

**FOURTEENTH ANNUAL
SOUTHERN SURETY AND FIDELITY CLAIMS
CONFERENCE**

**New Orleans, Louisiana
APRIL 10-11, 2003**

A (VERY) SHORT COURSE IN E-FIDELITY

PRESENTED BY:

**GREGORY R. VEAL, ESQ.
BOVIS, KYLE & BURCH, LLC
53 Perimeter Center East, 3d Floor
Atlanta, Georgia 30346-2298
Ph. (770) 391-9100
FAX (770) 668-0878**

A (VERY) SHORT COURSE IN E-FIDELITY

Consumer and commercial transactions involving computers and the Internet have increased exponentially in the past few years and show no sign of slowing. Many who deal with the commercial crime policy, the financial institutions bond, and other similar coverages have wondered when those e-commerce transactions, intersecting with traditional fidelity coverages, would result in unprecedented claims. So far, losses in cyberspace have not resulted in a flood of novel demands for payment under fidelity policies. Even so, recent conferences and publications demonstrate that the industry's curiosity remains strong.¹

What follows is a general discussion of the two primary statutory schemes that may come to impact fidelity coverages and the manner in which that impact may occur. Very little can be said with certainty at this early point in the development of e-commerce law, and some predictions previously made already have been called into question.² For now, the most practical goal is familiarity with the new landscape of enforceable electronic transactions and some of the issues it raises in the fidelity context.

UETA and E-SIGN: Bits of Paper or Bits and Bytes Are (Mostly) the Same

In 1999, the National Conference of Commissioners on Uniform State Laws drafted the Uniform Electronic Transactions Act and began working toward its adoption in all American jurisdictions. The uniform act, known as "UETA," is over 50 pages long, somewhat complicated in what it does and does not say, and has proven controversial with consumer groups.³ Because UETA was not taking hold in the states as quickly as some wanted, in 2000, Congress enacted the Electronic Signatures in Global and National Commerce Act, "E-Sign," which became effective about 18 months ago. E-Sign is only 15 pages long and is preferred by consumer groups because of express protections against potential abuses. It is intended primarily as an overlay statute to fill the gap where a state has not adopted UETA. The purpose of both acts is the same: to make most electronic signatures and transactions just as effective as if they had been done the old-fashioned, pen-and-paper way.

The Uniform Electronic Transactions Act

UETA, despite its length, is simple at the core. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form or an electronic record was used in its formation. If a record is required legally to be in writing or some act requires a signature, an electronic record and signature satisfy that legal requirement.⁴ UETA applies only when the parties to the transaction so agree, although agreement may be inferred from "the context and surrounding circumstances, including the parties' conduct."⁵ The parties also may vary the provisions of the act by agreement.

UETA does not displace a state's law of contracts or statutory recognition of and requirements for digital signatures.

[T]he purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a

general contracting statute—the substantive rules of contracts remain unaffected by UETA. Nor is it a digital signature statute. To the extent that a State has a Digital Signature Law, the UETA is designed to support and compliment [sic] that statute.

.....

. . . Specific areas of deference to other law in this Act include: (1) the meaning and effect of “sign” under existing law, (2) the method and manner of displaying, transmitting and formatting information in Section 8, (3) rules of attribution in Section 9, and (4) the law of mistake in Section 10.⁶

Among other areas excluded from the act’s scope, the Uniform Commercial Code is excepted from the effect of UETA other than Sections 1-106 and 1-207 and Articles 2 and 2a. The drafters specifically noted that Articles 5, 8, and 9 of the UCC already provide for electronic transactions,⁷ so UETA is not necessary in those areas either for enforceability or for uniformity. The inclusion of the UCC’s provisions on sales within UETA was necessary and assures that both commercial and consumer sales transactions may be accomplished electronically.

Although Articles 3 and 7 of the UCC are not included in UETA’s scope, Section 16 of UETA essentially incorporates those articles’ negotiability provisions for notes and documents of title. Such instruments created or signed electronically are effective and can be transferred to a holder in due course as long as the parties to the transaction so agree. Instruments that start out as paper cannot be converted into electronic form and then destroyed, which would raise issues concerning the true original and possible replacement instruments.⁸

Safeguards are required to make sure only one version of the electronic note or document of title is considered the “original” which is under only one entity’s control (as the electronic equivalent of “possession”). Leaving it to IT developers to come up with the products and methods, Section 16(c) of UETA requires the following:

- (1) a single “authoritative copy” of the transferable record that is unique, identifiable, and [with the limited exceptions below] unalterable;
- (2) that copy identifies the person with control—either the original recipient or the most recent transferee;
- (3) that copy is communicated to and maintained by the person with control or that person’s designated custodian;
- (4) the person with control is the only one who can transfer or assign the authoritative copy;
- (5) any version other than the authoritative copy (i.e. the original) is readily identifiable as a secondary copy; and

- (6) authorized or unauthorized revisions are readily identifiable.

Section 16 extensively refers to the UCC's provisions on negotiable instruments to make clear that UETA simply allows the same transactions, with the same rights and liabilities, to be accomplished electronically instead of on paper. In an important, express exclusion from the act, though, checks are not covered, because the commissioners thought electronic checks would be too disruptive to an unprepared banking industry. Without systems either in place or soon to be available to the industry, allowing "e-checks" would have required UETA to establish procedures and safeguards "beyond the ability of this Act to address."⁹

To make electronic transactions as effective as paper transactions, UETA had to overcome the distance that computers and the Internet create between actor and action. A party signing a contract applies ink to paper, often before witnesses or a notary public or even in the presence of the other contracting parties. Electronic transactions, on the other hand, may occur without the parties ever having communicated previously or knowing each other, much less ever having seen each other. Pushing buttons on the telephone to accept or reject options on a computer system, clicking buttons on a website, or sending or replying to an e-mail can establish transactions that UETA intends to have legal effectiveness. Even computer-to-computer transactions without direct human intervention or review are intended to be enforceable.

To accomplish these goals, UETA addresses attribution and automated transactions. Attribution is how one contracting party can rely on the electronic signals received as being the binding act of the other party. Section 9 of UETA provides that an electronic record or signature is attributable to a party if the recipient can show, "in any manner," that it was the act of the sender. That broad showing may include "the efficacy of any security procedures" that tie the act to the apparent actor. If a transaction requires a password to access the portion of the website at which the customer can click to contract, the use of the password assigned to that customer is evidence of the identity of the contracting party. On a simpler level, typing of the party's name or that of an employer is evidence that the act is attributable to the owner of that name.

Whether such evidence alone is sufficient to attribute the act is left to the finder of fact if the alleged actor denies having acted. If someone engages in "identity theft" and misuses my name and credit card number to make an Internet purchase, the use of that information is some, but certainly not conclusive, evidence that I was the purchaser. Contrary evidence that I reported the unauthorized transaction upon discovery, that other unauthorized transactions occurred about the same time, and that the address for shipment of the purchases was not my address should overcome the seller's attempt to attribute the electronic signature and transaction to me. All of the circumstances surrounding the transaction will be relevant, including the technical aspects of how the computer application operates and the record of Internet communications involved in the transaction.

Section 9 of the act also says that the same circumstances determine the legal effect of the electronic record or signature. Whether a particular electronic act has the legal result of binding the actor or creating a contract depends on "the context and surrounding circumstances at the time." Prior electronic dealings, Internet customs, norms in cyberspace,

website terms and conditions of use, and all of the more traditional circumstances will weigh in deciding the parties' intent to be bound and any other legal issues concerning the effect of the transaction.

One step even more removed from direct personal dealings are transactions conducted completely by automation. An example is where one company's computer is programmed automatically to send an e-mail order to a supplier when inventory falls below a certain level, and the receiving company's computer is programmed automatically to generate a purchase order e-mail in response. No human has acted directly or even reviewed and ratified the transaction, but UETA's Section 14 provides that the contract "may be formed by the interaction of electronic agents of the parties." Naturally, a transaction between a person and an "electronic agent" (i.e. computer or software application) is equally effective, as is a transaction where the person is acting for another, such as an employer. No immediate action by a person is required, though, to effectuate a legal transaction.

An employee could program the employer's computer to order, late at night, goods or services to be delivered to the employee's secret business address or directly to the employee's own business customers. The employee need not be present when the computer sends the order, no one need know that the order was sent, and the vendor's confirming e-mail purchase order may go (at the employee's electronic instruction) to some computer other than the employer's. None of those circumstances would invalidate the computer-to-computer transaction; the necessary intent to form a contract "flows from the programing and use of the machine."¹⁰

Because UETA is a uniform act that must be adopted by any jurisdiction to be enforceable, variations may be present in any particular version. Some states have added provisions about notarization of electronic records or concerning other formalities.¹¹ Also, UETA expressly dovetails with the adopting state's laws on the effect of contracts or other transactions, signature requirements, and record retention. Therefore, issues arising in any given jurisdiction must be analyzed only after taking into account all of the pertinent law, even if UETA has been adopted without amendment.

The Electronic Signatures in Global and National Commerce Act

E-Sign is a similar, overlapping statute but has the virtue of being federal law passed under Congress' power to regulate interstate commerce. Where UETA must be adopted by each jurisdiction and may be varied in the process, E-Sign became uniformly effective instantly in all 50 states, the District of Columbia, and all other U.S. possessions in October, 2001. One intent behind E-Sign, though, was to encourage the states to adopt UETA; to accomplish that intent, E-Sign expressly provides that it is preempted by any state's law that substantially is the uniform act. At this time, only 10 states have not enacted UETA in substantially the model form, and three of those have it under active consideration.¹² Eventually, only a handful of states will remain without either UETA or a substantially similar statute.

For those states, E-Sign either fills the gap (where no state law exists) or expressly provides that it preempts any substantially inconsistent state law as to any transactions in interstate commerce.¹³ As noted above, only a few states risk this preemption. One, New

York, has a similar but not identical Electronic Signatures & Records Act¹⁴ that gave rise to litigation over the validity of E-Sign's preemption. In *People v. McFarlan*,¹⁵ the police attempted to use a digital copy of the photographic lineup instead of the "original" as required by state statute. The court held that it did not have to decide between the statutes because the digital copy was acceptable under either E-Sign or the state's ESRA, but not before calling into serious question the constitutionality of E-Sign's preemption provision. The court wondered whether Congress had overreached its authority under the interstate commerce power in preempting any state's varying electronic transactions statute. While avoidable in that case, this argument probably will arise when the two statutes would yield different results concerning a substantial transaction. One day, when enough is at stake, such a dispute over the federal preemptive effect of E-Sign may have to be resolved by the Supreme Court.

For those few states without UETA, then, E-Sign presumptively establishes a similar framework for the validity of electronic transactions. Like UETA, it is simple at the core: a signature, contract, or record relating to such a transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form. Simply using an electronic record or signature in such a transaction cannot undermine it.¹⁶ Also, no one (except the government in noncontractual matters) is required to accept electronic records or signatures.¹⁷

Unlike UETA, E-Sign does not expressly require agreement by a party to accept an electronic transaction, unless that party is a consumer. E-Sign protects consumers by requiring consent confirmed electronically after disclosures to the consumer about the transaction.¹⁸ In this respect and several others,¹⁹ E-Sign is more consumer-friendly than UETA and therefore has been a basis for lobbying by consumer groups for state amendments to UETA as adopted. For nonconsumer transactions, E-Sign expects the party asserting the validity of the electronic record or signature to prove the other alleged party's agreement or acceptance to be bound electronically. Of course, even UETA allows proof of agreement or acceptance through evidence of all of the surrounding circumstances, so the omission of an express requirement for agreement or acceptance in E-Sign may make no practical difference.

E-Sign expressly provides that it applies to the business of insurance.²⁰ Health insurance or benefits and life insurance benefits cannot be cancelled or terminated using E-Sign's provisions, but other types of insurance (such as fidelity coverages) can be cancelled or terminated electronically.²¹ E-Sign also limits the liability of insurance agents and brokers who use electronic means to engage in transactions on behalf of their insurance customers, presumably including binding coverage, changing or cancelling policies, forwarding notice of discovery of loss or claim, etc. The agent or broker may not be held liable if the agent or broker

- (1) was not negligent, reckless, or intentionally tortious;
- (2) was not involved in developing or establishing the electronic procedures; and
- (3) did not deviate from the procedures set up by others.²²

The obvious negative implication is that an insurer that has "developed or established the electronic procedures," including allowing faxes, e-mails, or website interaction to be legally

effective, may be held liable if those procedures are deemed “deficient.”

E-Sign excludes from its scope all of UETA’s exclusions, and then some.²³ It excludes Arts. 3 and 7 of the UCC without including a provision to address transferability of all electronic records, as does UETA. E-Sign does save transferability for promissory notes and documents of title relating to loans secured by real estate, and the safeguards required to make such documents transferable are very similar to UETA’s.²⁴ By making no provision for negotiable instruments except where real-estate loans are involved, E-Sign’s scope in financial transactions is substantially less than UETA’s. The IT industry may or may not be able to meet the authenticity and attribution requirements of either UETA or E-Sign, given the capabilities of hackers to overcome access controls and other security features essential to establishing which is the “authoritative copy” and who e-signed it.²⁵

Recent Illustrative E-Cases

Both UETA as adopted in the states and E-Sign are too new to have generated many appellate decisions. A few cases, however, have illustrated some of the issues and outcomes discussed above.

Last October, the Second Circuit affirmed the unenforceability of an arbitration clause contained in a “clickwrap” license in *Specht v. Netscape Communications Corp.*²⁶ The individual plaintiffs sued Netscape on several bases related to invasion of privacy because a product they downloaded installed “cookies” to monitor their use of the product. Netscape moved to enforce an arbitration clause that was contained on a scroll-down portion of Netscape’s website from which the product had been downloaded onto the individual plaintiffs’ computers. Because the scroll-down screen came after the “download” button, so that the plaintiffs could obtain Netscape’s product without being required to scroll down and view the arbitration clause, both courts held that the plaintiffs were not bound by that clause.

The circuit court applied California law, although the case was filed in New York, and California’s version of UETA varies substantially from the uniform version, so E-Sign may apply.²⁷ That issue did not arise, since all parties agreed that the plaintiffs’ clicking on the download button constituted an electronic signature for purposes of creating an enforceable contract. The very cookies, or electronic identification tags, that caused the plaintiffs to sue Netscape were the means of attributing the contracts to those plaintiffs. The case turned on the legal effect of the plaintiffs’ button-clicks—to what did they agree? Applying a “reasonably prudent offeree” standard, the court held that, in the

emergent world of online product delivery, pop-up screens, hyperlinked pages, clickwrap licensing, scrollable documents, and urgent admonitions to “Download Now!” . . . [w]e are not persuaded that a reasonably prudent offeree in these circumstances would have known of the existence of license terms.²⁸

The court also noted that, while failing to read a paper contract may be no excuse, an exception to this rule is “when the writing does not appear to be a contract and the terms are not called to the attention of the recipient.”²⁹ That exception was held to apply in *Specht*.

At the end of last December, the Seventh Circuit applied Illinois' common law to an e-mail sent before E-Sign was effective and held that an employee's name in her e-mail to Hasbro Corporation was her employer's signature that satisfied the UCC Art. 2 statute of frauds.³⁰ The battle was about whether the parties had a contract in light of a disagreement over the quantity that the manufacturer, Cloud Corp., was to sell Hasbro. Judge Posner stated that, had E-Sign been effective at the time of the e-mail, it would have disposed of the question. Regardless, Illinois' common law and cases construing its version of the UCC established that the writing necessary to satisfy the statute of frauds need not be signed in handwriting and that a name typed on an e-mail could be sufficient. The court noted that the Eighth Circuit has "tugged the other way" on the question of e-mail signatures, but that decision also involved the absence of a material term of the purported agreement.³¹

Judge Posner added an interesting comment as an aside:

It is not customary, though it is possible, to include an electronic copy of a handwritten signature in an e-mail, and therefore its absence does not create a suspicion of forgery or other fraud--and anyway an electronic copy of a signature could *be* a forgery.³²

The courts apparently share the skepticism of some commentators in the infallibility and security of electronic records and signatures.

Less than two months ago, a district judge in Maine followed *Cloud Corp. v. Hasbro, Inc.* and held that Maine will accept a name on an e-mail as a signature, for purposes of the statute of frauds, in *Roger Edwards, LLC v. Fiddes & Son, Ltd.*³³ The parties, located in Maine and England, engaged in commercial transactions for years without formal written contracts but with a number of e-mails addressing their dealings. The court noted that its holding was based on a prediction of what the Maine courts would do and was consistent with E-Sign. Without explanation, the court did not mention Maine's version of UETA, adopted in May, 2000, or apply it to the e-mails at issue that all were sent and received after that date. Perhaps no one thought to mention UETA to the judge.

Finally, two cases from Florida wrap up this brief survey. In *Florida Department of Agriculture and Consumer Services v. Haire*,³⁴ landowners challenged a magistrate's issuance of search warrants (looking for canker-worm infestation) for, among other reasons, being signed electronically. Although Florida had enacted UETA, with express provision for governmental records to be signed electronically, the court did not mention Florida's statute. Instead, the court held that no Florida law prohibits electronically signing warrants in the magistrate's discretion.³⁵

In *Toca v. State*,³⁶ the *pro se* plaintiff refused to sign any documents filed with the court, other than to type "/s/ Jesse Toca (intended as original signature)" at the bottom of the page. The plaintiff contended that his religion (unspecified, but based on the Old Testament portion of the Bible, King James Version) forbid him to take any oath, and signing court documents had the effect of taking an oath before the court. The court ordered that he sign or have all unsigned documents stricken. One argument advanced by the plaintiff was that Florida's 1996 e-signature statute made electronic signatures valid. Again, without mentioning Florida's 2000

version of UETA as having superseded the 1996 statute, the court simply noted that Mr. Toca's typewritten name was not electronic and so was not made a "signature" by the 1996 statute.³⁷

How UETA and E-Sign May Affect Fidelity Coverages

Coverage Form or Insuring Agreement A—Employee Dishonesty

Both the crime policy and the FIB have similar definitions and coverage of employee dishonesty. The new laws concerning electronic signatures and transactions should have little effect on employee-dishonesty coverages, which depend on the employee's manifest intent to cause the loss and to obtain a benefit for the employee or someone else. *How* the employee implements that intent almost never has been relevant, nor is it likely to become relevant despite the new and expanded techniques available to the employee with computers and the Internet under UETA or E-Sign. Pinning down and valuing a loss may become more technical, requiring experts in computers and the Internet to track down the dishonest transactions, but those are matters of investigation and fact. Dishonest employees who cause losses that would be covered if created with paper are just as likely to cause covered losses if accomplished electronically.

Coverage Form C and Insuring Agreements B and C—On Premises or In Transit

The FIB insures against losses of a wide range of property resulting from theft, larceny, and false pretenses occurring as the result of actions by a wrongdoer who was physically on the insured's premises. No court to date has addressed whether sending e-mail to or "visiting" a website hosted by the insured could be considered being on the premises (virtually speaking). Two cases have ruled that sending electronic signals through a telephone wire terminating at telephones on the insured's premises nevertheless did not make the wrongdoer "constructively present" for purposes of fidelity coverage.³⁸ Courts have no reason to depart from the analysis and results of those cases when faced with a wrongdoer who sends electronic signals through telephone wires or other cables terminating at computers on the insured's premises.

The FIB also covers loss or mysterious disappearance of "Property" while on the insured's premises. The crime policy has similar but narrower coverage for money and securities. "Property" under the FIB includes, among other types, money, securities, negotiable instruments, and documents of title.³⁹ When and how is an electronic record on the insured's premises? Is it there when residing in a web-hosting computer in the insured's offices but available to outsiders who have a password? What if the record actually resides on a web-server hosted by a third party under contract with the insured, although the world never knows who hosts the insured's website? If an "authoritative copy" of a transferable record mysteriously disappears from the insured's web-server and is negotiated at the insured's expense, was covered property ever on the insured's premises? UETA and E-Sign purport to give such electronic property essentially the same legal effect as paper instruments, but an insurer can determine whether paper was or was not located on the insured's premises when it mysteriously disappears.

Similarly, is an Internet Service Provider or web host either a "messenger" (under both

types of policy) or a “transportation company” (under the FIB) for purposes of electronic records? They convey those records just as surely as others convey paper, and the policies insure against loss while the property is in the custody of a messenger or transportation company. Once courts begin construing UETA and E-Sign’s mutual intent to equate the virtual with the tangible, we will see how far courts are willing to analogize electronic records to paper.⁴⁰

Coverage Form B and Insuring Agreements D and E–Forgery/Alteration

The crime policy does not define the term “forgery,” which therefore is left to be defined by applicable law. (As noted above, both UETA and E-Sign indicate that an electronic signature created without authority would be unenforceable, but they do not use the term “forgery.”) The FIB defines “forgery” to be

the signing of the name of another person or organization with the intent to deceive; it does not mean a signature which consists in whole or in part of one’s own names signed with or without authority, in any capacity, for any purpose.⁴¹

By the same reasoning that recently has led courts to hold that the sender’s name on an e-mail qualifies as a signature, putting someone else’s name on an electronic record without authority should be a forgery under the FIB definition and probably under most state and federal law. Even if the electronic signature is nothing more than a click of a button on a webpage, the clicker must be claiming to be someone identifiable in order to enter into an electronic transaction. If the clicker claims to be someone other than he or she is without authority to do so, the clicked button probably is a forged signature.

Alteration of an original is one of the areas addressed by UETA and E-Sign, which contemplate cyber-systems making such alteration of the “authoritative copy” impossible. As stated above, that contemplation probably is highly optimistic. If someone can obtain “control” of the authoritative copy and alter it into a new electronic record, most of the requirements of Insuring Agreement E of the FIB have been satisfied. However, that agreement expressly requires that the insured have “actual physical possession . . . as a condition precedent to the Insured’s having relied on the faith of such items.” The very use of the term “physical” contradicts the idea that Insuring Agreement E covers loss involving electronic records at all. If the courts reject that argument, at a minimum the insured should be required to prove that it had exclusive possession or control of the forged or altered “authoritative copy” that caused the loss.

Computer Fraud Coverages

Beyond the FIB and the crime policy’s traditional provisions are coverages specifically designed for loss involving computers. Coverage Form F of the crime policy states in part:

We will pay for loss of, and loss from damage to, Covered Property resulting directly from the Covered Cause of Loss.

1. Covered Property: “Money,” “Securities” and “Property Other

Than Money and Securities.”

2. Covered Cause of Loss: “Computer Fraud.”

“Computer Fraud” means theft directly involving a computer to accomplish the fraudulent transfer of covered property from the insured’s premises to anyone (other than a messenger) or any place outside the premises.⁴² Employee dishonesty is excluded, so that it must be analyzed under Coverage Form A. For wrongdoers other than employees using computers fraudulently to remove the insured’s covered property from its premises, Coverage Form F provides the intended basis for recovery of the insured’s loss.

The limiting factor in this coverage primarily is the definition of “Covered Property.” “Money” is currency or coin; “Securities” includes negotiable and nonnegotiable instruments and other contracts representing money or other property; and “Other Property” must be tangible.⁴³ These limited classes of property that must be removed fraudulently from the insured’s premises by use of computer should limit the claims that actually are covered. An example, and the only known case construing this coverage form, is *Royal American Group, Inc. v. ITT Hartford*,⁴⁴ where an unidentified thief stole the insured’s security code that allowed unlimited long-distance telephone calls to be made over its “800” network. The trial court held that the thief had damaged the insured’s “securities,” i.e. its contracts with the telephone companies, and granted summary judgment to the insured, but the court of appeals reversed. In doing so, the court held that unauthorized long-distance charges cannot be characterized as “negotiable and nonnegotiable instruments or contracts representing either ‘money’ or other property,” quoting the crime policy definition.

Lloyd’s of London also has written at least one relevant coverage, the “Electronic All Risk Policy.” That policy covered “loss or damage to Electronic Securities ‘held by the Insured in any capacity or for which the Insured is legally liable’ from the fraudulent input of data into [the Insured’s] computer system and other similar acts.”⁴⁵ The existence and availability of such separate coverage bolsters the argument that the FIB never was intended to and does not cover loss involving electronic records such as those given validity by UETA and E-Sign.

Conclusion

The volume of e-commerce is growing, new laws are being enacted and challenged on a month-to-month basis, and commentators and courts are not in agreement on the issues that face fidelity carriers dealing with electronic transaction losses. Even when presented with facts falling under UETA or E-Sign, courts and apparently parties have missed the applicability of those laws. Perhaps some intriguing claim even now is winding its way through litigation toward a reported decision that will clarify the speculation on how electronic transactions and fidelity coverages mix. Even so, the complexities and unintended consequences of combining these two areas of commerce will give the judges and writers headaches for years to come.

Gregory R. Veal

ENDNOTES

1. The fidelity program at the 2001 ABA Midwinter Meeting of the Tort & Insurance Practice Section's Fidelity & Surety Law Committee was entitled, "Fidelity Coverage in the Age of E-Commerce." Six papers were presented on the topic. The October, 2002 Fall Meeting of the Fidelity Law Association included the topic, "The Electronic Signatures in Global and National Commerce Act: A Fidelity Bond Professional's Guide to E-Sign." VIII FID. L.J. 1 (2002). Much of the general information and background in this paper may be found in more detail in those publications.
2. See discussion of E-Sign's preemptive effect on New York's nonconforming law, below at fns. 14-15 and accompanying text.
3. For a point-by-point comparison of E-Sign and UETA from Consumer Union's perspective, visit www.consumersunion.org/finance/compwc600.
4. UETA, § 7.
5. UETA, § 5(b).
6. UETA, Prefatory Notes, at 6-7.
7. *Id.*
8. UETA, § 16, Comment 2
9. *Id.*
10. UETA, § 14, Comment 1.
11. UETA, § 11, provides that notarization may be done electronically but does not change any jurisdiction's other requirements, such as a rule that the notary must be present when the signer does the act that constitutes his or her signature (even if that is a mouse-click). Arizona and Florida, for example, have modified their versions of UETA to address in more detail electronic notarization.
12. Massachusetts, Missouri, and Vermont currently have UETA under legislative consideration and may enact substantially similar statutes this year. Alaska, Georgia, Illinois, New York, South Carolina, Washington, and Wisconsin have no statute similar to E-Sign. Some of those, such as Georgia, had an electronic transactions statute on the books before UETA or E-Sign; in Georgia's case, the provisions were so similar that the state may simply accept preemption by E-Sign rather than go to the trouble to repeal and enact UETA.
13. 15 U.S.C. § 7002(a).
14. N.Y. State Tech Law (McKinney's Art. 57-A, §§ 101-109).
15. 191 Misc. 2d 531, 744 N.Y.S.2d 287 (2002).
16. 15 U.S.C. § 7001(a)(1).
17. 15 U.S.C. § 7001(a)(2).
18. 15 U.S.C. § 7001(c).
19. See footnote 3, *supra*.

20. 15 U.S.C. § 7001(f).
21. 15 U.S.C. § 7003(b).
22. 15 U.S.C. § 7001(j).
23. 15 U.S.C. § 7003, which excludes wills and trusts, family law matters, the same UCC provisions as UETA, court documents, most notices concerning utility services, right to possession of or loan liability for a primary residence, product recalls, and documentation accompanying hazmat.
24. 15 U.S.C. § 7021. Compare UETA's requirements for transferability contained in Section 16(c).
25. VIII FID. L.J. at 11 and fn. 71.
26. 306 F.3d 17 (2d Cir. 2002). Netscape's parent, AOL/Time Warner, also was sued.
27. California's statute, for example, omits UETA's Section 16, which allows for negotiable electronic records generally. Of course, E-Sign's limit on transferability to electronic records relating to real-estate loans may mean that the omission of Section 16 would not negate UETA's enforceability.
28. 306 F.3d at 31.
29. *Id.* at 30.
30. *Cloud Corp. v. Hasbro, Inc.*, 314 F.3d 289 (7th Cir. 2002).
31. *Id.*, citing *Toghiyany v. AmeriGas Propane, Inc.*, 309 F.3d 1088 (8th Cir. 2002), which stated that e-mails are not signed for purposes of Missouri's statute of frauds. Missouri has not yet enacted UETA, and E-Sign was not effective when the underlying facts occurred. The duration of the contract was missing from the e-mail in *Toghiyany*.
32. *Id.* at 296.
33. No. 02-105-P-DMC, 2003 WL 342993 (D. Me. Feb. 14, 2003).
34. No. 4D02-3315, 2003 WL 118257 (Fla. App. 4 Dist., Jan. 15, 2003), reh. denied (Feb. 17, 2003).
35. *Id.* at 17.
36. 834 So. 2d 204 (Fla. App. 2 Dist., 2002).
37. *Id.* at 206, fn. 4.
38. *Oritani Savings & Loan Ass'n v. Fidelity & Deposit Co. of Md.*, 989 F.2d 635 (3d Cir. 1993); *Southern National Bank v. United Pacific Insurance Co.*, 864 F.2d 329 (4th Cir. 1989).
39. A more complete list includes "Certificated Securities, Uncertificated Securities, Certificates of Deposit, Acceptances, Evidence of Debt, Security Agreements, Withdrawal Orders, Certificates of Origin or Title, Letters of Credit, insurance policies, abstracts of title, deeds and mortgages on real estate, and tangible items of personal property." FIB, Definitions, § 1(p). Not all of these items implicate electronic records for purposes of UETA or E-Sign.
40. As one commentator has noted, the FIB (Definitions, § 1(o)) defines "negotiable instrument" to require a physical writing and a manual signature. Toni Scott Reed, "Bond Claims in the E-Commerce World," 36 TORT & INS. L.J. 735, 760 and fn. 116 (2001). Both UETA and E-Sign say that parties must agree to use electronic records, which the insurer has not, and that the parties may vary the provisions

of the acts, which the policies arguably do. Nothing in UETA or E-Sign expressly overrides the agreement between the insurer and the insured concerning a requirement that covered property be on paper or otherwise tangible.

41. FIB, Definitions, § 1(s).
42. Crime General Provisions, (D)(3)(b). "Theft" is "any act of stealing." Crime General Provisions, (D)(3)(f).
43. Crime General Provisions, (C)(2), (3), and (4).
44. No. 16246, 1994 WL 14888 (Ohio App. 1994).
45. Securities & Exchange Commission v. Credit Bancorp, Ltd., 147 F. Supp. 2d 238 (S.D.N.Y. 2001).