First Draft on E-Sign
Jonathan Stern
Mail Box: 845

Electronic commerce is rapidly redefining this nation's economy. This year's revenues will generate about $490 billion in U.S. online purchases. It is also expected that by 2004, the United States will transact online sales reaching $3.2 trillion.[1] The rapid growth of the Internet has stimulated the government to take concrete steps toward creating an electronic commerce infrastructure. In its July 1997 report, "A Framework for Global Electronic Commerce," the White House presented the Administration's policies regarding the law of the Internet.[2] In this proposal, President Clinton explained that a major impediment to the growth of electronic commerce is the fact that the public is "wary of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions."[3] In turn, the Administration created a framework that would promote the continued development of e-commerce through encouraging the private sector to lead and help create "a uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide."[4]

The Framework identifies several key principles that would guide in drafting these legal rules. First, parties should have the freedom to contract and order their contractual relationship as they see fit. Second, rules should be technology neutral and forward looking, that is, the rules should neither require nor assume a particular technology nor should it hinder the use of future technologies. Third, existing rules

---

[1] *The Forrester Brief, at* http://www.forrester.com/ER/research/brief.
[2] *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce, at* http://www.iitf.nist.gov/eleccomm/ecomm.htm.
[3] *Id.*
[4] *Id.*

should be modified and new rules adopted to the extent that it is necessary to support new technologies. Fourth, the process should involve the high-tech commercial sector as well as businesses that have not yet moved online. Through the application of these principles, the Administration hoped to achieve "a predictable, minimalist, consistent, and simple legal environment for commerce."[5]

The principles contained in the "Framework for Global Electronic Commerce" were applied in the Electronic Signatures in Global and National Commerce Act ("E-Sign").[6] The Act, which was signed on June 30, 2000 but primarily took effect on October 1[7], permits the creation of legally enforceable electronic signatures, contracts, and other records that affect interstate or foreign commerce.[8] E-Sign is significant for commerce generally and electronic commerce in particular since it provides equal legal validity for electronic and paper based agreements. Since "[l]egal uncertainty is the antithesis of strong and efficient markets," it is believed that E-Sign will revolutionize businesses in the United States by providing legal confidence in an area where lawful certainty has been glaringly absent.[9]

This Note will provide a brief overview of E-Sign's content, scope and its application to electronic commercial transactions. The Note will then explain the debate over the propriety of E-Sign's federal preemption over existing state laws governing electronic commerce. It will also highlight differences between E-Sign and the Uniform

---

[5] *Id.*
[6] Pub. L. 106-229.
[7] Section 107 of E-Sign provides certain exceptions to the requirement that E-Sign take effect. For example, all requirements by federal or state statute, regulation or other law that records be retained take effect on March 1, 2001. *Id.* at § 107(b)(1)(A)-(B).
[8] *Id.* at § 101(a)(1)-(2).
[9] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the Subcomm. on Finance and Hazardous Materials of the House Commerce Committee,* 106th Cong. (June 24, 1999) (statement of Michael Hogan, Senior Vice President and General Counsel, DLJ Direct, Inc.).

Electronic Transactions Act ("UETA"), which the Act permits the states to adopt in place of E-Sign. The analysis then shifts to describing the consumer protections that E-Sign currently provides and the rationale underlying E-Sign's technology-neutral approach to electronic transactions. Given the difficulty in securing the private keys and passwords that are used to identify a contracting party from theft, this Note will argue that E-Sign insufficiently protects the unsophisticated consumer. To remedy this defect, the Note will advocate for a flexible technology-specific approach that utilizes certification authorities that can feasibly shoulder the risk of a stolen password or key in a manner similar to today's credit card companies.

I. CREATING AN ELECTRONIC CONTRACT AND SIGNATURE

A. Electronic Contract Defined

The provisions of E-Sign provide a basis for creating documents that are electronically signed, recorded and available for future reference. E-Sign broadly defines an electronic signature as "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."[10] The term electronic record "means a contract or other record created, generated, sent, communicated, received, or stored by electronic means."[11] Finally, the "term 'electronic' means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." Combined, these definitions inform us that parties can bind themselves contractually by means other than the traditional ink and pen.

[10] E-Sign, § 106(5).
[11] *Id.* at § 106(4).

A significant distinction between electronic commerce and paper-based commerce is that electronic transactions can instantly be executed between computers.[12] E-Sign facilitates this continued ease in consummating transactions by broadly defining the term "electronic signature." The speed with which contracts can be effected is similarly promoted by E-Sign's efforts to promote the freedom of contract between parties. To this end, E-Sign requires that consent to create an electronic contract is voluntary[13] and that interested parties define what procedures will create an authentic signature or contract.[14] These provisions help permit the application of an array of technologies that can bind parties to a contract through means other than traditional signatures.

B. Variety of Electronic Signatures Permitted by E-Sign

Perhaps the easiest method in creating a binding electronic signature under E-Sign would be to accept a contract by clicking "yes" on an icon on your computer screen.[15] An individual could also bind oneself to a contract by signing an e-mail with one's name or by typing an "X." Under the provisions of E-Sign, this signature could be enforced so long as both parties bound itself to the contract and it was agreed between the parties that the placement of one's name or an "X" would constitute one's intent to sign the contract.[16] For businesses interested in creating a more instantaneously binding agreement, however, more advanced technological approaches have been created. One

---

[12] Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce,* 588 PLI/PAT 401, 404 (2000).
[13] E-Sign § 101(b)(2) (The Act does not "require any person to agree to use or accept electronic records or electronic signatures . . . .").
[14] *Id.* at § 101(c)(1)(A) (An electronic record satisfies the requirement that information be in writing if "the consumer has affirmatively consented to such use and has not withdrawn consent.").
[15] Harris Ominsky, *Oops! I Just Clicked My Life Away,* THE LEGAL INTELLIGENCER, July 26, 2000.
[16] David W. Carstens, *Contracts Have a New Look Thanks to E-Signature Act,* TEXAS LAWYER, July 31, 2000.

common method of creating a valid signature is the "shared secrets" method. This method involves the use of passwords or credit card numbers to create the necessary intent that will conclude a transaction.[17] For example, one might purchase a novel by selecting the desired publication and then entering a credit card number to both pay for a book and manifest intent to be bound to the sale.

A more complex method of signing a contract is through biometric authentication. Biometric authentication procedures require that some physiological characteristic of a user be sampled and electronically retained in an individual's user profile. Therefore, when the user invokes the authentication procedure, the characteristic is measured again and compared with the reference profile. Whenever an individual successfully replicates the previously stored physiological characteristic, the signature and identity of the individual is authenticated.[18] For example, biometric technology can identify an individual through recognition of a fingerprint, signature, voice or iris.[19] Hence, to bind oneself to a contract, one might simply place one's hand on a specially designed platform. When an individual's handprint matches that of the previously stored print that identifies the user, a binding electronic signature is then immediately created.

The digital signature is another significant means of creating an electronic signature. Its popularity has even led some states, prior to the enactment of E-Sign, to narrowly confine legally cognizable electronic signatures to digital signatures.[20] Digital signatures involve the use of a private and public key pair that are usually purchased by a

---

[17] *See, e.g., The Impact of the New Federal E-Sign Act on New York Law,* NEW YORK LAW JOURNAL, Aug. 8, 2000.
[18] *See, e.g.,* Benjamin Wright, *Eggs in Baskets: Distributing the Risks of Electronic Signatures,* 452 PLI/PAT 63, 69-70 (1996) (detailing the application of PenOp, a security pen biometric technology).
[19] *Allowing Use of Electronic Signature Before the House Commerce Committee's Subcomm. on Telecommunications, Trade and Consumer Protection,* 106th Cong. (June 9, 1999) (statement of John Seidlarz, President and Chief Executive Officer, IriScan).
[20] *See, e.g.,* UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (1997) (Utah's Digital Signature Law).

sender and issued by a Certification Authority ("CA").[21] A CA can be created through a Public Key Infrastructure ("PKI") and is a trusted third party that checks and verifies the identity of the person requesting the key pair.[22] The private key that an individual receives is to remain secret and is not to be disseminated to anyone other than the key owner. The public key, on the other hand, can be made widely available and can be found by accessing a CA's public database.[23] The public-private key pairs are mathematically related such that a message decrypted with a private key can only be decrypted with a public key. Therefore, if a sender signs a document with his private key, the recipient can use the sender's public key and signature to confirm the authenticity of the document.[24]

The technology operates in the following way. If Alice wishes to send confidential information to Bob, Alice performs a mathematical computation on her document, known as a "hash" function, which creates a unique string of code called a message digest.[25] Because the message digest is based on the specific content of Alice's original document, any changes to the document would yield a different message digest. Alice then encrypts this message digest using her private key, attaches this digital signature to the end of the document, and sends the document to Bob.[26] When Bob receives Alice's message, he can independently run the same hash function on the original message to determine what the content of the original message digest should be.

---

[21] *See supra* note 11 *at* 416.
[22] *Id.*
[23] One article has explained that the public-private key set is similar to secret decoder rings that are found in boxes of cereal in that each ring only fits into its companion ring and no other. Daniel J. Greenwood & Ray A. Campbell, *Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication,* 53 BUS. LAW. 307, 311 (1997).
[24] *Id.*
[25] C. Bradford Biddle, *Misplaced Priorities: The Utah Digital Signature Act and Liability Allocation in a Public Key Infrastructure,* 33 SAN DIEGO L. REV. 1143, 1149 (1996).
[26] *Id.*

He then decrypts Alice's digital signature, using Alice's public key. If Bob sees that the message digest in Alice's decrypted digital signature matches the message digest that Bob calculated from the message of his own, then Bob knows that the information has not been altered and that the message could only have been sent using Alice's private key.[27]

II IMPORTANT E-SIGN PROVISIONS

A. Preemption

E-Sign provides that all state laws related to electronic signatures and contracts are preempted unless they constitute an enactment or adoption of UETA[28], *or* they specify alternative procedures that are technologically neutral[29] and are consistent with Titles I and II of the Act.[30] The principle that undergirds this provision is the presumed importance of uniformity among the states.[31] Proponents of preemption claim that differences in electronic signature laws are an impediment to the growth of e-commerce because parties are unwilling to risk entering into a contract online without nationwide certainty regarding its legality.[32] Indeed, should conflicting state laws exist, companies

---

[27] *Id.*

[28] E-Sign § 102(a)(1)(A). The National Conference of Commissioners on Uniform State Laws approved the Uniform Electronic Transactions Act in July 1999 as a body of legislation validating the use of electronic records and electronic signatures. *See* The Uniform Electronic Transactions Act, *available at* http://www.law.upenn.edu/bll/ulc/fnact99/1990s/ueta99.txt.

[29] States acting as market participants are exempted from having to take a technology-neutral stance. *Id.* at § 102(a)(2)(b). It stands to reason that this exception was instituted because a state engaged in an electronic transaction is inevitably forced to select a particular technology in conducting its transaction. *See Allowing Use of Electronic Signature Before the House Commerce Committee's Subcomm. on Telecommunications, Trade, and Consumer Protection,* 106th Cong. (June 9, 1999) (statement of Andy Pincus, General Counsel, U.S. Dept. of Commerce) (explaining that an earlier version of the Electronic Signatures bill that did not contain the above provision compelled the government to undermine its technology neutrality when having to choose one among competing authentication providers).

[30] *Id.* at § 102(a)(2). Note that the Act's other Titles, III and IV, respectively address the responsibilities of the Secretary of Commerce in promoting electronic signatures and the authority of the Commission on Child Online Protection to accept gifts. Also note that

[31] *See, e.g.,* 146 CONG. REC. S5215-02 (daily ed. June 15, 200) (statement of Sen. McCain).

[32] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the House Judiciary Committee's Subcomm. on Courts and Intellectual*

would be forced to customize their services to meet the requirements of each state.[33] This, in turn, can lead to having a disproportionate impact on smaller businesses by raising costs and making it difficult to serve customers on a cost-effective basis.[34] Finally, advocates of preemption conclude that it took nine years for the Uniform Commercial Code to be adopted, and even then, Louisiana and the District of Columbia did not adopt it entirely.[35] Similarly, the Uniform Securities Act which was first proposed in the 1950s and was revised in the 1980s, still has failed to provide uniform state securities laws.[36] Thus, history has demonstrated that it is unwise to simply wait for the nation to uniformly enact UETA. Instead, by requiring states to either adopt UETA or legislation that is significantly, if not entirely, similar to E-Sign, the U.S. will provide nationwide consensus regarding the legal validity of an electronic contract in a timely manner.

Opponents to the preemption clauses contained in E-Sign argue that the Act unnecessarily infringes upon states' rights. To begin, since the federal government is responsible in determining whether a state has complied with the statute, it is possible that every contract case involving uncertainty as to the validity or legal effect of an electronic signature could contain a federal question. This would necessarily result in federal involvement in areas of contract law that have traditionally been reserved for the

---

Property, 106th Cong. (Sept 30, 1999) (statement of Howard Coble, Chairman, Subcommittee on Courts and Intellectual Property).

[33] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the Subcomm. on Finance and Hazardous Materials of the House Commerce Committee,* 106th Cong. (June 24, 1999) (statement of Thomas C. Quick, President and Chief Operating Officer, Quick & Reilly/Fleet Securities, Inc.).

[34] *Id.*

[35] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the Subcomm. on Finance and Hazardous Materials of the House Commerce Committee,* 106th Cong. (June 24, 1999) (statement of M. Hardy Callcott, Senior Vice President and General Counsel, Charles Schwab & Co., Inc.).

[36] *Id.*

states.[37] Second, since E-Sign was partly motivated by a desire to respond to changing market conditions, preemption should be discouraged because states are more capable than the federal government in making swift adjustments to shifts in the market.[38]

To the extent that the preemption provisions were enacted in order to create a uniform system of laws, this argument is somewhat undermined by the fact that there are differences between E-Sign and UETA and that even states that adopt UETA may still be subject to E-Sign.[39] This has led the General Counsel at the U.S. Commerce Department to recommend that once the UETA is adopted by a state, E-Sign should become unnecessary and should "sunset," leaving the transaction to be governed by state law.[40] Some of these differences are explained below.

B. Differences Between E-Sign and UETA

Like the "Framework for Global Electronic Commerce," the Uniform Electronic Transactions Act was formed in order to create a system of uniform rules to govern transactions in electronic commerce.[41] UETA is substantially similar to E-Sign although they differ in two important ways.[42] First, UETA addresses the evidentiary value of

---

[37] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the House Judiciary's Committee's Subcomm. on Courts and Intellectual Property,* 106th Cong. (Sept. 30, 1999) (statement of Pamela Mead Sargent, National Conference of Commissioners on Uniform State Laws).
[38] *Id.*
[39] *Electronic Signature: Hearing on H.R. 1714, The "Electronic Signatures in Global and National Commerce (E-Sign) Act" Before the House Judiciary's Committee's Subcomm. on Courts and Intellectual Property,* 106th Cong. (Sept. 30, 1999) (statement of Andrew J. Pincus, General Counsel, U.S. Dept. of Commerce).
[40] *Id.*
[41] Summary of the Uniform Electronic Transactions Act, *available at* http://www.nccusl.org/uniformact_summaries/uniformacts-s-ueta.htm.
[42] There are a few minor differences between UETA and E-Sign that go beyond the scope of this Note. However, the chair of the UETA Drafting Committee has authored a more thorough description of these differences. *See* Patricia Brumfield Fry, *A Preliminary Analysis of Federal and State Electronic Commerce Laws,* ELECTRONIC COMMERCE & LAW REPORT, Jul. 12, 2000.

material that is in electronic form while E-Sign is silent.[43] Second, UETA and E-Sign provide different consumer protections.

Unlike E-Sign, UETA contains explicit provisions dealing with the attribution of electronic records or signatures. It also describes the type of evidence that can be used to prove the authenticity of a record or signature. UETA states that "[a]n electronic record or signature is to be attributed to a person if it was the act of the person."[44] This fact can be established by any relevant evidence, including "a showing of the efficacy of any security procedure" which helps to establish who attached the signature.[45] UETA also clarifies that the effect of a record or signature on the person to whom it is attributed is to be determined from the context and surrounding circumstances at the time of the creation, execution or adoption of the record.[46] Furthermore, § 13 specifies that electronic records cannot be denied admissibility solely because it is in electronic format. Since E-Sign states that it does not affect any legal requirements beyond those requiring "that contracts or other records be written, signed, or in non-electronic form," E-Sign does not have any equivalent provisions.[47] Instead, those states that do not adopt UETA and retain E-Sign will only discover the evidentiary value of electronic records through the process of litigation.

Perhaps the most significant difference in treatment between UETA and E-Sign is found in the manner in which the two statutes deal with consumer protection issues. Whereas the federal legislation requires considerable consumer protection requirements (as described below), UETA provides few, if any, explicit consumer protections. Instead,

[43] UETA, § 9.
[44] *Id.* at § 9 (a).
[45] *Id.*
[46] *Id.* at § 9(b).
[47] E-Sign, § 101(b)

UETA protects all contracting parties prohibiting either party from inhibiting another's ability to retain and store an electronic record.[48] UETA also preserves additional state requirements concerning the manner of posting and displaying records.[49] Lastly, like E-Sign, UETA does not apply the electronic record provisions to laws governing the creation of wills, codicils, testamentary trusts[50] and Uniform Commercial Code section 1-107 and 1-206 and Article 2 and Article 2A[51]. The consumer protection provisions for E-Sign, meanwhile, are far more extensive.

C. Consumer Protections

As described above, E-Sign differs from UETA in that the federal legislation focuses on ensuring consumer assent to transact electronically[52], while UETA emphasizes how parties are to comply with state consumer protections.[53] To begin, E-Sign requires that if a statute, low, or regulation requires that information be provided or made available in writing to a consumer, the use of electronic records is permitted upon compliance with detailed specifications and disclosures. Not only must the consumer formally consent to receive records in electronic form[54], but the party required to furnish the information must also:

(a) inform the consumer of any right or option to receive a record in nonelectronic form[55];
(b) inform the consumer of the right to withdraw consent to receive electronic notice and stating any consequences or fees upon termination[56];

[48] UETA, § 8(a).
[49] *Id.* at § 8(b).
[50] *See* E-Sign, § 101(a)(1) and UETA, § 3(b)(1).
[51] *See* E-Sign, § 101(a)(3) and UETA, § 3(b)(2).
[52] *See generally* E-Sign, § 101(c).
[53] *See generally* UETA, § 8 as described above.
[54] *Id.* at § 101(c)(1)(A).
[55] *Id.* at § 101(c)(1)(B)(i)(I).
[56] *Id.* at § 101(c)(1)(B)(i)(II).

(c) inform the consumer whether the consent is to a particular transaction or to a category of notices made available during the course of the parties' relationship[57];

(d) describe the procedures for withdrawal of consent and to update information that is needed to contact the consumer electronically[58];

(e) inform the consumer on how to obtain a paper-based copy of an electronic record and whether a fee will be charged[59];

(f) notify the consumer of the necessary hardware and software requirements for access to and retention of records;[60] and

(g) ensure that the consumer consents electronically or confirms electronically in a manner that confirms that the consumer can access information in the necessary electronic form.[61]

You should note that the Act provides that a failure to obtain electronic consent or confirmation of consent does not immediately deny the legal effectiveness, validity or enforceability of any contract entered into with the consumer.[62] As a result, it is possible that an electronic contract can be enforced even when a business subject to the above provisions fails to provide a consumer with the option to obtain records in writing. You should also note that these provisions do not require consumer consent before *all* electronic dealings; rather, these provisions only apply where the law requires that information be provided or made available in writing to a consumer.[63] This means that e-businesses that are not currently required to provide paper-based records, such as Amazon.com, are not obligated to obey any of these provisions.

Even though the provisions described above only apply to a small class of consumers, E-Sign also contains provisions that benefit consumers who do not fall under

[57] *Id.* at § 101(c)(1)(B)(ii).
[58] *Id.* at § 101(c)(1)(B)(iii).
[59] *Id.* at § 101(c)(1)(B)(iv).
[60] *Id.* at § 101(c)(1)(C)(i).
[61] *Id.* at § 101(c)(1)(C)(ii).
[62] *Id.* at § 101(c)(3).
[63] *Id.* at § 101(c)(1).

those clauses. For instance, E-Sign requires that court orders[64], notices regarding utility termination[65], and regulations governing adoption, divorce or other matters of family law[66] continue to be processed through paper-based writings. It also calls for a federal study of the extent to which the provisions of E-Sign benefit or burden electronic commerce while charging the Department of Commerce[67] and the Federal Trade Commission[68] to recommend how the Act should be altered in order to better protect consumers. The Act also permits a federal regulatory agency, following notice to the public and an opportunity for public comment, to exempt a category or type of record from the above requirements. However, the exemption can only be effected if it is determined to be necessary to eliminate a significant burden on electronic commerce *and* will not materially harm consumers.[69] UETA does not contain any similar or parallel provisions.

D. Technology-Neutrality

Both E-Sign and UETA forbid any state or federal statute from requiring a specific technology in conducting electronic transactions.[70] This "minimalist" approach is consistent with the principles enumerated in the "Framework for Global Commerce."[71] In addition, this approach relies on the market to decide what technologies will best

[64] *Id.* at § 103(b)(1).
[65] *Id.* at § 103(b)(2)(A).
[66] *Id.* at § 103(a)(2).
[67] E-Sign, § 105(a)-(b).
[68] *Id.* at § 105(b).
[69] *Id.* at § 104(d)(1).
[70] *See Id.* at § 102(a)(2)(A)(ii) forbidding states from "accord[ing] greater legal status or effect to the implementation or application of a specific technology or technical specification for performing the functions of creating, storing, generating, receiving, communicating, or authenticating electronic records or electronic signatures."
[71] *See supra* note 2.

facilitate electronic commerce.[72] Naturally, technology-neutrality is a position that most businesses gladly embrace.[73] Without the hindrance of any specific technologies, businesses are free to construct the methods with which to transact business with its customers. It is less clear, however, that technology-neutrality is in the best interest of the consumer since, in E-Sign, technology-neutrality is accompanied by the absence of any particular security measures or description as to who should assume the risk in the event of a security breach. As a result, it is quite possible that the consumer will suffer the greatest losses in the event that the privacy of an electronic transaction is compromised. While it is certainly noble to believe that businesses "will use security procedures because it is good business, not because the law gives special legal effect if they are used,"[74] it is unlikely that this will be the case. Instead, it seems more likely that businesses will make the minimum security precautions that are necessary to retain its core customer base while forcing the consumer to shoulder the losses in the event that security is compromised.

III CREATING A SAFE ENVIRONMENT FOR CONSUMER TRANSACTIONS

It is becoming commonplace to find newspaper reporting on yet another incident where a web site has been hacked or information has been stolen from a personal computer. In the past year, hackers have penetrated and attacked prominent web sites such as Amazon.com, Yahoo, and eBay.[75] Computer-savvy criminals have also stolen

[72] *See supra* note 12, at 434-35.
[73] Among the most ardent supporters of E-Sign included some of the largest companies in America such as Microsoft, America Online, American Express, DLJDirect, Citigroup, Oracle and American Express. *See* 146 CONG. REC. S5215-02, S5218 (daily ed. June 15, 200) (statement of Sen. McCain).
[74] *See supra* note 12, at 435.
[75] M.J. Zuckerman, Hackers, *Security Pros Call Web Attacks Vandalism: Consultants Ponder Motive,* USA TODAY, Feb. 11, 2000.

information contained on large computer databases containing personal information and then sold that information for a profit.[76] Moreover, personal information has even been lifted off of individuals' personal computers. Last year, for instance, a flaw in Microsoft Excel's spreadsheet program was detected, which permitted computer hackers to copy private files from a person's home computer without their even knowing it.[77]

In light of these recent events, the results of a study conducted by the Information Technology Association of America in April 1999 should come as no surprise.[78] In measuring the perceptions of top executives from across the information technology industry and their customers, the study found that 62% of respondents believed lack of trust was the top overall barrier to e-commerce and that specific obstacles included privacy protection (60%), authentication (56%), and security (56%). It is results like these that have confirmed the White House's belief that the public is "wary of conducting extensive business over the Internet."[79] It is unfortunate, however, that both the Framework and E-Sign is likely to fail to provide the consumer confidence that it aims to provide.

In recognizing the porous security protection that the Internet provides, members of the digital community have been exploring the technological means of providing security to participants in electronic commerce and have debated on how to allocate the risk in the event of a security breach. Through this inquiry, three core issues have been

---

[76] *See* Ann Cavoikian, *Identity Theft: Who's Using Your Name, available at* http://www.ipc.on.ca/web_site.eng/matter/sum_pap/papers/ident-e.htm.
[77] Martha Mendoza, *Warning for Web Surfers: Hackers Able to Steal Off PCs with Excel,* ARIZ. REPUBLIC, Jan. 6, 1999.
[78] *Digital Signature and Electronic Commerce: Hearing on S.761, The Millennium Digital Commerce Act of 1999 Before the Senate Committee on Commerce, Science and Transportation,* 106th Cong. (May 27, 1999) (statement of Harris N. Miller, President, Information Technology Association of America).
[79] *See supra* note 2.

identified as security risks: authenticity, integrity and non-repudiation.[80] This Note will focus on the element on authentication in electronic transactions. Namely, it will examine which party should bear the risk of financial loss when the authenticity of a signature is raised.[81] The following will describe and analyze three prominent approaches towards ensuring the authenticity, integrity and non-repudiation of an electronic record. This Note will then suggest a fourth approach that can both provide for secure transactions while allocating the risk of fraud or other security breach in a way that is both cost-effective and protective of the consumer.

A. The Technology-Neutrality Approach

One justification for the technology-neutral approach is the concern that technology can easily become obsolete, thereby rendering a technology-specific approach unsafe or inefficient.[82] It is also argued that it would be imprudent to require a specific technology when conducting electronic transactions before more is known about the actual practices of merchants and consumers in the e-commerce marketplace.[83] While the technology-neutral approach does create room for improvements in technology, E-Sign also permits the continuation of insecure electronic commercial transactions even when inexpensive and easily accessible alternatives are available.[84]

---

[80] *See, e.g., supra* notes 12, at 416 and 25, at 1146. Authentication relates to the problem of identifying the source or sender of a message and authenticating that it did indeed come from the sender. Integrity addresses the issue of proving that a message is complete and has not been altered since it was not. Non-repudiation relates to the risk that a sender may repudiate a record after another party receives it. *See supra* note 12, at 416.

[81] *See generally supra* note 25 (critiquing various model for allocating risk when privacy is compromised). Note that the security risks of authenticity, integrity and non-repudiation are often inseparable. Therefore, much of the following discussion is equally relevant to the other categories as well.

[82] *See supra* note 12 at 441.

[83] Jane Kaufman Winn, *Open Systems, Free Markets, and Regulations of Internet Commerce,* 72 TUL. L. REV. 1177, 1183 (1998).

[84] An argument has also been made that it should be against public policy to allow large commercial transactions to take place without a minimum technology-specific threshold requirement. *See supra* note 29.

Perhaps the most pressing problem with E-Sign is that it mandates technology-neutrality without creating guidelines for attributing responsibility when the authenticity of a signature is called into question. For instance, say that due to her own negligent behavior, Alice misplaces her secret password that results in a loss of $25,000 and ultimately her home. It is possible that in this situation, existing legislation and common law tort and negligence laws could be relied upon in determining responsibility.[85] However, existing case law has not determined whether Alice would be held liable in the event that she exercised reasonable care and, nevertheless, her password is stolen off of her computer. As a result, Alice will be forced to prove to the court that she did indeed behave with reasonable care.[86] Should Alice succeed in proving that her behavior was not negligent, court costs and attorney's fees will mean that she will still fail to recoup all of her money.

The Uniform Electronic Transactions Act provides a framework for attributing responsibility in the event that an electronic signature is forged or stolen.[87] UETA states that "[a]n electronic record or signature is to be attributed to a person if it was the act of the person."[88] Relevant evidence in establishing this fact includes any "showing of the efficacy of any security procedure" that helps to establish who attached the signature.[89] UETA also clarifies that the effect of a record or signature on the person to whom it is attributed is to be determined from the context and surrounding circumstances at the time of the creation, execution or adoption of the record.[90] Like E-Sign, UETA establishes

[85] C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace,* 34 SAN DIEGO L. REV. 1225, 1236 (1997).
[86] *Id.*
[87] UETA, § 9.
[88] *Id.* at § 9 (a).
[89] *Id.*
[90] *Id.* at § 9(b).

that, in both of the above scenarios, Alice would have the burden of proof in showing that she was not responsible for the stolen signature. Again, not only does she not have any guarantee that she can prove her innocence but she will also need the resources with which to hire competent counsel.

To conclude, E-Sign's technology-neutral approach shifts an inordinate amount of risk on the unsophisticated consumer. Given the increasing difficulties in providing a safe environment with which to transact online business, it is worthwhile to examine other models that can create greater consumer security and confidence.

B. The Utah Digital Signature Law Statute and the Open PKI System

In 1995, Utah[91] became the first state to adopt a full-fledged digital signatures statute that supported a Public Key Infrastructure.[92] The Utah legislation was based on the efforts of the American Bar Association's Information Security Committee, which, following a four-year collaborative effort between attorneys and technologists, published a set of Digital Signature Guidelines.[93] The model presented by Utah statute and the American Bar Association is referred to as the "Open PKI" business model. An open PKI model assumes that subscribers obtain a digital certificate from a CA that will securely link their identity to their public key for all, or at least many, purposes. Generally, "the certificate issued by the CA has no boundaries upon the class or set of relying parties who are entitled to rely upon it."[94] Thus, in an open PKI environment, a person could obtain a digital certificate and then use it for a transaction requiring a digital signature, including

---

[91] UTAH CODE ANN. § 46-3-101 (1996). The 1996 legislation was a revision of legislation that originally became effective in 1995.
[92] *See supra* text accompanying notes 19-27.
[93] A copy of the Digital Signature Guidelines can be downloaded as http://www.abanet.org/scitech/ec/isc/dsgfree.html.
[94] Charles R. Merrill, *The Accreditation Guidelines – A Progress Report on a Work in Process of the ABA Information Security Committee,* 38 JURIMETRICS J. 345, 349 (1998).

the ordering of goods online, signing legally binding agreements, and even filing documents with a government entity.[95]

In creating its PKI, the Utah law attempts to create greater certainty as to the authenticity of an electronic signature. The Act authorizes the state to act as the root certification authority and provides for the licensing of certification authorities by the state. It is assumed that this provision will create greater assurances as to the validity of an electronic signature. However, like the technology-neutrality proposal, the Utah strategy shifts an inordinate amount of risk onto the consumer. For instance, assume that Alice cannot memorize her private key and instead stores the information on a Smart Card.[96] Should a hacker succeed in identifying the methods used to control a private key, then an attacker should be able to forge Alice's key with great ease and cause Alice great financial hardship.[97]

The Utah Act provides Regrettably, the Utah Act provides that if a digital signature is verified by the public key listed in a valid certificate issued by a licensed CA, (a) the subscriber has accepted the corresponding certificate (and thus assumed the duty to exercise reasonable care to protect the key, (b) the digital signature is the digital

---

[95] *See supra* note 23, at 316.

[96] A Smart Card is similar to a bank or credit card and contains an encrypted digital signature. Individuals using smart-card technology have special chips embedded in their personal computers that can read the encrypted information. In completing a transaction, an individual can simply insert her smart card into her computer and activate the signature using a PIN number. *See, e.g.* Tyler Prochnow, *From 'John Hancock' to Retinal Scans: What is your Signature on the Internet*, E-COMMERCE, Jul. 2000. There are also many other ways that a private key can be stolen. For instance, one can steal another's identity and receive a digital certificate in that person's name; an employee of a CA responsible for issuing certificates can be bribed; or a disgruntled employee can steal a key and enter into beneficial commercial transactions; or a criminal could break the underlying algorithm to discover a CA's private key by analyzing the CA's public key.. *See, e.g. supra note* 25, at 1189; Michael J. Osty & Michael J. Pulcanio, *The Liability of Certification Authorities to Relying Third Parties,* 17 J. MARSHALL J. COMPUTER AND & INFO. L. 961, 967-68 (1999); .

[97] Given recent events, this process should not be as difficult as it seems. For instance, in as early as 1994, a Russian computer programmer removed $10 million from Citibank customer accounts after discovering the code that authorizes fund transfers. *See* David Gow & Richard Norton-Taylor, *Surfing Superhighwaymen: Banks Have Good Reason to Fear Thieves Who Hack Into their Secret Files,* THE GUARDIAN, Dec. 7, 1996.

signature of the subscriber listed in the certificate, and (c) the digital signature was affixed with the intention of signing the message.[98] Thus, when Alice's key is stolen, it is up to her to provide evidence to rebut the presumption that she authenticated the signature. Hence, by concentrating risk on the original holder of the private key, Alice, despite her efforts to protect the key, will often have to pay for the loss.

Since the rationale of the drafters of the Utah Act was to limit the liability of CAs in order to foster development of a certification authority industry,[99] the cap on CA liability inappropriately shifts too much risk onto the consumer. First, the Act does not create incentives for CAs to take expensive precautions to protect their private key. Moreover, the negligent CA will be able to externalize the costs of their negligence onto otherwise defrauded subscribers and other parties.[100] The consumer, meanwhile, is completely responsible for her negligence. Similarly, the presumption that the a digital signature is signed by the owner of the private key, destroys the merchants incentive to gather or consider any evidence other than the digital signature when he evaluates whether to hold Alice responsible for the document.[101] It also allows the merchant to forgo the trouble of establishing a relationship with Alice in order to confirm her responsibility.[102] As a result, even though the Utah Act tends to provide more security than a technology-neutral approach, the open PKI system is similar to technology-neutrality in that both tend to shift the bulk of the risk onto the consumer.

C. The Credit Card Model

---

[98] *See supra* note 90, at §§ 46-3-401 and 46-3-406.
[99] *See supra* note 25, at 1192.
[100] *Id.*
[101] *See supra* note 18, at 68.
[102] *Id.*

The liability allocations and evidentiary burdens contained in UETA and the Utah Act contradict the spirit, and in certain circumstances, the letter, of consumer-protection statutes such as the Electronic Fund Transfer Act ("EFTA")[103] and the Truth in Lending Act.[104] The limitations on the liability of consumer credit cardholders for unauthorized payments are "among the most radical, and successful, consumer protection initiatives of the 1970s."[105] Regulation Z issued by the Board of Governors of the Federal Reserve System provides that a cardholder may not be held responsible for more than $50 or the actual amount of unauthorized charges, whichever is less. Even this small amount cannot be charged to the cardholder unless the card issue has met the following requirements:

a) the card was accepted by the consumer,
b) the card issuer provided the consumer with adequate notice of his or her personal liability,
c) the issuer provided the consumer with an adequate means of notifying the issuer in the event the card is lost or stolen,
d) the issuer provided consumer with an adequate means of notifying the issuer in the event the card is lost or stolen,
e) the issuer provided a means of identifying the authorized user of the card,
f) and the unauthorized use must have occurred prior to notification by the cardholder to the issuer of the loss or theft of the card.[106]

This loss allocation rule places almost all of the risk of unauthorized use squarely on the merchants accepting credit card charges as a form of payment, merchant banks processing charge slips, and card issuers.[107] As a result of this loss allocation rule, credit card companies have invested large sums of money to reduce the incidence of credit card losses. Fraud loss prevention techniques include the placement of photographs on credit cards to make it more difficult to replicate them and data mining techniques that permit

[103] 15 U.S.C. §§ 1693-1693r (1994).
[104] 15 U.S.C. §§ 1601-1667e (1994).
[105] *See supra* note 83, at 1235.
[106] *See* Federal Reserve Board, Official Staff Interpretations, 12 C.F.R. § 226.12(b)(2).
[107] *See generally,* Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems,* 22 RUTGERS COMPUTER & TECH. L.J. 1, 39-40 (1996).

the card issuer to spot usage patterns that correlate with theft or fraudulent credit card use before the cardholder may even be aware that their credit card has been compromised.[108]

With regard to Electronic Fund Transfers ("EFTs"), such as the use of ATM transfers or direct deposits from a consumer account, the provisions of Regulation E are similar to those of Regulation Z, although it is somewhat less generous to the consumer. Under Regulation E, non-negligent consumers are provided the same protection as credit card holders as consumer protections decrease when the consumer does not take immediate action to report a loss or theft.[109] The consumer who promptly reports the loss or theft of an "access device"[110] is liable for the lesser of $50 or the amount of the unauthorized EFTs. But, a consumer who fails to notify a financial institution within two days of learning of the loss or theft, may be liable for up to $500.[111] Meanwhile, a consumer who fails to report the loss or theft of the access device within sixty days of the account statement being transmitted to the consumer may be liable for the entire amount of unauthorized charges that occur after the sixty days and before the consumer finally gives notice to the institution.[112]

While this model provides an effective way to allocate risk in a way that has proven beneficial to the consumer, merchant and credit card companies,[113] this model cannot be effectively applied to a technology-neutral regime. While our heroine Alice would certainly be pleased to only have to pay $50 when a stolen password results in a

---

[108] *See id.* (citing Homer Brickey, *Credit Firms, Crooks at War: Fraud Losses Reach $1Billion A Year,* ARIZ. REPUBLIC, Jul. 15, 1995).
[109] *See* 12 C.F.R. § 205.6(b).
[110] That is, a card, code, or other means of accessing a consumer's account for the purposes of effecting an EFT. *See id.* at § 205.2-1
[111] *See supra* note 108.
[112] *Id.*
[113] *See supra* note 108, at 20-22.

$25,000 loss,[114] there is no reason to assume that merchants or other contracting parties would be willing to assume the risk of loss when the $25,000 were paid for in cybercash rather than on a credit card. Rather than assume the risk themselves, merchants will require consumers accept the merchants elimination of responsibility for fraud or misappropriation. As a matter of fact, since UETA provides that a signature is authentic unless proved otherwise,[115] merchants in states that have adopted UETA will often be shielded from liability with or without a disclaimer. For similar reasons, this model would fail under Utah law as well: even though a digital signature employs a particular type of technology, merchants can still continue to disclaim liability in the event of a security breach.

Furthermore, the credit card system is secure in the knowledge that consumer transactions can only be effected through specific means, such as providing a credit card number, PIN number, etc. However, in a technology-neutral regime there is a greater spectrum of devices and methods that can constitute an electronic signature. Therefore, it would not be feasible to apply the same $50 limit in both a situation where the merchant demands that signatures be effected through biometrics and under the circumstances that a merchant allows any form of technology to constitute a signature. That is because risk is calculated differently based on whether a biometrics system is applied and where a technology-neutral process is applied. In the credit card regime, however, credit card companies can structure how it issues credit cards or permits ATM transfers based on a uniform set of procedures.

III A PROPOSAL TO LIMIT CONSUMER LIABILITY THROUGH A MODIFIED CLOSED PKI SYSTEM

[114] *See supra* text accompanying notes 84-90.
[115] *See* UETA, § 8.

Much of the literature assessing the open PKI model has discussed the open PKI system in the closed of a closed PKI. Unlike the open PKI, a closed PKI model is one where users obtain a different digital certificate for each category of online transactions. For example, a closed PKI user could have one certificate for transactions with a bank, a different certificate for communications with an employer, and yet another certificate for dealings with a health care provider.[116] Whereas under the open PKI model, a person's certificate would potentially authenticate any document and thereby yield extremely severe consequences of the user's private key is compromised, the closed PKI model limits the risks of a fraudulently signed document because of the system's more narrowly defined scope.[117] While the closed PKI system can reduce the amount of risk in a given transaction, a closed PKI still does not specifically allocate the risk to any party. Moreover, a closed PKI does rely on a particular technology that, given the rapidly expanding advances in technology, can become obsolete. Below, this Note will attempt to combine the technology-neutral, credit card and PKI models in a way that advances growth of the e-commerce industry while shielding the consumer from shouldering the risk when private information is stolen or compromised.

A. The Benefits and Burdens of the Electronic Financial Services Efficiency Act

On November 8, 1997, Representatives Baker and Drier submitted a bill entitled the "Electronic Financial Services Efficiency Act of 1997."[118] Like the White House's Framework and the principles that belie E-Sign, the bill called for "the recognition of digital and other forms of authentication to existing paper-based methods . . ."[119]

---

[116] *See supra* note 23, at 316.
[117] *Id.*
[118] H.R. 2937, 105th Cong. (1997).
[119] *Id.* at § 2(b).

However, in creating a new format to authenticate electronic transactions, the bill called for the established of a National Association of Certification Authorities ("NACA").[120] Had the bill been enacted, the NACA, acting as the highest-level certification authority, would have been federally mandated to register all other CAs. The Electronic Financial Services Efficiency Act is the first and only federal proposal to create an open PKI system.

Because the federal proposal is substantially similar to the Utah Act in constructing an open PKI, the federal proposal would also suffer from shifting an inordinate amount of risk onto the consumer.[121] At the same time, however, since the federal bill also requires that digital signature technology be employed,[122] consumer transactions can be relied on to be more secure than in a technology-neutral regime that allows a brief e-mail message to constitute an electronic signature.[123] As a result, it seems that, at the very least, a regime that requires individuals to receive certification and to use a relatively secure technology, will provide greater security to the consumer than E-Sign's technology neutral approach. At the same time, however, the unavoidable reality of changing technologies necessitates that PKI will eventually become obsolete. Since passing new legislation is usually a lengthy and time-consuming process, it is unlikely that a new law could swiftly be enacted to replace outdated technology.

B. A Proposal for a Closed, Technology-Flexible Approach

It seems that both technology neutrality *and* the providing of consumer safety can be accomplished by placing a technology neutral approach into a closed regime. Through

[120] *Id.* at § 7(a).
[121] *See supra* text accompanying notes 94-8.
[122] *See supra* note 118, at § 6(b).
[123] *See supra* note 16.

the construction of a federal certification authority such as the NACA, any individual could be permitted to apply for a digital certificate. However, since a closed regime demands that certificates only be used for limited purposes, individuals would have to obtain many certificates for either: a) each category of transactions that one wishes to engage in, or b) for each business that an individual wishes to conduct business. This means that if an individual wishes to purchase books, he may either receive a digital certificate for the sole purchases of books or he might apply for a certificate to only purchase books from Amazon.com. In the event that a digital certificate for book purchasing is stolen or forged, for example, a criminal would be limited to acquiring books and nothing else.

A critical element to this proposal is in the manner that lower-tier certification authorities are structured. Under this proposal, CAs can distribute certificates for a closed set of transactions and they can also specify the type of technology that will be used in that category of transactions. CAs can also structure the prices of obtaining a certificate based on the type of technology employed in the transaction and the type of transaction to which the certificate will be used. In pricing a category of certificates, a CA will be able to price their certificates according to the types of risks and liabilities embedded in a certain category of transactions. Alternatively, since any entity is permitted to apply to become a certification authority, large companies could also create their own independent CAs. These CAs could distribute certificates to consumers that specifically govern transactions with their company. In that case, consumers who want to conduct business from a particular company will also have to register for a certificate with the same company. Furthermore since CAs will be able to allocate risk in way that

is similar to today's credit card companies, CAs would assume the risk for all liability in excess of $50.

This closed, technology-flexible approach seems to combine the best attributes of technology neutrality, the credit card model and Utah's reliance on certification authorities. First, this proposal permits a spectrum of technologies to be applied when conducting business electronically. Second, since the system is closed, fraudulent transactions will be significantly lower than privacy breaches in an open system. Third, consumer liability is limited in a way that, as the success of credit card companies proves, is not detrimental to businesses. As a matter of fact, it can be assumed that certificate authorities will be created precisely because the profits obtained by lawful transactions outweigh the costs of the less common fraudulent electronic record. Finally, this proposal solves the authenticity problem by making it a non-issue. Since CAs will be liable in a manner similar to credit card companies, the same procedures will apply whenever a consumer claims that their certificate has been absconded or abused. As a result, the consumer will have very limited responsibility in proving that an electronic signature is not authentic or attributable to the consumer.