

The Electronic Signatures In Global and National Commerce Act: A Fidelity Bond Professional's Guide to E-Sign

Michael Keeley
Theresa Gooley
Stuart Kasiske

I. Introduction

The technology of commercial business transactions is rapidly evolving. As computer hardware and software applications continue to advance, the efficiency and economy of utilizing these new technologies will play an even greater role in the international business infrastructure. In an effort to keep pace with this changing environment, the United States Congress enacted the Electronic Signatures In Global and National Commerce Act¹, which became effective on October 1, 2001.

The fundamental goal of E-Sign is to ensure that most commercial transactions will not be denied effect solely because they are executed with an electronic, rather than a conventional "pen and ink," signature. An unintended, but nevertheless real, consequence of E-Sign is the availability of yet another instrument of crime for dishonest employees and other thieves. The immediate question for many fidelity bond underwriters, risk managers, claims handlers and attorneys is how E-Sign, and the resulting increase in electronic crime, will impact them in the short term.

This article discusses the important aspects of E-Sign about which a fidelity bond professional should have at least general familiarity. This discussion is not intended to constitute an exhaustive analysis of the statute, nor the effect of e-commerce on the fidelity bond industry or commercial litigation in general. With these disclaimers in mind, Part II of this article examines the background of E-Sign and other e-commerce legislation. Part III considers some of the primary evidentiary, practical and procedural issues surrounding E-Sign. Finally, part IV analyzes E-Sign in the context of the primary insuring agreements of the standard form Financial Institutions Bond² and the Commercial Crime Policy.³

¹ 15 U.S.C. §§ 7001 – 7031 (2001) [hereinafter E-Sign].

² Financial Institution Bond, Standard Form No. 24 (Revised Jan. 1986) [hereinafter FIB], reprinted in STANDARD FORMS OF THE SURETY ASSOCIATION OF AMERICA (Surety Ass'n of Am. 1995).

³ Commercial Crime Policy, ISO Form, Coverage Form (A) (Revised 1986) [hereinafter CCP], reprinted in MILLER'S STANDARD INSURANCE POLICIES ANNOTATED (Legal Research Systems, Inc. 1995).

Michael Keeley is a partner, and Stuart Kasiske is an associate, with Strasburger & Price, L.L.P., in Dallas, Texas. Theresa Gooley is a Claims Attorney with The St. Paul Insurance Companies in St. Paul, Minnesota. The opinions expressed in this article are those of the authors and are not necessarily shared by The St. Paul Companies or Strasburger & Price, L.L.P.

II. Background of E-Sign and Other E-Commerce Legislation

Contrary to popular belief, E-Sign was not created overnight. Rather, a number of legal and technological developments over the last decade prompted the legislation. Specifically, the significant increase in global electronic commerce and the proactive stances taken by various state and foreign governments created a perception among the Executive and Legislative branches of the United States government that some semblance of uniformity was a worthy and necessary objective.

A. THE INCREASING SIGNIFICANCE OF ELECTRONIC TRANSACTIONS

Electronic commerce is rapidly redefining this nation's economy. For example, a recent study found that 55% of companies indicated that they would increase e-business spending by an average of 4.4% in 2003, despite current economic concerns.⁴ The same study found that e-business budgets are expected to account for a higher percentage of most companies' overall technology budgets, at 26.8% of IT spending in 2003, up from an average 18.0% in 2002.⁵

Businesses want to contract electronically for practical reasons, such as more efficient transactions and reduction of paperwork.⁶ Moreover, electronic contracting can save money. Banks and other large companies can store their electronic contracts on computer hard drives instead of in vaults. The insurance industry also has predicted a big financial boost from electronic contracting.⁷ Likewise, after the Department of Education started allowing college students to process their student loans online in July of 2001, more than 330,000 loans were processed in the first year. This amount is expected to triple once the number of schools using the program and the public's general awareness of the program increases.⁸

Consumers also will account for a substantial increase in e-commerce. For example, the first person to purchase a home with a paperless mortgage completed the transaction in less than three hours, compared with the average of forty-five days normally required to process a paper mortgage.⁹ Both the consumer and the lender accordingly can save substantial administrative costs, as well as valuable time, in the home buying process. As a result, many of today's business and individual consumers

⁴ See Steve Butler, *Looking Ahead to E-Business in 2003*, at <http://www.emarketer.com/news> (August 26, 2002).

⁵ *Id.*

⁶ See Tom Fowler, *Digital Signatures to Allow Distribution of Documents Online, Cutting Time Needed to Complete Transactions/A Signature Moment*, HOUS. CHRON., Oct. 8, 2000, at 2000 WL 24516917.

⁷ See *Landmark E-Sign Law, Boon for Business, Starts Oct. 1*, CONGRESSDAILY/A.M., Sept. 26, 2000 at 2000 WL 24187519. Of note, E-Sign's restrictions on cancellation of life and health insurance policies should not affect other forms of insurance, such as fidelity bonds.

⁸ This information was provided by David Whitaker, a partner with the Washington, D.C. office of Godwin Proctor, LLP. The authors wish to thank Mr. Whitaker for this factoid and a plethora of additional insight into E-Sign from the perspective of a seasoned electronic commerce litigator.

⁹ See Kate Marquess, *Sign on the Dot-Com Line: Electronic Signature Act Facilitates Commerce Over the Net*, 86 A.B.A. J. 74 (Oct. 2000).

simply are not concerned about the security issues, authenticity problems and perceived lack of formality in electronic transactions that trouble many attorneys. Thus, even those attorneys who previously were unwilling or simply not prepared to join the world of electronic commerce have little choice after E-Sign.

B. THE DEVELOPMENT OF ELECTRONIC COMMERCE LEGISLATION

1. The Three Types of Electronic Signature Legislation

Governments traditionally have favored three distinct approaches to incorporating electronic contracts into their overall scheme of law.¹⁰ First, some governments have designated one particular technology, usually digital signature technology, as the only method of creating an enforceable electronic contract. This has been termed the "prescriptive" approach.¹¹ Legislation passed in the State of Utah often is cited as an early example of this approach. The biggest problem with the prescriptive approach is that it does not change with technology and inhibits those persons without access to the specified technology.

A second approach, labeled the "two-tiered" approach,¹² similarly grants electronic contracts the same enforceability as written contracts but also affords electronic contracts conducted via digital signature technology a presumption of evidentiary validity. This approach recently was adopted in a directive by the European Union, and generally is well regarded by legal scholars and e-commerce attorneys. However, it requires slightly more governmental regulation than the third approach discussed below.

Under the third approach to e-commerce, also known as the "minimalist" approach,¹³ still other governments have enacted legislation that seeks only to place electronic contracts on par with written contracts, affording them the same recognition of enforceability without regard for the technology used to create the electronic contract. This approach has the advantage of being technology neutral, and requires only limited governmental involvement at the federal level.¹⁴ The most glaring concern with the minimalist approach is that it has less stringent requirements for enforcing electronic signatures.¹⁵

E-Sign adopts the minimalist approach to electronic signature legislation. However, professionals should be cognizant of the two other types of e-commerce

¹⁰ See generally Jennifer L. Koger, Note, *You Sign, E-Sign, We All Fall Down: Why the United States Should Not Crown the Marketplace as Primary Legislator of Electronic Signatures*, 11 *TRANSNAT'L L. & CONTEMP. PROBS.* 491, 503-07 (Fall 2001).

¹¹ See Internet Law & Policy Forum, *Survey of International Electronic Digital Signature Initiatives* (1998), available at <http://www.ilpf.org/groups/survey.htm> (last visited Aug. 24, 2002).

¹² *Id.*

¹³ *Id.*

¹⁴ See Michael J. Hays, Note, *The E-Sign Act of 2000: The Triumph of Function over Form in American Contract Law*, 76 *NOTRE DAME L. REV.* 1183, 1200 (June 2001).

¹⁵ See Jonathan E. Stern, *The Electronic Signatures in Global and National Commerce Act*, 16 *BERKELEY TECH. L.J.* 391, 406 (2001).

legislation, particularly when dealing with governmental entities, international businesses and claims involving the substantive law of multiple states.

2. Electronic Commerce Legislation in the United States

The first unified efforts to facilitate the use of electronic commerce in the United States was in the early 1990s, when the American Law Institute,¹⁶ together with the National Conference of Commissioners on Uniform State Laws,¹⁷ sought to amend the Uniform Commercial Code,¹⁸ creating a new vocabulary where documents would be “authenticated,” not just “signed,” and a “record” would be created instead of a “writing.”¹⁹ Eventually, this reform effort lost the support of the ALI, and the NCCUSL decided to title the proposed amendments the Uniform Computer Information Transactions Act²⁰ and seek adoption through each state legislature.²¹ These efforts were unsuccessful, but the UCITA ultimately was created and now is used for purchases of computer software and similar applications.²²

Also in the 1990s certain states began their own efforts to legislate electronic commerce. Utah was the first state to do so in 1994, adopting a technology specific framework that focused on digital signatures.²³ Certain states such as Mississippi²⁴ and New Mexico²⁵ followed form with Utah, while others adopted a technology neutral statute.²⁶ Still other states enacted very narrow statutes authorizing electronic communications in only certain specific situations.²⁷ Still other states combined these approaches or did nothing at all.

As a result of the inconsistent approach taken by the various states, the NCCUSL once again undertook to produce a uniform law with the intent to provide the electronic commerce world with some level of statutory uniformity on a national level. The result was adoption of the Uniform Electronic Transactions Act.²⁸ UETA is an “overlay”

¹⁶ Hereinafter ALI.

¹⁷ Hereinafter NCCUSL.

¹⁸ Hereinafter U.C.C.

¹⁹ See Michael H. Dessent, *Digital Handshakes in Cyberspace under E-Sign: “There’s a New Sheriff in Town!”* 35 U. RICH. L. REV. 943, 946 (January 2002).

²⁰ Hereinafter UCITA.

²¹ See David G. Mayhan & Patricia A. Fennelly, *The Uniform Computer Information Act: Ready or Not, Here it Comes*, COLO. LAW., Dec. 28, 1999, at 63.

²² See generally Dessent, *supra* note 19, at 947-48.

²³ See UTAH CODE ANN. §§ 46-3-201 – 46-3-504 (1998).

²⁴ Mississippi Digital Signature Act of 1997, MISS. CODE. ANN. §§ 25-63-1 – 23-63-11 (1999).

²⁵ New Mexico Electronic Authentication of Documents Act, codified at N.M. STAT. ANN. §§ 14-15-1 – 14-15-6 (Michie 1999); see also Minnesota Electronic Authorization Act, codified at MINN. STAT. ANN. § 325(k) (West 2000); Missouri Digital Signature Act, codified at MO. ANN. STAT. §§ 28.600 – 28.684 (West 2000); Washington Electronic Authentication Act, codified at WASH. REV. CODE. ANN. §§ 19.34.010 – 19.34.010 (West 2000).

²⁶ See Oklahoma Electronic Records and Signatures Act of 1998, codified at OKLA. STAT. ANN. tit. 15, § 1960-68 (West 2000); S.B. 525, 100TH Gen. Assembly (Tenn. 1997), codified at TENN. CODE. ANN. §§ 1-3-105, 29-2-101; VA. CODE ANN. ANN. §§ 1-13-32 and 2.1 – 7.4 (Michie 2000).

²⁷ See, e.g., Alabama Electronic Tax Return Filing Act, codified at ALA. CODE §§ 40-30-1 – 40-30-6 (2000) (authorizing the filing of electronic tax returns).

²⁸ Hereinafter UETA.

statute which permits any legal requirement for a writing or signature to be replaced with an electronic equivalent, while leaving existing law in place. UETA is procedural, as opposed to substantive.

The essential rules of UETA are straightforward. First, a record or signature cannot be denied legal effect solely because it is in electronic form.²⁹ And, a contract cannot be denied legal effect simply because an electronic record was used in its formation. If a law requires a record to be in writing, an electronic record satisfies the law.³⁰

UETA is technology neutral. It does not require the use of any specific type of security procedure. Thus, contracting parties may use whatever type of signature technology security procedures they wish.

The use of electronic transactions or signatures under UETA is wholly voluntary.³¹ UETA applies only where each party to an agreement has agreed to conduct the transaction in electronic form.³² UETA also allows parties to vary or disclaim various provisions of the Act by agreement.³³

Finally, certain transactions are excluded from UETA, including those governed by the U.C.C. (except transactions governed by articles 2 and 2a in sections 1-107 and 1-206), the Uniform Computer Information Transactions Act, laws governing estates and trusts, and other laws identified by any state adopting UETA.³⁴

By the time E-Sign was enacted in June 2000, eighteen states had enacted UETA, and it was under consideration in eleven others. Nevertheless, the financial services and high-tech industries lobbied Congress to act, primarily because of the modifications being made to the text of UETA by the states that were adopting it, and due to concerns about the length of time it would take before UETA was adopted nationwide.³⁵ Thus, industry groups lobbied Congress to follow UETA as a model for a federal statute. As a result, President Clinton formally signed E-Sign into law in June 2000. Interestingly, after signing the Act first with a pen, as is required by statute, President Clinton then used a signature card to electronically approve the act.³⁶

As with UETA, E-Sign is an overlay statute which validates electronic contracts affecting interstate or foreign commerce, and provides that a contract relating to such a transaction may not be denied legal effect solely because an electronic signature or record

²⁹ *Id.* § 2(13).

³⁰ *Id.* § 7.

³¹ *Id.* § 5(a).

³² *Id.* § 5(b).

³³ *Id.* § 5(d).

³⁴ *Id.* § 3.

³⁵ Robert A. Wittie & Jane K. Winn, *Survey: Electronic Records and Signatures Under the Federal E-Sign Legislation and the UETA*, 56 BUS. LAW 293, 296 (Nov. 2000).

³⁶ See Bill Zoelick, *Wide Use of Electronic Signatures Awaits Marked Decisions About the Risks and Benefits*, 72 N.Y. ST. B.J. 10, 11 (2000).

was used in its formation.³⁷ Many of the important provisions of UETA were carried over into E-Sign, including its technology neutral stance, its voluntary format, and its recognition of underlying state laws. On the other hand, many provisions of UETA were not carried over to E-Sign, and conversely, E-Sign contains certain provisions, such as consumer consent requirements, that vary significantly from UETA.

C. LEGISLATIVE INTENT BEHIND E-SIGN

E-Sign's coverage of electronic transactions is intentionally broad. Congress has recognized that “the promotion of growth in private sector electronic commerce through federal legislation is in the national interest because that market is globally important to the United States.”³⁸ Thus, E-Sign is intended to encompass both interstate and foreign commerce. Congress summarized the purposes of E-Sign as follows:

1. to permit and encourage the continued expansion of electronic commerce through the operation of free market forces rather than proscriptive governmental mandates and regulations;
2. to promote public confidence in the validity, integrity, and reliability of electronic commerce and online government under federal law;
3. to facilitate and promote electronic commerce by clarifying the legal status of electronic records and electronic signatures in the context of writing and signing requirements imposed by law;
4. to facilitate the ability of private parties engaged in interstate transactions to agree among themselves on the terms and conditions on which they use and accept electronic signatures and electronic records; and
5. to promote the development of a consistent national legal infrastructure necessary to support electronic commerce at the Federal and State levels within existing areas of jurisdiction.³⁹

Hearings during the United States legislature's consideration of E-Sign indicate widespread approval of the legislation's technology-neutral stance.⁴⁰ Two primary arguments were set forth in support of technology-neutral legislation. First, the electronic signature technology of today might not prevail tomorrow.⁴¹ In all likelihood, no single electronic signature technology will prevail, meaning that there may be different technologies for different uses. Thus, putting too much time into developing

³⁷ 15 U.S.C. § 7001(a).

³⁸ See H.R. Rep. No. 106-341, pt. 2, at 2 (1999).

³⁹ *Id.* at 2-3.

⁴⁰ See Koger, *supra* note 10, at 507. Of note, E-Sign's legislative history included lobbying efforts by businesses, consumers, governmental agencies, and even the judiciary. The American Bankers Association was one of several vocal lobbyists in favor of the legislation. See Mark Ballard, *E-Sign a Nudge, Not a Revolution: Oct 1 is a Big Day, But State, Business Have Work to Do*, NAT'L L.J., Sept. 25, 2000, at B1.

⁴¹ See Koger, *supra* note 10, at 507.

infrastructure around a single electronic signature technology could prove counterproductive. Second, there was concern that legislating for one technology would impede international regulatory uniformity.⁴² As summarized by two members of Congress, "This act is intended to operate very broadly to permit the use of electronic signatures and electronic records in all business and consumer contexts."⁴³

D. KEY PROVISIONS OF E-SIGN

1. General Rule of Validity

The heart and soul of E-Sign is that electronic signatures, contracts or records relating to transactions in, or affecting, interstate or foreign commerce "may not be denied legal effect, validity, or enforceability solely because [they are] in electronic form."⁴⁴ E-Sign also states that, "a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation."⁴⁵ More specifically, section 7001 of E-Sign provides as follows:

- (a) In General. Notwithstanding any statute, regulation, or other rule of law (other than this title and title II [15 U.S.C.S. §§ 7001, *et seq.* and 15 U.S.C.S. 7021]), with respect to any transaction in or affecting interstate or foreign commerce –
 - (1) A signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and
 - (2) A contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.

As with the UETA, while E-Sign invalidates state and federal writing and signature requirements, it does not alter the underlying substantive law applicable to a transaction.⁴⁶ Also as with UETA, both the use and acceptance of electronic transactions is wholly voluntary. E-Sign provides that, except for certain governmental transactions, the act does not "require any person to agree to use or accept electronic records or electronic signatures."⁴⁷ And, other than certain required consumer consents, E-Sign does not affirmatively require that there be an agreement to use or accept electronic records or signatures in order for them to be valid. Instead, E-Sign's rule is negative,

⁴² *Id.* at 507-8.

⁴³ 146 Cong. Rec. S5282 (daily ed. June 16, 2000) (colloquy between Sens. Gramm and Abraham).

⁴⁴ See 15 U.S.C. § 7001(a)(1).

⁴⁵ *Id.* § 7001(a)(2).

⁴⁶ Wittie & Winn, *supra* note 35, at 298.

⁴⁷ 15 U.S.C. § 7001(b).

providing only that parties are not required to use or accept them.⁴⁸ By specifying that the use and acceptance of electronic records and signatures is voluntary, E-Sign preserves the ability of individuals to agree to limitations on, or adopt specific criteria for, their use. The voluntary requirement of the statute is satisfied if the party assents to the use of electronic signatures and records or manifests behavior consistent with acceptance.⁴⁹

E-Sign contains significant protection requirements concerning consumer disclosures and retention of accurate records when electronic signatures are involved.⁵⁰ E-Sign helps to ensure that consumers are informed about the contents and the form of the electronic record, and that consumers consent to the use of electronic records in their individual transactions. For example, many existing statutes require information concerning transactions in or affecting interstate commerce to be provided or made available to a consumer in writing. Under E-Sign, an electronic record can be provided in place of a written record if the consumer consents and is provided with a "clear and conspicuous statement" informing the consumer of certain rights.⁵¹

Notwithstanding E-Sign's general rule of validity, the statute provides that, if a statute, regulation, or other rule of law requires a contract or other record to be in writing, the legal effect and enforceability of an electronic record of such contract or other record may be denied if "such electronic record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or persons who are entitled to retain the contract or record."⁵²

Interestingly, E-Sign provides that it was the "specific intent of the Congress" that E-Sign apply to the business of insurance.⁵³ It further provides, however, that an insurance agent or broker acting under the direction of a party that enters into a contract by means of an electronic record or signature may not be held liable for any deficiency in the electronic procedures agreed to by the parties if: (1) the agent or broker has not acted in a negligent, reckless, or intentionally tortuous manner; (2) the agent or broker is not involved in the development or establishment of such electronic procedures; and (3) the agent or broker did not deviate from such procedures.

2. Technology-Neutral Format

As noted previously, E-Sign and UETA are technology-neutral. E-Sign's technology-neutral stance received wide-spread approval during Congressional hearings.⁵⁴ Three main arguments were made in favor of this technology-neutral approach.⁵⁵ First, the electronic signature technology of today might be outdated

⁴⁸ *Id.* § 7001(b)(2).

⁴⁹ *Id.* § 7001(c).

⁵⁰ See Carl Carl *et al.*, Note, *eCOMMERCE: Are Online Business Transactions Executed by Electronic Signatures Legally Binding?* 2001 DUKE L. & TECH. REV. 5 (February 28, 2001).

⁵¹ See 15 U.S.C. § 7001(c)(1)(A) & (B).

⁵² *Id.* § 7001(e).

⁵³ *Id.* § 7001(f).

⁵⁴ See Koger, *supra* note 10, at 507.

⁵⁵ *Id.*

tomorrow.⁵⁶ Thus, the time and expense necessary to develop an infrastructure for today could be worthless tomorrow. Thus, proponents of E-Sign argued that the law should remain neutral enough to accept any technology that the market develops.⁵⁷ Second, corporate lobbyists testified that technology neutrality “fosters innovation, whereas regulating specific technologies inhibits the marketplace from continuing to develop more effective technologies than current E-Sign technology.”⁵⁸ Finally, supporters expressed concern that adopting one technology would “impede international regulatory uniformity.”⁵⁹

3. Specific Exceptions

E-Sign expresses particular sensitivity to consumer protection issues. It includes specific exceptions for certain documents and transactions that, for important public policy reasons, mandate a hard copy of a document and/or signature. For instance, E-Sign does not apply to state statutes governing the creation and execution of wills, codicils, or testamentary trusts; adoption, divorce, or other matters of family law; or the Uniform Commercial Code, as in effect in any state, other than sections 1-107 and 1-206, and Articles 2 and 2A.⁶⁰

Also for public policy reasons, the provisions of E-Sign do not apply to any cancellation or termination of utility services; certain real estate default and repossession issues; the cancellation or termination of health insurance or benefits or life insurance benefits; recall or material failure of a product that endangers public health or safety; and any document required to accompany any transportation or handling of toxic or dangerous materials.⁶¹ Additionally, E-Sign provides that it does not apply to “court orders or notices, or official court documents (including briefs, pleadings, and other writings) required to be executed in connection with court proceedings.”⁶²

4. Transferable Records

Congress included a separate provision in E-Sign to help facilitate the use of electronic promissory notes in connection with the real estate market, and specifically the

⁵⁶ *Id.*

⁵⁷ *Id.*

⁵⁸ *Id.* at 508.

⁵⁹ *Id.*

⁶⁰ *Id.* § 7003(a)(1)-(3). While some have argued that E-Sign accordingly has little impact on the U.C.C., this view is somewhat myopic. As pointed out by David Whitaker, referenced *supra* at n. 8, Article 5 (letters of credit), Article 8 (securities), and Article 9 (secured interests) already incorporate the use of electronic transactions. Similarly, Article 3 (negotiable instruments) and Article 7 (warehouse receipts and bills of lading) now have electronic equivalents. Article 6 (bulk transfers) no longer exists, and Article 4A (funds transfers) does not have a writing requirement. Thus, the only chapter of the U.C.C. which is excluded in its entirety is Article 4 (bank deposits and collections). The Federal Reserve staunchly refused to consider abrogating the writing requirements for checks, due primarily to the practical problems it would create for banks to alter their entire infrastructure to process e-checks.

⁶¹ See 15 U.S.C. § 7003(b).

⁶² *Id.* § 7003(b)(1).

secondary mortgage markets.⁶³ Under E-Sign, a “transferable record” is the electronic equivalent of a negotiable instrument or document.⁶⁴ The term “transferable record” was coined in the drafting of UETA, and was carried over to E-Sign. It rightfully was believed that industries that rely heavily on negotiable instruments needed more than just the general enabling provisions of E-Sign and UETA in order to make the switch from paper to electronic media.⁶⁵

Section 7021 of E-Sign sets forth certain standards that must be met before an electronic version of a promissory note can be treated as the equivalent of a paper note.⁶⁶ These require that the electronic note be created, transferred, and stored under highly secure conditions that are sufficient to “reliably establish” that only one person can control what is done with the electronic note at any point in time.⁶⁷ If such conditions are met, then “control” of the electronic promissory note is the equivalent of “possession” of a paper promissory note. And, a party that is in control of the electronic note may be a holder-in-due-course, just as a party in possession of a paper promissory note may be.⁶⁸

Section 7021 of E-Sign provides:

A person has control of a transferable record if a system employed for evidencing the transfer of interests in the transferable record reliably establishes that person as the person to which the transferable record was issued or transferred.⁶⁹

The key to control under E-Sign is establishing a system to ensure that the “transferable record reliably establishes that person” as the person to whom the record was issued or transferred.

Section 7021(c) sets forth the benchmark that the drafters of E-Sign presumably believed would ensure such reliability. It provides as follows:

A system satisfies subsection (b), and a person is deemed to have control of a transferable record, if the transferable record is created, stored, and assigned in such a manner that

- (1) A single authoritative copy of the transferable record exists which is unique, identifiable and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;
- (2) The authoritative copy identifies the person asserting control as

⁶³ See Jane K. Winn, *What Is a Transferable Record and Who Cares?*, 7 B.U. J. SCI. & TECH. L. 203, 203-04 (Summer 2001).

⁶⁴ 15 U.S.C. § 7021(a).

⁶⁵ Winn, *supra* note 63, at 204-05.

⁶⁶ 15 U.S.C. § 7021(b), (c).

⁶⁷ Wittie & Winn, *supra* note 35, at 316.

⁶⁸ *Id.*

⁶⁹ 15 U.S.C. § 7021(b).

-
-
- A. The person to which the transferable record was issued; or
 - B. If the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;
- (3) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;
 - (4) Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;
 - (5) Each copy of the authoritative copy and a copy of a copy is readily identifiable as a copy that is not the authoritative copy; and
 - (6) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.⁷⁰

Clearly the statute seeks to equate an “authoritative copy” with an “original,” and “control” with “possession.” But is it really. This and other issues pertinent to the analysis of a fidelity bond claim will be discussed in detail in section IV of this article.

Unfortunately, few computer systems in use today can meet the security standards set by E-Sign. As one commentator has noted:

IT professionals familiar with conventional computer security principles might believe that the use of a sophisticated computer and security technology such as digital signature technology might be adequate to meet the transferable record control requirements, but this is not correct. In effect digital signature technology can confirm “chain of title” but cannot alone provide the equivalent of possession of a tangible object. Digital signatures can guarantee the authenticity of signatures and the integrity of the contents of a transferable record, but unless combined with strong access controls, would not be sufficient to produce an “authoritative copy” of a transferable record.⁷¹

And, while systems likely can be built that are capable of so restricting access to transferable records, they will be considerably more expensive to create and maintain than systems used by most businesses.

While E-Sign addresses holder-in-due-course issues, other Article 3 issues remain unresolved. These include what modifications, if any, need to be made in the liability of indorsers or in the content of transfer and presentment warranties in light of the elimination of the paper negotiable instrument and its replacement by an electronic

⁷⁰ *Id.* § 7021(c).

⁷¹ *Id.* at 212.

record.⁷² Also, an important difference between the two sections is that the E-Sign provision is more narrowly drawn, referring only to promissory notes secured by real property, whereas the UETA provision refers to promissory notes and documents without limitation.⁷³ These provisions are important because they ultimately might determine whether an insured or someone else has liability for a loss resulting from an e-commerce transaction.

A drafting committee was convened by the NCCUSL to make revisions to Article 3, but the recognition of electronic negotiable instruments apparently was outside the scope of the drafting committee's mandate.⁷⁴ Furthermore, some bank regulators have expressed skepticism and even hostility to the idea of granting legal recognition to electronic negotiable instruments, arguing that the lack of experimentation to date in real estate or equipment financing markets may be evidence of lack of interest among lenders in such an option.⁷⁵ However, with the kind of statutory recognition UETA and E-Sign now provide, purchasers of electronic negotiable instruments face less uncertainty in claiming title to assets.

5. Electronic Filing

E-Sign does not expressly permit parties to make electronic filings with governmental agencies. In fact, several provisions of E-Sign imply different answers to the question of whether electronic filings are affirmatively permitted or whether agencies are merely encouraged to accept them.

Implicit in E-Sign is that a state may not deny the legal effect of filings with governmental agencies solely because they are made with an electronic record.⁷⁶ However, E-Sign also makes it clear that parties generally are not required to use or accept electronic records or signatures. Thus, to the extent governmental agencies are covered by this voluntary standard, it follows that individual governmental bodies will be free to determine whether they will accept electronic filings. Thus, this appears to be at least a potential conflict between two important provisions of E-Sign as they apply to electronic filings.⁷⁷

6. Interstate and Foreign Commerce

As mentioned above, E-Sign applies to electronic records and signatures “relating to” transactions in or affecting interstate or foreign commerce. E-Sign defines the term “transaction” as:

⁷² See Winn, *supra* note 63, at 205.

⁷³ Compare 15 U.S.C. 7021, with UETA § 16.

⁷⁴ See Wittie & Winn, *supra* note 35, at 312 n.97.

⁷⁵ *Id.* In fact, with no adequate basis for developing new regulations, bank regulators balked at the notion of authorizing electronic checks. As a result, the transferable record provisions of both UETA and E-Sign do not extend to checks.

⁷⁶ Wittie & Winn, *supra* note 35, at 337.

⁷⁷ *Id.* at 314-15.

An action or set of actions relating to the conduct of business, consumer, or commercial affairs between two or more persons, including any of the following types of conduct:

- A. The sale, lease, exchange, licensing or other disposition of (i) personal property, including goods and tangibles, (ii) services, and (iii) any combination thereof; and
- B. The sale, lease, exchange, or other disposition of any interest in real property, or any combination thereof.⁷⁸

This definition is intended to be broadly construed and “covers the full range of business, consumer, and commercial conduct, including, but not limited to, the types of conduct specifically described within the definition which are intended to be exemplary, not limiting.”⁷⁹

III. General Issues of Concern

A. EVIDENTIARY AND PRACTICAL CONCERNS

Due to the inherent differences between paper-based and electronic communications, a number of evidentiary and practical issues arise when transacting business electronically.

1. Admissibility of electronic records

a. The Writing and Signature Requirements. If electronic signatures are considered valid, this arguably begs the question as to what constitutes an electronic signature. The answer: almost any symbol can suffice as an electronic signature. For example, an electronic signature is established by the following: a traditional ink signature; a typed name; a click-through dialog box; biometric identification; a digitized reproduction of a handwritten signature; digitally encrypted transmissions; and virtually any other identifying mark, so long as the signer intends that it be afforded legal effect.

Statutes and regulations that require transactions to be in writing and signed generally are perceived to constitute barriers to e-commerce that must be removed if e-commerce is to flourish.⁸⁰ In other words, there is a concern that writing and signature requirements are satisfied only by ink on paper.⁸¹ However, this perception does not necessarily reflect reality.

⁷⁸ 15 U.S.C. § 7006(13).

⁷⁹ Wittie & Winn, *supra* note 35, at 319.

⁸⁰ See Steven Domanowski, Comment, *E-Sign: Paperless Transactions in the New Millennium*, 51 DEPAUL L. REV. 619, 623 (Winter 2001).

⁸¹ See Thomas J. Smedinghoff & Ruth Hill Bro, *Moving With Change: Electronic Signature Legislation as a Vehicle for Advancing E-Commerce*, 17 J. MARSHALL J. COMPUTER & INFO L. 723, 734 (1999).

Both the U.C.C. and most state laws include a Statute of Frauds provision.⁸² Thus, a paramount issue for electronic contracting is how an electronic signature, as contrasted with a written signature, fulfills the goals satisfied by the typical Statute of Frauds provision. A simple reading of the U.C.C. Statute of Frauds does not appear to supply a sufficient analysis of the "writing" or "signature" requirements. However, section 1-201 of the U.C.C. contains additional definitions. For example, section 1-201 defines "written" or "writing" as including "printing, typewriting or any other intentional reduction to tangible form."⁸³ The section also defines "signed" as including "any symbol executed or adopted by a party with the present intention to authenticate a writing."⁸⁴ The established rule is that a signature is whatever symbol, mark, or device one chooses to use as a representative of oneself.⁸⁵ There is no requirement that a traditional signature be in any particular form. The type of instrument a party uses to make his or her signature also is immaterial.⁸⁶ The flexible definition afforded a "writing" pursuant to the U.C.C. indicates an underlying intention that electronically-formed contracts should constitute a writing.⁸⁷ Furthermore, an electronic contract can be reduced to tangible form, whether stored on an internal drive or a floppy disk.

Unlike the U.C.C., E-Sign is not accompanied by any official comments. However, the UETA, upon which the text of E-Sign largely was based, does include such commentary from its drafters. The official Comment on the identical definition of the term "electronic signature" in UETA states that the term is intended to be broadly encompassing and is "not specifically defined." Specifically:

No specific technology need be used in order to create a valid signature. One's voice on an answering machine may suffice if the requisite intention is present. Similarly, including one's name as part of an electronic mail communication also may suffice as may the firm's name on a facsimile

The definition requires that the signer execute or adopt the sound, symbol or process with the intent to sign the record. The act of applying a sound, symbol or process to an electronic record could have differing meanings and effects. The consequences of the act as a signature are determined under other applicable law. However, the essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally

⁸² Unless additional requirements are imposed by a particular state statute, a contract will satisfy the Statute of Frauds if there is a writing, signed by, or on behalf of, the party to be charged, which: (1) reasonably identifies the subject matter of the contract; (2) is sufficient to indicate that a contract has been made between the parties or that the signing party has made an offer; and (3) states with reasonable certainty the essential terms of the contract. *See* RESTATEMENT (SECOND) OF CONTRACTS § 110 (1981).

⁸³ *See* U.C.C. § 1-201(46).

⁸⁴ *Id.* § 1-201 (39).

⁸⁵ *Id.*

⁸⁶ *See* Deborah L. Wilkerson, *Electronic Commerce Under the U.C.C. Section 2-201 Statute of Frauds: Are Electronic Messages Enforceable?*, 41 KAN. L. REV. 403, 415 (1992).

⁸⁷ *Id.*

significant act. It is that intention that is understood in the law as a part of the word "sign," without the need for a definition.⁸⁸

The intention of the UETA drafters was to leave the decision of whether something constitutes an electronic signature to be determined primarily under the existing body of jurisprudence.⁸⁹ While this Comment from the UETA does not formally apply to E-Sign, one would expect that federal courts may refer to it in interpreting the federal statute.

The digital signature provides more security than that of the average written signature, and it also provides increased reliability because any changes to an already digitally signed document can be detected. Specifically, the recipient of a document with a digital signature can authenticate the data source, verifying its origin and data integrity to ensure that the document has not been intercepted and changed somewhere along the way. In addition, the recipient enjoys proof of the transaction to fulfill the function of non-repudiation. For these reasons, more complex agreements should favor digital signatures over other, less advanced technologies that enable electronic contracting.

b. Authentication versus Attribution. Many attorneys have expressed confusion as to whether an electronic signature now can be enforced even where the identity of the sender or the security of the message is uncertain. This common mistake illustrates the distinction between authentication and attribution. By way of introduction, electronic transactions often occur between parties without pre-existing relationships.⁹⁰ Therefore, it often is extremely difficult for one party to clearly ascertain the identity of another party with whom it is contracting.

Under both the UETA and E-Sign, a contract may be "authentic" regardless of commercial reasonableness.⁹¹ In contrast, authentication under the U.C.C. is much more strict in application.⁹² Some scholars accordingly have commented that the biggest problem with modern e-commerce is the attribution issue.⁹³ Because the burden of proof is on the party seeking to enforce the electronic signature, attribution can present a significant obstacle, indeed. For this reason, various attribution procedures have been developed.

An attribution procedure is a procedure to verify that an electronic signature, message, or record is that of the person purporting to provide it.⁹⁴ An attribution procedure confirms that the electronic signature is provided by its owner, and that the owner of the electronic signature intended to sign the electronic record.⁹⁵ In short, indicia

⁸⁸ UETA § 2, cmt. 7.

⁸⁹ See Holly K. Towle, *E-Signatures – Basics of the U.S. Structure*, 38 HOUS. L. REV. 921, 987 (Fall 2001).

⁹⁰ See Scott R. Zernick, Note, *The E-Sign Act: The Means to Effectively Facilitate the Growth and Development of E-Commerce*, 76 CHI.-KENT L. REV. 1965, 1973 (2001).

⁹¹ See, e.g., UETA § 7 (giving legal effect to electronic records, signatures, and contracts, without requiring commercial reasonableness).

⁹² See Towle, *supra* note 89, at 931.

⁹³ *Id.* at 951 (referring to attribution as the "achilles heel of e-commerce").

⁹⁴ See UCITA § 102(a)(5) (2000).

⁹⁵ See Towle, *supra* note 89, at 953.

of the E-Signor's intent still is relevant, and the attribution procedure often is the means by which this intent is established.⁹⁶ Authentication, at least under E-Sign, does not necessarily establish capacity to contract or other traditional prerequisites to a binding agreement.

The distinction between attribution and authentication is illustrated in *Federal Trade Commission v. Verity International, Ltd.*,⁹⁷ in which the court determined that telephone line subscribers were not liable for calls made from the subscriber's number unless the biller for online services could prove that the subscriber was the person who consented to the online contract.⁹⁸ Thus, in the context of electronic transactions, a distinction should be drawn between authenticity, which concerns the integrity of the transmission, and attribution, which concerns whether the transaction is from the expected party or whether the transaction is from an imposter trying to transmit a forgery.⁹⁹

Critics argue that E-Sign's lack of minimum standards for authentication and intent might have the effect of legally endorsing a technology that lacks even the minimum safeguards and leaves the recipient unknowingly unprotected.¹⁰⁰ The worst-case scenario is that incompatible technologies and contractual uncertainty could lead to a significant increase in litigation. The more likely result is that sophisticated parties will learn to utilize more than the minimum allowable electronic signature standards.

c. Message Integrity and Security Concerns. Closely related to the issue of attribution are the issues of transaction integrity and security. Naturally, the parties to an electronic transaction want to know that the electronic record received is the same as the one sent, and that only the proper parties have had access to the electronic record during the course of the transaction. Under E-Sign, almost any identifying mark can constitute an electronic signature.¹⁰¹ However, document integrity and security are enhanced, and attribution therefore is more clearly established, if the parties elect to use more advanced technologies such as "digital" signatures. In essence, a digital signature is the electronic

⁹⁶ *Id.*

⁹⁷ 124 F. Supp. 2d 193 (S.D.N.Y. 2000).

⁹⁸ *See id.* at 202 (reasoning that if a contract is formed by clicking "I accept," it only binds the person who clicked, and the telephone line subscriber is not automatically that person).

⁹⁹ *See* Margaret J. Radin & Daniel L. Appelman, *Doing Business in the Digital Era: Some Basic Issues*, in *eCommerce: Strategy Resources in the Digital Economy*, 51, 55 (PLI Pats., Copyrights, Trademarks, and Literary Prop. Course, Handbook Series No. 570, 1999).

¹⁰⁰ *See* Alan Goldstein, *Digital Signatures Need Seal of Security Approval*, DALLAS MORNING NEWS, Sept. 20, 2000, at 2000 WL 26904019. Goldstein warns e-stakeholders to "expect a messy fight over standards" because E-Sign does not favor any one particular technology. *See id.* Instead, the marketplace will engage in the survival of the fittest battle, and the winner may likely be the company with the biggest marketing budget, similar to what happened in the VHS/Beta debate. *See id.* With the marketplace choosing the technology, consumers will be left to decide whether the technology that has been "chosen" is secure and safe, not just highly marketable and inexpensive to the producer. *See id.*

¹⁰¹ *See* discussion *supra* at III.A.1.a.

equivalent of a notarized signature.¹⁰² For sake of clarity, the two most widely used forms of digital encryption technology are summarized below.¹⁰³

First, the Data Encryption Standard¹⁰⁴ establishes a standard mathematical algorithm for encoding and decoding messages. The sender uses a key (a series of numbers) to scramble the message with the DES algorithm, and the recipient uses the same key to unscramble the message.¹⁰⁵ DES encryption is commonly used in electronic funds transfers.¹⁰⁶ DES requires that the key be closely guarded, because anyone with the key can use the widely-known DES algorithm to decode messages made with the same key.¹⁰⁷

A second encryption system is public key infrastructure.¹⁰⁸ This is the kind of encryption upon which digital signature statutes generally have been based. Here again the algorithm must be known by both the sender and the recipient.¹⁰⁹ Each person using the public key encryption system has two keys: a public key and a private key.¹¹⁰ The public key decodes a message encoded with the same person's private key, and vice versa. If each person keeps the private key confidential, he or she can distribute the public key widely to others who can then read the person's messages encoded with the private key.¹¹¹ Anyone who is able to decode a message with the public key can be certain that only the owner of the private key could have sent it. Also, someone with the public key can send a secure message to the owner of the private key, because only the private key will decode the message.¹¹² The secret to the PKI technology's security is a "hashing algorithm" which notifies the recipient if even one character of the message is changed after signing.¹¹³ If the message digest sent matches the message digest created by the recipient, the recipient knows that only the sender could have sent the message (unless he or she lost control of the private key), and that the message did not change during transmission. Thus, while almost any electronic signal can qualify as an electronic signature, very few transmissions can satisfy the digital signature standard.¹¹⁴

In any event, vendors in the security market continue to experiment with alternative technologies that offer similar levels of reliability. One such technology that might compete with digital signatures, biometrics, uses bodily measures to perform the same security functions as a digital signature.¹¹⁵ Examples of biometrics include

¹⁰² See Koger, *supra* note 10, at 501.

¹⁰³ See BENJAMIN WRIGHT, *THE LAW OF EDI, E-MAIL AND INTERNET: TECHNOLOGY, PROOF, AND LIABILITY* 1.3.1-1.3.2 (2d ed. 1997).

¹⁰⁴ Hereinafter DES.

¹⁰⁵ See WRIGHT, *supra* note 103, at 1.3.1.

¹⁰⁶ *Id.*

¹⁰⁷ *Id.*

¹⁰⁸ Hereinafter PKI.

¹⁰⁹ See WRIGHT, *supra* note 103, at 1.3.2.

¹¹⁰ *Id.*

¹¹¹ *Id.*

¹¹² *Id.*

¹¹³ *Id.*

¹¹⁴ For example, digital reproduction of a typed signature is not a true digital signature, nor is a personal identification number.

¹¹⁵ See Koger, *supra* note 10, at 502.

fingerprints, eye-scanning or iris recognition, facial recognition, voice recognition, and body odor recognition.¹¹⁶ However, these technologies are not widely available and will be cost prohibitive in most contexts in the foreseeable future.¹¹⁷ Biometrics also raise fundamental privacy issues not present with digital signatures.¹¹⁸ Nevertheless, it is worth recognizing that the technology in this area is under constant development.

d. Nonrepudiation. Another related issue is that of nonrepudiation, a legal requirement where one party seeks to hold another party to a contract.¹¹⁹ Nonrepudiation is essential to e-commerce in situations where a party is willing to rely on a communication, electronic contract or a funds transfer request, because an individual can hack into a computer network and send a communication with the address of another party.¹²⁰

Parties to electronic transactions may have legitimate claims that one of the parties did not send the communication or that the contents of the communication as received were not the same as originally sent. A somewhat common occurrence of such a situation occurs in "click-wrap" contracts where a user claims that he or she did not click the button to accept the contract or that he or she clicked the button accidentally without intending to do so.¹²¹

2. Record Retention and Access to Data

a. Data Storage Issues. Regardless of the medium, data storage always is a concern. Physical documents are bulky and tend to deteriorate over time. Consequently, the amount of attention devoted to this topic is perhaps a little overstated. Nevertheless, it will become sound practice for all parties to electronic transactions to arrange for offsite backup of electronic data. Similarly, parties should be aware of the possibility that certain electronic media may eventually deteriorate. Finally, companies with specialized security concerns should conduct thorough employee background checks.

b. Access to electronic records. A more unique e-commerce concern is whether parties to an electronic transaction are legally entitled to a copy of, or access to, the electronic record.¹²² The U.C.C. does not require a contracting party to provide a copy of a contract to the other party, so there arguably is no basis to require such access. To complicate matters, electronic records are not always created in a tangible or easily reproduced form.¹²³ Consequently, contracting parties may want to enter a mutual agreement that one of the parties will maintain the "original" electronic records or provide access to such records at its web site or another location.

¹¹⁶ *Id.*

¹¹⁷ *Id.* at 502-03.

¹¹⁸ *Id.* at 502.

¹¹⁹ See Zemnick, *supra* note 90, at 1974. Repudiation of a contract occurs with words or actions indicating that a party is not going to perform his or her duty or obligation owed to the other party in the future. See BLACK'S LAW DICTIONARY 903 (6th ed. 1991).

¹²⁰ See Zemnick, *supra* note 90, at 1974.

¹²¹ *Id.* at 1975.

¹²² *Id.* at 1984.

¹²³ See Towle, *supra* note 89, at 981.

c. *Impact of future technologies.* One justification for E-Sign's technology-neutral approach is the concern that technology can easily become obsolete, thereby rendering a technology-specific approach unsafe or inefficient.¹²⁴ With this in mind, modern information systems no longer rely exclusively on the use of physical tokens, such as paper negotiable instruments, to track ownership of assets. Modern systems for tracking rights in assets include: U.C.C. filing offices, which are a form of registry; registries maintained by issuers or registration agents, which are used by the U.S. Treasury and mutual fund issuers to track ownership of the financial assets they issue; motor vehicle title registration systems, which rely on a combination of a paper document of title and an entry in a central registry to track ownership of motor vehicles; and customer account systems maintained by regulated financial intermediaries, which are used by issuers to track ownership of financial assets such as most bonds and stocks issued by corporations as well as money in bank accounts.

For example, one of the goals of the drafters of Revised Article 9 was to accommodate electronic filings. In order to do so, the drafters eliminated the requirement that a financing statement must be signed in order to be effective.¹²⁵ Not only does Revised Article 9 eliminate the signature requirement, the suggested uniform form of a financing statement set forth in the statute does not have a space for a signature.¹²⁶ However, while all fifty states legally allow the electronic filing of security agreements, not all Secretaries of State have authorized the filings due to lagging electronic infrastructure. Thus, the administration of transactions in markets for real estate mortgages or equipment financing loans still requires someone to keep track of each note or loan agreement. Until the assets can be converted from paper to electronic form, it is unlikely that there will be dramatic efficiency gains in the handling of these assets.

3. Ripe For Change: The Electronic Mortgage Industry

Most banks now utilize some form of online business activity, and offer most of their services online to customers. Before the passage of E-Sign, lending and title insurance companies often were unwilling to complete transactions online because the legal enforceability of such transaction was uncertain.¹²⁷ Moreover, mortgages previously could be transferred electronically, but the results were not instantaneous because the transaction still required a signed document.¹²⁸ Although all of the paperwork was filled out online, the form still had to be printed, signed, and mailed back to the biller.¹²⁹ Approximately fifty percent of customers dropped out of the transaction

¹²⁴ *Id.* at 948-49.

¹²⁵ See U.C.C. § 9-502 cmt. 3 (1999). Conspicuously absent from the requirements for a financing statement is the debtor's signature.

¹²⁶ *Id.* § 9-521.

¹²⁷ See, e.g., Ted Cornwell, *E-Loan Hangs On*, BANK TECH. NEWS, July 2000, at 26 (discussing the opportunities provided to pure online loan companies when traditional "brick-and-mortar" lenders do not enter the Internet world).

¹²⁸ See generally *E-Billing and Customer Service: Realizing the Potential*, WALL ST. & TECH., July 1, 2000, News Group File (explaining previous problems with electronic funds transfers).

¹²⁹ *Id.* See also Tatiana Helenius, *Digital Signatures to Send Transactions Skyrocketing*, WALL ST. & TECH., Oct. 1, 2000, News Group File (explaining the online mortgage process before E-Sign).

at this point because they disliked the extra time it took to print, sign and return mail the copy of the transaction.¹³⁰

The E-Sign legislation will reduce the problems that result from working with paper transactions because a signature sent to the bank electronically will have the same legal effect as one that is signed and sent via regular mail. In addition, the process of introducing a mortgage into a secondary market can be cut from an average of forty-five days to as little as three hours, considerably cutting costs.¹³¹

The first paperless residential mortgage closing was executed on July 24, 2000, less than a month after President Clinton signed E-Sign.¹³² The home was sold to Mr. Jose Arroyo who electronically executed the promissory note and mortgage at Enterprise Title in Florida.¹³³ The mortgage for Mr. Arroyo was processed and approved using online lending tools provided by Mortgage.com.¹³⁴ All closing documents were prepared electronically by Enterprise Title and were executed by Mr. Arroyo and the seller electronically.¹³⁵ Mortgage.com performed online quality control of the settlement documents after they were electronically executed.¹³⁶ The documents were then transferred to the Broward County Records Division.¹³⁷ Once the county clerk received the documents, they were verified and recorded, and the fees were collected electronically.¹³⁸ After this process, Mortgage.com electronically transferred ownership of the loan to Fannie Mae.¹³⁹ The loan was closed and recorded in less than five hours, confirming that there are faster, less expensive ways to conduct loan transactions.¹⁴⁰ Consumers, however, are not the only ones who benefit. In fact, Mortgage.com saved approximately \$1,000 in the Arroyo transaction as a result of the time that otherwise would have been spent on administrative tasks.¹⁴¹

The problems with implementing these types of programs lie in the amount of people and the technology that must be involved, including that available to county recording offices. The problem is not that recording offices do not want to update their system, but that it will be an expensive process.¹⁴² Furthermore, although the infrastructure is currently in place to complete mortgages online, the number of people

¹³⁰ See generally *E-Billing*, *supra* note 128.

¹³¹ See Marquess, *supra* note 9, at 74.

¹³² See Carrie A. O'Brien, Note, *E-Sign: Will the New Law Increase Internet Security Allowing Online Mortgage Lending to Become Routine?*, 5 N.C. BANKING INST. 523, 530 (April 2001) (citations omitted).

¹³³ *Id.* at 531.

¹³⁴ *Id.*

¹³⁵ *Id.*

¹³⁶ *Id.*

¹³⁷ *Id.*

¹³⁸ *Id.*

¹³⁹ *Id.*

¹⁴⁰ *Id.*

¹⁴¹ *Id.* at 532; see also Robyn Friedman, *Real Estate Testing Digital Signatures*, ARIZ. REPUBLIC, Dec. 29, 2000, LEXIS, News Library, AZREP File.

¹⁴² See Bonnie Sinnock, *Title Searches Seen as an Obstacle in E-Originations*, ORIGINATION NEWS, Jan. 26, 2001, LEXIS, News Library, ABBB File.

applying for mortgages online has not increased.¹⁴³ Regardless, the Property Records Information Association recently went to NCCUSL to request that a model electronic recording act be drafted. NCCUSL agreed and has stated plans to begin drafting the act this fall.¹⁴⁴

Even if electronic signatures become widely used in online real estate lending, there still are unanswered questions regarding their security. Since E-Sign does not call for any specific type of electronic signature to be used, and security concerns arise from the lack of technical uniformity regarding electronic signatures. The volume of online transactions has created an increase in the theft of personal information, and identity theft shows no signs of slowing down.¹⁴⁵ This increase affects financial institutions directly because sixteen percent of identity thieves open a bank account with a phony identity or write checks from the victim's account.¹⁴⁶ In addition, in approximately four percent of identity theft cases, the criminals even take out fraudulent loans.¹⁴⁷

B. PROCEDURAL CONCERNS

For many practitioners, the most immediate E-Sign concerns will be of a procedural nature. How is personal jurisdiction determined? What substantive law will apply? What if the law of the state, the language of the contract and the language of E-Sign all are in conflict? These issues are discussed briefly below.

1. Personal Jurisdiction

In 1958 in *Hanson v. Denkla*,¹⁴⁸ the United States Supreme Court commented: "[a]s technological progress has increased the flow of commerce between States, the need for jurisdiction has undergone a similar increase."¹⁴⁹ More recently, in *Burger King v. Rudzewicz*,¹⁵⁰ the Court noted that jurisdiction could not be avoided "merely because the defendant did not physically enter the forum State."¹⁵¹ Even though courts have had occasion to examine the problem of personal jurisdiction in an electronic world, "[c]ases applying the familiar personal jurisdiction analysis to the Internet are thus far relatively scarce."¹⁵² Furthermore, the results have been inconsistent.¹⁵³ Generally, there are three

¹⁴³ See Whitaker, *supra*, at n.8.

¹⁴⁴ *Id.*

¹⁴⁵ See Paul Korzeniowski, *Internet Ups the Ante For Growing Issue Of Identity Theft*, INVESTOR'S BUSINESS DAILY, Dec. 21, 2000 at 10.

¹⁴⁶ *Id.*

¹⁴⁷ *Id.*

¹⁴⁸ 357 U.S. 235 (1958).

¹⁴⁹ See *id.* at 250-51.

¹⁵⁰ 471 U.S. 462 (1986).

¹⁵¹ See *id.* at 476.

¹⁵² *GTE New Media Servs., Inc. v. BellSouth Corp.*, 199 F.3d 1343, 1347 (D.C. Cir. 2000).

¹⁵³ See generally Suzanna Sherry, *Haste Makes Waste: Congress and the Common Law in Cyberspace*, 55 VAND. L. REV. 309, 363-76 (March 2002).

different approaches for the resolution of the personal jurisdiction issue in electronic commerce.¹⁵⁴

First, there are those who argue that the proper resolution is found by applying the traditional principles of personal jurisdiction.¹⁵⁵ Using these principles, a court would look to whether the forum's long arm provision allowed exercise of personal jurisdiction, whether the defendant has made the requisite contacts for the exercise of personal jurisdiction, whether the defendant purposefully availed herself of the benefit of the state's laws, and whether exercise of personal jurisdiction comports with the constitutional due process requirements.

Second, some scholars advocate the shaping of the traditional principles of personal jurisdiction - such as purposeful availment, procedural fairness, and the burden placed on the defendant to defend in a different forum - to the unique characteristics of the Internet.¹⁵⁶ Proponents of this position explain that "courts should de-emphasize considerations of purposeful availment at least in cases concerning the Internet, [and] they should correspondingly increase their emphasis on concerns of procedural burdens and fairness."¹⁵⁷

Finally, there are those who take a radical approach, arguing for example, that the Internet is a self-regulating community in which cybercitizens should decide which laws would apply to them.¹⁵⁸ An example of this so-called radical approach is the proposal of a new federal court with jurisdiction solely over cyberspace activities.¹⁵⁹

A practical example of applying personal jurisdiction rules to cyberspace is *CompuServe, Inc. v. Patterson*,¹⁶⁰ where a Texas resident entered into an agreement with CompuServe, a computer information service headquartered in Ohio, in which CompuServe would make Patterson's software available for download from its database.¹⁶¹ CompuServe later marketed a shareware product similar to Patterson's and Patterson thought that such activity was in violation of his agreement with CompuServe.¹⁶² After the district court granted Patterson's motion to dismiss for lack of personal jurisdiction, the Sixth Circuit Court of Appeals reversed this decision, explaining that Patterson "purposefully contracted . . . to market a product in other states,

¹⁵⁴ See Tyler Anderson, Comment, *An Analysis of Personal Jurisdiction and Conflict of Laws in the Context of Electronically Formed Contracts*, 37 IDAHO L. REV. 477, 482 (2001) (citing *Civil Procedure-D.C. Circuit Rejects Sliding Scale Approach to Finding Personal Jurisdiction Based on Internet Contacts*- GTE New Media Services v. BellSouth Corp., 199 F.3d 1343 (D.C. Cir. 2000), 113 HARV. L. REV. 2128 (2000)).

¹⁵⁵ See, e.g., Dan L. Burk, *Jurisdiction in a World Without Borders*, 1 VA. J.L. & TECH. 3 (Spring 1997).

¹⁵⁶ See, e.g., Martin H. Redish, *Of New Wine and Old Bottles: Personal Jurisdiction, the Internet, and the Nature of Constitutional Evolution*, 38 JURIMETRICS J. 575, 578-80, 609-10 (1998).

¹⁵⁷ See Anderson, *supra* note 154, at 483.

¹⁵⁸ See, e.g., David R. Johnson & David Post, *Law and Borders- The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1374-78 (1996).

¹⁵⁹ Henry H. Perritt, Jr., *Jurisdiction in Cyberspace*, 41 VILL. L. REV. 1, 100-03 (1996).

¹⁶⁰ 89 F.3d 1257 (6th Cir. 1996).

¹⁶¹ *Id.* at 1260-61.

¹⁶² *Id.* at 1261.

with Ohio-based CompuServe operating, in effect, as his distribution center. Thus, it is reasonable to subject Patterson to suit in Ohio, the state which is home to the computer network service he chose to employ."¹⁶³ The court went on to explain that Patterson "set in motion an ongoing marketing relationship with CompuServe, and he should have reasonably foreseen that doing so would have consequences in Ohio."¹⁶⁴

2. Choice of Law Issues under E-Sign

An intricate analysis in any case, conflict of law analysis is even more complicated in cyberspace.¹⁶⁵ The Internet exacerbates the problematic and often uncertain analysis because it is difficult to define: (1) where a transaction is "located" or formed; (2) where its effects are felt; and (3) where the harm actually occurs.¹⁶⁶ Because the Internet is transnational, legitimate arguments even can be made that any conflict of laws analysis must be international in scope.¹⁶⁷ Regardless, the most common approach today is the "most significant relationship" test, which weighs various factors before determining which state's law is applied.¹⁶⁸

Specifically, with regard to contracts of insurance lacking a valid choice of law provision, the principles of section 188 of the Restatement (Second) of Conflict of Laws¹⁶⁹ are instructive. According to the Restatement, the relevant factors include the following: (1) the place of contracting; (2) the place of negotiation; (3) the place of performance; (4) the location of the subject matter of the contract; and (5) the domicile, residence, nationality, place of incorporation and place of business of the parties.¹⁷⁰ Generally speaking, if the dispute concerns contract formation, the law of the forum in which the contract was made should apply.¹⁷¹ Similarly, if the dispute concerns contract performance, the law of the place where performance was to occur should apply.¹⁷²

The problem is that the definition of "place" is difficult, if not impossible, to quantify in the context of cyberspace. An argument often can be made supporting adjudication of a contract dispute in any number of jurisdictions because no physical place of formation or performance may exist. Some states have attempted to legislate the forum of cyberspace disputes, but the extent to which these statutes will be upheld is still open for debate.¹⁷³ Consequently, the bottom line is that parties to a contract over the

¹⁶³ *Id.* at 1263.

¹⁶⁴ *Id.* at 1265.

¹⁶⁵ See generally Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199 (1998); Matthew R. Burnstein, Note, *Conflicts on the Net: Choice of Law in Transnational Cyberspace*, 29 VAND. J. TRANSNAT'L L. 75 (1996).

¹⁶⁶ See Richard A. Mann & Barry S. Roberts, *Cyberlaw: A Brave New World*, 106 DICK. L. REV. 305, 343-44 (Fall 2001).

¹⁶⁷ See Goldsmith, *supra* note 162.

¹⁶⁸ See generally RESTATEMENT (SECOND) OF CONFLICT OF LAWS § 6 (2001).

¹⁶⁹ *Id.* § 188.

¹⁷⁰ *Id.*

¹⁷¹ See Burnstein, *supra* note 165, at 95.

¹⁷² *Id.*

¹⁷³ See generally Shawn E. Tuma & Christopher R. Ward, *Contracting over the Internet in Texas*, 52 BAYLOR L. REV. 381, 411-14 (2000).

Internet may want to consider writing an enforceable choice of law provision into the contract, particularly in light of E-Sign's preemptive effects on certain state laws, which are discussed below.

3. The Effect of E-Sign on State E-Commerce Legislation

The interaction between E-Sign and state legislation is one of the most hotly debated and least resolved areas of electronic commerce.

a. Introduction to Preemption Issues. Congress enacted E-Sign in an attempt to quickly create a standard across the United States for the recognition of electronic signatures and records that is technologically neutral. E-Sign attempts to provide a uniform and consistent set of laws on these issues. As discussed previously, there are a number of reasons behind Congress' enactment of E-Sign. The perceived non-uniformity of state legislation on electronic records and signatures was one of the driving forces behind the enactment of E-Sign.¹⁷⁴ Congress believed a uniform standard would promote the growth of e-commerce while creating an environment of greater legal certainty and predictability in these types of business transactions. Another suggested purpose is as a gap filler: because E-Sign regulates an area traditionally reserved to the states, it only is intended to provide a set of uniform and consistent laws until UETA makes its way through the states.

In E-Sign Congress attempted to create a national standard for the recognition of electronic signatures and records. E-Sign preempts non-exempted state laws that touch on the subject of electronic records and signatures. Despite E-Sign's seemingly broad impact on state laws, substantive aspects of contract law continue to be governed by state law. Under Section 7002, E-Sign provides that state law may modify, limit, or supersede the substantive provisions of E-Sign section 7001 if the state law either (1) is an enactment of the UETA as approved by the NCCUSL in 1999; or (2) is consistent with E-Sign, technologically neutral and, if adopted after E-Sign, makes specific reference to E-Sign.¹⁷⁵

Given E-Sign's espoused purpose of uniformity among state laws and the fact it is regulating an area traditionally within the realm of the state, the preemption provisions of E-Sign are important. Despite Congress' intent, the extent of the preemption provision is not clear. Moreover, the legislative history provides little guidance given the varying opinions expressed throughout the drafting and enactment of E-Sign. Finally, there are no court decisions or administrative decisions which provide guidance regarding the scope of the preemption provision.

¹⁷⁴ There is great disparity between the state laws governing electronic signatures and records. For instance, Utah and Washington only recognize digital signatures, whereas Massachusetts law on the issue of electronic signatures is technologically neutral. Other states fall somewhere in between the two extremes.

¹⁷⁵ 15 U.S.C. § 7002(a); *see also* Shea C. Meehan & D. Benjamin Beard, *What Hath Congress Wrought: E-Sign, the UETA, and the Question of Preemption*, 37 IDAHO L. REV. 389 (2001).

b. Section 7002(a)(1). E-Sign creates a uniform standard by preempting inconsistent state laws with a test outlined in section 7002. Under the first prong of the preemption provision, section 7002(a)(1), state law may modify, limit, or supersede the substantive provisions of Section 7001 if the state law is an enactment of the UETA as approved by the NCCUSL in 1999.¹⁷⁶ This exemption does not apply to any exceptions to UETA enacted by the state under section 3(b)(4) to the extent such exemption is inconsistent with this title or title II.¹⁷⁷ This latter provision commonly is referred to as the reverse preemption provision. Assuming a state adopts the prescribed version of UETA, it should be exempted from the requirements of E-Sign. The extent of the exemption, however, is unclear. Is it a total exemption from E-Sign or are only those provisions consistent with E-Sign exempted? How does the exemption apply in areas regulated by UETA, but not E-Sign? In the alternative, how does the exemption apply in areas that are more extensively regulated by E-Sign than UETA?

The foregoing questions arise because the provisions of UETA and E-Sign are not identical. Specifically, the UETA is much more comprehensive in its regulation of electronic signatures and records, with the exception of consumer disclosure requirements. It includes many provisions not found in E-Sign. UETA contains provisions on how an electronic signature or record is attributed to a person or machine engaged in a transaction, rules and responsibilities that apply when changes or errors occur in an electronic record during transmission, and default rules regarding when an electronic record is sent and received.¹⁷⁸ As indicated, E-Sign has much more stringent consumer protection provisions than UETA. Under E-Sign, the consumer must consent to receiving the information electronically.¹⁷⁹ In addition, the merchant must provide the proper hardware and software requirements for accessing and retaining the information.¹⁸⁰ Finally, the consumer must consent electronically, in a manner that reasonably demonstrates the consumer can access the information.¹⁸¹ In contrast, UETA simply comments that “whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties conduct.”¹⁸² Also unlike E-Sign, UETA is not consumer specific.

Assuming there is an effective adoption of UETA for purposes of section 7002(a)(1), what portions are modified, limited or superceded by the UETA? Unfortunately, there is disagreement on the extent of the preemption. Unlike section

¹⁷⁶As of April 2001, twenty-three states had enacted UETA: Arizona, California, Delaware, Florida, Hawaii, Idaho, Kansas, Kentucky, Maine, Maryland, Michigan, Minnesota, Nebraska, North Carolina, Ohio, Oklahoma, Pennsylvania, Rhode Island, South Dakota, Utah, and Virginia. Ten other states currently are considering adopting UETA: Arkansas, Connecticut, Mississippi, Montana, New Jersey, New Mexico, North Dakota, Oregon, Texas, and Vermont.

¹⁷⁷ See 15 U.S.C. § 7002(a)(1).

¹⁷⁸ UETA also has a loophole provision giving states the discretion to pass laws requiring a record to be posted or displayed, sent or communicated . . . in a certain manner. Theoretically, a state would be able to prevent certain transactions from being conducted electronically, through regulations, which establish a writing requirement. However, this provision is strictly prohibited by E-Sign.

¹⁷⁹ See 15 U.S.C. § 7001(c)(1)(a).

¹⁸⁰ *Id.*

¹⁸¹ *Id.*

¹⁸² See UETA § 5(b).

7002(a), (2) there is no general requirement of consistency. Moreover, the legislative history provides little guidance on this issue as it supports both total exemption and partial exemption to the extent consistent with E-Sign.¹⁸³ In addition, the articulated purpose behind E-Sign supports both interpretations.¹⁸⁴ The espoused purpose of consistency and uniformity would support total exemption. In contrast, the purpose of consumer protection supports partial exemption only to the extent consistent with E-Sign. Because UETA is not consistent with E-Sign and E-Sign affords the consumer greater protection, the consumer protection provisions of E-Sign may preempt UETA. Some suggest the plain language of the Section 7002(a)(1) provides a complete exemption to the preemptive provision if the pristine UETA is adopted.¹⁸⁵ Unless the state qualifies for an exemption under 7002(a)(1), E-Sign's consumer protection provisions would apply given the consistency analysis required under section 7002(a)(2). In contrast, others suggest the preemption only applies to those provisions consistent with E-Sign.¹⁸⁶ Therefore, E-Sign would preempt state law in the area of consumer protection.

The preemptive provision of E-Sign should not apply in areas that are regulated by UETA, but not E-Sign. Some suggest that operative provisions of UETA that have no analog in E-Sign should be considered inconsistent with E-Sign and thereby modify, limit, or supercede E-Sign.¹⁸⁷ However, these provisions do not directly contradict E-Sign. In addition, provisions without an analog in E-Sign merely provide rules that modify and supplement E-Sign and can be seen as furthering the goal of certainty in electronic transactions.¹⁸⁸ These provisions should be considered consistent as long as they expand the types of transactions validated by UETA.¹⁸⁹ Finally, when areas are regulated in UETA but not E-Sign, these areas are beyond the scope of E-Sign and therefore beyond Section 7002's preemptive authority.¹⁹⁰ For the above reasons, areas regulated by UETA but not E-Sign should not be preempted by Section 7002.

Another preemption issue is whether a version of UETA passed by a state with minor amendments or modifications would qualify for exemption under 7002(a)(1). The exception to the exemption under 7002(a)(1) for 3(b)(4) transactions supports an interpretation that Section 7002(a)(1) does not require a pristine adoption of UETA.¹⁹¹ Instead, the provisions of UETA adopted with amendments or minor modifications should be analyzed under Section 7002(a)(1) and 7002(a)(2). Those provisions consistent with the pristine UETA should be exempted under 7002(a)(1). In contrast, the minor modifications and amendments should be analyzed under Section 7002(a)(2) for consistency.¹⁹² Interpreting E-Sign Section 7002(a)(1) to approve of any state law that constitutes a provision of the UETA reflects Congress' approval of the UETA, receives

¹⁸³ See Andrew D. Stewart, Comment, *Navigating the E-Sign Nebula: Federal Recognition of Electronic Signatures and Impact on State Law*, 24 HAWAII L. REV. 309, 323 (Winter 2001).

¹⁸⁴ *Id.*

¹⁸⁵ See Meehan & Beard, *supra* note 175, at 409.

¹⁸⁶ See Stewart, *supra* note 183, at 324.

¹⁸⁷ See Meehan & Beard, *supra* note 175, at 409.

¹⁸⁸ *Id.*

¹⁸⁹ *Id.*

¹⁹⁰ See Stewart, *supra* note 183, at 328 (citations omitted).

¹⁹¹ See Meehan & Beard, *supra* note 175, at 402.

¹⁹² *Id.* at 404.

support from the presumption against preemption by exposing less of the statute to a section-by-section analysis and acknowledges inclusion of a severability clause in the UETA.¹⁹³ Moreover, this interpretation is consistent with the presumption against preemption: courts should invalidate as little as possible in order to achieve Congress' intent.¹⁹⁴

c. Sections 7002(a)(2). E-Sign preempts non-exempted state laws that touch on the subject of electronic records and signatures. Under the second prong of the E-Sign Preemptive Provision, Section 7002(a)(2), state law may modify, limit, or supersede the substantive provisions of Section 7001 if the state law is consistent with E-Sign, technologically neutral and, if adopted after E-Sign, makes specific reference to E-Sign.¹⁹⁵

In cases where the state adopted UETA with modifications or adopted its own legislation with respect to electronic signatures and records, the modification or new legislation would be analyzed under 7002(a)(2)(i),(ii). To satisfy the requirements of Section 7002(a)(2), the provision must be consistent with E-Sign and be technologically neutral. When a state adopts UETA with only minor modifications, the exemption analysis requires a two-pronged analysis under Section 7002(a)(1) and 7002(a)(2).¹⁹⁶ Those UETA provisions adopted without modification would be exempt under Section 7002(a)(1). Only the modification or amendments to UETA would be analyzed under Section 7002(a)(2). Although this appears to be the most reasonable application of the E-Sign, whether a law is consistent with E-Sign will ultimately be a question for the courts.

The second requirement of Section 7002(a)(2) is that the state law must be technologically neutral. Whether state law is technologically "neutral" is not always clear under the language of E-Sign. Some commentators suggest the neutrality requirement of Section 7002(a)(2)(ii) may be the most troublesome and perhaps the most overlooked.¹⁹⁷ The typical disagreement results from the different possible interpretations of the phrase "legal status or effect."¹⁹⁸ According to E-Sign:

such alternative procedures or requirements do not require, or accord greater legal status of effect to, the implementation or application of a specific technology or technical specification for performing functions of creating, storing, generating, receiving, communication, or authenticating electronic records or electronic signatures¹⁹⁹

In addition to UETA, numerous other state laws purport to regulate electronic signatures and records. Generally, these laws fit into the three categories mentioned

¹⁹³ *Id.*

¹⁹⁴ *Id.*

¹⁹⁵ See 15 U.S.C. § 7002(a).

¹⁹⁶ See Meehan & Beard, *supra* note 175, at 409.

¹⁹⁷ See Stewart, *supra* note 183, at 326 (citations omitted).

¹⁹⁸ *Id.*

¹⁹⁹ See 15 U.S.C. § 7002(a)(2)(A)(ii).

above.²⁰⁰ The first group consists of statutes described as “prescriptive” statutes, which only recognize signatures that utilize technology prescribed by law.²⁰¹ Examples include the states of Washington and Utah. A second category are comprised of statutes that are “criteria-based” statutes, which only recognize electronic signatures that meet specified evidentiary standards.²⁰² Examples of this approach are found in Illinois and California. Finally, the “signature enabling approach” statutes recognizes all electronic signatures and records.²⁰³ This structure is in place in Massachusetts and South Carolina.²⁰⁴

The analysis of whether a state law meets the technologically neutral requirement under E-Sign is clear only under two of the three general statutory schemes.²⁰⁵ A prescriptive statute would be preempted because it only recognizes electronic signatures based on certain technologies. In contrast, the signature enabling statutes would be exempt from preemption because they are technologically neutral. Whether criteria-based statutes are preempted is unclear. A broad reading of the terms “legal effect” would result in preemption of these state statutes.²⁰⁶ The argument is that when states designate certain types of electronic signatures as secure electronic signatures and provide them evidentiary presumptions not attributed to other types of electronic signatures, based on technological differences, the state provides secure electronic signatures heightened “legal effect.”²⁰⁷ While others opine that “states should not be prohibited from discriminating between different types of electronic signatures regarding the issue of attribution, as long as their statute legally recognizes the validity of all electronic signatures,”²⁰⁸ this interpretation is premised on a narrow reading of the phrase “legal effect” and is limited to whether a state recognizes or validates an electronic signature based on technological characteristics of the signature -- not whether it is afforded additional evidentiary presumptions.²⁰⁹ Another argument in support of a narrow reading, is that because “attribution” is beyond the scope of section 7001 (or E-Sign for that matter), it likewise is beyond the scope of Section 7002’s preemptive authority.²¹⁰

A broad reading of the terms “legal effect” is more appropriate given the avowed purpose behind E-Sign. E-Sign is technologically neutral and recognizes the simplest device as an electronic signature as long as it serves the function of identifying the signer or sender’s intent to assent to the terms of the document. It does not require an electronic

²⁰⁰ See Stewart, *supra* note 183, at 326.

²⁰¹ *Id.*

²⁰² *Id.*

²⁰³ *Id.*

²⁰⁴ See Renard Francois, Comment: *Fair Warning: Preemption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws*, 19 J. MARSHALL J. COMPUTER & INFO. L. 401, 408-409 (Winter 2001).

²⁰⁵ See Stewart, *supra* note 183, at 326.

²⁰⁶ *Id.* at 327 (citations omitted).

²⁰⁷ *Id.* at 327 (citations omitted).

²⁰⁸ *Id.* (citing Raymond T. Nimmer, *Electronic Signatures in Global and National Commerce Act of 2000: Effect on State Laws*, at 7, available at <http://www.bmck.com/ecommerce/topic-esignatures.htm> (February 2001)).

²⁰⁹ *Id.* at 328.

²¹⁰ *Id.* at 328 (citations omitted).

signature to perform document authentication or dictate the type of security procedure an electronic signature should provide. UETA is also technologically neutral. Allowing state laws that favor one form of electronic signature over another to be exempt from preemption is inconsistent with the purpose of E-Sign. It would create divergent state laws – a condition which E-Sign sought to rectify. E-Sign was enacted in effort to create uniformity and consistency. By allowing some states to favor one form of electronic signature over another would compromise that goal. Moreover, E-Sign was initially drafted as stopgap legislation until all states passed UETA. As indicated above, UETA is technologically neutral. To read the terms “legal effect” broadly and allow state laws that are not technologically neutral would be inconsistent with E-Sign and UETA.

Unfortunately, there are no clear answers as to what state laws are exempt from preemption under Section 7002(a) of E-Sign. Whether Congress achieved its purpose of uniformity and consistency with respect to electronic signatures and records is questionable given the inherent ambiguity in the Exemptions to Preemption Provision in E-Sign. Because the determination whether a state provision preempts or is preempted by E-Sign involves a detailed analysis, and given the number of variables and unknowns, it is not clear what constitutes compliance. Instead of uniformity and consistency, businesses are left with a cumbersome framework in which to analyze compliance. It appears the safest course of action for businesses generally is to follow the mandates of the UETA without amendments or modifications and the E-Sign provisions on consumer protection.

IV. The Effect of E-Commerce in the Fidelity Bond Context

As recent accounting scandals have shown, corporate fraud is not at all on the decline in the computer age. With the advent of e-commerce, dishonest employees and other criminals now have additional means at their disposal with which to embezzle funds, steal property, and forge documents. For the fidelity bond professional, the question of immediate concern is how, if at all, coverage for losses caused by such e-commerce crimes will be impacted.

In all likelihood, the actual coverage analysis in most claims will not be directly affected. This primarily is due to the fact that the majority of claims under either the FIB or CCP involve employee dishonesty. And, while electronic commerce certainly increases the way in which employees can embezzle, the primary coverage questions will remain the same: whether the insured’s loss was caused by an employee who acted with the manifest intent to cause the insured to sustain a loss. The fact that the employee used a computer to facilitate his or her embezzlement will have little, if any, direct impact on the analysis of coverage. On the other hand, interesting questions likely will arise under other parts of the bond, particularly Insuring Agreements (D) and (E) of the FIB, providing potential coverage for losses caused by the forgery or alteration of certain types of documents. For instance, can there ever be a forgery of an electronic signature? And, is there an actual “original” of an electronic document that an insured actually can “possess”? The following discussion analyzes the potential impact of E-Sign on the various sections of the FIB and Commercial Crime Policy.

A. EMPLOYEE DISHONESTY CLAIMS

Insuring Agreement (A) of the FIB provides, in pertinent part, as follows:

Loss resulting directly from dishonest or fraudulent acts committed by an Employee acting alone or in collusion with others.

Such dishonest or fraudulent acts must be committed by the Employee with the manifest intent

- (a) To cause the Insured to sustain such a loss; and
- (b) To obtain financial benefit for the Employee or another person or entity.²¹¹

A similar insuring agreement is found in the CCP.²¹²

The primary issues typically arising in an employee dishonesty claim are: (1) whether a loss was incurred; (2) whether such loss was caused by an Employee who acted dishonestly; and (3) whether that Employee acted with the manifest intent to cause the insured to sustain a loss and to obtain a benefit for himself or another person or entity. Analysis of these issues will not change in claims involving e-commerce losses. For instance, if an employee steals her employer's "signature" and uses it to purchase goods or otherwise to enter into contracts for her benefit at the expense of her employer, one of the first questions to be answered is whether the insured actually sustained a loss as a result of the signature theft. Analysis of this issue is no different than if the employee had entered into unauthorized contracts using an actual "pen and ink" signature. Similarly, whether the employee's actions were dishonest, and committed with the manifest intent to cause her employer to sustain a loss and to obtain a financial benefit, also will be no different than if her crime was committed manually.

What about the disgruntled employee who somehow sabotages his employer's electronic business deal, either by going on-line and changing the terms of the transaction, or taking steps to altogether terminate the transaction? Or the disgruntled employee who infects her employer's computer system with an expansive virus? Questions here might be the calculation of the loss, and more importantly, whether the employee had the manifest intent to obtain a financial benefit. Once again, analysis of these issues is no different than in a claim where the disgruntled employee manually changed the terms of her employer's deal or physically damaged her employer's computer system.

Finally, another possible E-Sign loss might be the dishonest loan officer who now can facilitate "straw man" loans through the computer. Once again, however, the issues in this e-commerce loan loss would be no different than the typical dishonest loan claim,

²¹¹ FIB, Insuring Agreement (A).

²¹² CCP, Coverage Form A.

although it might prove more difficult for the bank to prove that the employee was the one “signing” the straw-customer’s loan documents.

B. FORGERY OR ALTERATION CLAIMS

Unlike Insuring Agreement (A), Insuring Agreements (D) and (E) seem ripe for debate in connection with e-commerce losses. As discussed previously in this article, authentication and attribution issues are not directly addressed by E-Sign, but instead are left to the ingenuity of the contracting parties. As a result, signature theft should be a real concern in e-commerce, particularly for less sophisticated businesses or those using computer systems without the appropriate level of security. Such theft inevitably will lead to claims under Insuring Agreements (D) and (E) of the FIB.

Insuring Agreement (D) of the FIB provides potential coverage for loss resulting directly from the forgery or alteration “on or in any Negotiable Instrument (except an Evidence of Debt), Acceptance, Withdrawal Order, Receipt for the withdrawal of Property, Certificate of Deposit or Letter of Credit,”²¹³ as well as for paying funds on the faith of written instructions or advices which bear a signature which is a Forgery or has been altered. Insuring Agreement (E) provides potential coverage for loss resulting directly from “the Insured having, in good faith, for its own account or for the account of others,” having “acquired, sold or delivered, or given value, extended credit or assumed liability, on the faith of, any “original” Evidence of Debt, or various other listed documents, which bear a signature which is a Forgery or which have been altered. In order for there to be coverage under Insuring Agreement (E) of the FIB, “[a]ctual physical possession of the [covered items] by the Insured” is a condition precedent to coverage. As noted above, several coverage questions are likely to arise in analyzing an e-commerce loss under these insuring agreements.

1. Forgery

The term “forgery” is defined by the FIB as the “signing of the name of another person or organization with intent to deceive; it does not mean a signature which consists in whole or in part of one’s own name signed with or without authority, in any capacity, for any purpose.”²¹⁴ The CCP does not specifically define forgery, and so individual state laws will be looked to under the CCP. For instance, in Texas the crime of forgery is broader than the definition set forth in the FIB, and includes executing any writing so that it purports to be the act of another with the intent to defraud or harm. “Writing” extends to any method of recording information, including “symbols of value, right, privilege, or identification.”²¹⁵

Under the FIB, the focus is on the signing of the name of another. Signing, of course, simply means to “affix one’s signature.”²¹⁶ And, a signature is defined as the “act

²¹³ FIB, Insuring Agreement (D).

²¹⁴ FIB, Definitions, § 1(s).

²¹⁵ TEX. PENAL CODE ANN. § 32.21(a)(b) (Vernon 1994).

²¹⁶ THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 1619 (2000).

of signing one's name."²¹⁷ It further is defined as a "distinctive mark, character, or sound indicating identity."²¹⁸ In e-commerce, the signature that is affixed to a document might or might not be the actual "name" of a person or entity. For instance, if a digital signature is used, it will be a set of "1s" and "0s," as opposed to someone's name. While the electronic signature obviously is intended to denote approval by the person who owns the signature, the mark does not duplicate the "name" of the person or entity. Or does it? Older dictionaries define the term "name" as "a word or combination of words by which a person, place or thing . . . is designated, called, or known."²¹⁹ More recent dictionaries define the term more broadly, such as "a word or words by which an entity is designated and distinguished from others."²²⁰

The above analysis highlights the potential problem in analyzing e-commerce losses under the typical language in most fidelity policies, including the FIB; that is, it was not drafted with e-commerce claims in mind. This alone arguably is one reason to deny coverage for such losses. Many insurance companies already are addressing this issue through riders. Additionally, the Surety Association of America is in the process of revising the FIB so that there can be no question but that the standard form language does not apply to losses caused through e-commerce, and it is preparing standard form riders to be used where a business desires coverage for losses relating to electronic transactions.²²¹ Of course, new bond forms are of no help to e-commerce claims under the current form of the FIB or CCP.

This analysis would not seem to be an issue under the CCP, where forgery is not specifically defined. Thus, in states such as Texas, it is arguable that the unauthorized use of an electronic signature can constitute a forgery given the broader definition of "signature," which includes symbols and other methods of identification. Under E-Sign, the term "electronic signature" is defined to mean "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."²²² Although not specified by the statute, an electronic signature would seem to include typed names, a "click-through" on a software program, dialog box, biometric measurements, a digitized picture of a handwritten signature, or a more complex, encrypted authentication system. Thus, an electronic forgery arguably can occur under the CCP where a thief steals an electronic signature and uses it as his own.

Setting aside the above issues, can there otherwise be a forgery of an electronic signature? What about the situation where an employee, as part of his job responsibilities, regularly uses his employer's electronic signature on documents? For example, the president of a mortgage company, E-Mortgage, completes a \$5 million warehouse loan arrangement with E-Bank to fund residential mortgages made by E-

²¹⁷ *Id.*

²¹⁸ *Id.*

²¹⁹ RANDOM HOUSE UNABRIDGED DICTIONARY 1276 (1993).

²²⁰ THE AMERICAN HERITAGE DICTIONARY OF THE ENGLISH LANGUAGE 1167 (2000).

²²¹ This information is based upon discussions with Edward G. Gallagher, General Counsel to the Surety Association of America, whom the authors thank for his insight on this issue.

²²² 15 U.S.C. § 7006(5).

Mortgage. Subsequently the president, now acting without authority, requests an increase in the line of credit, again using his employer's electronic signature to execute an amended promissory note in the amount of \$10 million. The president then absconds with the extra \$5 million. Clearly the president has used his employer's electronic signature without authority. However, is this a forgery? In this situation, isn't the president tantamount to E-Mortgage? If this is the case, then the use of the electronic signature is not the signing the name of another, but instead the signing of one's own name.

This issue was the impetus for the addition of the definition of forgery to the FIB as a result of the Second Circuit's decision in *Filor Bullard & Smythe v. Insurance Co. of North America*.²²³ In that case the president of a bank traded on his own account, paying for the trades with checks drawn on the account of the bank. Each check was signed by the president, followed by the printed legend "Auth. Sig." The issue was whether an unauthorized signature constituted a forgery under New York law. The district court, relying upon an earlier Second Circuit decision, *Fitzgibbons Boiler Co. v. Employers Liability Insurance Co.*,²²⁴ held that the bank president's unauthorized signatures on behalf of the bank did not constitute forgeries. The Second Circuit reversed, finding that while *Fitzgibbons* was correct when decided, New York had substantially revised its criminal law such that forgeries specifically includes unauthorized writings. The court also found that the term "forgery" in the bond was ambiguous because it was not defined, later leading to the addition of the definition of forgery to the standard form bond. In our example, of course, the FIB does define forgery. That definition does not include an unauthorized signature as a forgery.

There are a number of published decisions discussing a similar issue in the context of the unauthorized use of stamps on the back of checks. For instance, in *Elmer Fox & Co. v. Commercial Union Insurance Co.*,²²⁵ an employee of the insured was authorized to affix the insured's rubber stamp to the back of checks in order to deposit those into the company's bank account. The rubber stamp read as follows:

For deposit only.
Edsons Inc.
1701 Security Life Building
Denver, Colo. 80202

The employee then would have an authorized representative of the company sign their name below the stamp. He then would deposit the checks into authorized company bank accounts. However, at some point he began depositing the checks into bank accounts he opened in the name of the company without the company's authorization. The court found that the use of the rubber stamp endorsement "was neither 'unauthorized' or a 'signature.'"²²⁶ The court explained:

²²³ 605 F.2d 598 (2nd Cir. 1978).

²²⁴ 105 F.2d 893 (2nd Cir. 1939).

²²⁵ 274 F. Supp. 235 (D. Colo. 1967).

²²⁶ *Id.* at 239.

The plaintiff's statement of facts discloses that [the employee] was authorized to use the rubber stamp endorsement. The rubber stamp endorsement consists of the words "For deposit only" with the name and address of the company. This is not a signature. (See BLACK'S LAW DICTIONARY, 4th ed., and WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY.) The statement that the endorsements are "mechanically reproduced facsimile signatures . . ." is unsound for the same reason.²²⁷

Thus, in the court's view there was no forgery because the employee was authorized to use the stamp, and also because the typed name of the company on the stamp was not, in the court's view, a "signature."

*William Iselin & Co. v. Firemen's Fund Insurance Co.*²²⁸ is a similar case, although the employee who used the stamp in this case was never authorized to use it. The stamp, which was applied to various bills of lading and other delivery documents, read: "Lawson Trucking Co., Inc., J. Lawson, President."²²⁹ Firemen's Fund argued that the documents were not forged because they did not include a handwritten or facsimile handwritten signature. The court disagreed, finding that Firemen's argument would be a "hypertechnical definition of the word 'signature.'"²³⁰ The court went on to explain that the "stamped signatures of 'Lawson Trucking Co., Inc., J. Lawson, President' affixed to the bills of lading and delivery documents were forged by an employee of Lawson Cotton since the stamp was being so utilized without the knowledge or consent of Jordan Lawson."²³¹ Thus, in a situation where the employee was never authorized to utilize the stamp, a forgery was found. On the other hand, the court's explanation for its decision seems to imply that a forgery might not have been found if the employee also was authorized to use the stamp under certain circumstances, as was the case in *Elmer Fox*.²³²

These two cases arguably are indistinguishable from a claim in which an employee or other person misuses the electronic signature of a company. In the case where the employee is authorized to use the electronic signature for certain purposes, but then misuses it, this arguably would not be a forgery. On the other hand, it is arguable that where the employee was never authorized to use the electronic signature, or in the case where a non-employee steals an electronic signature, this is a forgery, assuming that the electronic signature constitutes a "name."

2. Possession of an "Original"

Insuring Agreement (E) provides potential coverage for loss caused by the forgery of certain instruments. In order for there to be coverage, the insured must establish that it acted on the faith of an "original" of the document. In order to establish that it acted on the faith of such original, it also must establish that it had "[a]ctual physical possession"

²²⁷ *Id.* at 239-40.

²²⁸ 501 N.Y.S.2d 846 (N.Y. App. Div. 1986).

²²⁹ *Id.* at 848.

²³⁰ *Id.* at 849.

²³¹ *Id.*

²³² 275 F. Supp. 235.

of the original. Understandably, courts have read the original and possession requirements together.²³³ In the context of Insuring Agreement (E), courts have defined an “original” to be “the first copy or archetype; that from which another instrument is transcribed, copied, or imitated.”²³⁴ The interpretation of the term “original” as used in the FIB has been quite literal.²³⁵ Thus, photocopies are not originals within the meaning of the FIB.²³⁶

Returning to the example above, assume that the warehouse agreement requires E-Mortgage to submit the original residential promissory note and related loan documents to E-Bank, which is out of state, prior to E-Bank funding any of the residential mortgage loans pursuant to the warehouse agreement. In order to facilitate business, the loan documents all are forwarded electronically. E-Bank funds the full \$20 million in loans, only later to learn that, while valid loans were made by E-Mortgage, E-Bank and several other lending banks each extended credit for the funding of such loans, all receiving the same electronic loan documents as collateral for the loans. As a result, all but the first lender lost all amounts funded.

Two questions arise in this scenario. First, were the loan documents sent to E-Bank actual “originals”? Similarly, did E-Bank “physically possess” the loan documents. As discussed previously, the transferable records provision of E-Sign²³⁷ impacts these issues. Under this section of E-Sign, if a person has “control” of a transferable record in a secure manner, as delineated in subpart (c) of the section, then he is considered a “holder” of the note just as he would be under section 1-201(20) of the U.C.C.²³⁸ And, this section also seeks to equate an “authoritative copy” of the transferable record with an “original.”²³⁹ Yet, can any version of an electronic document, other than the true “original” version, ever be an “original”? Even an “authoritative copy” is a “copy,” particularly once it is transmitted to another, regardless of the safeguards put into place. Similarly, is “control” of an electronic document the same as actual “physical possession”?

This analysis is more than mere semantics. One important reason Insuring Agreement (E) requires that the insured have possession of the original of a document before extending credit upon it is to ensure that it is the only “holder” of the note, and also to allow the insured to examine the note and other loan documents in order to reduce any risk of loss. Other than the ones at the Pentagon (and perhaps not even them) few, if any, computer systems in existence provide the same protection as the actual receipt and review of an original document.

²³³ See, e.g., *Hamilton Nat'l Bank v. Ins. Co. of N. Am.*, 557 A.2d 747, 751 (Pa. 1989).

²³⁴ *Id.* at 749 (quoting BLACK'S LAW DICTIONARY).

²³⁵ See Toni Scott Reed, *Bond Claims and the Impact of the Uniform Electronic Transactions Act, and Other Technological Developments*, 36 TORT & INS. L.J. 735, 766 (Spring 2001).

²³⁶ *Hamilton Bank*, 557 A.2d at 751.

²³⁷ 15 U.S.C. § 7021.

²³⁸ *Id.* § 7021(d); see U.C.C. § 1-201(20).

²³⁹ See, e.g., Wittie & Winn, *supra* note 35, at 316.

Similarly, an insured's "control" of an "authoritative copy" is not the same as its "possession" of an "original." Without a completely secure system a hacker always can steal the "authoritative copy," often without the "holder" knowing a theft has occurred. Even E-Sign seems to recognize this fact. Section 7021(d) provides that a person having control of a transferable record is a holder, and goes on to note that "[d]elivery, possession, and endorsement are not required to obtain or exercise any of the rights under this subsection."²⁴⁰ Thus, the drafters recognize that "control" truly is not the same as "possession." And, Insuring Agreement (E) similarly seems to answer this question by requiring "physical possession," as opposed to simply "possession," which might cause an ingenious insured to make a "constructive possession" argument, similar to the "constructive presence" argument discussed in the next section of this article.²⁴¹

While E-Sign is forward looking in its efforts to facilitate use of electronic promissory notes in the secondary mortgage markets, it does not ensure a system as safe as that contemplated by Insuring Agreement (E) of the FIB. Thus, the risk of an Insuring Agreement (E) loss would seem to be considerably greater in the e-commerce context. For this reason, coverage would not seem appropriate under the current wording of Insuring Agreement (E). There seems to be little question that such a claim would not be covered.

3. On Premises Losses

Insuring Agreement (B) of the FIB provides potential coverage for loss of Property from the insured's premises. It provides:

Loss of Property resulting directly from:

- (a) robbery, burglary, misplacement, mysterious unexplainable disappearance and damage thereto or destruction thereof, or
- (b) theft, false pretenses, common-law or statutory larceny committed by a person present in an office or on the premises of the Insured.

while the Property is lodged or deposited within offices or premises located anywhere.

The potential loss in the e-commerce context, of course, is a thief hacking into someone's computer system and gaining access to that person's electronic records or bank accounts. Does the premises of a bank suddenly expand in "cyberspace"? The answer would seem to be "no" just as the bank's premises do not expand due to the use of the telephone or the wire. For instance, in *Oritani Savings & Loan Ass'n v. Fidelity & Deposit Co. of Maryland*,²⁴² the insured bank suffered a loss as a result of telephone fraud, where a purported customer telephoned a bank officer and requested him to wire transfer money to certain accounts outside the bank. Analyzing coverage under the

²⁴⁰ 15 U.S.C. § 7021(d).

²⁴¹ FIB, Insuring Agreement (E).

²⁴² 989 F.2d 635 (3rd Cir. 1993).

second part of Insuring Agreement (B), the court found that Insuring Agreement (B) allowed the perpetrator of the fraud to be “constructively present” at the bank. The Third Circuit reversed, finding that the language of Insuring Agreement (B) was clear and that the thief actually had to be physically present in the insured’s offices for coverage to be available.²⁴³

Similarly, in *Southern National Bank v. United Pacific Insurance Co.*,²⁴⁴ the bank sustained losses as a result of a fraudulent securities scheme. The loss arose because the bank wire transferred \$2.8 million from its North Carolina office to its securities broker’s bank account in New York, bypassing third-party safekeeping arrangements that it ordinarily used. The bank made the transfer after it received a telephone call from the broker, asking the bank to make the direct transfer so that the funds could be immediately used to purchase securities for the bank. The funds disappeared and the securities were never purchased for the bank.

The policy at issue provided potential coverage for losses resulting directly from theft by a person who either was present in an office or on the premises of the insured, or on the premises in which the Property was lodged or deposited.²⁴⁵ The court concluded that the bank could not support its claim because the dealer did not use false pretenses to obtain the property in question while he was at the bank’s offices or while the dealer was on the same premises where the bank’s money was deposited.²⁴⁶ The bank argued that the funds had been obtained by false pretenses and that the money was constructively on the broker’s premises when it was deposited in the broker’s New York bank account. The bank further argued that, although the broker was not physically present at the bank, he should have been constructively deemed to be there. The court rejected the insured’s arguments, and emphasized the important element before coverage was the actual physical location of the thief in relation to the location of the property in question.²⁴⁷

Similarly, the thief who steals a company’s electronic signature, or otherwise causes a loss due to electronic larceny, is not “present in an office on the premises of the Insured,” any more than the thieves in *Oritani Savings*²⁴⁸ or *Southern National Bank*.²⁴⁹

a. System Damage Due to Hackers. The risk of loss from a computer hacker is present regardless of whether a company is transacting business electronically. Thus, whether there is coverage for such a loss under either the FIB or the CCP is better covered elsewhere. However, because E-Sign at least indirectly increases the risk of loss, this subject is briefly touched upon.

For purposes of Insuring Agreement (B), an ingenious insured might argue that a hacker actually is on the insured’s premises if he or she is in the insureds computer

²⁴³ *Id.* at 642.

²⁴⁴ 864 F.2d 329 (4th Cir. 1989).

²⁴⁵ *Id.* at 330.

²⁴⁶ *Id.* at 331.

²⁴⁷ *Id.* at 333.

²⁴⁸ 989 F.2d 635.

²⁴⁹ 864 F.2d 329.

network. In attacks known as “denial of service,” the objective is to disable the target system without necessarily gaining access to it.²⁵⁰ A common denial of service crime occurs when an Internet Service Provider's central computer, or server, is intentionally flooded with e-mails (“mail bombings”) that “bring it down,” or freeze it.²⁵¹ As a result, customers using the ISP cannot gain access to the Internet and thus are denied service.²⁵²

Similarly, some hackers may use the access to a web site as a vehicle to hack further into a company's computer system where they can steal sensitive pass-words, alter web sites, copy credit card numbers, plant damaging programs, and create "back doors" which would allow the hacker to re-enter the system at a later date.²⁵³ Other hackers plant malicious codes, such as viruses, worms, logic bombs, or Trojan horses, which infect a computer and cause damage to it without the user realizing until it is too late. Can this vandalism or malicious mischief be the cause of loss of “books or account and other records, whether recorded in writing or electronically,” which are included within the definition of Property covered by Insuring Agreement (B).²⁵⁴ What about damage resulting from subsequent malfunctions of computer controlled HVAC or fire protection systems? In these cases, although the original act occurred off site, the damage to the insured's property clearly would occur onsite.

The CCP, as well as non-standard form fidelity bonds issued by various companies, include coverage forms for various types of computer fraud. Loss as a result of system damage caused by a hacker might or might not be covered, depending upon the wording of these various coverage forms. Once again, this topic is beyond the scope of this article, other than to emphasize that the coverage form involved must be studied carefully because the various forms vary greatly.

V. Conclusion

The Electronic Signatures in Global and National Commerce Act is a prime example of the mercurial nature of commercial business. Just as the notary public now is accepted where only a wax seal once would suffice, and the efficiency of facsimile transmissions has caused us to forget the days of the Pony Express, business now must confront the reality of electronic commerce. Fear of technology is no longer a valid defense.

²⁵⁰ See Mann & Roberts, *supra* note 166, at 363.

²⁵¹ *Id.*

²⁵² *Id.*

²⁵³ *Id.* In light of these recent security breaches, the results of a study conducted by the Information Technology Association of America in April 1999 should come as no surprise. See Millennium Digital Commerce Act of 1999: Hearing on S.761 Before the Senate Comm. on Commerce, Science and Transportation, 106TH CONG. (1999) (statement of Harris N. Miller, President, Information Technology Association of America). Measuring the perceptions of top executives and their customers from across the information technology industry, the study found that 62% of respondents believed lack of trust was the primary barrier to e-commerce and that specific obstacles included privacy protection (60%), authentication (56%), and security (56%). See *id.*

²⁵⁴ FIB, Definition (p).

As with any innovation, E-Sign may create as many problems as it solves. Thus, it is important to become familiar with the pertinent technology in its virtual infancy, before the learning curve becomes too steep. Likewise, it is just as important to spot the legal issues as it is to know the solution because, in many cases, there is no absolute right or wrong answer. The fidelity bond's role in global commerce is not diminished by E-Sign, but it must transcend its historical focus on physical documents and outmoded forms of communication. Likewise, by reapplying many of the same legal principles that have been relevant for decades, the fidelity bond e-practitioner can stay afloat in the stream of electronic commerce.