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

Electronic commerce is rapidly redefining this nation's economy. This year's revenues will amount to about $490 billion in United States online purchases.[1] By 2004, the United States will transact online sales reaching an estimated $3.2 trillion.[2] The Internet boom motivated President Clinton to publish a July 1997 report encouraging the private sector to respond to the public's "war[iness] of conducting extensive business over the Internet because of the lack of a predictable legal environment governing transactions,"[3] and help create "a uniform commercial legal framework that recognizes, facilitates, and enforces electronic transactions worldwide."[4]

The principles expressed in the Administration's proposal were reflected in the Electronic Signatures in Global and National Commerce Act ("E-Sign").[5] The Act, which was signed on June 30, 2000 but primarily took effect on October 1, 2000,[6] permits the creation of legally enforceable electronic signatures, contracts, and other electronic records that affect interstate or foreign commerce.[7] E-Sign is significant for commerce in general and electronic commerce in particular because 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

---

[1] *The Forrester Brief, at* http://www.forrester.com/ER/research/brief.
[2] *Id.*
[3] *See* William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce, available at* http://www.iitf.nist.gov/eleccomm/ecomm.htm.
[4] *Id.*
[5] Pub. L. 106-229, 79 Stat. 464 (codified as 15 U.S.C. § 7001 (2000)).
[6] Section 107 of E-Sign provides certain exceptions to the requirement that E-Sign take effect on October 1. 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).
[7] *Id.* at § 101(a)(1)-(2).

businesses in the United States by providing a basis for legal confidence in an area where lawful certainty has been glaringly absent.[8]

Although E-Sign is certain to increase business and consumer trust in creating electronic contracts, the Internet continues to be an environment where individuals can anonymously penetrate into computers and databases, and cause companies and individuals great financial harm.[9] Computer hackers[10] have regularly stolen private identifying information such as private keys and passwords, in order to purchase goods and commit crimes in other people's names.[11] Because of the Internet's porous security protection, members of the digital community have been exploring how to allocate risk in

---

[8] *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.).

[9] In the past year, for instance, hackers have penetrated into and attacked prominent web sites such as Amazon.com, Yahoo, and eBay. M.J. Zuckerman, Hackers, *Security Pros Call Web Attacks Vandalism: Consultants Ponder Motive,* USA TODAY, Feb. 11, 2000. Computer-savvy criminals have also appropriated personal information contained on large computer databases and then sold that data for a profit. *See* Ann Cavoikian, *Identity Theft: Who's Using Your Name, available at* http://www.ipc.on.ca/english/pubpres/sum_pap/papers/ident-e.htm. Moreover, private information has even been uploaded from individuals' personal computers. In 1999, for instance, a flaw in Microsoft's Excel spreadsheet program was detected, which permitted computer hackers to copy private files from a person's home computer without his knowledge. Martha Mendoza, *Warning for Web Surfers: Hackers Able to Steal Off PCs with Excel,* ARIZ. REPUBLIC, Jan. 6, 1999. More recently, hackers broke into Microsoft's computer systems and may have stolen source code to newer versions of its Windows operating system as well as portions of Word and Excel. Janet Rae-Dupree, *Windows Hack Attack: Worming into Microsoft*, U.S. NEWS & WORLD REPORT, Nov. 6, 2000, at 44.

[10] Webopedia defines hack as "to modify a program, often in an unauthorized manner, by changing the code itself." *Webopedia*, *at* http://webopedia.internet.com/TERM/h/hack.html.

[11] *See* Cavoikian, *supra* note 12. In light of these recent security breaches, the results of a study conducted by the Information Technology Association of America in April 1999 should come as no surprise. *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). Measuring the perceptions of top executives and their customers from across the information technology industry, the study found that 62% of respondents believed lack of trust was the primary barrier to e-commerce and that specific obstacles included privacy protection (60%), authentication (56%), and security (56%). *Id.* Results like these support the White House's belief that the public is "wary of conducting extensive business over the Internet." *See supra* note 3.

the event of a security breach. Through this inquiry, three core issues have been identified as security risks: authenticity, integrity, and non-repudiation.[12]

This Note focuses on the element of authentication in electronic transactions[13] and examines which party should bear the risk of financial loss when the authenticity of a signature is raised.[14] Part I of this Note provides a brief overview of state legislation prior to E-Sign's enactment, as well as the various types of electronic signatures that can be used to create an electronic contract. Part II describes E-Sign's most important provisions, including its scope; federal preemption clauses; and consumer protection provisions. Part III describes E-Sign's approach and two other approaches to authenticating electronic signatures. Part IV illustrates the insufficiency of each model in fairly allocating risk to either the merchant or the unsophisticated consumer. This Note concludes with an overview of these schemes and suggests which features of these different plans should be incorporated to create a law that provides consumer protections while also promoting the growth of e-commerce.

---

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

[13] Note that the authentication element was identified by 56% of the respondents in the ITAA survey as an obstacle to e-commerce's development. *See supra* note 11.

[14] *See generally* Biddle *supra* note 25 (critiquing various model for allocating risk when privacy is compromised). 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.

I. CREATING AN ELECTRONIC CONTRACT AND SIGNATURE

Electronic signatures can be created in a variety of ways. Prior to E-Sign's enactment, states were inconsistent in defining which methods could create an authentic electronic signature. This Section describes those state provisions that preceded E-Sign's enactment as well as the range of electronic signatures that the Act currently permits.

A. Electronic Signatures Prior to E-Sign

Before E-Sign became law, legislation differed on what would constitute a valid electronic signature. Originally, digital signatures[15] were the favored technology in electronic signatures statutes, as they supposedly offered "a technology-based cure for many of the security risks encountered in online commerce."[16] For example, in 1995, Utah[17] (followed by Minnesota and Washington) became the first state to enact an electronic signature statute setting forth specific rules governing digital signatures and public key infrastructures ("PKI's").[18] By 1999, the popularity of digital signature statutes had waned significantly and a technology-neutral approach became increasingly popular.[19] Just prior to October 1, when E-Sign came into effect, 18 states, including Utah and Minnesota, had already adopted the Uniform Electronic Transactions Act ("UETA"), which permits any form of electronic symbol or message to qualify as a

---

[15] *See infra* text accompanying notes 18-25 for a thorough description of how digital signatures work.
[16] Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce,* 588 PLI/PAT 401, 404 (2000). *See* discussion *infra.*
[17] UTAH CODE ANN. § 46-3-101 (1996).
[18] A public key infrastructure is a system consisting of digital certificates, , Certification Authorities, and other registration authorities that verify and authenticate the validity of the parties involved in an online transaction. Currently, there is no existing uniform standard for constructing a PKI. *See Webopedia, at* http://webopedia.internet.com/TERM/P/PKI.html.
[19] *See, e.g. 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 Daniel Greenwood, Deputy General Counsel, Information Technology Division Commonwealth of Massachusetts) (commenting that the Utah digital signature law reflected many "outdated trends.").

signature.[20] Under UETA, these signatures are valid whenever an electronic symbol or message is coupled with the signer's intent to authenticate the contract.[21]

Although most states that had adopted an electronic signature statute eventually implemented a technology-neutral approach, businesses wishing to execute electronic contracts continued to lack certainty that their contracts would be recognized nationwide.[22] As a result, E-Sign was enacted to create greater uniformity and bolster the public's confidence in the legal validity of electronic contracts throughout the nation.

B. Variety of Electronic Signatures Permitted by E-Sign

E-Sign 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."[23] Perhaps the easiest way to create a binding electronic signature under this provision would be to accept a contract by clicking "yes" on an icon on a computer screen.[24] An individual could also bind oneself to a contract by signing an e-mail with one's name or by typing an "X."[25] Currently, many commercial transactions are effected using more advanced technological approaches. One common method of creating a valid signature is the "shared secrets"

---

[20] UETA, § 2(8). These 18 states are Arizona, California, Florida, Idaho, Indiana, Iowa, Kansas, Kentucky, Maine, Maryland, Minnesota, Nebraska, Ohio, Oklahoma, Pennsylvania, South Dakota, Utah, and Virginia.
[21] *Id.*
[22] *See supra* text accompanying notes 30-41.
[23] E-Sign, § 106(5).
[24] Harris Ominsky, *Oops! I Just Clicked My Life Away,* THE LEGAL INTELLIGENCER, July 26, 2000. While it is true that companies such as Amazon.com did permit click-through shopping prior to E-Sign, the Act formalizes the validity of these contracts. Until E-Sign, Amazon was forced to either rely on conflicting state laws that had enacted electronic or digital signature statutes or assume the risk that federal or state courts would enforce these contracts. In other words, Amazon did not have any clear indication that a consumer's click on the "I Agree" or "yes" icon would necessarily bind either Amazon or the consumer to fulfill the terms of a contract.
[25] David W. Carstens, *Contracts Have a New Look Thanks to E-Signature Act,* TEXAS LAWYER, July 31, 2000. It has also been suggested that an individual could accept an offer by producing an electronic sound such as a musical note. Harris Ominsky, *Oops! I Just Clicked My Life Away,* THE LEGAL INTELLIGENCER, July 26, 2000.

method. This process involves the use of passwords or credit card numbers to create the necessary intent to conclude a transaction.[26] 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 by the sale.

A more complex method of signing a contract is through biometric authentication.[27] Biometric authentication operates by sampling and electronically retaining a physiological characteristic of a user in that individual's user profile. 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.[28] Biometric technology can identify an individual through recognition of a fingerprint, signature, voice, or iris.[29] Therefore, to bind oneself to a contract, one might simply place one's hand on a specially designed platform. When an individual's handprint matches the previously stored print identifying the user, a binding electronic signature is immediately created.

The digital signature is another significant means of creating an electronic signature. As discussed above,[30] its initial popularity led some states, prior to the enactment of E-Sign, to narrowly confine legally cognizable electronic signatures to

---

[26] *See, e.g., The Impact of the New Federal E-Sign Act on New York Law,* NEW YORK LAW JOURNAL, Aug. 8, 2000.

[27] *See, e.g.,* American Biometric Company, *What is Biometric Authentication*, *at* http://www.biomouse.com/whitepapers/biometric.htm. Biometric authentication has recently become popular in the insurance and financial industries and its appeal continues to grow. *See, e.g.,* Sam Costello, *With Biometrics, You Are Your Own Password*, INFOWORLD DAILY NEWS, Nov. 15, 2000; Elizabeth Weise, *Body May be Key to a Foolproof ID*, USA TODAY, Aug. 8, 1998.

[28] *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).

[29] *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).

[30] *See supra* text accompanying notes 10-11.

digital signatures.[31] Digital signatures involve the use of a private and public key pair[32] that are usually purchased by a sender and issued by a Certification Authority ("CA").[33] A CA can be created through a Public Key Infrastructure ("PKI"),[34] and it represents a trusted third party who checks and verifies the identity of the person requesting the key pair.[35] The private key that an individual receives is to remain secret and is not to be distributed 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.[36] The public-private key pairs are mathematically related such that a message encrypted 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.[37]

---

[31] *See, e.g.,* UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (1997) (Utah's Digital Signature Law).

[32] Public and private keys are made through the composition of complex mathematical algorithms that disguise messages and information. Michael Lee, Sean Pak, Tae Kim, David Lee, Aaron Schapiro, and Tamer Francis, *Electronic Commerce, Hackers, and the Search for Legitimacy: A Regulatory Proposal,* 14 Berkeley Tech. L.J. 839, 850-51 (1999).

[33] *See* Boss, *supra* note 11 at 416.

[34] *See supra* note 13; *infra* text accompanying notes 94-96.

[35] *See* Boss, *supra* note 11 at 416.

[36] 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).

[37] *Id.* The technology operates in the following way. If Alice wishes to send secure 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." 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). 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. *Id.* 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. 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. *Id.* If, on the other hand, the digests do not match, then the authenticity of the message is instantly called into question.

II. IMPORTANT E-SIGN PROVISIONS

A. Electronic Contract Defined

E-Sign's terms provide a basis for creating legally valid documents that are electronically signed, recorded, and available for future reference.[38] It therefore allows parties to bind themselves contractually by means other than the traditional pen and paper.[39] For instance, by clicking "I Agree" on an online purchase form for the casebook INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE,[40] one has simultaneously created a legally binding electronic signature and electronic record.

A significant distinction between electronic commerce and paper-based commerce is that electronic transactions can be executed instantly between computers.[41] E-Sign facilitates this ease in consummating transactions by broadly defining the term "electronic signature." The speed with which contracts can be given effect is similarly enhanced by E-Sign's efforts to promote the freedom of contract between parties.[42] To this end, E-Sign requires that consent to create an electronic contract is voluntary[43] and that interested parties define what procedures will create an authentic signature or contract.[44] These provisions help to permit the application of an array of technologies

---

[38] *See infra* Part I.B. An electronic signature is broadly defined 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." E-Sign, § 106(5). The term electronic record "means a contract or other record created, generated, sent, communicated, received, or stored by electronic means." *Id*, at § 106(4). Finally, the term "electronic" means "relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities." *Id.*

[39] *See supra* text accompanying notes 16-29.

[40] ROBERT P. MERGES ET AL. (2000).

[41] Amelia H. Boss, *Searching for Security in the Law of Electronic Commerce,* 588 PLI/PAT 401, 404 (2000).

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

[43] E-Sign § 101(b)(2) (The Act does not "require any person to agree to use or accept electronic records or electronic signatures.").

[44] *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.").

that can bind parties to a contract through means such as click-through provisions, digital signatures, and biometrics.[45]

B. Preemption

E-Sign provides that all state laws related to electronic signatures and contracts are preempted unless they constitute an adoption of UETA[46] or specify alternative procedures that are technologically neutral[47] and consistent with Titles I and II of the Act.[48] The principle underlying this provision is the presumed importance of uniformity among the states.[49] Proponents of E-Sign argue that differences in electronic signature laws impede the growth of e-commerce because parties are unwilling to risk entering into an online contract without certainty regarding its legality nationwide.[50] Indeed, should conflicting state laws exist, companies would be forced to customize their services to

---

[45] *See supra* Part I.B.

[46] 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; Summary of the Uniform Electronic Transactions Act, *available at* http://www.nccusl.org/uniofrmact_summaries/uniformacts-s-ueta.htm. With exception to the issue of determining the authenticity of a signature (*see discussion infra*), 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.

[47] 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).

[48] *Id.* at § 102(a)(2). 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.

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

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

meet the requirements of each state.[51] This, in turn, could disproportionately harm businesses by raising costs and making it difficult to serve customers cost-effectively.[52]

E-Sign's advocates also point out that, barring preemption, it could take many years before states independently enact uniform laws. For instance, 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.[53] 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.[54] Thus, history has demonstrated that it is unwise to simply wait for the nation to uniformly enact UETA.[55] Instead, by requiring states to either adopt UETA or legislation that is significantly, if not entirely, similar to E-Sign, the United States immediately provides nationwide uniformity regarding the legal validity of an electronic contract.[56]

---

[51] *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.).

[52] *Id.*

[53] *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.).

[54] *Id.*

[55] Recent developments appear to undermine this claim. Indeed, it appears that UETA has swiftly gained nationwide recognition. In addition to the 18 states that have already adopted UETA, as of August 2000, 10 other states and the District of Columbia were considering its adoption. D. Benjamin Beard, *Removing Barriers to E-Commerce: The Uniform Electronic Transactions Act*, A.L.I. - AMERICAN BAR ASSOCIATION CONTINUING LEGAL EDUCATION (Aug. 17, 2000).

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

C. Consumer Protections

E-Sign appears to provide extensive consumer protections against unintentionally entering into an electronic contract; however, these provisions can be misleading. E-Sign mandates that if a statute, law, 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.[57] In this case, the consumer must not only formally consent to receive records in electronic form,[58] but the party required to furnish the information must also:

(a) inform the consumer of any right or option to receive a record in non-electronic form;[59]
(b) inform the consumer of the right to withdraw consent to receive electronic notice and explain any consequences or fees upon termination;[60]
(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;[61]
(d) describe the procedures for withdrawal of consent and to update information that is needed to contact the consumer electronically;[62]
(e) inform the consumer on how to obtain a paper-based copy of an electronic record and whether a fee will be charged;[63]
(f) notify the consumer of the necessary hardware and software requirements for access to and retention of records;[64] 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.[65]

Although these requirements appear extensive, the Act limits their reach with a provision holding that a failure to obtain electronic consent or confirmation of consent

[57] E-Sign at § 101(c).
[58] *Id.* at § 101(c)(1)(A).
[59] *Id.* at § 101(c)(1)(B)(i)(I).
[60] *Id.* at § 101(c)(1)(B)(i)(II).
[61] *Id.* at § 101(c)(1)(B)(ii).
[62] *Id.* at § 101(c)(1)(B)(iii).
[63] *Id.* at § 101(c)(1)(B)(iv).
[64] *Id.* at § 101(c)(1)(C)(i).
[65] *Id.* at § 101(c)(1)(C)(ii).

does not immediately deny the legal effectiveness, validity, or enforceability of any contract entered into with the consumer.[66] It is therefore unclear whether a contract is valid when a business that is statutorily required to make information available in writing fails to do so. Should a court find such contracts to be enforceable, all of the above provisions would effectively be rendered moot. It is also significant that these provisions do not require consumer consent before *all* electronic dealings. Rather, these clauses only apply when an existing law requires that information be provided or made available in writing to a consumer.[67] This means that e-businesses that are not currently required to provide paper-based records, such as Amazon.com, are not obligated to abide by any of these provisions.

Even though the sections described above only apply to a small class of consumers, E-Sign also contains provisions that benefit all individuals who fall outside of these clauses. For instance, due to the loss of "ceremonial psychology" that is involved when an individual signs a document while sitting in the presence of a notary who affixes seals to verify the signer,[68] E-Sign requires that certain writings remain paper-based so that contractual parties can maintain awareness regarding the gravity of their signing.[69] Therefore court orders,[70] notices regarding utility termination,[71] and regulations governing adoption, divorce or other matters of family law[72] are all still processed

[66] *Id.* at § 101(c)(3).
[67] *Id.* at § 101(c)(1).
[68] Harris Ominsky, *Oops! I Just Clicked My Life Away,* THE LEGAL INTELLIGENCER, Jul. 26, 2000.
[69] Much of this ceremony is lost on the Internet since individuals can now create valid contracts by simply clicking "yes" on an icon on their computer screens. *Id.*
[70] *Id.* at § 103(b)(1).
[71] *Id.* at § 103(b)(2)(A).
[72] *Id.* at § 103(a)(2).

through physical, nonelectronic documentation.[73] E-Sign also calls for a federal study of the extent to which the provisions of the law benefit or burden electronic commerce while charging the Department of Commerce[74] and the Federal Trade Commission[75] to recommend how the Act should be altered in order to better protect consumers. Finally, the Act permits any federal regulatory agency, following notice to the public and an opportunity for public comment, to exempt a category or type of record from requirements relating to consumer consent to the use of electronic records.[76] However, this exemption can only be effected when it will not materially harm consumers and is necessary to eliminate a significant burden on electronic commerce.[77]

III. THREE LEGISLATIVE MODELS FOR AUTHENTICATION

Although E-Sign makes significant strides in creating a national standard for forming electronic contracts, the Act does not formally address the problem of who should be responsible for proving the authenticity of a signature.[78] Consequently, E-Sign creates the possibility that consumers will be liable when their secret passwords and codes are stolen and fraudulently used.[79] Given the increasing difficulties in providing a safe environment in which to transact online business,[80] it is worthwhile to examine E-Sign and other models that contain elements that can help generate greater consumer confidence and security protection. This section provides a description of the different models and Part IV then analyzes the success and failure of each proposal in safeguarding

[73] Uniform Commercial Code sections 1-207 and 1-206 and Articles 2 and 2A are also exempted from the electronic record provisions. *Id.* at § 101(a)(3).
[74] E-Sign, § 105(a)-(b).
[75] *Id.* at § 105(b).
[76] *Id.* at § 104(d)(1).
[77] *Id.*
[78] *See supra* text *accompanying* notes 12-14.
[79] *See infra* text *accompanying* notes 99-102.
[80] *See supra* text *accompanying* notes 9-11.

the consumer while stimulating the growth of the digital economy. Table 1 summarizes the key provisions of each model and Table 2 highlights the relative risks of each proposal.

A. E-Sign and UETA's Technology-Neutral Approach

E-Sign forbids any state or federal statute from requiring a specific technology for electronic transactions.[81] This technology-neutral approach instead allows the market to decide which technologies will best facilitate electronic commerce.[82] Naturally, this is a position that most businesses gladly embrace.[83] Without the hindrance of any specific technologies, businesses are free to construct their own methods and security procedures to transact business with customers.[84]

In addition to its promotion of technology-neutrality, E-Sign does not enumerate any standards for attributing responsibility in the event that an electronic signature is forged or stolen. Instead, E-Sign presumably relies on existing laws or future litigation to determine who will carry the evidentiary burden of proving the inauthenticity of a signature. The Uniform Electronic Transactions Act,[85] on the other hand, also adopts a technology-neutral regime but creates a framework for attributing an electronic signature. It states that "[a]n electronic record or signature is to be attributed to a person if it was the

---

[81] *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." This "minimalist" approach is consistent with the principles enumerated in the "Framework for Global Commerce." *See supra* note 2.

[82] *See supra* note 12, at 434-35.

[83] 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).

[84] As discussed in Part IV however, though this is beneficial for merchants, it is unclear that this approach adequately protects consumers.

[85] *See supra* text accompanying note 36.

act of the person."[86] Relevant evidence in establishing this fact includes any "showing of the efficacy of any security procedure" that helps to establish who attached the signature.[87] 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.[88] These provisions inform the individual that, in the absence of any identifiable abnormalities in the transmission of a signature, a consumer will likely have the burden of proving that a fraudulent signature does not belong to her.[89]

B. The Credit Card and Automatic Teller Machine Model

The liability allocations and evidentiary burdens contained in the Electronic Fund Transfer Act ("EFTA")[90] and the Truth in Lending Act[91] are "among the most radical, and successful, consumer protection initiatives of the 1970s."[92] Both Acts place significant limitations on the liability of consumer credit cardholders for unauthorized payments. 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;

---

[86] *Id.* at § 9 (a).
[87] *Id.*
[88] *Id.* at § 9(b).
[89] *Id.* at § 9 cmmt 1.
[90] 15 U.S.C. §§ 1693-1693r (2000).
[91] 15 U.S.C. §§ 1601-1667e (2000).
[92] *See* Biddle *supra* note 83, at 1235.

d) the issuer provided the 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; and
f) the unauthorized use occurred prior to notification by the cardholder to the issuer of the loss or theft of the card.[93]

This loss allocation rule places the risk of unauthorized use chiefly on the financial institutions responsible for issuing and processing the credit cards.[94] 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.[95]

With regard to Electronic Fund Transfers ("EFTs"), such as the use of Automatic Teller Machine ("ATM") transfers or direct deposits from a consumer account, the provisions of Regulation E are similar to those of Regulation Z, except that Regulation E establishes that consumer protections decrease when the consumer does not take immediate action to report a loss or theft.[96] As a result, Regulation E provides protection for the conscientious EFT user but requires that the consumer assume liability for failing to report a genuine theft in a timely manner.

---

[93] *See* Federal Reserve Board, Official Staff Interpretations, 12 C.F.R. § 226.12.
[94] 15 U.S.C. § 1693g (2000).
[95] 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 the card issuer to spot usage patterns that correlate with theft or fraudulent credit card use before the cardholder may even be aware that her credit card has been compromised. *See* Henry H. Perritt, Jr., *Legal and Technological Infrastructures for Electronic Payment Systems,* 22 RUTGERS COMPUTER & TECH. L.J. 1, 40. (citing Homer Brickey, *Credit Firms, Crooks at War: Fraud Losses Reach $1Billion A Year,* ARIZ. REPUBLIC, Jul. 15, 1995).
[96] *See* 12 C.F.R. § 205.6. The consumer who promptly reports the loss or theft of an "access device"-that is, a card, code, or other means of accessing a consumer's account for the purposes of effecting an EFT - is liable for the lesser of $50 or the amount of the unauthorized EFTS. *Id.* at § 205.2-1. 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. *See supra* note 107. 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. *Id.* Also note that the financial institution has the burden of proving that a loss or theft was not reported in a timely manner. *Id.*

C. Digital Signature Laws and the Open PKI System

In 1995, Utah became the first state to adopt a full-fledged digital signatures statute[97] that supported a Public Key Infrastructure.[98] 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.[99] The model presented by the 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 certification authority that will securely link their identity to their public key in creating electronic contracts. Generally, "the certificate issued by the CA has no boundaries upon the class or set of relying parties . . . entitled to rely upon it."[100] Thus, in an open PKI environment, a person could obtain a digital certificate and then use it for any transaction requiring a digital signature, including the ordering of goods online, signing legally binding agreements, and even filing documents with a government entity.[101] Under the Utah Act, the state acts as the root certification authority and provides for the licensing of certification authorities.

In creating its PKI, the Utah law attempted to generate greater certainty as to the authenticity of an electronic signature. 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, it is

---

[97] UTAH CODE ANN. § 46-3-101 (1996). The 1996 legislation was a revision of legislation that originally became effective in 1995. However, the Utah digital signature provisions have again been replaced by UTAH CODE ANN. § 46-4-101, which adopts UETA *in toto*.
[98] *See supra* text accompanying notes 19-27.
[99] A copy of the Digital Signature Guidelines can be downloaded at http://www.abanet.org/scitech/ec/isc/dsgfree.html.
[100] 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).
[101] *See* Greenwood & Campbell *supra* note 27, at 316.

established that (a) the subscriber has accepted the corresponding certificate and thereby assumed the duty to exercise reasonable care to protect the key, (b) the digital signature is that of the subscriber listed in the certificate, and (c) the digital signature was affixed with the intention of signing the message.[102] These provisions inform us that there is a presumption that a digital signature contained in a contract belongs to the signature owner.

Table 1
Summary of Key Electronic Signature Provisions

	Permissible Technologies	Parties Involved	Presumption/Evidentiary Burden
E-Sign/UETA	All	Merchant and Consumer	Signature Owner
Regulation Z	All	Merchant, Consumer, and Credit Card Company	Consumer and Merchant do not have any evidentiary burdens
Regulation E	All	Merchant, Consumer, and Credit Card Company	Consumer must report fraud or negligence in a timely manner
Utah's Digital Signature Act	Digital Signatures	Merchant, Consumer, and Certification Authority	Owner of Private Key

IV. COMPARATIVE ANALYSIS OF THE LEGISLATIVE MODELS

A. Technology Neutrality Under E-Sign and UETA

One justification for E-Sign's technology-neutral approach[103] is the concern that technology can easily become obsolete, thereby rendering a technology-specific approach

[102] *See* UTAH CODE ANN., §§ 46-3-401; 46-3-406.
[103] *See supra* Part II.D.

unsafe or inefficient.[104] This can result in the consumer's use of technology that is relatively easy for a hacker to manipulate in order to steal an individual's identity and commit fraud. Nevertheless, some academics argue that it is 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.[105] 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.[106]

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. Presently, current legislation and common law tort and negligence laws can be relied on when a consumer is found to have negligently protected confidential information or passwords. For instance, if Alice negligently types her secret password in a chat room and a computer hacker discovers it and conducts transactions totaling $25,000, current law mandates that Alice is responsible for her irresponsible behavior.[107] However, existing case law has not yet determined whether Alice would be held liable in the event that she exercised reasonable care and her password was nevertheless stolen from her computer.[108] Today, hackers can break into

---

[104] *See* Boss *supra* note 12 at 441.
[105] Jane Kaufman Winn, *Open Systems, Free Markets, and Regulations of Internet Commerce,* 72 TUL. L. REV. 1177, 1183 (1998).
[106] 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* Pincus *supra* note 29.
[107] C. Bradford Biddle, *Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace,* 34 SAN DIEGO L. REV. 1225, 1236 (1997).
[108] For example, a corrupt computer repairman might search Alice's files and copy her personal codes in the process of repairing her broken computer. There are also many other ways that a private key can be stolen: one can steal another's identity and receive a digital certificate in that person's name; an employee

an individual's computer with almost complete anonymity, and oftentimes, with impunity.[109] Consequently, not only will it be very difficult for Alice to locate the elusive password-snatcher but she will also be forced to prove to the court that she indeed behaved with reasonable care.[110] Moreover, given that the thief will almost never be found, there still are not any specific provisions that dictate legal certainty as to who should be held liable for the loss: Alice, the business who accepted her stolen password, or perhaps the company who originally issued Alice her password.

Although UETA does contain a framework for attributing responsibility, its clauses virtually guarantee the same result that could potentially occur under E-Sign. By requiring the sender to prove the (in)authenticity of a signature,[111] UETA formally establishes that, in the above scenarios, Alice would have the burden of proof in showing that she was not responsible for a stolen signature or password. As in E-Sign, 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. Thus, regardless of whether states adopt UETA or embrace E-Sign, consumers will not often have any legal protection when contracts are made using their stolen signatures.

In sum, the technology-neutral approach of both E-Sign and UETA can create a dangerous environment for consumers entering contracts using inferior technology. The

---

of a CA responsible for issuing certificates can be bribed; 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).

[109] Gaining anonymity on the Internet is frightfully easy. For instance, Anonymizer.com provides a free service whereby anyone accessing its web site can anonymously surf other web pages. *See* htttp://www.anonymizer.com. This reality has also been illustrated by a cartoon from THE NEW YORKER magazine featuring a conversation between two doges seated next to a computer. The caption reads: On the Internet, nobody knows you're a dog. Peter Steiner, THE NEW YORKER, July 5, 1993, at 61.

[110] *See* Biddle *supra note* 84 at 1236.

[111] UETA, § 9.

laws also shift an inordinate amount of risk onto the unsophisticated consumer. Although UETA initially appears to be more valuable to the consumer by presenting a framework for attributing the authenticity of a signature, these guidelines will tend to favor businesses at the expense of consumers.

B. The Credit Card Scheme

Currently, both merchants and consumers are protected from liability in credit card transactions.[112] However, were Regulations Z or E applied to non-credit card transactions, then the burden of proving the authenticity of a signature would unfairly shift to the merchant, who would be required to assume all responsibility for negligent or fraudulent losses in excess of $50.[113] By virtually eliminating consumer responsibility in the event of consumer negligence or fraud, the consumer would be well protected in the digital economy.[114] Yet, just as consumers are severely limited in their ability to prove that a fraudulent signature does not belong to them, merchants have little ability to detect whether an individual is providing passwords or digital signatures that do not belong to him.

---

[112] Many credit card companies including American Express, Visa, and MasterCard have waived the $50 liability limit in an effort to convince consumers to continue to use credit cards online. *See, e.g.,* Andrea Bennett, *The Best Ways to Pay Online*, MONEY MAGAZINE, Oct. 15, 2000, at 104 (discussing the "zero liability" programs offered by American Express, Visa, and MasterCard).

[113] While it is true that consumers and merchants are usually protected from liability since most electronic transactions are effected using credit cards, the growing popularity of cybercash and other non-credit card means to pay for goods requires this examination of alternative means to protect the parties involved. *See, e.g.,* Paul D. Glenn, *The Law of E-Commerce in the Financial Services Sector*, 1156 PLI/CORP 771, 787-88 (1999); Cymonie Rowe, *Technological Advances in Banking: A Move to a Global Economy*, 4 ILSA J. INT'L & COMP. L. 1303, 1304-05 (1998) (describing the growing importance of cybercash and other internet payment schemes).

[114] Barring statutory obligations, merchants would be reluctant to accept the scheme voluntarily. For instance, our heroine Alice would certainly be pleased to only have to pay $50 when a stolen password results in a $25,000 loss, but there is no reason to assume that merchants or other contracting parties would be willing to assume the risk of loss. *See supra* text accompanying notes 84-90. Instead, merchants are apt to require consumers to accept a merchant's disclaimer denying responsibility in the event of fraud or misappropriation. Currently, both UETA and the former Utah statute explicitly side with merchants in these scenarios when stating that a signature is considered authentic unless proven otherwise. *See* UETA, § 8.

Regulation Z and E-type legislation in non-credit card transactions is also less practical in a technology-neutral digital economy. Unlike the credit card system, where a company is secure in the knowledge that consumer transactions can only be effected through specific means—such as providing a credit card number or Personal Identification Number—this model cannot easily be applied to electronic signature transactions where there is a greater variety of devices and methods that can constitute an electronic signature. It would not be fair, for example, to apply the same $50 limit to both a situation where the merchant demands that signatures be effected through biometrics and where a merchant allows any form of technology to constitute a signature.[115] The level of risk is calculated differently based on the technology used. In the credit card regime, however, credit card companies can structure how they issue credit cards or permit ATM transfers based on a uniform set of procedures. As a result, the ease with which Regulations Z or E can be applied to e-commerce transactions is limited.

C. The Utah Act

Although the Utah Act ensures that a minimum technology threshold will govern all electronic transaction, the Act functions in a similar way to E-Sign by shifting an inordinate amount of risk onto the consumer. For instance, a hacker that succeeds in identifying the methods used to control Alice's private key could forge her signature with great ease, potentially causing Alice significant financial hardship.[116] By requiring the

[115] It is also unadvisable to promote such legislation in a technology-specific regime since technology is liable to become obsolete and, over time, will become more susceptible to manipulation and fraud. In addition, it is impractical to require that, to prevent fraud, consumers purchase expensive and more secure technology such as biometrics since its cost would be prohibitive to many and would effectively bar millions from contracting on-line.

[116] 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

sender to prove the (in)authenticity of a signature,[117] Utah's provisions indicate that in this scenario, it will be up to Alice to provide evidence to rebut the presumption that she authenticated the signature. Hence, by concentrating risk on the original holder of the private key, consumers will often have to pay for the loss.

The Utah law's state-sanctioned licensing arguably creates greater assurances as to the validity of an electronic signature. However, since the drafters of the Utah Act limited the liability of CAs in order to foster development of a certification authority industry,[118] the cap on CA liability, combined with the other provisions of the statute, will nevertheless inappropriately shift too much risk onto the consumer. First, by permitting only digital signatures to authenticate contracts, the statute runs the risk that the technology will become easier to steal or imitate, as hackers will focus solely on cracking this one type of technology. Second, not only may digital signatures become obsolete and render digital signatures a vastly inferior technology to other alternatives,[119] digital signatures are already less reliable and more subject to fraud than signatures created through biometric technology.[120] Third, the Act does not create incentives for CAs to take adequate precautions to protect their private keys from fraudulent use. A more concerned CA, such as one facing financial liability, would be stimulated to take extensive safety measures, such as creating complex digital signature algorithms that are

---

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.

[117] *See* UTAH CODE ANN., §§ 46-3-401; 46-3-406.

[118] *See* Biddle *supra* note 25, at 1192.

[119] Note that consumer risks related to the use of inferior technology in the marketplace absent guidelines for protecting the non-negligent consumer have already been discussed above. *See supra* text *accompanying* notes 86-91

[120] See R.R. Jueneman & R.J. Robertson, Jr., *Biometrics and Digital Signatures in Electronic Commerce*, 38 JURIMETRICS J. 427, 453-54 (1998).

difficult for hackers to crack, or limiting the types of transactions with which an electronic signature can be used.[121]

The Utah statute is also unfair because a CA that negligently distributes an individual's electronic signature can externalize the cost of its negligence onto otherwise defrauded subscribers. Meanwhile, since the Utah Act assumes that a digital signature verified by a public key belongs to the certificate holder, the consumer is likely to be held completely liable for all fraudulent uses of her signature, regardless of whether it was stolen or negligently distributed by a third party.[122]

The presumption that a digital signature is signed by the owner of a private key also destroys a merchant's incentive to gather or consider any evidence other than the digital signature when he evaluates whether to hold a consumer responsible for a document.[123] It instead also allows a merchant to forgo the trouble of establishing a relationship with a consumer in order to confirm her responsibility.[124] As a result, even though the Utah Act tends to provide more security than E-Sign's approach, it suffers from the danger that digital signatures will become obsolete and that, similar to E-Sign, the consumer will bear the bulk of the risk.

---

[121] *Id.* It is also worth noting that even if the market will ultimately eliminate a particular negligent CA that does not mean that the market will succeed in significantly eliminating the problem of CA negligence altogether. That is because it can conceivably take many months to identify a negligent party. Even after that party has been identified, the CA-owner can easily reinvent the company by shutting down the web site and re-opening under a different name. Moreover, even though the Utah statute requires state approval for CAs, it does not require the state to conduct any policing efforts that would deny negligent CAs from re-registering. Lastly, such a scheme is particularly easy on the Internet where the start-up costs of an e-business are small relative to most brick-and-mortar companies.

[122] It is conceivable that comparative negligence rules may apply in those states that have enacted comparative negligence statutes.

[123] *See* Wright *supra* note 18, at 68.

[124] *Id.*

Table 2
Summary of Electronic Signature Proposals: Relative Risks

	Risk to Consumer	Risk to Merchant	Risk to CA	Risk to Credit/ATM Card Issuer[125]	Evidentiary Burden on Consumer	Risk of Unsafe Technology	Possibility of Obsolete Technology
Technology Neutrality Under E-Sign & UETA	High	Low	N/A	Moderate	High	High	Low
Utah Digital Signature Statute	High	Low	Low	Moderate	High	Moderate	Moderate
Regulation Z (in the digital economy)	Low	High (in non- credit card transactions)	N/A	Moderate	Low	Low	Low
Regulation E (in the digital economy)	Low	High (in non- credit card transactions)	N/A	Moderate	Low	Low	Low

V. CONCLUSION: SEARCHING FOR A PRACTICAL SOLUTION

As Table 2 indicates, all of the above proposals contain distinct advantages and disadvantages. A technology-neutral regime such as E-Sign avoids the risk that outdated and increasingly insecure technology will be *required* in creating electronic contracts. However, technology neutrality also creates the likelihood that inferior and insecure

[125] This column *only* applies to all credit card and ATM card related transactions.

technology *may* be applied when concluding contracts. The Utah statute remedies this difficulty by requiring the use of digital signatures, thereby guaranteeing that, in the immediate future at least, contracts will not be made with significantly inferior technology. At the same time, however, both E-Sign and the Utah law run the risk of making the consumer liable for both negligent and non-negligent behavior.

If Regulations Z or E were applied to the digital economy, the consumer would obtain significant protections, but, the regulations would also result in the merchant's assumption of an inordinate amount of risk. Clearly, none of the above proposals can cleanly apply to the world of e-commerce. Nevertheless, these schemes suggest the components that are needed to construct a fair system for authenticating electronic signatures.

The historic success of the credit card and ATM schemes[126] demonstrates that one economically efficient solution to the problems of authentication is to allocate the risk of loss to a third party such as a Certification Authority. Since there does not appear to be any just way to allocate risk to either the consumer or the merchant, such a scheme would have the immediate effect of relieving both parties from the burdensome evidentiary requirements of proving the (in)authenticity of an electronic signature. In addition, since the CAs will be the parties assuming the risk, they should be allowed to determine the type of technology to be applied when using their certificates to authenticate a signer. Should this type of proposal be adopted, the key challenge for future legislators would be to create an economic model that aids in the profitability of CAs while shielding the consumer from having to prove fraud or non-negligence. Otherwise, rather than

[126] *See* Perritt *supra* note 108, at 20-22.

promoting the growth of electronic commerce, E-Sign and its progeny may become a great impediment.