A Brief Guide to Using Electronic Signatures in Securities Transactions

By Margo H. K. Tank, Sara E. Emley, and R. David Whitaker

Margo Tank is a partner of BuckleySandler LLP.*

Sara Emley is a Partner of BuckleySandler LLP.**

David Whitaker is counsel in the Washington, DC, office of BuckleySandler LLP.***

The securities industry has been at the forefront of adopting and using electronic technology to comply with its regulatory obligations. The industry has been slower, however, to adopt electronic signatures, in part because of the complex interaction of the laws and regulations affecting their use, and in part because of uncertainty concerning enforcement. The use of electronic signatures is also inexorably tied to the delivery and management of the records to be signed. This article will summarize the key sources of law impacting the use of electronic signatures in securities transactions, and then discuss some of the practical issues to consider when implementing electronic signature solutions.

Key Sources of Law

ESIGN and the UETA

The Three Pillars

The Electronic Signatures in Global and National Commerce Act ("ESIGN") and the Uniform Electronic Transaction Act ("UETA") are the primary U.S. laws governing the use of electronic records and signatures in commercial transactions. ESIGN, enacted by Congress, is designed to promote the use of electronic commerce by permitting the use of electronic signatures in connection with contracts and other records in transactions in interstate and foreign commerce. The UETA is a set of uniform rules for electronic equivalents of writing and signatures which has been adopted into law by 47 states, the District of Columbia, Puerto Rico, and the U.S. Virgin Islands.

For the laws and transactions within the scope of the UETA and ESIGN, the following three basic rules apply:

- 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.[1]

©2013, Margo H. K. Tank, Sara E. Emley, and R. David Whitaker.

These rules are sometimes called the "Three Pillars." 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."[2] An "electronic record" is "a record created, generated, sent, communicated, received, or stored by electronic means."[3] The term is intended to cover any type of record which is generated or stored electronically; as such, it would cover records created on a computer and stored on any type of media.

As a general proposition, participants in a transaction must agree to use electronic records and signatures in lieu of paper documents and traditional signatures.

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."[4]

Since the adoption of ESIGN and the UETA, a growing body of case law has affirmed the enforceability of properly implemented electronic signatures. Across the country, electronically signed documents have been accepted and enforced by the courts in a wide variety of circumstances, including sales contracts, real estate contracts, loans, insurance transactions, employment agreements, arbitration agreements, and service agreements. The legal consequences of an electronic signature and the question of whether it may properly be attributed to a particular person are interpreted under applicable law using the same legal standards used for a traditional ink signature.[5]

Consent to Use Electronic Signatures

As a general proposition, participants in a transaction must agree to use electronic records and signatures in lieu of paper documents and traditional signatures. Except with respect to certain consumer transactions, this agreement may be either expressly stated, or implied from the circumstances. However, ESIGN and certain state UETA enactments require a more formal consumer consent process in some circumstances.[6] For example, electronic records may be used to satisfy any law that requires that records be provided to consumers "in writing" only if the consumer has affirmatively consented to the use of the electronic records, and has not withdrawn the consent (the "ESIGN Consumer Consent Process").[7] Prior to obtaining consent, the electronic record provider must deliver a clear and conspicuous statement of certain information (collectively, the "ESIGN Consumer Consent Disclosures").[8] A "consumer" is, for purposes of ESIGN, "an individual who obtains, through a transaction, products or services which are used primarily for personal, family, or household purposes, and also means the legal representative of such an individual."[9]

Furthermore, the consumer must consent electronically, or confirm his or her consent electronically, in a manner that "reasonably demonstrates" that the consumer can access information in the electronic format that will be used to provide the information.[10] Thus, any in-person transaction which concludes in a paper agreement to engage in business electronically should be followed up by an electronic confirmation and consent – which must occur before any information that must be provided "in writing" is delivered. A literal reading of ESIGN's statutory language suggests that the demonstration requirement must be effected as part of the consent itself. What satisfies the requirement is subject to interpretation. One view is that the reasonable demonstration test may be flexibly satisfied by a consumer's e-mail confirming that the consumer can access the electronic records or a consumer's acknowledgement or affirmative response to a provider's query asking if the consumer has the necessary hardware and software.[11] However, the more conservative view is that the consumer must demonstrate that the consumer can access the information through an actual test using the electronic formats in which the information will be delivered.[12]

Special Rules for electronic records

ESIGN and the UETA 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 does not 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. The UETA does not state for how long it 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.[13]
- If a particular writing is required by law to be displayed in a particular format, the UETA does not change that requirement. 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 the UETA.
- If a law expressly requires a writing to be delivered by U.S. mail or by hand delivery, the UETA does not change those delivery rules.[14]

A record or signature may not be excluded from evidence solely because it is in electronic form.[15] 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.[16] Beyond that, the ordinary rules of evidence will generally apply.[17]

Delivery

ESIGN is largely silent on delivery.[18] The UETA provides default rules for determining when an electronic record has been sent from one party to another, and when it has been received. The default rules only address the functional requirements for sending or receiving the record; they do not presume that the record is intelligible or effective at the time it is transmitted.[19] The effect of a garbled or incomplete transmission is left to other provisions of the UETA and to other law.

An electronic record is considered "sent" when the following criteria are met:

- The record is addressed or directed to an information processing system:
  - Specified or used by the recipient for receiving records of the general type being transmitted, and
  - From which the recipient is able retrieve the record;
- The information is in a form the recipient's system is capable of processing; and
- The information leaves an information system under the sender's control, or, if the sender and the recipient are using the same system, enters a part of the system under the recipient's control.[20]

For the record to be "sent," the recipient must be able to retrieve it, and it must be in a form the recipient's system can process.[21]

The UETA's receipt rule is essentially a subset of the sending rule. To be received, it does not matter how the record was addressed, so long as:

- it actually arrives at a system to which the recipient has access for retrieving the record,
- The system has been designated or actually used by the recipient for receipt of the type of record in question, and
- The system is capable of processing the record.

It is not necessary for the recipient to actually access the electronic record in order for it to be considered received.[22]

The default rules for what constitutes "sending" or "receiving" an electronic record may be varied by agreement. The place of sending and receipt may be varied by agreement, or specified in the electronic record itself. The force and effect of variations from the default rule is left to other law.

The UETA does contain one rule concerning sending and receipt that cannot be modified by agreement. If one of the parties to a transmission is aware that a record was not actually sent or actually received, even though it was purportedly sent or received under the terms of the UETA's default rules, then the effect of the electronic record and its transmission is determined by other law. [23] Most judicial decisions considering delivery of information via email have endorsed the notion that if the sender's business records establish that an email was transmitted to the correct email address, a "rebuttable presumption" of delivery arises.[24] It is not clear, however, whether this presumption survives the sender's receipt of an actual notice, whether system-generated or otherwise, that the email was not delivered.

Articles 8 and 9 of the UCC

Two articles of the Uniform Commercial Code that are relevant to securities transactions are excluded from coverage under both the UETA and ESIGN – Article 8, covering the ownership and transfer of investment securities, and Article 9, covering security interests in personal property (including some aspects of security interests in investment securities not addressed in Article 8). However, Article 8 and 9 both permit the use of electronic records and signatures for most purposes, according to their own terms.

UCC Revised Article 8 covers the issuance, registration, transfer and ownership of investment securities. It reflects the securities industry's wholesale adoption of electronic communication.

Interests in securities may be evidenced and transferred electronically. Contracts for the sale or purchase of securities need not be in writing.[25] In addition, for certain purposes, signed writings otherwise required by Revised Article 8 may be replaced with electronic transmissions if the parties have agreed to do so.[26] Most of the residual provisions in Revised Article 8 mandating a signed writing are related to certificated securities.

Revised Article 9 of the UCC permits the use of electronic records and signatures to create a security interest in personal property, and by recognizing electronic collateral. Revised Article 9 permits electronic creation of a security interest via an "authenticated" security agreement.[27] The definition of "authenticated" includes both (i) the signing of a writing and (ii) the validation of a record by executing or adopting a symbol, or encrypting a record in whole or in part, with present intent to identify the authenticating party, adopt or accept a record or term, or establish the authenticity of a record or term that contains the authentication or to which a record containing the authentication refers.[28] The definition of the term "record," in turn, is identical to the definition in the UETA.[29] Revised Article 9 has also adopted a scheme for perfecting a security interest against electronic records that will serve the same purpose as chattel paper. The scheme preserves the functionality of chattel paper as readily transferable to a buyer in the ordinary course of business, while permitting perfection without requiring physical possession of written documents.[30]

SEC Regulations and Guidance

Use of electronic signatures

The SEC has generally authorized the use of electronic records and signatures for most purposes.[31] Electronic records may be used with respect to most documents related to government submissions and filing, where the regulations themselves do not require the documents to be created or maintained on paper.[32]

Delivery

Although they do not directly address the use of electronic signatures, the SEC's statements regarding electronic delivery of required documents are both instructive and a necessary consideration in rolling out the use of electronic signatures in connection with securities and investment transactions. The SEC first directly addressed the use of electronic media in connection with securities transactions in 1995, noting that "delivery of information through an electronic medium generally could satisfy delivery or transmission obligations under the federal securities laws."[33] The 1995 Release specifically pointed to the necessity of establishing recordkeeping procedures to evidence satisfaction of applicable requirements and of taking reasonable precautions to insure integrity and security of information provided.[34] The SEC also noted that "[a]s is the case with paper delivery, there should be an opportunity to retain a permanent record of the information[,]" and posited that "[a]n issuer or other party that structures its delivery in accordance with the principles and examples set forth [in the 1995 Release] can be assured that it is satisfying its delivery obligations under the federal securities laws."[35]

In noting the central role that notice and access play in the acceptable retrieval of documents provided by electronic means, the SEC suggested that the process of accessing such documents should generally not be burdensome, but nonetheless sanctioned a level of difficulty consistent with that used to authenticate an individual entitled to access such documents, such as through the use of a user ID and PIN.[36]

Observing that providing information through regular mail provides reasonable assurance that a delivery requirement is satisfied, and noting that delivery by electronic means should as well, the SEC pointed out that:

> Examples of procedures evidencing satisfaction of the delivery requirements include: (1) obtaining an informed consent from an investor to receive the information through a particular electronic medium coupled with assuring appropriate notice and access, as discussed above; (2) obtaining evidence that an investor actually received the information, for example, by electronic mail return-receipt or confirmation of accessing, downloading, or printing; (3) disseminating information through certain facsimile methods; (4) an investor's accessing a document with hyperlinking to a required document; and (5) using forms or other material available only by accessing the information.[37]

In elaborating on the first of these illustrative alternatives, the SEC noted that:

> If a consent is used, the consent should be an informed consent. Recipients generally should be apprised: that information provided would be available through a specific electronic medium or source (*e.g.*, via a limited proprietary system, or at a World Wide Web site); of the potential that

> investors may incur costs (*e.g.,* on-line time); and of the period during, and the documents for, which the consent will be effective.[38]

With respect to notice, the SEC registered its view that electronic communications providers:

> should consider the extent to which the electronic communication provides timely and adequate notice to investors that information for them is available and, if necessary, consider supplementing the electronic communication with another communication that would provide notice similar to that provided by delivery in paper.[39]

Additionally, with respect to access, the SEC cautioned against using a medium that was so burdensome that "intended recipients cannot effectively access the information provided[,]" and noted that, "as is the case with a paper document, a recipient should have the opportunity to retain the information or have ongoing access equivalent to personal retention."[40] The SEC also noted that providing the ability to electronically download the document via a clearly labeled hyperlink would be sufficient to satisfy such a need.[41]

The SEC once again validated these procedures in a 1996 interpretive release providing guidance on the use of electronic media by broker dealers, transfer agents and investment advisors.[42] In 2000, the SEC issued its latest interpretive release on the use of electronic media to fulfill delivery and associated requirements of federal securities laws, noting its intent "to provide guidance to issuers of all types, including operating companies, investment companies and municipal securities issuers, as well as market intermediaries, on several issues involving the application of the federal securities laws to electronic media."[43] The 2000 Release was specifically targeted to "[f]acilitate electronic delivery of communications by clarifying that

- investors may consent to electronic delivery telephonically;
- intermediaries may request consent to electronic delivery on a "global," multiple-issuer basis;
- issuers and intermediaries may deliver documents in portable document format, or PDF, with appropriate measures to assure that investors can easily access the documents; [and]
- an embedded hyperlink within a Section 10 prospectus or any other document required to be filed or delivered under the federal securities laws causes the hyperlinked information to be a part of that document[.]"[44]

The SEC also affirmed the framework it established regarding electronic delivery in its 1995 and 1996 Releases, and encouraged issuers and intermediaries to "continue to assess their compliance with legal requirements in terms of the three areas identified in the releases—notice, access and evidence of delivery."[45]

In July 2000, in response to a Congressional mandate embedded within ESIGN, the SEC also adopted an interim final rule essentially clarifying that supplemental sales literature appearing on the same website as or hyperlinked to a mutual fund prospectus did not require an investor's consent under the ESIGN Consumer Consent Process, as long as investors are provided with reasonably comparable access to both the prospectus and the sales literature.[46] Note, however, that the exemption to ESIGN's Consumer Consent requirements does not apply to other contexts in which documents are required to be provided under federal or state law. Therefore, ESIGN's consumer consent provisions will continue to apply to many documents that must be provided to investors. [47]

Record Retention

Generally, the SEC has been liberal in permitting the use of electronic business records. Registered investment companies and investment advisors, for example, are permitted to maintain most records in electronic form.[48] The SEC, in amending its rules in 2001, explained:

> Under revised rules 31a-2 and 204-2, funds and advisers are permitted to maintain records electronically if they establish and maintain procedures: (i) To safeguard the records from loss, alteration, or destruction, (ii) to limit access to the records to authorized personnel, the Commission, and (in the case of funds) fund directors, and (iii) to ensure that electronic copies of non-electronic originals are complete, true, and legible. We are also amending the rules to clarify the obligation of funds and advisers to provide copies of their records to Commission examiners. The amendments make clear that funds and advisers may be requested to promptly provide (i) legible, true, and complete copies of records in the medium and format in which they are stored, and printouts of such records; and (ii) means to access, view, and print the records.[49]

The SEC also has electronic record maintenance requirements in place for broker-dealers[50] and transfer agents.[51]

However, the SEC's rules for broker-dealers place some significant limitations on the types of storage media that the broker-dealer may use for storing business records electronically, by requiring that certain records be stored on non-erasable, non-rewritable media.[52]

Implementation Considerations

A broker-dealer or investment adviser who wishes to implement the use of electronic signatures should consider the following:

Authentication

A key element to any transaction is proper identification of the parties. Thus, establishing that an electronic signature can be legally attributed to the signing party is essential. "Authentication" refers to the process used to confirm an individual's identity as a party in a transaction. Authentication of identity in an electronic transaction occurs in two contexts:

- When the relationship between the parties is *first created.*
- When a transaction occurs in the course of an existing relationship.

There are a number of methods available for verifying identity initially when creating a relationship. They range from requiring a personal appearance and presentation of identification to self-identification of parties without any verification. Different methods of authentication, with different levels of risk for the person accepting proof of identity, are appropriate in different circumstances. A key element in selecting a strategy for authenticating identity is risk assessment. The more risk involved in mis-identifying another party to the transaction, the more important authentication becomes.

Initial authentication is often critical because the process leads to multiple future transactions, each of which represents a potential loss if authentication has failed. Frequently, the authenticated person receives an access or identification device, often called a "Credential", which is used to streamline or automate identification during future transactions.

For ongoing transaction authentication, a credential may be a variety of things – a user name, a password or pin, a number generated at random, a biometric measurement, a digital certificate, or a combination of these and other technology tools for controlling access to a system. The process for issuing the credential may be relatively informal, or extremely rigorous and tightly controlled, as appropriate to the risks associated with the underlying transactions that will be completed using the credential. Depending on the transaction and its potential risks, multi-factor authentication (such as the use of both a standing password and a one-time password, randomly generated number or biometric measurement) may be appropriate.

Consent to Use Electronic Signatures

Given the emphasis ESIGN, UETA, Article 8 and the SEC all place on the need for clear, voluntary consent and agreement to use electronic records and signatures, any process for delivering or signing electronic records will need to address:

- How to obtain or establish each participant's express or implied agreement to transact business electronically, and
- When a transaction involves a consumer, how to comply with the ESIGN Consumer Consent Process, if applicable.

An express agreement can provide certainty that the transaction participants have agreed to use electronic records and signatures. However, such an express agreement is not strictly necessary before conducting transactions electronically, especially in business-to-business transactions. In the absence of an express agreement, the requisite "agreement," for purposes of satisfying UETA and ESIGN may be implied, and determined from all available circumstances and evidence.

As discussed above, if a provider of a financial or investment product or service is required by a law or regulation to provide or make available certain information to a consumer in writing ("Required Consumer Information") the process may need to build a system to comply with the ESIGN Consumer Consent Process. Given the variety of circumstances in which the SEC permits electronic delivery of information without reference to ESIGN, or permits a more informal consent process, it may be necessary to examine the underlying law governing the transaction very carefully to determine whether the ESIGN Consent Process applies. If it does, ESIGN Consumer Consent Disclosures should be presented to the consumer clearly and conspicuously prior to obtaining consent, and include:

- Notice of the consumer's right to receive Required Consumer Information in writing.
- An explanation of the scope of each consumer's affirmative consent that addresses:
  - A description of the transaction or types of transactions to which the consent applies; and
  - If applicable, a statement that the consumer's consent covers the general use of electronic records and electronic signatures in connection with the transaction.

- A statement advising the consumer of the consequences of refusing to provide consent to receive disclosures or other records by electronic means, for example:
  - Any delay in completing the transaction that may result;
  - Any additional fee or cost that may be imposed as a result;
  - Other modes of communication that the consumer will be asked to use in order to continue the transaction (*e.g.* telephone, appearance at branch office, etc.).
- A statement advising the consumer of the right to withdraw his or her consent at a later time, including:
  - Instructions on how to withdraw consent; and
  - The consequences of withdrawing consent.
- A statement providing the consumer with instructions on how to update his or her contact information.
- A statement providing consumers with a general description of the hardware and software required to receive and access electronic records. The description generally should include, if applicable:
  - The minimum version of any Internet browser software required;
  - Any specific viewer or other software required to view records;
  - Any specific software required to sign the records; and
  - Any limitations on the popular operating system platforms which may be used, based on the other required software.
- Instructions as to how a consumer may, after consenting and upon request, obtain a paper copy of any disclosure or other record, and whether any fee will be charged for such a copy.

The ESIGN Consumer Consent Process must also "reasonably demonstrate" the consumer's ability to access the formats the sender will use to deliver Required Consumer Information. With the emphasis on "reasonable," the goal should be to avoid the scenario where Required Consumer Information is presented in odd, outdated or cutting-edge formats such that an ordinary consumer's computer would not be able to read or display the information from the record provider. To establish a reasonable demonstration, consider these questions:

- How the consumer will access the Required Consumer Information (e.g., via the Internet, email, other software, or a combination);
- What format will the Required Consumer Information be presented; and
- The appropriate mechanism, method or process for obtaining the consumer's consent that reasonably demonstrates that the consumer can access the format of the Required Consumer Information.

Required Consumer Information may be provided on a web site, via email or through a combination of both methods, or within a proprietary software download process. In addition to the method (web, email, proprietary software) of providing the Required Consumer Information, the format (html, word, PDF, etc.) of that information also needs to be considered. In other words, there will need to be a demonstration that the consumer can access the Required Consumer Information both via the method and in the format chosen by the record provider.

Once the access mechanism and format decisions are answered, there is a range of strategies that may be employed in designing the ESIGN Consumer Consent Process. The strategies may include:

- A complex technology test,
- Relying on completion of the ESIGN Consumer Consent Process itself (when the records will be presented in the same format), or
- Self-reporting by the consumer (especially with respect to email and formats with universally available readers, like PDF).

Whether one strategy is better than the other will depend on the nature and complexity of the transaction, the delivery methods being used, and the extent to which the information is being delivered in common formats.

Electronic Signatures

Broadly speaking, the functions of an electronic signature fall into one of four categories:

- Affirming the accuracy of information in the record ("this record contains the correct information, because I signed it");
- Affirming assent or agreement with the information in the record ("I have agreed to the terms and conditions described in this record, because I signed it");
- Affirming the signer's opportunity to become familiar with information in the record ("I must have had this record in front of me, because I signed it"); or
- Affirming the source of the information in the record ("this record must have come from me, because I signed it").

A single signature can perform one or more of these functions in any combination. The particular functions a signature fulfills depend on the circumstances. Frequently, either the

record being signed or a *related* record describes the functions of the signature.

Examples of possible methods for creating electronic signatures, when coupled with the necessary intent, include:

- A typed name
- A click-through
- A recorded voice
- A keypad response to a prompt from a Voice Response Unit
- A Personal Identification Number
- A Password (composed of numbers and/or alpha characters)
- A biometric measurement (*e.g.,* retina scan, fingerprint matching, and voice recognition)
- A digitized image of a handwritten signature
- An identification number created using a number generator
- A sophisticated cryptographic system, like a digital signature

Note that a number of the potential signature methods involve the use of a credential. A credential can also serve as a signature, if that is the signer's intent. Usually, if a credential is used to create a signature the credential itself will not appear as the signature – in other words, a PIN used to sign an electronic record will not usually appear on a display or print-out of the final record as a "symbol" signature, since that could destroy the PIN's value as a credential. Instead, the PIN will be used to create a "process" signature, which will often be reflected on the record as a recitation, such as "Signed by Fred Smith on May 5, 2013 at 12:45 PM."

A record or signature may not be excluded from evidence solely because it is in electronic form.

As discussed above, a credential can also be used to authenticate an individual before a signature is created using another process entirely. Bear in mind that different types of electronic signature techniques offer different levels of security against unauthorized use and different levels of assurance of "attribution" – that the signature was applied by a particular individual.

In some cases, the need for security may be minimal. The nature or structure of some transactions makes it difficult for the signer to repudiate a signature. For example, if a person orders custom computer equipment and signs a lease, takes delivery and uses the equipment for six months, it may be difficult for the signer to repudiate even a simple signature, such as a typed name. More secure signature methods may be desirable for categories of transactions more likely to produce disputes concerning the authenticity of signatures. Furthermore, as the discussion of applicable law at the beginning of this article illustrates, there are a few types of electronic records for which only certain types of electronic signatures may be used. The most significant of these are records that evidence a personal property security interest, where Revised Article 9 of the Uniform Commercial Code requires that the signature must either be a symbol or a process utilizing encryption. This restriction may be of particular importance for parties taking a security interest in investment properties or securities entitlements as part of an investment or brokerage services agreement.

In remote transactions, the desired level of security for the signature process may depend, in part, on the extent to which the circumstances make it difficult for the signer to repudiate the signature later. Many environmental factors may also affect the choice of a particular type of electronic signature. For example, if the signer is appearing to sign in person, it may be impractical for the electronic signature to be stored on the signer's computer. If the signer is engaging in a one-time transaction, a relatively simple signature process may be preferred in order to control cost and the complexity of the transaction. On the other hand, if it is desirable for the signature to function both as an authenticator of identity and as protection against post-signature alteration of the document, then a more sophisticated type of signature, such as asymmetric encryption, may be preferable. If there are to be a series of remote transactions, then a type of signature easily activated by use of a PIN, password or token may be more appropriate. Alternatively, the signer may first be authenticated by the system via personal information or shared secrets, a credential created, and then a record signed during a secure session. In that case, authentication occurs prior to the signing event, and is tied to the signature by an audit trail, rather than being part of the signature itself.[53]

There are circumstances that may limit the available selection of electronic signature types. For example, if records are to be signed as part of a remote transaction with consumers using equipment in their homes, a digitized signature may not be a feasible option because most consumers do not have

the necessary hardware and will not be willing to acquire and install it in order to complete the transaction.

The number of signatures needed on the record may also influence the choice of a signature technology. The same signer may need to sign in multiple places on the record, or the record may need to be signed by multiple people.

Note that various electronic signature techniques may be combined. For example, a signature process may use both a PIN and a randomly generated number. As another example, a biometric measurement may be combined with a typed name or digitized signature. Combining techniques may serve a number of purposes. It may make it easier to demonstrate, when necessary, that the signature is correctly attributed to the signer. It may also make it easier to create or display a graphic representation of the signature, by using a "traditional" name or symbol to complement a more sophisticated security device.

All in all, there is a wide variety of factors to take into account when selecting the appropriate signature technique for a particular transaction. Successfully choosing the correct technique is a function of analyzing and balancing those factors.

An electronic signature is only effective if the Signer intends to create a signature. The signature process should minimize the risk that Participants could legitimately claim later that that they created an electronic signature without realizing what they have done, or its legal significance. This risk may be greater if innovative or technologically sophisticated signature methods are employed. For those signatures that are created or applied by clicking on an on-screen button or striking a key on the keyboard, such as "enter", the process should be designed to minimize the possibility that signers might later claim that they did not intend to, or did not understand they were being asked to create, a legally binding signature.

A confirmation process may be particularly useful as a way to avoid disputes over intent. Using various techniques, it may be possible to demonstrate that, even after an electronic signature is created, the transaction participant was made aware that a signature was created and was given an opportunity to recant.

Record Retention Related to Electronic Signatures

The requirements for retaining business records required under the securities laws have been addressed in detail by the SEC. While maintaining electronic signature records in accordance with this guidance is likely sufficient for regulatory purposes, ESIGN and the UETA also contain guidance which is helpful in maintaining electronic records in a manner that will assure their successful introduction, in the event of a dispute, under the rules of evidence. "Record retention" under ESIGN and the UETA focuses on accurate preservation of, and access to, the information contained in the electronic record. What information must be preserved is determined by the purpose the associated record serves. The information needing to be preserved, accessed or retained may, depending on the circumstances, include the format (e.g., file format) and presentation (e.g., images, text formatting, and document design) of the electronic record, as well as the record's content (e.g., data, text). For example, IP address information related to an email or other electronic transmission might be helpful to retain as evidence of the source, or the format or font of a particular Disclosure might be helpful to retain to show that a particular version was used or that particular Disclosure requirements were met.

In the event of a dispute, the record holder must be prepared to demonstrate that the electronic record:

- Accurately reflects the information contained in the record at the time it was signed or delivered,
- Is accessible to anyone entitled to access the record holder's copy of the record under an applicable law or regulation or Agreement,
- Can be accurately reproduced for later reference.

The record management system should:

- Protect the accuracy of the information contained in the record by building physical, processing and technical safeguards;
- Develop methods for preserving "access" that address the issue of technology obsolescence and develop procedures for converting the record, should conversion become necessary to preserve accessibility;
- Determine the applicable period of time for which the records must be accessible; and
- Describe the process for retaining and accessing documents to persons entitled to have access.

There is a variety of factors to take into account when managing record integrity and access, including:

- Control over consistency of data and acceptance of incomplete or inaccurate records. It may be desirable for the record management system to offer a variety of automated error and process checks to enhance quality control and workflow. Electronic records may, if the system is properly designed, be checked for inconsistent or incomplete data, proper signature execution, timely preparation and accessibility, order of presentation, and a variety of other parameters, as the specific situation requires.

- Control over access and alteration. Credentials may be used to identify individuals entitled to have access to the records, and also to define and limit the ways in which they may interact with the records. For example, one person may be entitled to view the records, but not add or change data, while another may have authority to alter the records at will. Alterations of records may be prevented by the system, or detected and classified as authorized and unauthorized. Alterations may be tracked and logged over time, providing a historical view of the electronic record often unavailable with a paper document. As discussed above, the SEC requires especially strong controls to avoid alteration of certain kinds of records, especially records held by broker-dealers.

The question of whether an alteration is "authorized" depends on a number of factors:

- Who is entitled to make a change to the record;
- What type of changes is the person authorized to make; and
- When during the life of the record are changes permitted?

None of these questions is answered by the UETA and ESIGN. Instead, these questions must be answered by custom, common usage, agreement, and the relationship among the transaction participants. About the only rules that are relatively universal are that generally (i) an electronic record should not be altered after it has been signed without the signer's express or implied consent (except for the addition of other signatures), and (ii) an electronic record should not be altered after it has been delivered for effect without either the recipient's consent or notice to the recipient of the change.

Protection of data accuracy and integrity is an area where there is a wide variety of potential approaches, any of which may be valid under appropriate circumstances. The questions to consider include:

- Who is entitled to have access to the record, for what purposes, and how will access be controlled?
- How will records be filed, indexed, and associated to permit easy management and recovery?
- What type of integrity checks should be performed on documents added to the transaction (e.g., detection of alteration, all necessary signatures, error and consistency checks, etc.)?
- How should multiple documents related to a single transaction be maintained?
- Should there be a method for notifying Participants that a new document has been added to a website or executed in connection with a transaction?

Conclusion

The securities industry is well-positioned to leverage the use of electronic signatures in connection with a wide variety of products and services. The relevant underlying law and the SEC Releases provide both legal authorization and useful guidance on when, and how, electronic records and signatures may be used in securities and brokerage transactions. Key considerations will include authenticating signers, getting appropriate agreement from the counter-party, effectively presenting records for signing, selecting an appropriate type of signature, and managing the electronic records after signing. With careful planning, it should be possible to use electronic signatures in connection with most customer-facing securities and investment-related transactions.

ENDNOTES

* Margo Tank advises financial services providers and technology companies on how to structure business programs and online platforms in compliance with the Electronic Signatures in Global and National Commerce Act (ESIGN) and the Uniform Electronic Transactions Act (UETA), and comply with other state and federal laws governing electronic and mobile financial services transactions, including laws related to privacy and data security, electronic record management, money transmission and other payment methods (plastic or virtual), advertising and unfair or deceptive acts and practices.

** Sara Emley advises financial services firms on various regulatory and other legal issues. Her clients include investment advisers, broker-dealers, banks, investment companies, private funds and insurance companies. Her practice focuses on providing clients with advice on the laws and regulations applicable to investment advisers, investment companies, broker-dealers and other specialized regulatory provisions applying to financial services providers, including credit card issuers. Ms. Emley also advises financial services firms with respect to compliance with ERISA and other laws and regulations applicable to retirement accounts.

***David Whitaker advises financial services companies in transactional, legal and regulatory matters. Mr. Whitaker's practice also focuses on assisting firms in their efforts to structure and implement platforms and processes that conform to the requirements of the Electronic Signatures in Global and National Commerce Act (ESIGN), the Uniform Electronic Transactions Act (UETA), other applicable state and federal laws, and various industry standards.

1 UETA § 7; ESIGN § 101(a).

2 UETA § 2(13); ESIGN § 106(9). The requirement that the record be "retrievable in perceivable form" is an objective, not subjective, requirement. To qualify as a record, it is not necessary that a specific recipient be able to comprehend the information contained in the record, just that someone could comprehend it. Also, it is not required that the record be retrievable by everyone who might conceivably have a

connection to the transaction. It is only required, for purposes of the definition, that it be retrievable by someone.

[3] UETA § 2(7); ESIGN § 106(4).

[4] UETA § 2(8); ESIGN § 106(5).

[5] UETA § 5(e), 9(b).

[6] 15 U.S.C. § 7001(c)(1). Several states have incorporated the requirements of the ESIGN Consumer Consent Process into their adoption of UETA. *See, for example,* N.J. Stat. Ann. § 12A:12-21.

[7] *Id.*

[8] 15 U.S.C. §§ 7001(c)(1)(B). The information to be provided includes:

- Any right or option of the consumer to have the record provided or made available in paper form;
- The right of the consumer to withdraw consent and any conditions or consequences (which may include termination of the parties' relationship) of such a withdrawal;
- Whether the consent applies (i) only to the particular transactions which gave rise to the obligation to provide the record, or (ii) to all identified categories of records that may be provided during the course of the parties' relationship;
- The procedures the consumer must use to withdraw consent and to update information needed to contact the consumer;
- How the consumer may after consenting, upon request, obtain a paper copy of the electronic record and whether any fee will be charged for such a copy; and
- The hardware and software requirements for access to and retention of the electronic records.

[9] 15 U.S.C. § 7006(1).

[10] 15 U.S.C. § 7001(c)(1)(C).

[11] 146 Cong. Rec. S5282 (daily ed. June 16, 2000) (colloquy between Senators Abraham and McCain). For example, the Senators exchanged in the following discussion:

Mr. McCAIN. Does the Senator also agree with me that the "reasonable demonstration'' requirement would be satisfied, for instance, if the consumer responds affirmatively to an electronic query asking if he or she can access the electronic information or if the affirmative consent language includes the consumer's acknowledgement that he or she can access the electronic information in the designated format?

Mr. ABRAHAM. Yes. A consumer's acknowledgment or affirmative response to such a query would satisfy the ``reasonable demonstration'' requirement.

Mr. McCAIN. Would the ``reasonable demonstration requirement'' be satisfied if it is shown that the consumer actually accesses records in the relevant electronic format?

Mr. ABRAHAM. Yes. The requirement is satisfied if it is shown that the consumer actually accesses electronic records in the relevant format.

[12] *See* 146 Cong. Rec. S5215, S5216 (daily ed., June 15, 2000) (statement of Sen. Wyden) ("It is not sufficient for the consumer merely to tell the vendor in an email that he or she can access the information in the specified formats. There must be meaningful two-way communication electronically between the vendor and consumer.")

[13] 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.

[14] UETA §§ 8 and 12(a); ESIGN §§ 101(d) and (e). There is a special provision in ESIGN that would permit use of electronic delivery in lieu of mail delivery if certain conditions are met. See ESIGN § 101(c)(2)(B). Generally speaking, these rules are not variable by agreement under either ESIGN or the 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 waive. d UETA § 8(d).

[15] UETA § 13; ESIGN §101(a).

[16] UETA § 12(d); ESIGN § 101(d)(3).

[17] For a comprehensive discussion of the rules evidence as they apply to electronic business records, see Lorraine v. Markel, 241 F.R.D. 534 (D.Md. May 4, 2007).

[18] There is a special provision in ESIGN that would permit use of electronic delivery in lieu of mail delivery if certain conditions are met. See ESIGN § 101(c)(2)(B).

[19] Official Comment 1, UETA § 15.

[20] UETA § 15(a). The second alternative accommodates the situation where the sender and recipient are using the same system, and that system is controlled by the sender. Common circumstances could include an email from an internet service provider to one of its customers, or from an employer to an employee via an internal email system. In such circumstances, the record would not be considered sent until it is reflected in the recipient's "in basket" as an incoming email.

[21] According to Official Comment 1 to UETA § 15, satisfaction of this element of the rule is not affected by errors in transmission that might garble an otherwise readable record, if the record is not so badly damaged that it cannot be processed. In other words, if Harry sends a word processing file to Mike, and Mike receives a damaged but accessible file, the file would be considered sent. If, on the other hand, the damage is so severe that the file cannot be opened and inspected, even to determine that it has been garbled, then presumably it has not been sent, since it is not in a form the recipient's system is capable of processing. As a technical matter, it may also make a difference when the fatal damage occurs. If the record is damaged after it leaves the system, or the part of a system, under the sender's control, then presumably it has been sent for purposes of UETA § 15, since, at the moment it left the sender's control, it was capable of being processed by the recipient's system.

[22] UETA § 15(e).

[23] UETA § 15(f). A few states have modified this rule, stating that under specific circumstances the sender's receipt of a notice of non-delivery, such as an email "bounceback" notice from a system administration program, automatically prevents the record from being considered sent or received. *See, for example*, Pa. Stat. Ann., tit. 73 § 2260.115.

[24] *American Boat Co., Inc. v. Unknown Sunken Barge*, 418 F.3d 910, 914 (8th Cir. 2005) (holding that the same presumption of delivery applicable to paper communications should apply to email); *Kennell v. Gates,* 215 F.3d 825, 829 (8th Cir.2000) (absent evidence to the contrary, e-mails properly dispatched via a generally reliable method are presumed delivered and received); *Roling v. E*Trade Sec. LLC*, 860 F. Supp. 2d 1035, 1043 (N.D. Cal. 2012) (finding that an email notice sent within a reasonable time before a fee increase was sufficient); *In re Leventhal*, No. 10 B 12257, 2012 WL 1067568 (Bankr. N.D. Ill. Mar. 22, 2012) (holding the concept that "a properly addressed item mailed to someone is presumed to have been received" applies equally to email); *Abdullah v. Am. Exp. Co.*, 3:12-CV-1037-J-34MCR, 2012 WL 6867675 (M.D. Fla. Dec. 19, 2012) ("As Defendant has provided evidence showing . . . email was properly delivered to Plaintiff, a rebuttable presumption was created that Plaintiff received that email."); *Ball ex rel. Hedstrom v. Kotter*, 746 F. Supp. 2d 940, 953 n. 10 (N.D. Ill. 2010) (presuming that because no evidence was presented to the contrary, the plaintiff had received and had knowledge of information sent to him by the defendant via email); *SEC v. Global Online Direct, Inc.*, No. 1:07-cv-0767-WSD, 2007 WL 4258231 (N.D. Ga. Nov. 29, 2007) (holding that Email notice to investors are appropriate if the process creates a reasonable expectation that the investors will (1) receive notice, (2) understand what it relates to, and (3) make a knowing and deliberate decision to read or disregard the communication).

[25] UCC §8113 (Revised).

[26] UCC §8102(a)(6) (Revised) defines "communication" as either a signed writing or any other method of transmission agreed upon by the parties. Official Comment 6 explains:

The term "communicate" assures that the Article 8 rules will be sufficiently flexible to adapt to changes in information technology. Sending a signed writing always suffices as a communication, but the parties can agree that a different means of transmitting information is to be used. Agreement is defined in Section 1201(3) as "the bargain of the parties in fact as found in their language or by implication from other circumstances including course of dealing or usage of trade or course of performance." Thus, use of an information transmission method might be found to be authorized by agreement, even though the parties have not explicitly so specified in a formal agreement. The term "communicate" is used in Sections 8102(a)(7) (definition of entitlement order), 8102(a)(11) (definition of instruction), and 8403 (demand that issuer not register transfer).

[27] UCC §§9205(a) and 9102(5) (Revised).

[28] UCC §9102(7) (Revised). Note that the Article 9 definition of 'authenticated" is more limited than the ESIGN/UETA definition of "electronic signature", and would appear to limit the ability to use certain types of electronic signatures on a security agreement, including a security agreement covering investment property, securities entitlements and securities. In 2010, NCCUSL promulgated amendments to Revised Article 9 that included a

new definition of "authenticated" that parallels the ESIGN/UETA definition of electronic signature, which will go into effect July 1 of 2013 in roughly 37 states. As of this writing, New York is not one of those states – in New York the pre-2010 definition of "authenticated" will presumably continue to apply.

[29] UCC §9102(69) (Revised).

[30] A comprehensive discussion of Article 9's approach to perfecting and prioritizing security interests in electronic chattel paper is beyond the scope of this article. For a more comprehensive discussion of electronic chattel paper, see Jane K. Winn, *Electronic Chattel Paper: Invitation Accepted* (September 25, 2010). Available at SSRN: http://ssrn.com/abstract=1682783 or http://dx.doi.org/10.2139/ssrn.1682783.

[31] The SEC has carved out one significant exception to this general rule:

> Regulation S-T…requires issuers to retain manually-signed signature pages or other documents that signatories must execute ("authentication documents") to authenticate, acknowledge or otherwise adopt their signatures that appear in typed form within electronically filed documents. These authentication documents must be executed before or at the time an issuer makes an electronic filing. The filer must retain each authentication document for a period of five years and furnish it to us upon request. Comparable requirements exist under the Securities Act and the Exchange Act where typed, duplicated or facsimile signatures appear on a document that we permit issuers to file with us in paper form.
>
> We believe that these requirements to retain authentication documents are not subject to E-SIGN because authentication documents are records generated principally for governmental purposes rather than in connection with a business, consumer or commercial transaction. Moreover, these authentication documents arise in the context of a governmental filing. Governmental filings are expressly excluded from E-SIGN. Accordingly, issuers subject to these retention requirements should continue to retain the paper original of all authentication documents.
>
> Application of the Electronic Signatures in Global and National Commerce Act To Record Retention Requirements Pertaining to Issuers Under the Securities Act of 1933, Securities Exchange Act of 1934 and Regulation S-T, 66 FR 33175 (June 21, 2001) (citations omitted).

[32] *Id.*

[33] 1995 Release at 53459-60.

[34] *Id.* at 53460.

[35] *Id.*

[36] *Id. See also* 1995 Release at 53466.

[37] 1995 Release at 53461 (footnote and other citations omitted).

[38] *Id.*

[39] *Id.* at 53460.

[40] *Id.*

[41] *Id.* In providing further illustrations of the kinds of procedures that would evidence satisfaction of a delivery requirement using hyperlinks, the SEC noted:

> Company XYZ places its sales literature in a discussion forum located on the Internet World Wide Web. The sales literature contains a hyperlink to the Company's final prospectus. While viewing the literature the individual can click on a box marked "final prospectus," and almost instantly the person will be linked directly to the Company's Web site and the final prospectus will appear on the person's computer screen.
>
> Sales literature, whether in paper or electronic form, is required to be preceded or accompanied by a final prospectus. The hyperlink function enables the final prospectus to be viewed directly as if it were packaged in the same envelope as the sales literature. Therefore, the final prospectus would be considered to have accompanied the sales literature. Consequently, the placing of sales literature in a discussion forum on a Web site would satisfy delivery obligations provided that a hyperlink that provides direct access to the final prospectus is included.
>
> The SEC also provides a similar illustration for its hyperlink example in the context of mutual fund disclosures:
>
> A fund posts its supplemental sales literature and prospectus on a file server for open access over the Internet. The supplemental sales literature contains hyperlinks to the fund's electronic prospectus and includes a caption referring the investor to the prospectus. The investor would not need any additional software or need to take burdensome steps to access the prospectus and thus has reasonably comparable access to both documents. This system also provides for the downloading or printing of prospectuses and sales literature. An investor would not be required to retrieve, download, or print a prospectus before viewing the sales literature. The system does not require any consent by its users.
>
> When a user accesses the supplemental sales literature, electronic delivery of the prospectus can be inferred. This scenario is analogous to an investor's selecting an envelope containing a paper prospectus and supplemental sales literature from a display at an office of a broker-dealer. This electronic delivery of the prospectus would be sufficient for other purposes if the fund could reasonably establish that the investor has actually accessed the sales literature or the prospectus.

[42] 1996 Release at 24647, 24650.

[43] 2000 Release at 25844.

[44] Id.

[45] 2000 Release at 25845. The SEC also declined an invitation from commenters to rule that in providing access to a document, the document would be considered presumed to have been delivered, noting that while more prevalent than at the time of the 1995 Release, internet access was still not widespread enough to assume all investors could access their documents electronically. 2000 Release at 25853.

[46] See *Exemption From Section 101(C)(1) of the Electronic Signatures in Global and National Commerce Act for Registered Investment Companies, Investment Company Act Release No. 24582*, 72 S.E.C. Docket 2201 (July 27, 2000).

[47] For a more detailed discussion of the SEC delivery requirements and the interplay with ESIGN's consent provisions, see *Requirements Pertaining to the Electronic Delivery of Documents,* Sara E. Emley and Margo H. K. Tank, The Investment Lawyer, Vol. 14, No. 5 (May 2007), pp. 3-10.

[48] 17 CFR 270.31a-2; 17 CFR 275.204-2.

[49] Investment Company Act Release No. 24991; 66 FR 29224 (May 30, 2001).

[50] 17 CFR 240.17a-4(f). The SEC has explained:

> To the extent Rule 17a-4 requires the retention of the types of contracts and transactional records identified in the Electronic Signatures Act, broker-dealers will be able to retain them electronically under Section 101(d)(1), provided the electronic records are accurate, accessible, and capable of being accurately reproduced for later reference. Under paragraph (f) of Rule 17a-4, broker-dealers are already permitted to retain all required records—not just these contracts and transactional records—using electronic means, subject to the requirements set forth in that paragraph…[W]e find that the electronic storage requirements of Rule 17a-4(f) meet, and are consistent with, the accuracy, accessibility, and accurate reproduction requirements of Section 101(d)(1) of the Electronic Signatures Act. Therefore, broker-dealers must continue to comply with the electronic storage requirements of Rule 17a-4(f) after June 1, 2001.
>
> Exchange Act Release No. 44238, 66 FR 22916 (May 7, 2001).

[51] Exchange Act Release No. 44227 66 FR 21648 (May 1, 2001).

[52] See 17 CFR 240.17a-4(f).

[53] See, for example, Zulkiewski v. General American Life, Unpublished, LC No. 09-047293-CZ, Mich. Ct. of Appeals, June 12, 2012.

This article is reprinted with permission from *Practical Compliance and Risk Management for the Securities Industry,* a professional journal published by Wolters Kluwer Financial Services, Inc. This article may not be further re-published without permission from Wolters Kluwer Financial Services, Inc. For more information on this journal or to order a subscription to *Practical Compliance and Risk Management for the Securities Industry,* go to **pcrmj.com** or call **866-220-0297**