Bloomberg Law Reports® Technology Law

Enhancing the Admissibility and Enforceability of Electronically Signed Documents

Article contributed by: Gregory T. Casamento, Patrick Hatfield, and Mike Hjörleifsson

Companies in U.S. are given little guidance by the federal or state electronic signature laws on how to assure the enforceability of records signed using electronic signatures. The electronic signature laws state that electronic signatures and electronic records may not be denied legal effect solely because they are in electronic form.[1] These laws do not, however, describe or require any specific technology or process which, if followed, would result in an electronic signature on an electronic record being admissible in court or otherwise legally enforceable.[2] This creates a gap between the recognition of electronic signatures and their admissibility and enforceability.

This article introduces a six-point risk framework to help evaluate the overall effectiveness of an electronic signature process, with a particular focus on admissibility and enforceability. This article also discusses how the effective deployment of readily available technology can help improve the admissibility and, ultimately, the enforceability of electronic records signed using an electronic signature.

Because there is often confusion between the terms "electronic signature" and "digital signature," this article also explains, briefly and for purposes of the admissibility and enforceability discussion, the differences between these two terms.

Getting the Terminology Right

A brief discussion of the differences between an "electronic signature" and a "digital signature" may help readers to understand the six-point framework.

"Electronic Signature" — A Legal Term

The term "electronic signature" means "an electronic sound, symbol, or process, attached to or logically associated with a contract or other record and executed or adopted by a person with the intent to sign the record."[3] The laws across the United States recognize that an electronic signature may be made in a variety of ways, including:

- clicking "I agree";
- typing one's name into a signature block;
- selecting certain numbers on a telephone touch pad;
- proceeding through to the next page of a website;
- saying "I agree";

- using a cursor or other pointing device to manually scroll one's name on a device that captures the image (and possibly other aspects) of the image created; or
- inserting a digital representation of an individual's signature, which may or may not be cryptographic, such as a digital image of the signature or a public key infrastructure generated signature.

To be effective, the sound, symbol, or process must evidence the signer's intent to be bound to the particular terms and conditions associated with that action, and must be attributable to the specific person against whom those terms and conditions are intended to be enforced. It is the surrounding context that evidences the signer's intent to be so bound. For example, typically, there would be text above an "I agree" selection that clearly indicates that by selecting the "I agree" button, the person agrees to be bound to specified terms and conditions.

The term "electronic signature" refers to the legally significant act of a person signing a document or record to reflect the person's intent to be bound, where the signature is created and recorded electronically, rather than in wet ink and paper. In contrast, the term "digital signature," described below, refers to a particular technology of associating an entity (who could be a person or could be a device) to a given electronic record, and the securing of that record.

"Digital Signature" — A Technology Term

The term "digital signature" refers only to a particular type of technology or method, which may or may not result in a legally effective electronic signature.

In contrast to an electronic signature, a digital signature involves an arrangement that includes:

- an entity (person or device) who has been issued a digital certificate that includes private and public "keys" (essentially long strings of unique numerical codes), that are obtained from a trusted third party called a Certificate Authority or "CA";
- once affixed to a record, the digital signature renders that record nearly impossible to alter without detection and provides a way for the parties to verify that the document containing the digital signature remains valid after signature; and
- the digital signature may, if used correctly, provide a reliable method of attributing that signature to an entity agreeing to the terms and conditions expressed in the document.

Digital signatures use a technology called public-key infrastructure ("PKI"), which requires the use of two "keys," one private to the person signing in this fashion and one public (or at least available to the counterparty to the transaction using the digital signature). The public key and the private key are mathematically related, but it is infeasible to derive or guess the private key from the public key.

The term "digital signature" refers to the result of using the PKI process (the two keys) to render an electronic record virtually incapable of being altered without

detection, and associating that record with a given person or entity. A critical element of the PKI process relates to what is referred to as the "hash function." A hash value is generated from the record being digitally signed. If there is any change to the record digitally signed in this fashion, the record will not generate the same hash value generated using the original record and the private key. By comparing the hash value of the original (which was based on the record and the private key) with the hash value of a later copy of that record, one may be nearly certain whether there have been any changes to the record originally digitally signed.[4]

The recipient of the record (the counterparty to the transaction) may verify that the record received from the sender was not altered in transit by verifying the hash value of the record. This is done by the recipient generating a new hash value using the same hash function used to create the digital signature. Using the public key and the new hash result, the recipient may validate that the digital signature for that record was in fact created using the corresponding private key and that the newly generated hash value matches the original hash value. If the hash value generated by the receiving party matches the hash value generated by the sending party, the recipient can be confident that the record was not altered after the sender originally digitally signed the record.

The digital signature technology does not require the signing parties to have agreed in advance to use the digital signature process, but the party receiving a digitally signed record would need to be able to verify the signer by referring to a trusted third party. For the digital signature process to work reliably, the parties to the transaction need to be have a reliable way to associate a given signer of a record to a given public key. This is accomplished through the use of trusted third parties, known as "certification authorities." The certification authorities use recognized procedures to validate public keys and records digitally signed using this technology.

The PKI digital signature technology and related infrastructure, if properly deployed, provide a reliable means for:

- verifying that electronic records digitally signed have not been altered subsequent to being digitally signed; and
- authenticating the identity of the person signing a document using a private key.

Receiving the benefits of the PKI digital signature technology requires, as is the case with all technology, that the technology be properly deployed. For example, if public and private keys are issued to individuals without anyone actually verifying the true identity of those individuals and their affiliations and associations, the PKI digital signature technology will offer little assurance about the true identity of the person signing records using digital certificates.

The PKI technology may be used to encrypt records from being viewable by third parties as well. Maintaining the confidentiality of terms and conditions of records signed is separate and apart from the risks discussed in the six-point framework below.

Thus, the phrase "digitally sign" in the context of signing a document most likely refers to a technical process that may or may not include the required elements of a legally enforceable "electronic signature" in accordance with the law.

Electronic vs. Digital Signature

As described above, an "electronic signature" differs from a "digital signature," although a digital signature may, in some circumstances, function as an electronic signature. For a digital signature to be an electronic signature recognized by law, that digital signature must also evidence the person's intent to be bound to certain terms and conditions associated with that digital signature and be attributable to the person signing. A digital signature deployed in a process that does not properly signify or evidence the person's intent to be bound to particular terms and be attributable to a particular person or entity would not qualify as an effective electronic signature.

The digital signature technology requires the person signing to have been issued a certificate prior to signing. One should critically review the process for issuing those certificates. In particular, one should evaluate the steps taken by the trusted authority to actually authenticate the true identity of the person issued the certificate. If the trusted authority issues a certificate to any applicant without taking the appropriate steps to verify the true identity of the applicant, an imposter may be issued a certificate in the name of another person. If that certificate is used by a person to sign records claiming to be someone else, the digital signature will still be a forged signature.

In sum, it is not a certainty that a digital signature will result in specific terms and conditions being legally enforceable against the person whose name is associated with a digital signature. The process surrounding the digital or electronic signature must evidence the person's intent to be bound to those certain terms and conditions associated with such signature.

Introduction to the Risk Assessment Framework

There are six distinct risks for the electronic signature process, each of which can be examined relative to those same risks in dealing with paper and wet ink signatures. These six risks and the benefit of examining each risk in context in this fashion comprise the Six-Point Framework identified and discussed in more detail below:

- Authentication Risk — This is the risk that the signer[5] signing a record, accepting delivery of a record, or providing a record is an imposter using a false identity; the records would then be unenforceable by the user[6] against the person the user thought it was dealing with via electronic means.
- Repudiation Risk — This is the risk that the signer claims that the electronic records that were signed were altered after they were signed, such that the person against whom enforcement is sought attempts to repudiate the actual terms and conditions in the signed electronic record.
- Admissibility Risk — This is the risk that the other party to a transaction

successfully challenges the admissibility of the necessary records, such as the signed contract or acknowledgment of receipt of certain disclosures, on the grounds of reliability.

- Compliance Risk — This is the risk that the records signed or presented do not comply with other substantive laws, such as laws mandating certain content in documents to be presented or signed, or the records do not comply with the basic requirements of ESIGN and/or UETA for delivery of such records.
- Adoption Risk — This is the risk that in managing the risks above, an electronic signature process is so burdensome that the intended users are not satisfied with the process or find ways to avoid certain steps in the process, thereby undermining the process.
- Relative Risk — In examining the risks above, users should evaluate the risk with a proposed electronic signature process relative to the corresponding risk in the process using paper and a wet ink signature, in the belief that an electronic signature process may not be risk free, but should not, on the whole, be any riskier than the paper and wet ink signature process, if feasible.

For the reasons explained below, it is possible to design an electronic signature process that is no riskier than, and in some areas, significantly less risky than, using paper and a wet ink signature. By examining the risks from these perspectives, it is easier to assess the particular risk and then determine the optimal means to mitigate that risk.

Assessment and Mitigation of the Risks

Different categories of transactions present different risk profiles. For this reason, when designing an electronic signature process, one should assess the risks from various perspectives and design into the process the appropriate measures to mitigate the risk, in light of the risk tolerance of the person implementing the process for the particular documents to be signed in this fashion.

Authentication Risk

As mentioned above, Authentication Risk refers to the risk that a signer is in fact not the person he or she claims to be. A user may authenticate, or verify, the identity of each signer in various ways. Such verification steps may include confirmation of the identity of such person from a trusted source, such as a single sign-on process deployed by, or otherwise determined to be reliable by, the user. Alternatively, the results from an identity verification process conducted by an independent third party can be used for this purpose, such as a consumer reporting agency or other trusted third party offering such services. A further method can be used, such as the answer to a shared secret question that the user determines adequately verifies the identity of the signer. Having signatures notarized is another form of authentication of the identity of the signer. If there are documents required to be notarized, the electronic signature process should allow the notary verifying another signer's signature to enter the notary's signature and other credentials, in accordance with applicable state notary laws.

The method and results used to authenticate each signer should be included in the archived signing session, or audit trail, which should then be securely archived and be capable of being retrieved securely. Where the user opts not to include the authentication process in the audit trail, the user may need to have access to other reliable evidence to establish the actual identity of the person completing the transaction.

If the process is to rely on the PKI infrastructure to verify the identity of the entity signing an electronic record, one should examine the methods actually used by the trusted third parties to verify the identity of the person issued the private and public keys initially. As secure as digitally signed records may be from a non-repudiation perspective (see discussion below), there may be little or no assurance that the person using a private key to sign an electronic record is in fact who he claims to be, simply because the trusted authority issuing the digital certificates in the first instance did little to verify the person's true identify. In addition, if the identity of the person issued the digital certificate was properly validated but did little to protect the private key from unauthorized use, there may be little assurance that the person using the private key later is in fact who he claims to be.

Users should critically evaluate the likelihood of forgers, or even signers who seek to disavow a given transaction claiming that a forger signed the documents. Such evaluation should consider what motive a forger might have to forge the signature of another person in the proposed process. This evaluation may lead to the conclusion that the authentication risk is low.

At least one court has addressed the Authentication Risk.[7] In *Kerr v. Dillard Store Services, Inc.*, the employer, Dillard's, sought to enforce a mandatory arbitration agreement against Ms. Kerr, Dillard's employee. The issue was whether Ms. Kerr did in fact electronically sign the electronic agreement containing mandatory arbitration provisions. The court was persuaded that Ms. Kerr did not sign the record containing the mandatory arbitration provisions, in large part because Ms. Kerr's supervisor had access and the opportunity to sign such record using Ms. Kerr's credentials. Had Ms. Kerr's supervisor not had such access to Ms. Kerr's user name and ability to change her password to obtain access to the secure site where the record in question was presented for signature, the court may have reached a different conclusion.

Repudiation Risk

Repudiation Risk refers to the risk of a signer acknowledging he or she signed a document, but claiming that the electronic signature is attached to or logically associated with a document containing terms and conditions different than those in the signed document. The risk is that the signer repudiates the terms and conditions in the document attached to or logically associated with his or her signature and thereby reduces the chance that the document will be admissible and, even if admitted into evidence, that the trier of fact will be persuaded that the signer did in fact agree to be bound by all such terms and conditions.

The PKI digital signature technology can render a record unalterable and eliminate the chance that the record will be later revealed to have been altered. In other

words, the PKI digital signature technology allows one to state with confidence that because the hash values for the original record (which may contain terms and conditions associated with an electronic signature) match those in a later copy of that record, it is infeasible the later record could have been altered. Regardless of the form of electronic signature, the electronic record signed using the chosen method, i.e., by clicking "I agree" or using a signature pad, should be digitally signed using the PKI technology. Doing so can reduce the repudiation risk far below the repudiation risk associated with paper documents and wet ink signatures.

Immediately after signing, each electronic record should be digitally signed, thereby rendering it infeasible that the record containing the terms and conditions, as well as the electronic signature, could be altered without detection. Records digitally signed in this fashion are likely to pass the admissibility threshold (see discussion below), and once such records are admitted into evidence, users are likely to have meaningful, persuasive evidence as to why that record could not have been altered without detection.

The digital certificate provided with the digital signature process should be stored to ensure that verification can be performed again at a later time. The audit trail for each transaction should include each document presented and signed during a given transaction where each such document has been signed as described above. Relevant parts of the audit trail should also be digitally signed to render those portions of the audit trail unalterable without detection.[8]

Admissibility Risk

Admissibility Risk is the risk that a court refuses to admit into evidence copies of electronic documents generated, presented, signed, secured, archived, and retrieved by the electronic signature process. All of the rules of evidence and evidentiary foundations that apply to paper documents and wet ink signatures also apply to documents signed electronically, stored electronically and retrieved electronically.

The Federal Rules of Evidence, or their state equivalents, govern the admissibility of evidence and thus govern the admissibility of a copy of a document presented, signed, secured, archived, and retrieved by the electronic signature process.[9] The electronic signature process should satisfy the admissibility standards in the Federal Rules to prove the authenticity of a document if the electronic signature process creates a reliable record of the entire signature process, including:

- the terms and conditions presented to the signer with which the electronic signature will be logically associated;
- the specific act of the signer expressing his or her intent to be bound to those terms and conditions; and
- the circumstances under which the electronic signatures were obtained.

This information all goes to establish the authenticity of the document containing the terms and conditions retrieved by the electronic signature process. The electronic signature process should enable users to securely archive and retrieve the

documents in a way to show that the documents containing the signatures could not have been altered without detection. The electronic signature process should also enable the appropriate witness on behalf of the user to provide an affidavit or live testimony as to items (a)—(c) above. For the reasons described below, such copies of documents generated by the electronic signature process based on documents presented, signed with an effective electronic signature, secured using a digital signature process, archived, and retrieved by the electronic signature process should be as admissible under the Federal Rules as such documents containing the same terms and conditions generated, presented, and signed in hard copy and wet ink signature, where such paper copy is secured, archived, and retrieved using conventional archival and retrieval methods.[10]

The standard for the authentication of evidence under the Federal Rules of Evidence is contained in Rule 901, Requirement of Authentication or Identification, which provides that "the requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."[11] As stated throughout the case law regarding the admissibility of computer generated information, "[r]eliability must be the watchword" in determining the admissibility of computer generated evidence.[12] The "factors [must] effectively address a witness' familiarity with the type of evidence and the method used to create it, and appropriately require that the witness be acquainted with the technology involved in the computer program used to generate the evidence."[13]

Certain Subsections of Rules 901 and 902 are particularly suited to address the admission of electronic signatures and records: 901(b)(1), (3), (4), and (9), and 902(7) and (11). While Rules 901(b)(1), (3), (4), and (9) require witness testimony to authenticate proffered evidence, Rules 902(7) and (11) allow for self-authentication. Magistrate Judge Paul W. Grimm's opinion in *Lorraine v. Markel American Insurance Co*. provides one of the best analyses to date of the admissibility of electronic evidence, which broadly could include electronic signatures.[14] In addition to the express provisions of Rule 901(b)(9) discussed above, Imwinkelried's Evidentiary Foundations provides an eleven-step process under the Rule for the admission of computer generated records.[15]

Critical in the analysis of admissibility and the overall enforceability of documents executed using a given electronic signature process is the requirement of a secure method to archive and retrieve the documents so they cannot be altered after signature. In addition to the method or process, there must be a credible person called by the user who is suitably qualified to explain the process, including that:

- the documents submitted to enforce the transaction are true, accurate, and complete hard copies of each document signed by each signer that accurately reflect what the signer was presented in connection with each signer using the electronic signature process;
- the electronic signature process generates a true, accurate, and complete hard copy of the audit trail for each transaction; and
- the documents submitted to enforce the transaction were generated from electronic records that were cryptographically signed in such a way that each

record, as accurately represented by such hard copies, could not have been altered without detection, in the absence of a person using supercomputing power to break the signing method used, currently thought to require several years of such supercomputing power.

Users should consider who would be qualified, willing, and able to testify on the above items in designing the electronic signature process.

Compliance Risk

The electronic signature process should assure that:

- each document presented or signed by a signer complies with the legal requirements for the content, presentation, sequence, and information to be obtained for each such document;
- for certain consumer disclosures required by law to be given in writing, the signer is provided the appropriate information to make the informed consent in compliance with the consumer disclosure requirements of ESIGN, where such consumer disclosure will be provided exclusively via electronic means;
- each document required to be presented and signed is in fact presented and signed as required by law governing the particular transaction; and
- The significance of each step in the signature process (whether on an acknowledgement of receipt, unilateral consent, application for goods or services, or contract) is abundantly clear to each signer.

The audit trail should record each step required to meet the regulatory requirements, such as the sequence and timing of presenting certain forms and the actual contents of records presented. By using an electronic signature process with an audit trail containing reliable, admissible evidence that each step was taken using the required content, a user may reduce the compliance risk considerably lower that the risk in transactions using paper and wet ink signatures.

The courts have been presented with a variety of disputes where a person alleged to have electronically signed a record disputes having signed the record. Where the significance of the steps involved in signing a particular record was made adequately clear to the person challenging the enforceability, the courts have enforced the electronic signature process. Where the significance was not sufficiently clear to the challenger, the courts have not enforced the terms against the challenger.[16]

Adoption Risk

The Adoption Risk refers to the risk that the electronic signature process, in an attempt to reduce the authentication, repudiation, compliance, and admissibility risks, is overly burdensome, such that the intended signers do not use the process or find alternatives that undermine the overall effectiveness of the proposed electronic signature process. This risk can, and should be, managed by conducting a series of pilot (or beta) tests before introducing the electronic signature process to potential signers for the user. By conducting such tests, the user can obtain feedback from the

signers and make the appropriate adjustments to reduce this risk when the process is fully launched.

Relative Risk

As noted throughout this article, the risks of a given electronic signature process should be considered relative to the risks associated with a paper and wet ink signature. This allows the user to better assess the risks inherent in the particular electronic process. It is often easy to configure the electronic signature process to reduce the risks considerably below the corresponding risks of using paper and a wet ink signature. For example, the electronic signature process can be configured to prevent a record from being signed if there are any blanks or otherwise incomplete responses in the record. The process is also able to prevent any document relating to a transaction from being submitted to the user or by the user unless all the required steps, including execution or acknowledgement of receipt of all consumer disclosures, are provided and acknowledged, and then once signed, securing documents through the digital signature process to prevent those documents from being altered without detection. This can significantly reduce the compliance risk below that for paper and wet ink signatures.

Conclusion

The overall effectiveness of a given electronic signature process depends on how well the user determined the means to mitigate the risks for particular documents and records to be presented, signed, and archived. The user who carefully considers the risks associated with the types of transactions to be processed can design and implement an electronic signature process that is no riskier than, and in most cases less risky than, the same transaction using paper and a wet ink signature. Doing so provides greater confidence that the electronic signature, when affixed within the United States, will be admissible into evidence and enforceable.

From the court decisions to date, there appears to be a premium placed on making it very clear to the person against whom enforcement is sought the significance of the act that affixes the electronic signature. The clearer the significance to the person signing, the more likely courts are to enforce the electronic signature.

It is to be expected that as the significance of actions comprising the electronic signature are made clearer, persons aiming to avoid obligations in signed agreements will look for other ways to avoid liability, such as challenging the admissibility of the electronic records for various reasons. The framework described in this article should help companies critically evaluate those risks with the aim of determining what measures to implement that are appropriate within the risk assessment profile discussed in this article.

Gregory T. Casamento is a Partner based in the New York office of Locke Lord Bissell & Liddell. He practices in the area of electronic commerce, intellectual property and related litigation matters, including e-discovery and e-admissibility. He can be reached at gcasamento@lockelord.com.

Patrick J. Hatfield is a Partner based in the Austin office of Locke Lord Bissell & Liddell, and co-chair of the Firm's Technology Transactions Section. He practices in the electronic commerce, intellectual property, and technology areas. He can be reached at phatfield@lockelord.com.

Michele (Mike) Hjörleifsson has been a technologist since the Apple][+, implementing network and remote access security technologies since the early '90s. He has worked with the nation's largest corporations and government institutions, as well as authoring white-papers, technical magazine articles, and topical discussions at IETF (Internet Engineering Task Force), and other organizations on security topics and podcasting with Apple Podcast Producer. He is currently working with companies worldwide on Apple and PKI Security consulting for PrimeKey Solutions A.B in Stockholm. He can be reached at mikeh@primekey.se.

---

[1] The two bodies of laws are the federal act, the Electronic Signatures In Global and National Commerce Act (ESIGN), 15 U.S.C. § 7001 et seq, and the various state enactments of the version of the Uniform Electronic Transactions Act (UETA), as published by the National Conference of Commissioners on Uniform State Laws. 47 states and the District of Columbia have enacted some version of UETA.

[2] Enforcement of the electronic signature will not, however, overcome terms and conditions otherwise unenforceable for reasons having nothing to do with the electronic signature process, such as a court finding terms unconscionable or ambiguous.

[3] 15 U.S.C. § 7006(5).

[4] The recipient of the record (the counterparty to the transaction) may verify that the record received from the sender was not altered in transit by verifying the hash value of the record.

[5] The term "signer" refers to the person, often a consumer, signing the electronic record, whether the record is a contract, application, consent, authorization, or acknowledgement of receipt of terms.

[6] The term "user" refers to the person, often a company, that has established the electronic signature process for enforceable and compliant transactions.

[7] *See Kerr v. Dillard Store Services, Inc.*, 2009 BL 30588 (D. Kan. Feb. 17, 2009).

[8] The reader should be aware of the long-term viability of digital signatures when archiving digital documents protected by a digital signature. *See* Stefanie Fischer-Dieskau and Daniel Wilke, *Electronically Signed Documents: Legal Requirements and Measures for Their Long-term Conservation*, DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW, 3, 40–44 (2006).

[9] Many states have adopted rules of evidence that track the Federal Rules of Evidence. For purposes of this discussion, all cases cited are based on the Federal Rules or state law that follows the Federal Rules.

[10] This would require the user to identify who, by name and title, is qualified to testify (in person or via an affidavit) as to how each document was presented, signed, secured after signature to render it unalterable without detection, archived, retrieved, and printed. This person will also testify as to the integrity and security of each system involved in creating, securing, archiving, retrieving, and printing the document.

[11] Fed. R. Evid. 901(a). *See also Lorraine v. Markel American Insurance Co.*, 241 F.R.D. 534, 541–42 (D. Md. 2007).

[12] *State v. Swinton*, 268 Conn. 781, 812 (2004) (applying the federal standard to a state case).

[13] *Id.* at 813–14.

[14] *Id.*

[15] Edward J. Imwinkelried, *Evidentiary Foundations*, 58–59 (LexisNexis 6th ed. 2005). The list provides: (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 readout certain data; (7) the witness used the proper procedures to obtain the readout; (8) the computer was in working order at the time the witness obtained the readout; (9) the witness recognizes the exhibit as the readout; (10) the witness explains how he or she recognizes the readout; and (11) if the readout contains strange symbols or terms, the witness explains the meaning of the symbols or terms for the trier of fact. *See also* Stephen Mason, *Electronic Evidence: Disclosure, Discovery & Admissibility*, 4.23 (LexisNexis Butterworths, 2007), for further comments on Professor Imwinkelried's list.

[16] For example, see *Bell v. Hollywood Entertainment Corp.*, 2006-Ohio-3974 (Ohio Ct. App. 2006), where the court enforced a mandatory arbitration provision against an executive of the defendant employer. The court found that it was sufficiently clear to the executive what the consequences were of selecting "yes" in the electronic signature process. See also *Brueggemann v. NCOA Select, Inc.*, No.08-80606-CIV, 2009 BL 139993 (S.D. Fla. June 29, 2009), where the court enforced an electronic signature comprised of the process of continuing to use the website where the significance of proceeding was made sufficiently clear to a consumer purchasing consumer goods. In contrast, see *Campbell v. General Dynamics Gov't Systems Corp.*, 407 F.3d 546 (1st Cir. 2005), where the court concluded that the significance of not objecting to the terms was not sufficiently clear, and the court refused to enforce the mandatory arbitration terms against the employee.