
<td>Minimum Requirements</td>
<td>Additional Guidance</td>
</tr>
<tr>
<td>-------</td>
<td>----------------------</td>
<td>---------------------</td>
</tr>
<tr>
<td><strong>Attribution</strong></td>
<td>The electronic signature process must create and preserve evidence of the identity of the person who signed for the signed electronic record to be enforceable against the signer.</td>
<td>A signature is attributable to a person if it was the act of the person. The act may be shown in any manner, including a showing of the efficacy of any security procedure (such as a password or PIN) applied to determine the person to whom the electronic signature was attributable. Moreover, the effect of an electronic signature attributed to a person is determined by the context and surrounding circumstances at the time of its execution or adoption, including the transaction participants’ agreement.</td>
</tr>
</tbody>
</table>
| **Audit trails** | Evidence of each electronic signature that is either incorporated into, or logically associated with, a signed electronic record should be captured in an audit trail and should include data relevant under the circumstances and appropriate to the type of Electronic Signature and the transaction. | Data captured by the audit trail will usually include the following:  
- The date and time the person accesses the system  
- Confirmation that the person accessing the system has successfully completed the applicable authentication process  
- The date, time, and system identifier of each electronic record accessed by the person on the system for review and signing, and the identity of the person accessing the electronic records  
- The date and time each electronic record is signed, the system identifier for the electronic record being signed, and the identity of the person signing the electronic record  
- The role in which the person was signing  
- Association of the authentication process with the person to whom the user ID and password was assigned, and also, as of the date of signing, the actions the person was authorized to take on the system. |
| **Record retention by the provider of the electronic record** | To satisfy the rules of evidence related to business records, it must be possible to establish that the integrity and reliability of the Electronic Records have been protected since the time they were first presented for effect or signed, as applicable. | It should be possible to logically associate material transaction data through identifiers that may be both used within the transaction system and transmitted to other systems for management and storage. For electronic records to be validly retained, it is necessary:  
- That each electronic record accurately reflects the information in the document  
- That the electronic record remains accessible to all persons entitled by law to access for the period of time required by law and  
- That the electronic record is in a form capable of being accurately reproduced for later reference. |
<table>
<thead>
<tr>
<th>Topic</th>
<th>Minimum Requirements</th>
<th>Additional Guidance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Record retention by the recipient of the electronic record</td>
<td>Counterparty must have opportunity to retain copies of the documents, including a fully executed copy that includes FCA’s signature.</td>
<td>The transaction process should include the ability to print or save documents while the transaction is ongoing and delivering fully executed copies of all documents once the transaction is concluded.</td>
</tr>
</tbody>
</table>

### Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication</td>
<td>Authentication refers to the process of identifying a transaction participant. There are two types of authentication (each defined in this glossary):</td>
</tr>
<tr>
<td></td>
<td>• Initial authentication</td>
</tr>
<tr>
<td></td>
<td>• Ongoing authentication</td>
</tr>
<tr>
<td>Authentication process</td>
<td>Refers to the process chosen to perform initial or ongoing authentication, and can include the following:</td>
</tr>
<tr>
<td></td>
<td>• Self-authentication</td>
</tr>
<tr>
<td></td>
<td>• Positive authentication</td>
</tr>
<tr>
<td></td>
<td>• Logical authentication</td>
</tr>
<tr>
<td></td>
<td>• Negative authentication</td>
</tr>
<tr>
<td></td>
<td>• Third-party authentication</td>
</tr>
<tr>
<td></td>
<td>• Credentials</td>
</tr>
<tr>
<td></td>
<td>• KBA (see definition below)</td>
</tr>
<tr>
<td>Commercial transaction</td>
<td>A commercial transaction is a transaction between a company and FCA for a business purpose.</td>
</tr>
<tr>
<td>Audit trail</td>
<td>Documentation and electronic records generated by a technology platform or system which evidence the delivery of, display of, presentation of, access to, consent to, and/or signing of, and ongoing integrity and accuracy of, electronic records.</td>
</tr>
<tr>
<td>Company</td>
<td>Legal entities that are created by law. The most common types include corporations, general partnerships, limited partnerships, limited liability companies and trusts.</td>
</tr>
<tr>
<td>Consumer</td>
<td>An individual who is entering into a relationship or participating in a transaction for personal, family or household purposes, and also a legal representative (such as a guardian) of such an individual.</td>
</tr>
<tr>
<td>Consumer transaction</td>
<td>A Transaction entered into between a consumer and FCA.</td>
</tr>
<tr>
<td>Credential</td>
<td>A token, device or process provided to a transaction participant to authenticate his or her identity in connection with a transaction or series of transactions. Examples include PINs, passwords, digital certificates, stored biometric measurements and random-number generators.</td>
</tr>
<tr>
<td>Electronic record</td>
<td>A record created, generated, sent, communicated, received or stored by electronic means.</td>
</tr>
<tr>
<td><strong>Electronic signature</strong></td>
<td>An electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.</td>
</tr>
<tr>
<td>-------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td><strong>ESIGN Act</strong></td>
<td>The federal Electronic Signatures in Global and National Commerce Act</td>
</tr>
<tr>
<td><strong>ESIGN consumer consent process</strong></td>
<td>The process required under the ESIGN Act and under the UETA in some states for obtaining consent from consumers for electronic delivery of information otherwise required by law to be delivered in writing</td>
</tr>
<tr>
<td><strong>ESIGN contract terms</strong></td>
<td>Provisions added to transaction agreements concerning specific issues related to the use of electronic records (e.g., delivering notices electronically).</td>
</tr>
<tr>
<td><strong>Initial authentication</strong></td>
<td>Initial authentication is generally performed in connection with the creation of a relationship and can refer to the authentication of a transaction participant's actual identity or the transaction participant's identity as an authorized representative of an organization.</td>
</tr>
<tr>
<td><strong>KBA</strong></td>
<td>Knowledge-based authentication. KBA uses private information about an individual to prove that the person providing such information is the person being identified.</td>
</tr>
<tr>
<td><strong>Logical authentication</strong></td>
<td>The information provided by the transaction participant is checked to make sure it is logically consistent.</td>
</tr>
<tr>
<td><strong>Negative authentication</strong></td>
<td>The information provided by the transaction participant is checked to determine if it has previously been associated with fraudulent transactions or identity theft.</td>
</tr>
<tr>
<td><strong>Ongoing authentication</strong></td>
<td>Ongoing authentication is generally performed in connection with the transaction participant's participation in a transaction and can be used to confirm a transaction participant's identity as established during the initial authentication.</td>
</tr>
<tr>
<td><strong>Participant</strong></td>
<td>See transaction participant below.</td>
</tr>
<tr>
<td><strong>PDF</strong></td>
<td>Portable document format.</td>
</tr>
<tr>
<td><strong>Positive authentication</strong></td>
<td>The information provided by the transaction participant is confirmed with a trusted external source of information.</td>
</tr>
<tr>
<td><strong>Record</strong></td>
<td>Information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. All paper documents are records, but not all records are paper documents.</td>
</tr>
<tr>
<td><strong>Rule of law</strong></td>
<td>A statute, court decision, regulation or ordinance.</td>
</tr>
<tr>
<td><strong>Self-authentication</strong></td>
<td>The transaction participant provides a declaration of identity.</td>
</tr>
<tr>
<td><strong>SMS</strong></td>
<td>Short message service. Commonly referred to as text messaging.</td>
</tr>
<tr>
<td><strong>Third-party authentication</strong></td>
<td>The identity of the transaction participant is confirmed by a trusted third party.</td>
</tr>
<tr>
<td><strong>Transaction</strong></td>
<td>An action or set of actions occurring between two or more persons relating to the conduct of business, consumer or governmental affairs. Transactions include, but are not limited to, the following: consumer loans and leases, including post-funding authorizations; commercial loans and leases, including crop insurance and post-funding authorizations; equipment loans and leases; real estate related loans and leases; procurement contracts; routine third-party contracts; internal signature processes, including HR; and intellectual property.</td>
</tr>
</tbody>
</table>
agreements.

Transaction participant (or participant)
A person that is an active participant in a transaction.

Trusted third party
A person, other than the signer or the person entitled to enforce the signed record, who is in the business of providing services intended to enhance (i) the trustworthiness of the process for signing electronic records using an electronic signature; or (ii) the integrity and reliability of the signed electronic records.

UETA
The Uniform Electronic Transactions Act as approved and recommended by the Uniform Law Commission in July 1999.

---

3 UETA §§ 3, 2(16).
7 UETA § 3(b)(2); 15 U.S.C. § 7001(b)(2).
9 UETA § 2(13); 15 U.S.C. § 7006(9).
10 UETA § 2(7); 15 U.S.C. § 7006(4).
11 UETA § 2(8); 15 U.S.C. § 7006(5).
12 UETA § 5(e), 9(b).
14 UETA §§ 8 & 12(a); 15 U.S.C. § 7001(d) & (e)
15 UETA § 8(d).
17 UETA § 12(d); 15 U.S.C. § 7001(d)(3).
19 15 U.S.C. § 7001. Note that the other provisions of ESIGN are not superseded by state law.
20 id.
21 Subject to special rules under § 9-105 of the Uniform Commercial Code.
22 Subject to special rules under 15 U.S.C. § 7021 and UETA § 16.

AUTHORS

Margo H. K. Tank
Partner
Washington, DC | T: +1 202 799 4000
[email protected]