

Electronic Signatures, Agreements & Documents; The Recipe for Enforceability and Admissibility

*By: Bruce S. Nathan &
Terence D. Watson*

Abstract

More and more businesses are conducting their transactions electronically. Congress and state legislatures have facilitated this expansion of electronic commerce by enacting laws that govern the validity of electronically signed documents and electronic transactions. The Electronic Signatures in Global and National Commerce Act, enacted in 2000 and frequently referred to as the “E-Sign Act”, is the federal statute governing electronic transactions and electronic signatures. The Uniform Electronic Transaction Act (“UETA”) is the state law counterpart to the E-Sign Act. UETA has been adopted by 47 states, the District of Columbia, Puerto Rico and the United States Virgin Islands.¹ UETA makes the E-Sign Act applicable to electronic signatures and electronic transactions that are governed by state law. The E-Sign Act and UETA treat electronic transactions and signatures the same as conventional ink and paper documents and transactions.

The E-Sign Act, UETA and the other laws governing electronic transactions also prescribe the rules that must be followed in order to ensure the validity of electronically signed documents and electronic transactions. For example, the E-Sign Act and UETA require parties to agree to conduct their transactions electronically. However, these laws do not prescribe all of the requirements for admitting electronic agreements and other electronic documents into evidence in a court proceeding. This article discusses the requirements for both valid electronic agreements and other electronic documents, and admitting them into evidence in a litigation.

Ink and Paper v. Electronic Transactions

Legally valid and binding ink and paper and electronic agreements contain an offer, an acceptance, and consideration. An offer contains the terms on which one party, the offeror, is willing to enter into an agreement with a second party, the offeree. Acceptance occurs when the offeree accepts the offer according to the specific terms that were offered, thereby creating a

¹ The three states that have not adopted UETA (Illinois, New York and Washington) have enacted other statutes governing electronic transactions.

“meeting of the minds” between the parties.² Finally, consideration is something of value that one party to an agreement provides to the other party in exchange for an act or a promise.

A contract party proves the requisite “meeting of the minds” for a valid agreement by:

- Identifying the parties to the agreement; and
- Confirming the parties’ knowledge and acceptance of the terms of the agreement.

Satisfying the requisite “meeting of the minds” is relatively straightforward when dealing with a traditional ink and paper agreement. The parties to an ink and paper agreement are typically identified by their signatures on the written agreement. The parties are deemed to have knowledge of the terms of their agreement that are contained in the written document. Finally, the parties’ signatures on the ink and paper agreement show their acceptance of, and their requisite intent to be bound by, the terms of the agreement.³

However, proving the requisite “meeting of the minds” can be more difficult in an electronic transaction. The unique format of an electronic agreement requires verifying the identity of the parties, and their intent to be bound by the terms of their agreement. In addition, procedures must be implemented to preserve the integrity and retrievability of the contents of an electronic agreement because they are subject to the risk of unauthorized alterations, and are not readily viewable. These issues are more fully discussed below.

The Elements of a Valid Electronic Signature

The E-Sign Act and UETA require that an electronic signature possess the following three characteristics in order to be considered the functional equivalent of a handwritten signature:

- The signature may be a sound, symbol, or process;
- The signature must be attached to or logically associated with an electronic record⁴
- The signature must be made with the intent to sign the electronic record.

Bottom line, the enforceability of a party’s electronic signature requires proof that the party actually affixed its electronic signature to the agreement, and also intended to be bound by the terms and conditions of the agreement. There are many ways to sign a document electronically.

² A response to an offer that proposes different terms than those contained in the initial offer is technically both a rejection of the initial offer, and a new offer.

³ The acceptance of an oral agreement is evidenced by some other form of assent, such as verbal acquiescence, a handshake, or performance of the act that is the subject of the agreement.

⁴ The E-Sign Act and UETA define an electronic record as “created, generated, sent, communicated, received or stored by electronic means.” It, therefore, includes electronic records created on computer and stored on any type of media flash drive.

They include the following:

- Typing the sender's name at the end of an email message;
- Providing a scanned image of a handwritten signature that is attached to an electronic document;
- Providing a secret code, password, or PIN to identify the sender to the recipient;
- Providing a unique biometrics-based identifier, such as a fingerprint, voice print, or a retinal scan;
- Using a computer mouse to click on an "I agree" button;
- Creating a sound, such as the sound by pressing "9" on a telephone, to indicate acceptance; and
- Creating a "digital signature" through the use of public key cryptography.

Whether Emails Constitute a Contract

The courts have addressed the issue of whether, and under what circumstances, an email satisfies the requirements for a valid and enforceable contract. An email will be considered a sufficient writing, provided that it is signed or subscribed to by the signer authorized to bind the party, and sets forth the terms of the agreement.

In *Naldi v. Grunberg*, the plaintiff asserted a claim for enforcement of a contractual right of first refusal to purchase a unit of real property. The plaintiff and the defendant had allegedly agreed to this right of first refusal *via* email. The defendant sought to dismiss the claim, partially based on the argument that an agreement evidenced by an email cannot satisfy the statutory requirement that contracts for the conveyance of real property must be in writing, and signed by the party against which the agreement is sought to be enforced.

The New York State Appellate Division for the First Department, an intermediate state court, rejected this argument in its 2010 decision. The court relied on the E-Sign Act's requirement that an electronic signature have the same legal effect as a paper contract. The court also noted that the statute of frauds (which requires certain types of contracts to be written) is designed to ensure an objective record of both the existence of an agreement and its terms. The court concluded that allowing an electronic transmission, like an email, to evidence a contractual agreement, does not hamper these objectives. However, the court then held that the email in question was just a counteroffer that was not accepted because the email did not show any meeting of the minds between the parties on the terms of any purported right of first refusal.

The courts have also addressed the circumstances under which an email could be considered properly "signed" or "subscribed" in order to be enforceable under the statute of frauds. For example, the United States District Court for the Southern District of New York, in its 2005

decision in *Bazak International Corp. v. Tarrant Apparel Group*, held that a letter sent by the plaintiff's president *via* email was a writing that satisfied the statute of frauds. The court also held that plaintiff's president's typed signature appearing on the signature line constituted a sufficient signature to bind the plaintiff to its terms. The court noted that an email, like a letter, telegram or fax, could be the basis of an agreement.

Similarly, in *Stevens v. Publicis, S.A.*, the court held that modifications to an employment agreement that were negotiated and agreed upon *via* email were enforceable where each of the emails in the chain included the sender's typed name at the bottom. The court concluded that the emails from the plaintiff constituted "signed writings" satisfying the statute of frauds because plaintiff's name at the end of his email signified his intent to authenticate the contents.

However, in *Bayerische Landesbank v. 45 John Street*, another New York State Appellate Division First Department decision in 2013, the court held that an email was not properly subscribed for purposes of the statute of frauds because the email bore only a pre-printed signature. The United States District Court for the District of Colorado in a 2010 decision in *Buckles Management LLC v. Investordigs*, also held that an email was not properly signed because the author of the email lacked authority to bind the defendant to its terms. Finally, in *Pepco Energy Services Inc. v. Geiringer*, the United States District Court for the Eastern District of New York held that an unsigned letter attached to an email was not a signed document. Neither the forwarding email nor the presence of a typed signature in the letter constituted an enforceable signature. In fact, the court noted the existence of ample evidence that the alleged signatory had not intended to sign the letter.

Verifying the Identity of the Parties to an Electronic Transaction

Verifying the identity of the parties to an electronic transaction is complicated by the fact that the parties might not have met face-to-face, but instead may have always interacted remotely by computer, mobile device, or over the internet. The failure to verify the identity of a party signing an electronic agreement, like an ink and paper agreement, raises the risk of a forged signature.

The identity of a signatory of an electronic agreement can be verified in several ways. The parties can use a reliable sign-on process, such as by providing a password, PIN or secured secret code to enable the parties to identify themselves. Alternatively, the parties could require an answer to a shared secret question. This is typically done in conjunction with sending a link to a trusted email address, and thereafter, limiting access to the documents until the correct answer to the shared question is provided. Independent third parties might also conduct an identity verification process based on personal data provided by the contract counterparties to such third party.

The United States District Court for the District of Kansas, in *Kerr v. Dillard Store Services, Inc.*, addressed the difficulty of verifying the identity of a signatory of an electronic agreement. The plaintiff's employer had sought to enforce a mandatory arbitration provision contained in an electronic agreement between plaintiff and her employer. The court addressed the enforceability of an arbitration clause where the plaintiff denied executing the electronic agreement containing that provision. The court held that the plaintiff's employer did not prove that the plaintiff had executed the electronic agreement. In reaching its conclusion, the court noted that the plaintiff's

supervisor had access to plaintiff's user name and could have reset plaintiff's password. That would have improperly granted the supervisor access to the secure website where the agreement was available to be signed. As a result, plaintiff's supervisor might have improperly executed the agreement in plaintiff's name.

Proof of the Parties' Knowledge and Acceptance of the Terms of an Electronic Agreement

Next, the signatories must have knowledge of and intend to be bound by the particular terms and conditions associated with their electronic signatures. Unlike an ink and paper agreement, when the parties sign a written agreement that contains the terms of the transaction, an electronic signature must be attached to, or logically associated with an electronic record containing the terms of the agreement. This requirement raises questions about a party's knowledge and understanding of the terms of an electronic agreement, and that party's intent to be bound by those terms. To further complicate the issue, the courts have analyzed this issue and reached different holdings on enforceability depending on whether the agreement in question is characterized as a shrink-wrap agreement, a click-wrap agreement, or a browse-wrap agreement.

A "shrink-wrap" agreement is a "money now, terms later" arrangement. An example of a shrink-wrap agreement is one where a party purchases a product and the terms and conditions of the sale are contained in the same sealed package that also contains the product. After opening the package, the purchaser can either accept the terms and conditions by keeping the product (thereby creating a binding agreement), or reject the terms and conditions by returning the product.

The United States Court of Appeals for the Seventh Circuit, in *Hill v. Gateway 2000, Inc.*, addressed the validity of a shrink-wrap agreement. The plaintiffs had ordered a computer over the phone from Gateway, and the computer arrived with the terms and conditions of the agreement, including an arbitration clause, inside the box containing the computer. The plaintiffs argued that the arbitration clause did not stand out. While conceding that they noticed the terms and conditions, they denied reviewing them closely enough to notice the arbitration clause. The plaintiffs could have rejected the terms of sale by returning the computer within thirty (30) days, but failed to do so. Following the expiration of the thirty (30) day period, the plaintiffs complained about the performance and components of the computer they had purchased. When the dispute could not be resolved, the plaintiffs commenced a class action lawsuit. Gateway moved to dismiss the litigation and have the dispute resolved through arbitration based on the arbitration clause.

The court initially held that Gateway could structure the transaction as a "money now, terms later" arrangement as long as the purchasers were aware of the nature of the transaction from the outset. The court also upheld the validity of the terms and conditions of the sale, including the arbitration clause, because the "terms inside of a box of software bind consumers who use the software after an opportunity to read the terms and to reject them by returning the product." Consequently, the court held that the plaintiffs intended to be bound by the terms and conditions of the sale, including the arbitration clause, by not returning the computer within the thirty (30) days provided in the terms and conditions.

A “click-wrap” agreement is the form of an electronic agreement that is most likely to be enforceable. A party to a click-wrap agreement, such as a seller, presents the other party, such as a buyer, with a web-page display that contains the terms and conditions of the agreement. Typically, a “click-wrap” agreement appears on an internet web-page and requires that the user consent to any terms and conditions by clicking on an “I agree” button or other type of link on the screen in order to proceed with the internet transaction. This act confirms the user’s assent to the agreement and all of its terms.

The Texas Court of Appeals, in *Barnett v. Network Solutions, Inc.*, addressed the validity of a “click-wrap” agreement. In *Barnett*, the plaintiff argued that he did not have adequate notice of a forum selection clause because it was “hidden” in the on-line agreement he had entered into with Network Solutions. The online agreement required users to scroll through the entire agreement, including all of its terms, before clicking on a button acknowledging their assent to the terms. The court, therefore, upheld the enforceability of the forum selection clause because the plaintiff had the opportunity to read and understand the forum selection clause, and, therefore, had adequate notice of the clause. The plaintiff could not complain that he had failed or otherwise chosen not to review the clause because the plaintiff had to scroll past the clause prior to clicking the “I agree” button acknowledging his assent to the terms of the agreement.

The United States District Court for the Eastern District of Pennsylvania, in *Feldman v. Google, Inc.*, also upheld the enforceability of a forum selection clause included among the terms of an online advertising contract because it was contained in a click-wrap agreement. Plaintiff could not open an online account with Google without visiting the web-page that displayed the agreement containing the terms and conditions, including the forum selection clause. A notice in bold print also appeared, stating “Carefully read the following terms and conditions. If you agree with these terms, indicate your assent below.” Finally, the words, “Yes, I agree to the above terms and conditions” appeared at the bottom of the web-page and had to be clicked in order for plaintiff to proceed to the next step in the transaction. Plaintiff also obtained a printer-friendly full screen version of the agreement. The court, therefore, concluded that the plaintiff had adequate notice of, and agreed to all of the terms of the agreement, including the forum selection clause.

Browse-wrap agreements, in contrast to “shrink-wrap” and “click-wrap” agreements, are prone to be unenforceable because the user can scroll through a website without ever viewing or knowing the existence of the terms and conditions of such agreements. Furthermore, the agreement does not require the user to assent to the terms. Instead, assent is established by continued use of the website. The courts have enforced the terms contained in browse-wrap agreements only upon the submission of proof of adequate notice of, and confirmation of agreement to, the terms.

The United States Court of Appeals for the Second Circuit, in *Specht v. Netscape Communications Corp.*, addressed the validity of a browse-wrap agreement. In *Specht*, Netscape argued that web users were compelled to arbitrate their disputes with Netscape because they had agreed to be bound by the software license terms, including an arbitration clause, by downloading software from Netscape’s web-page. The web users rejected the enforceability of the arbitration clause in the software license agreement, arguing that they had never agreed to it.

The terms and conditions, including the arbitration clause, were located on Netscape's web-page below the button the web users had to click in order to download the software. The only way the web users could have learned about the terms was by scrolling down the web-page to an area located *below* that button. Nevertheless, Netscape argued that the presence of the terms, including the arbitration clause, on the same page as the software download button was sufficient to bind the web users.

The Second Circuit disagreed and held that the arbitration clause was unenforceable. The court found that Netscape had failed to provide the web users with adequate notice of the terms of the license, including the arbitration clause. Although the website stated "Please review and agree to the terms of the . . . license agreement before downloading and using the software," the court noted this was not a condition to downloading the software. A web user's clicking a download button does not confirm assent to the terms of an online agreement if the offer did not make clear that clicking the download button signifies acceptance of the terms. Therefore, the court concluded that the plaintiff had never agreed to the terms of the license agreement, including the arbitration clause, by downloading the software.

The United States Court of Appeals for the Ninth Circuit recently addressed the same issue in *Nguyen v. Barnes & Noble*. Barnes & Noble had placed its "terms of use" links on the bottom of every page of its website. Barnes & Noble had also presented a link to its "terms of use" on each page of the website's online checkout process that was underlined and in green type. However, the plaintiff had neither clicked on the links nor read the terms. Plaintiff argued that he did not agree to the arbitration clause contained in the terms because he had no notice of, and did not agree to the terms. Barnes & Noble responded that the terms, including the arbitration clause, were enforceable because plaintiff had sufficient constructive notice of the terms based on the placement of links to the terms on its website. The Ninth Circuit sided with the plaintiff and held that the plaintiff was not bound by the terms because he had no constructive notice of the terms, notwithstanding the proximity or conspicuousness of the link to the terms. Nor was plaintiff prompted to take any affirmative action to confirm agreement to the terms.

Enforceability of Online Terms and Conditions Incorporated Into a Written Contract

The courts have also addressed the enforceability of terms and conditions contained on a contracting party's website. The enforceability of these online terms and conditions generally depends on whether they were properly incorporated by reference into a written or electronic agreement.

In *Micrometl Corp. v. Tranzact Technologies, Inc.*, the United States District Court for the Southern District of Indiana addressed the enforceability of a forum selection clause in a document that was retrievable from a secure link on the service provider's (Tranzact's) website. Under the operative contract, TranzAct had agreed to manage freight shipping and audit MicroMetl's shipping expenses. MicroMetl commenced an action alleging that TranzAct had overbilled for the services it had provided. TranzAct moved to dismiss the action, or in the alternative, transfer venue, based on a forum selection clause contained in a document posted on its website.

The enforceability of the forum selection clause depended on whether the clause was “sufficiently incorporated” into the contract. The court ruled that the plain language of the contract sufficiently referenced, and thereby incorporated, the “principles” (*i.e.*, the terms) contained on TranzAct’s web-site because:

The Contract provides that the principles in their entirety can be found at a secure link on TranzAct’s website, which would be provided before joining as a partner. *The Contract clearly and specifically note[d]: ‘These written principles are what govern both our commitments and we want them readily available at all times so you can access them for your understanding and use.’* The Contract continue[d]: ‘These services are subject to standard principles that are on the secure link on our website.’ Finally, the Contract provide[d]: ‘These rules govern both of our commitments that arise from our signatures implementing your membership in the FREEDOM LOGISTICS NETWORK.

The court also noted that by executing the contract, both parties proved their intent to be bound by all of the terms of the contract. The fact that Micrometl did not thoroughly read the contract, including the principles contained on TranzAct’s website (which included the forum selection clause) did not preclude the enforceability of the forum selection clause because, according to the court, it is a fundamental principle of contract law that a person who signs a contract is presumed to know its terms and consents to be bound by them. Micrometl, was, therefore, presumed to have read the entire contract, including all of the references to the governing principles on TranzAct’s website. Additionally, the fact that the contract referred to the website’s governing body as “principles” and “rules,” instead of as “terms” or “conditions” or as even “forum selection clause,” did not alter the court’s conclusion. The court concluded that the contract’s use of both “principles” and “rules” was sufficient to put Micrometl on notice that it would be bound by the additional provisions contained on TranzAct’s website, including the forum selection clause.

Similarly, in *International Star Registry of Illinois v. Omnipoint Marketing, LLC*, the United States District Court for the Northern District of Illinois ruled that defendant’s invoice referencing terms and conditions (including a forum selection clause) contained on defendant’s website and signed by an officer of the plaintiff (International Star Registry) was an enforceable contract. The invoice stated in pertinent part as follows:

By my signature below, I certify that I have read and agree to the provisions set forth in this invoice and to the terms and conditions posted at [http:// www.omnipointmarketing.com/genterms.html](http://www.omnipointmarketing.com/genterms.html), and that I am duly authorized to bind the following organization (“client”) to such provisions.

This provision clearly stated that International Star Registry had intended to be bound by the terms and conditions contained on defendant’s website, including the forum selection clause, by virtue of plaintiff’s officer’s execution of the invoice.

Likewise, in *Spartech CMD, LLC v. International Automotive Components Group North Americam Inc.*, the United States District Court for the Eastern District of Michigan upheld the enforceability of an arbitration clause. The arbitration clause and defendant's other terms and conditions were posted on defendant's website, and all these terms were incorporated by reference into defendant's purchase orders sent to plaintiff. The court relied on state (Michigan) law that permits a party to incorporate terms or documents from other writings.

However, in *Feldman v. United Parcel Service, Inc.*, the United States District Court for the Southern District of New York refused to grant summary judgment in favor of UPS over whether the plaintiff had adequate notice of UPS' published tariff so as to be bound by a limitation of liability provision contained in the tariff. The plaintiff was able to complete its transaction with UPS using a self-service computer kiosk in a UPS store, but was not required to either view the terms of service containing the limitation of liability, or opt out of viewing the terms of service, in order to complete the transaction. Nor was there any evidence indicating whether UPS employees had copies of the terms of service to provide to customers.

The United States District Court for the Eastern District of Michigan in *Manasher v. NECC Telecom*, refused to enforce an arbitration clause contained in a document entitled "Disclosures and Liabilities Agreement" that was posted on defendant's website. Defendant's invoices submitted to plaintiff stated, among other things, that the "Disclosures and Liabilities Agreement" was available on defendant's website. The court held that this statement was insufficient to incorporate by reference the separate Disclosure and Liabilities Agreement because the language in the invoices did not indicate a clear intent that the Disclosure and Liabilities Agreement would be considered part of the contract between the parties. In this regard, nothing in the statement clearly indicated that the Disclosure and Liabilities Agreement applied to any part of, or was intended to be incorporated into the agreement between the parties. Instead, the statement merely informed a reader of where to find the Disclosure and Liabilities Agreement. Furthermore, the statement was the last of five statements appearing on the invoices, and was written in plain text, and appeared on the second page of the invoices.

The District Court of Appeals of Florida, in *Affinity Internet, Inc. v. Consolidated Credit Counseling Services, Inc.*, took a very restrictive view towards incorporating online terms into written and electronic agreements. The court refused to uphold the enforceability of an arbitration provision that was contained in terms and conditions posted on a website. The underlying contract stated that: "This contract is subject to all of SkyNetWEB's terms, conditions, user and acceptable use policies located at <http://www.skynetweb.com/company/legal/legal.php>."

The court noted, however, that although the contract stated that it is "subject" to all of SkyNetWEB's terms and conditions found at a stated website, that simple statement alone was insufficient to prove an agreement to arbitrate. The contract contained no clear language evidencing an intention of the parties to incorporate the terms and conditions into the contract. Also, the terms were not attached to the contract, and the seller failed to provide a copy of the terms to the buyer.

Integrity and Retrievability of Electronic Agreements and Signatures

Both the E-Sign Act and UETA also require that valid electronic agreements and signatures accurately reflect the data contained in an electronic record and be readily accessible. This requires securely archiving the record in order to preserve the integrity of an electronic agreement and signature, prevent unauthorized alternations, and ensure the completeness of the document. This also requires the implementation of measures to protect against improper modification or destruction of information in an electronic agreement. These measures include limiting access to the record to minimize the risk of any claim that an electronic agreement was modified or otherwise altered.

The implementation of an audit trail is vital to preserving the integrity of an electronic record. The purpose of an audit trail for an electronic record is to provide assurance of the integrity and trustworthiness of an electronic record. In effect, the audit trail is a record of the events related to, and the transactions concerning an electronic record. In addition to showing the evidence used to verify the identity of the signatory to an electronic agreement, record or other electronic document, the audit trail should also reflect any activities related to the electronic record including (i) any successful and unsuccessful attempts to log on to the database containing the electronic record, (ii) any alterations to the electronic record, and (iii) information sufficient to determine the date, time and source of any modifications to the electronic record. Accordingly, the contents of an audit trail should include the identity of the signatories, a date and time stamp, identification of the person making any changes to the electronic record, the original, unmodified terms, the modified terms, and the reason for the changes to the electronic agreement, record or other electronic document. The preservation of this data in an audit trail will enable the custodian of the record or any other interested party to follow the history of the electronic transaction, recover any incorrectly updated or deleted data, investigate the cause when an electronic record is found to be incorrect, and correct any incorrect information in the electronic record. By the same token, a “clean” audit trail that confirms the absence of any attempt to improperly access an electronically signed agreement after it has been agreed to by the parties, or any improper modifications to such an electronic agreement, will make it increasingly difficult for a contracting party to repudiate the terms of the agreement on the basis that the terms are not the terms that were agreed to at the time of entry of the agreement.

Admissibility of Electronic Documents in Court Proceedings

Aside from the foregoing concerns regarding the validity of an electronic signature, agreement, or other document, there is a separate set of concerns regarding their *admissibility*. Neither the E-Sign Act nor UETA provide any guidance on the requirements that must be satisfied for admitting an electronic signature, agreement or other document into evidence in a court proceeding.

The Federal Rules of Evidence (“FRE”), and their state law equivalents, govern the admissibility of evidence, including the admissibility of documents that are presented, signed, secured, archived and retrieved by an electronic signature process.⁵ The party seeking the admission of

⁵ Many states have adopted rules of evidence which track the FRE. Therefore, references herein will be limited to the FRE.

an electronic document into evidence has the burden of satisfying admissibility requirements. The failure to satisfy this burden can prove costly to a creditor that cannot collect its claim if the court refuses to admit into evidence the electronic document on which the claim is based.

In 2007, the United States District Court for the District of Maryland addressed the admissibility of electronic documents in *Lorraine v. Markel Am. Ins. Co.* In *Lorraine*, the plaintiff's yacht was damaged, and as a result, a claim was made to recover insurance proceeds. The plaintiff challenged the amount of an arbitrator's award in plaintiff's favor. Neither party, however, provided an evidentiary foundation to enable the court to rely on the various emails and other electronic documents that were offered in support of, and in opposition to, the award. Consequently, the court discussed how an electronic document could be admitted into evidence, as well as examples of the essential elements of an effective "e-contracting" process. That process includes authenticating an electronic signature by verifying the identity of the person purporting to sign an electronic document, creating an audit trail for the entire electronic transaction process from verifying the signatory of the electronic document, confirming the absence of any modifications or alterations to an electronic agreement, signature or other document after its creation, all the way through electronically sealing the electronic document, and then securely archiving and ensuring the retrievability of the electronic document. Anyone failing to satisfy the authentication requirements risks an unenforceable electronic document because of a court's refusal to admit the electronic document into evidence.

The Ninth Circuit Bankruptcy Appellate Panel (the equivalent of a United States District Court), in its 2005 decision in *American Express Travel Related Services, Co. v. Vinhnee*, also addressed the authentication of electronic documents in connection with efforts to admit them into evidence. In that case, American Express sought to block the discharge of the full amount of its claims in the amount of \$41,597.63 against a debtor in bankruptcy, which the debtor had scheduled for a lesser amount. American Express produced computer records along with a witness to testify regarding the computer system from which the records derived in order to prove the amount of the claims. Although there was no objection to the admissibility of the computer records (indeed, the debtor had failed to appear at trial), the court, on its own, required American Express to provide the ". . . authentication foundation regarding the computer and software in order to assure the continuing accuracy of the records."

The bankruptcy court refused to block the discharge of the full amount of American Express' claims against the debtor because of the court's refusal to admit American Express' computer records into evidence. This resulted from American Express' failure to properly authenticate its computer records supporting the amount of its claims.

On appeal, the Ninth Circuit Bankruptcy Appellate Panel affirmed the bankruptcy court's refusal to block the discharge of the full amount of American Express' claims. The court held that proof that a document being proffered into evidence is an accurate representation of the document as it originally was created is a condition for satisfying the authentication requirement for admissibility. The court further noted that authenticating an electronic record requires proof that the retrieved record is the same as the record that was originally created and archived. Although this is also a requirement for ink and paper documents, the format in which an electronic document is maintained makes the manner of proving its authenticity significantly different from

proving the authenticity of an ink and paper document. To prove the authenticity of an electronic document, the “focus is not on the circumstances of the creation of the record (as it is with ink and paper documents), but rather on the circumstances of the *preservation* of the record after its placement in a file, so as to ensure that the document being proffered is the same as the document that was originally created.”

Consequently, where the admissibility of an electronic document is contested, the issues to be resolved are likely to extend beyond the mere identification of the particular computer equipment and programs used, and may involve the entity’s policies and procedures for the use of the equipment, database, and programs, and how access to the pertinent database is controlled. Likewise, the possibility of alteration of an electronic document (which impacts its authenticity) would be impacted by how changes in the database are logged or recorded, as well as the structure and implementation of backup systems and audit procedures for assuring the continued integrity of the database. Although similar questions may be asked in connection with ink and paper documents, the increasing complexity of ever-developing computer technology necessitates more precise focus in connection with an electronic document.

Turning to the appropriate standard to determine the authenticity of an electronic document, the Ninth Circuit Bankruptcy Appellate Panel adopted an eleven-step foundation for computer records, referred to as the “Imwinkelried foundation.” This requires proof of the following:

1. The business uses a computer.
2. The computer is reliable.
3. The business has developed a procedure for inserting data into the computer.
4. The procedure has built-in safeguards to ensure accuracy and identify errors.
5. The business keeps the computer in a good state of repair.
6. The witness had the computer generate a printout of certain data.
7. The witness used the proper procedures to obtain the printout.
8. The computer was in working order at the time the witness obtained the printout.
9. The witness recognizes the exhibit as the printout.
10. The witness explains how he or she recognizes the printout.
11. If the printout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact.

The court placed particular emphasis on item no. 4 – proving that the procedure has built-in safeguards to ensure accuracy and identify errors. The court noted that this requirement includes the “details regarding computer policy and system control procedures, including control of

access to the database, control of access to the program, recording and logging of changes, backup practices, and audit procedures to assure the continuing integrity of the records.”

The Ninth Circuit Bankruptcy Appellate Panel upheld the bankruptcy court’s refusal to admit the evidence American Express had provided to support the amount of its claims. The court found the testimony of the American Express witness, that its computer system would not automatically change numbers, to be vague, conclusory and unpersuasive. The witness also showed a lack of knowledge regarding anything of consequence about either the software or the hardware. The court also noted that the witness’ declaration submitted on behalf of American Express was equally defective because it (a) omitted the declarant’s/witness’ qualifications, such as training or other knowledge regarding American Express’ computer system, and (b) failed to provide information regarding American Express’ computer policy and system control procedures, including control of access to the pertinent databases, control of access to the pertinent programs, recording and logging of changes to the data, backup practices, and audit procedures utilized to assure the continuing integrity of the records.

Bottom line, American Express could not prove the amount of its claims after the bankruptcy court’s refusal to admit American Express’ computer records into evidence, which, in turn, resulted from American Express’ failure to authenticate them.

Although the use of electronic documents and the technology supporting electronic documents continue to expand, their admissibility is still governed by rules of evidence that were enacted long before the inception of electronic documents. Consequently, as the court in *Lorraine* pointed out, litigants who wait until the time of trial to start thinking about whether an electronic document is admissible into evidence in a court proceeding may find that it is already too late because the company will not be able to properly authenticate the electronic documents, which is a condition for their admissibility.

Conclusion

Certain measures must be implemented at the inception of the electronic transaction to ensure the validity of an electronic signature, agreement or any other electronic document or record, and to ensure their admissibility in court in the event litigation concerning the agreement is required. For instance, in the event the agreement is evidenced by an email, the counter-party to the agreement should be required to attach his or her signature to the email (which could even be a manually typed name), rather than simply rely on the signature that is automatically generated on the email. In addition, the counter-party’s knowledge of, and intent to be bound by the terms of the agreement must be evidenced, such as through a click-wrap agreement. Online terms that are to be incorporated into the agreement should be specifically identified. They should also be made available to the counter-party, such as by providing the counter-party with both access to the full website where the terms and conditions can be downloaded, and also with a hard copy of the online terms. The agreement should also explicitly state that it is to be governed by those online terms and conditions. Finally, adhering to *Lorraine*’s requirement of verifying the identity of an electronic signatory, creating an audit trail for the entire transaction, and securely archiving and ensuring retrievability of the electronic document, and the Ninth Circuit Bankruptcy Appellate Panel’s requirements for admissibility in the *American Express* case, will increase the likelihood that electronic documents will ultimately be admitted into evidence in any litigation.

Credit professionals considering utilizing electronic credit applications, terms and conditions, and contracts must be cognizant of the requirements for their enforceability and admissibility into evidence in a court proceeding. Otherwise, they will be confronted with the ultimate horror scenario of being unable to enforce their contracts and collect their claims.

Bruce S. Nathan, Partner in the firm's Bankruptcy, Financial Reorganization & Creditors' Rights Department, has more than 30 years' experience in the bankruptcy and insolvency field, and is a recognized national expert on trade creditor rights and the representation of trade creditors in bankruptcy and other legal matters. Bruce has represented trade and other unsecured creditors, unsecured creditors' committees, secured creditors, and other interested parties in many of the larger Chapter 11 cases that have been filed, and is currently representing the liquidating trust and previously represented the creditors' committee in the Borders Group Inc. Chapter 11 case. Bruce also negotiates and prepares letters of credit, guarantees, security, consignment, bailment, tolling, and other agreements for the credit departments of institutional clients.

Bruce is co-chair of the Avoiding Powers Committee that is working with the American Bankruptcy Institute's Commission to Study the Reform of Chapter 11 and also participated in ABI's Great Debates at their 2010 Annual Spring Meeting, arguing against repeal of the special BAPCPA protections for goods providers and commercial lessors, and was a panelist for a session sponsored by the American Bankruptcy Institute ("ABI") and co-sponsored by Georgetown University Law Center.

Terence D. Watson is a member of Lowenstein Sandler's Bankruptcy, Financial Reorganization & Creditors' Rights Department. An experienced bankruptcy attorney and general commercial litigator, he represents debtors, creditors and official committees in Chapter 11 proceedings, specializing in the telecommunications, technology, manufacturing and financial services industries. Terence also has extensive experience prosecuting and defending adversary proceedings seeking the avoidance and recovery of preferential or fraudulent transfers.

The general commercial litigation aspect of Terence's practice includes advising clients on matters related to contract disputes, business torts, fiduciary duties and trade secrets in the technology, apparel, manufacturing and financial services industries.

Prior to joining Lowenstein Sandler, Terence was a Bankruptcy and General Litigation partner at two New York City law firms. Terence was raised in Tokyo, Japan and speaks conversational Japanese.