

2004

Mechanisms for the Protection of Online Consumers: A Comparative Analysis of the U. S. E-Sign Act and Thai E-Transactions Act

Watchara Neitivanich

Follow this and additional works at: <http://digitalcommons.law.ggu.edu/annlsurvey>



Part of the [Consumer Protection Law Commons](#)

Recommended Citation

Neitivanich, Watchara (2004) "Mechanisms for the Protection of Online Consumers: A Comparative Analysis of the U. S. E-Sign Act and Thai E-Transactions Act," *Annual Survey of International & Comparative Law*: Vol. 10: Iss. 1, Article 5.

Available at: <http://digitalcommons.law.ggu.edu/annlsurvey/vol10/iss1/5>

This Article is brought to you for free and open access by the Academic Journals at GGU Law Digital Commons. It has been accepted for inclusion in Annual Survey of International & Comparative Law by an authorized administrator of GGU Law Digital Commons. For more information, please contact jfischer@ggu.edu.

MECHANISMS FOR THE PROTECTION OF ONLINE CONSUMERS

A COMPARATIVE ANALYSIS OF THE U.S. E-SIGN ACT AND THAI E-TRANSACTIONS ACT

WATCHARA NEITIVANICH¹

I. INTRODUCTION

Internet technology has been increasingly used for borderless commerce as well as for global communications. The technology has also had a profound effect on global electronic commerce in goods and services² by providing online businesses with many benefits, such as reducing the size of staffs, providing secure means for conducting long distance transactions, increasing promptness in contacting consumers, and improving overall cost-effectiveness. Since online purchasers seldom have an opportunity to meet and see online merchants in person, consumers are rightfully concerned with security and fraud potential when purchasing merchandise over the Internet.³

Some websites selling online products do not provide adequate means for consumers to contact them. Some provide only e-mail addresses, without disclosing their office location and telephone numbers. This creates

1. Dr. Neitivanich holds an LL.B. (Hons.) from Thammasat University (Thailand); an LL.M. in International Business Law from Kyushu University (Japan); an LL.M. in International Banking and Financial Law from Boston University (U.S.A.); and an S.J.D. in International Legal Studies from Golden Gate University (U.S.A.). Dr. Neitivanich became a Barrister-at-Law of the Thai Bar Association in 1996.

2. YAMAN AKDENIZ ET AL., *THE INTERNET, LAW AND SOCIETY* 349 (2000).

3. EFRAIM TURBAN ET AL., *ELECTRONIC COMMERCE: A MANAGERIAL PERSPECTIVE* 367 (1999).

understandable uncertainty for online consumers. Even though the websites list a head office location and means to reach them, consumers may not be certain that they are the persons who they claim to be. Persons negotiating business deals via videoconference also need to authenticate the identity of the other parties, unless they have previously dealt with him or her.⁴

The issue of how to verify Internet websites can be resolved by the use of trusted third parties performing verification services and issuing digital certificates for commercial websites (*see, next page* Fig. 1). Trusted third parties, widely known as certification authorities, also issue digital certificates for individuals who have met the qualifications set forth in the authorities' certification practice statements or policies. Any website that discloses a digital certificate to online consumers can be trusted in terms of its existence. Identities of individuals who possess digital certificates may be trusted because a certification authority has verified his or her identity at the time of issuance of the certificate. To increase level of security, widely popular commercial auction website *eBay*, for example, assures online consumer confidence by employing third party verification of participant identity.⁵

According to Taylor Nelson Sofres Interactive⁶, future online shopping rates will continue to soar. Online shopping continues to be more popular in the United States than elsewhere because American consumers value its convenience.⁷ Online commerce can satisfy consumers' needs in terms of information and price comparison. However, transaction security seems to be the main impediment to the growth of online commerce in certain countries such as Thailand. The percentage of Internet users who plan to shop online within the next six months in Thailand has only grown by one percent.⁸ This indicates that Thai consumers are not confident in conducting online purchases and prefer to shop at conventional discount stores or supermarkets.

To promote consumer confidence in transaction security, businesses need to provide them with technologies to provide sufficient levels of security. Application of improved security technology will help slow the growth

4. *Id.* at 371.


5. GEORGE B. DELTA & JEFFREY H. MATSUURA, *LAW OF THE INTERNET* 11-76 (1997).

6. Taylor Nelson Sofres Interactive is one of the world's leading market information groups providing continuous and custom research and market analysis in over 50 countries.

7. *E-Commerce: Security Issues*, THANSETTHAKIT 44, July 4-6, 2002.

8. *Id.*

of high-tech fraud.⁹ The application of digital signature technology provides high levels of security in terms of the identity of parties involved in online commerce. Although digital signature techniques using encryptions may be not appropriate for low-value transactions,¹⁰ they may be worthwhile for high-value business-to-business or business-to-consumer transactions.



**WWW.DIRECTCASE.COM is a
VeriSign Secure Site**

Security remains the primary concern of on-line consumers. The VeriSign Secure Site Program allows you to learn more about web sites you visit before you submit any confidential information. Please verify that the information below is consistent with the site you are visiting.

Name	WWW.DIRECTCASE.COM
Status	Valid
Validity Period	06-DEC-01 - 17-DEC-03
Server ID Information	Country = US State = Wyoming Locality = Jackson Organization = RHINOSKIN, INC. Organizational Unit = Web Operations Common Name = www.directcase.com

If the information is correct, you may submit sensitive data (e.g., credit card numbers) to this site with the assurance that:

- This site has a VeriSign Secure Server ID.
- VeriSign has verified the organizational name and that RHINOSKIN, INC. has the proof of right to use it.
- This site legitimately runs under the auspices of RHINOSKIN, INC..
- All information sent to this site, if in an SSL session, is encrypted, protecting against disclosure to third parties.

To ensure that this is a legitimate VeriSign Secure Site, make sure that:

1. The original URL of the site you are visiting comes from WWW.DIRECTCASE.COM.
2. The URL of this page is <https://digitalid.verisign.com>.
3. The status of the Server ID is Valid.

Figure 1 -- Security Certificate, Source: <http://digitalid.verisign.com>

Ideally, digital signature technology makes forgery and repudiation so difficult as to be impractical and provides means of detecting modifications and other forms of tampering with the content of digitally signed transactions.¹¹ Digital signature technology provides advantages

9. Andrew J. Sherman, *The Legal and Strategic Aspects of E-Commerce Series*, Tech Council of Maryland, at <http://www.mdhitech.org/News/articles/34.html> (April 2001).

10. HENRY H. PERRITT, JR., *LAW AND THE INFORMATION SUPERHIGHWAY* 562 (2d ed. 2001).

11. *Id.*

to both sides. Digital certificates assure online shoppers that the online merchants with whom they are considering doing business in fact exist and that they are who they claim to be. Similarly, online merchants can also be certain that persons who place orders are really who they claim to be, and the order cannot be repudiated once it has been digitally signed. Authenticated digital signatures provide stronger evidence of the source and integrity of a message than an electronic replica of a physical handwritten signature affixed on hard copy output.¹² Digital signature technology is not an absolute answer to all problems, but it provides today's most secure, practical solution.¹³

Both the E-Sign Act and Thai E-Transactions Act prohibit courts from denying legal effect of electronic signatures purely on the ground that they are in electronic form. Both Acts recognize digital signatures. Courts may, however, deny the legal effect of any electronic signature on the grounds of unreliability. The legal effect of a digital signature may also be attacked on the ground of forgery.¹⁴

Although the E-Sign Act and Thai E-Transactions Act have addressed some legal issues regarding validity, certain issues concerning burden of proof of reliability and mechanisms for consumer protection still remain insufficiently addressed. This chapter presents the following recommendations.

II. MECHANISMS FOR CONSUMER PROTECTION

A. CAPS ON CONSUMER LIABILITY

The Federal Trade Commission (FTC) is the key United States agency dealing with online consumer protection concerns.¹⁵ One key concern is the exposure of consumer liability in the case of misuse of technology or fraud committed by third parties. Fraud and forgery are effective defenses to online agreements.¹⁶ Signatories may defend themselves by

12. *Id.* at 582.

13. Jonathan Angel, *PKI and the Law*, NETWORK MAGAZINE, Oct. 2000, at 3, <http://www.networkmagazine.com/shared/pastIssues.jhtml?year=2000>.

14. *Electronic Signature Law Enacted*, Newsroom Legal Counsel News, at http://www.asmma.com/Newsroom/Legal/Leg_Sum_00/leg_sum_00.htm (last visited Nov. 2, 2002).

15. STANLEY MORGANSTERN, *LEGAL PROTECTION FOR THE CONSUMER* 1 (2d ed. 1978).

16. Richard L. Brown, *The E-Signature Act—A Brief Overview*, at http://www.ecsi.net/updates/news_00049.html (last revised Oct. 25, 2001).

claiming that the transactions were electronically signed without authority, or by a person who lacked capacity.¹⁷

Consumers who apply or use digital signatures may sometimes lack the necessary technical knowledge and expertise, or they may be deceived into digitally signing something they did not intend to sign. Even though digital signatures are unique and encrypted, it is possible for hackers to steal the algorithms and forge a signature.¹⁸ Signatories who store their private keys in hard drives, even if enforced by additional password protection are vulnerable to brute force attacks.¹⁹

It is not as easy to prove that someone has fraudulently misused a digital signature as it is to prove forgery in a handwritten signature.²⁰ To prevent false claims of private key losses, and to strengthen the efficiency of digital signature technology, signatories bear the risk of liability if they lose their key and fail to give proper notice.²¹

A forgery of a traditional signature is null and void under the Thai Civil and Commercial Code.²² With electronic signatures, a forged electronic

17. Maureen Dorney, *Electronic Signatures in Global and National Commerce Act*, FindLaw Corporate Counsel Center, <http://articles.corporate.findlaw.com/articles/file/00051/004974/title/subject> (last visited Nov. 2, 2002). See also EOGHAN CASEY, *DIGITAL EVIDENCE AND COMPUTER CRIME: FORENSIC SCIENCE, COMPUTERS AND THE INTERNET* 199 (2000). The signatory may adduce digital evidence as "alibi." The key pieces of information in an alibi are time and location. When an individual uses a computer or connects to the Internet, the time and location is often noted, generating digital evidence that can be used to support or refute an alibi. Thus, the signatory may adduce this digital evidence (detailed logs of activities) to convince the court that he was not using the computer or signing that transaction.

18. Mike France, *Snares of the E-Signatures Act*, BusinessWeek online, at <http://www.businessweek.com/ebiz/0101/ep0108.htm> (Jan. 8, 2001).

19. Jane Kaufman Winn & Carl Ellison, *Regulating the Use of Electronic Authentication Procedures by US Consumers in the Global Electronic Market*, ¶ 6, at <http://www.ftc.gov/bcp/icpw/comments/revwin-1.htm> (Mar. 26, 1999).

20. France, *supra* note 18. See Utah Code Ann. § 46-3-103(12) provides that to "forge a digital signature" means either:

- (a) to create a digital signature without the authorization of the rightful holder of the private key; or
- (b) to create a digital signature verifiable by a certificate listing as subscriber a person who either:
 - (i) does not exist; or
 - (ii) does not hold the private key corresponding to the public key listed in the certificate.

See also THOMAS P. VARTANIAN ET AL., *21ST CENTURY: MONEY, BANKING & COMMERCE* 460 (1998). Unlike a forged paper check that can be identified and examined by handwriting experts, an unauthorized electronic check will be digitally identical to one validly issued by the signatory.

21. PERRITT, *supra* note 10, at 592.

22. For example, C.C.C. § 1008 says that "where a signature on a bill is forge or placed thereon without the authority of the person whose signature it purports to be, the forged or unauthorized signature is wholly inoperative...." See U.C.C. Article 3 provides, in relevant part: any authorized signature is wholly inoperative as that of the person whose name is signed unless he

signature is also invalid, but the law, such as the Thai E-Transactions Act has imposed a duty of care upon a signatory.²³ If a signatory has breached his or her duty of care, he or she will be held accountable for his or her action.

Relying parties are also consumers in digitally signed transactions. The E-Transactions Act imposes a duty upon relying parties to take reasonable care in verifying the reliability of electronic signatures.²⁴ Relying parties who fail to authenticate digital signatures bear the risk of loss even where such failure resulted from a failure in the online certification authority's computer system. Therefore it is also reasonable for relying parties to have protection in this situation.²⁵

The long history of consumer protection legislation makes it reasonable that the liability of customers should be limited even in situations where they have not acted reasonably.²⁶ The question whether consumers have acted reasonably or not is a question of law. Laws should not place the risk of fraud or error losses from online transactions on customers, but on the providers and online merchants who profit from the use of technology.²⁷ Laws that shift the risk of fraud or error losses to consumers create a moral hazard and will produce economically inefficient outcomes.²⁸

It is fair to place on consumers the risks that they can realistically be expected to control, but with some limitations.²⁹ Establishing caps on liability for consumers who apply digital signature technology in cases of technology misuse is a reasonable protective measure. Technology misuse includes a fraudulent misuse by third parties or signatories. If everyone involved in the digitally signed transaction has acted reasonably, the risk of fraud and loss should be placed on digital signature service providers and online merchants who create and

ratifies it or is precluded from denying it; but it operates as the signature of the unauthorized signer in favor of any person who in good faith pays the instrument or take it for value.

23. Electronic Transactions Act § 27(1) B.E. 2545 (2001) (Thai.) provides that each signatory "shall exercise reasonable care to avoid unauthorized use of his signature creation data."

24. E-Transactions Act, *supra* note 23 at § 30(1).

25. PERRITT, *supra* note 10, at 590.

26. *The Role of Certification Authorities in Consumer Transactions*, Internet Law and Policy Forum-Working Groups and Publications, at <http://www.ilpf.org/groups/ca/exec.htm> (last visited Nov. 1, 2002).

27. PAUL D. SHAW, *MANAGING LEGAL AND SECURITY RISKS IN COMPUTING AND COMMUNICATIONS* 118 (1998).

28. Winn & Ellison, *supra* note 19, at 2.

29. *Id.* at 6.

maintain the use of digital signature technology system, in order to encourage them to improve the system.³⁰

All other risks allocated to more sophisticated parties, such as online merchants, and digital signature technology providers can be compensated by insurance. Allocating liability for unauthorized use of digital signatures to online certification service providers and merchants will promote further investment to develop and maintain the security of the system.³¹

For credit cards and debit cards, the liability of cardholders is limited to \$50 in case of lost or stolen cards according to Regulations Z and E.³² Those rules mandate that no customer can be held accountable for the unauthorized use of their credit cards or for unauthorized electronic fund transfers unless they accepted the credit card and or access device such as an ATM card or debit card, and the rules concerning liability for unauthorized were disclosed.³³ Regulation Z protects cardholders from all liability in excess of \$50 for failure to safeguard the credit card, while

30. See Winn & Ellison, *supra* note 19, at 2.

31. *Id.*

32. See Truth in Lending Act (Regulation Z) 12 C.F.R. § 226.12 (b) “provides: liability of cardholder for unauthorized use ... of a credit card shall not exceed the lesser of \$50 or the amount of money, property, labor, or services obtained by the unauthorized use before notification to the card issuer under paragraph (b)(3) of this section....” See also Electronic Fund Transfers (Regulation E) 12 C.F. R. § 205.6 stipulates:

a) Conditions for liability. A consumer may be held liable, within the limitations described in paragraph (b) of this section, for an unauthorized electronic fund transfer involving the consumer's account only if the financial institution has provided the disclosures required by § 205.7(b)(1), (2), and (3). If the unauthorized transfer involved an access device, it must be an accepted access device and the financial institution must have provided a means to identify the consumer to whom it was issued.

b) Limitations on amount of liability. A consumer's liability for an unauthorized electronic fund transfer or a series of related unauthorized transfers shall be determined as follows:

(1) Timely notice given. If the consumer notifies the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$50 or the amount of unauthorized transfers that occur before notice to the financial institution.

(2) Timely notice not given. If the consumer fails to notify the financial institution within two business days after learning of the loss or theft of the access device, the consumer's liability shall not exceed the lesser of \$500 or the sum of:

(i) \$50 or the amount of unauthorized transfers that occur within the two business days, whichever is less; and

(ii) The amount of unauthorized transfers that occur after the close of two business days and before notice to the institution, provided the institution establishes that these transfers would not have occurred had the consumer notified the institution within that two-day period.

33. Winn & Ellison, *supra* note 19, at 9.

Regulation E provides a progressive limit starting from \$50 to \$500.³⁴ The use of credit cards may be abused in some situations and statutes still protect the cardholders.

Currently, neither the E-Sign Act nor the Thai E-Transactions Act addresses the issue of limitations on liability for consumers who apply electronic signatures. Digital signature technology may be misused either by negligence of signatories or by hackers. Consumers should not be bound by unauthorized use of online authentication procedures unless, after full disclosure of the risks involved, the consumer has agreed to be bound.³⁵ Although the consumer has agreed to be accountable for an unauthorized use, such liability exposure must be limited.

The limitations of digitally signed transactions should be the same amounts as for credit cards. The risk of loss due to fraud should be placed on the shoulders of online merchants and technology providers in order to provide incentives for investment in the improvement of the technologies.³⁶ It is appropriate for online merchants to insure their businesses against risk of fraud. Thus, insurance coverage against risk of technology misuse should be provided.

Another type of insurance coverage may be additionally provided for consumers who are signatories to insure against risks of liability arising from a legal or contractual obligation to exercise reasonable care to protect their private signing keys from being disclosed. Under this coverage, the policy should protect the signatories from liability for damages arising out of the use of the digital signatures. This helps the signatories bare the risks of liability. If the signatories are sued on the ground of breach of their duties which created losses to relying parties, the insurance company can compensate such loss.

Under some circumstances, however, although the signatories have not acted in violation of any duty of care, a third person, such as a hacker may have obtained the private signing key by high-tech theft, and has created loss to an individual who reasonably relied on the digitally signed documents in the name of the signatories. The principle of no-fault should be applied in order to compensate the individual who has reasonably acted on the basis of such digital signatures.³⁷ The insurance

34. *Id.* at 12. See also 12 C.F.R. § 226.12 (b) and 12 C.F. R. § 205.6.

35. *Id.* at 2.

36. *Id.* at 2.

37. EMMETT J. VAUGHAN & THERESE M. VAUGHAN, FUNDAMENTALS OF RISK AND INSURANCE 543-544 (8th ed. 1999). Under this no-fault system, a relying party does not need to prove that the

company has to compensate for the loss even though the signatories are not legally liable for such loss.

With a mechanism to cap their liability and to insure against liability and technology misuse, consumers will feel more confident in applying digital signatures and they will become more widely accepted. Consumers will know that even if there is any misuse of technology they will be protected.

B. CONSUMER CONSENT

In the United States, the E-Sign Act governs only transactions in which the parties have agreed to conduct business with each other through electronic means.³⁸ A major concern in the area of consumer protection is that companies would make crucial information available to their consumers only through the Internet.³⁹ There are concerns that consumers might consent to future electronic transactions which they may not have the technological capability of receiving, reading or retaining.⁴⁰ It is essential for Congress to incorporate consumer protection provisions requiring consumer consent in the E-Sign Act. Subject to the Act, consumers must explicitly agree to the use of all electronic contracts and records prior to the initiation of any transaction that involves an electronic signature or results in an electronic record as the official copy of the transaction.⁴¹

The E-Sign Act should shield consumers from technological abuse from the business sector due to the difference in bargaining power. Requirements for technological access are also incorporated in the E-Sign Act so that consumers are notified if the business has upgraded or changed any software to access and retain the electronic records.⁴² The

signatory is at fault. If the relying party suffers damages from relying on the forged or unauthorized digital signature, he would seek recovery for his losses from the signatory's insurer.

38. Anthony M. Ballon, *From Wax Seals to Hypertext: Electronic Signatures, Contract Formation, and a New Model for Consumer Protection in Internet Transactions*, 50 EMORY L. J. 905, 926 (2001).

39. Robert MacMillan, *E-Sign Law Appears To Work Fine So Far- Govt. Study*, at <http://www.newsbytes.com/news/01/167338.html> (2001).

40. *The Dynamics of Consumer Protection in Light of UETA and E-Sign*, at 4, at http://www.consumerlaw.org/initiatives/e_commerce/dynamics_of_consprotection.shtml (last visited Nov. 2, 2002).

41. Electronic Signatures in Global and National Commerce Act § 101 (c)(1)(A), 15 U.S.C. 7001-7031 (2000) [hereinafter E-Sign Act].

42. E-Sign Act, *supra* note 41 at § 101(C)(D) provides that if a change in the hardware or software requirements needed to access or retain electronic records creates a material risk that the consumer will not be able to access or retain a subsequent electronic record that was subject of the consent, the person providing the electronic record must provide the consumer

requirement for consumer consent not only protects customers who lack capacity to access to electronic records, but also ensures that they will in fact receive such electronic communications.⁴³

Consumers, by definition are “individuals who obtain through transactions, products, or services which are used primarily for personal, family, or household purposes, and also means the legal representatives of such individuals.”⁴⁴ Consumers can be any natural persons who purchase goods or services via commercial Internet websites and other electronic means for their own use, not for resale. This protection is intended to cover only private consumers, not business or corporate consumers.⁴⁵

Congress also integrated the principle of party autonomy provisions in the E-Sign Act. According to the Act, no consumer can be forced to enter into online contracts or online transactions without their clear and conspicuous consent.⁴⁶ Such consent must be made prior to the commencement of any transactions that involve electronic signatures, including digital signatures.⁴⁷ The Act provides that consent be granted or confirmed electronically, excluding voice messages. This means that the consumer must be engaged in electronic communications prior to an electronic delivery of required notices.⁴⁸ Clicking an “I agree” icon or click-checking an unchecked box indicates assent.⁴⁹

Where laws require information be provided to consumers in writing,⁵⁰ consumer consent is required. Businesses intending to correspond with consumers through electronic means must have consumer consent before transmitting electronic notices to consumers; otherwise they are in

with a statement of (I) the revised hardware and software requirements for access to and retention of the electronic records....

43. *The Dynamics of Consumer Protection in Light of UETA and E-Sign*, *supra* note 40, at 4.

44. E-Sign Act, *supra* note 41 at § 106(1).

45. RICHARD D. WILLIAMS & BRUCE T. SMYTH, *COMPUTER AND INTERNET LIABILITY: STRATEGIES, CLAIMS AND DEFENSES* 8-9 (2d ed. 2000).

46. E-Sign Act, *supra* note 41 at § 101(c)(B).

47. E-Sign Act, *supra* note 41 at § 101(c)(A).

48. Gail Hillebrand, *E-Sign Study-Comment P004102*, Consumers' Union, at <http://www.ftc.gov/bcp/workshops/esign/comments/consumersunion.pdf> (last visited Nov. 2, 2002).

49. Ryan J. Casamiquela, *Contractual Assent and Enforceability in Cyberspace*, 17 *BERKELEY TECH. L. J.* 475, 479 (2002). According to *Caspi v. Microsoft Network LLC*, 732 A.2d 528 (N.J. App. Div. 1999), the court upheld clickwrap license when user was prompted by vendor to view license and had opportunity to click either “I agree” or “I don't agree”.

50. *Electronic Signature Law Enacted*, Newsroom Legal Counsel News, at http://www.asmma.com/Newsroom/Legal/Leg_Sum_00/leg_sum_00.htm (last visited Nov. 2, 2002). See also RAYMOND T. NIMMER, *THE LAW OF COMPUTER TECHNOLOGY: RIGHTS, LICENSES, LIABILITIES*, 2001 CUMULATIVE SUPPLEMENT NO.1 14-21 (3d ed. 2001). The E-Sign Act endorses the consumer protection laws by requiring the information regarding disclosures or notices be made available to a consumer in writing.

violation of the consumer protection provision. If the law does not require businesses to provide electronic notices or information to consumers (such as Amazon.com selling books online) they are not subject to the requirements.⁵¹

Requirements for affirmative consent by consumers ensure that no business can force any consumers to accept required notices in electronic form against their will.⁵² To protect consumers effectively, the E-Sign Act requires specific electronic consent processes that reasonably demonstrate the capacity of the consumer involved to access to the Internet or related electronic documents⁵³ in the form of e-mail or in HTML format on a web site.⁵⁴ Electronic consent may be demonstrated by means of clicking through procedure that permits a consumer to enter into an online transaction only after acknowledging his or her consent.⁵⁵ This requirement ensures that consumers in the online marketplace are properly protected at the same level as in the conventional paper-based world.⁵⁶

The E-Sign Act unambiguously states that consumers are entitled to be informed of their rights to use conventional approaches for receiving notices or mailings, as well as minimum technical requirements necessary to receive electronic notices.⁵⁷ E-mails attached with files sent to consumers may not be in formats that consumers' computers can read.⁵⁸ Because of incompatibilities in technology in use, this may lead consumers to lose their rights to be notified. Thus, there should be requirements that notice transmitted to the consumer be in readable format intelligible to the consumer.⁵⁹

51. Jonathan Stern, *Briefing Paper on the Electronic Signatures in Global and National Commerce Act*, at 4, at <http://www.law.berkeley.edu/institutes/bclt/pubs/annrev/exmplrs/bp/jsbp.pdf> (Sep. 18, 2000).

52. Jay Inslee, *What Features of an E-Sign Bill Will Most Effectively Impact E-Commerce: E-Sign Bill Must Include Protections for Consumers*, at 2, at <http://www.rollcall.com/pages/pb/00/03/pb27h.html> (Mar. 27, 2000).

53. Consumer Union, *The Need to Protect Consumers — Especially Low-Income Consumers— from UETA*, at <http://www.consumersunion.org/finance/uetawc201.htm> (Feb. 1, 2001).

54. Louis F. Rosenthal, *Statement Before the House Financial Service Subcommittee on Domestic Monetary Policy, Technology and Economic Growth*, at http://commdocs.house.gov/committees/bank/hba73743.000/hba73743_0.htm (June 28, 2001).

55. Robert J. Marchant, *Electronic Commerce Under the Federal E-sign Legislation*, 74 *Wisconsin Lawyer*, (Jul. 2001), at <http://www.wisbar.org/wislawmag/2001/07/marchant.html> (last visited Nov. 2, 2002).

56. Rosenthal, *supra* note 54, at 3.

57. Brown, *supra* note 16.

58. Consumer Union, *supra* note 53.

59. *Id.*

The E-Sign Act gives rights to consumers not only to terminate their consent to receive electronic notices at anytime, but also to continue receiving paper-based notices as well.⁶⁰ Businesses cannot require consumers to accept or sign their signatures electronically. If the consumers prefer to have their transactions on paper, the business may not force them to accept electronic transactions. If the consumer is unable to open, retain and print an electronic record because it is not in the format in which he or she agreed to receive it, the electronic record will not satisfy the delivery requirements under the E-Sign Act.⁶¹ If consumers are mistaken about the capacity of their computers to receive, retain or print electronic records, they are entitled to withdraw their consent to receive such electronic documents.⁶²

Consumer consent provisions under the E-Sign Act apply to online transactions regardless of the amount or value of a particular transaction.⁶³ Consent requirements apply only to electronic records that are provided or made available to consumers, not to electronic records that are obtained from them.⁶⁴ The consumer need not consent to the electronic recording of agreements that they electronically signed and transmitted to businesses unless the online transactions they have to receive electronic confirmations in order to make the transaction valid.⁶⁵

Businesses are seeking to amend consumer protection provisions because they place the burdens on businesses.⁶⁶ For example, Visa recently stated that the Demonstration Requirement is unnecessary since it underestimates the capacity of consumers to operate in cyberspace.⁶⁷ The more the consumer needs to do to conduct a transaction, the possibility that they will finish through that process is greatly decreased.⁶⁸ Consumer protection provisions have worked out in the marketplace.⁶⁹ It appears reasonable not to amend or repeal provisions for consumer protection since their benefits outweigh the burdens of businesses

60. Brown, *supra* note 16.

61. Inslee, *supra* note 52, at 2.

62. *Id.*

63. Marchant, *supra* note 55, at 2.

64. Robert A. Wittie & Jane K. Winn, *Electronic Records and Signatures under the Federal E-Sign Legislation and the UETA*, 54 *The Business Lawyer* 293, 299 (2000), available at <http://faculty.smu.edu/jwinn/ESIGN-UETA.htm> (last visited Nov. 2, 2002).

65. *Id.*

66. Patrick Thibodeau, *Business Seeking Changes to E-Sign Act*, *Computerworld*, at <http://www.itworld.com/Man/2681/CWD010402STO59147/> (Apr. 2, 2001).

67. Russell W. Schrader, *Re: E-Sign Study-Comment P004102* (Mar. 15, 2001).

68. Thibodeau, *supra* note 66.

69. MacMillan, *supra* note 39.

conducting online commerce, according to the California Department of Consumer Affairs.⁷⁰

It is interesting to note that the E-Sign Act does not address mechanisms for enforcement if businesses failed to obtain consumer consent. There should be sanctions imposed upon the businesses that fail to obtain consumer consent where the law requires them to do so. For instance, if businesses commit violations regarding consent, there should be sanctions that result in the invalidity and unenforceability⁷¹ of the notice or information that has been transmitted electronically. Most businesses will not enforce such electronic messages against consumers or take advantage of the validity provisions. On the other hand, the E-Sign Act provides protection to consumers where their consent has not been given. The E-Sign Act, however, recognizes the legal effectiveness, validity, or enforceability of any contract executed by consumers even though the business has failed to obtain electronic consent or confirmation of consent by that consumer.⁷²

To comply with the consumer consent provisions under the E-Sign Act, certification service providers may need to use both online and off-line processes to contact its clients during the certificate issuance process.⁷³ They may ask applicants to provide their e-mail address at the time they apply for digital certificates. This enrollment can be done online through websites and offline via paper-based application forms.

The use of the e-mail address serves dual purposes, viz., the identification and authentication of applicants.⁷⁴ Before processing digital certificates, certificate service providers will transmit a message to the e-mail address given by the client. If the messages bounce back, the certificate service providers may decline to issue the certificate⁷⁵ or may contact its client by traditional means to confirm the accuracy of the e-mail address. In order to prove that the client has capacity to conduct transactions in a manner that reasonably demonstrates his or her ability to access online information, certification service provides may send out paper-based activation codes to the client by first class mail.⁷⁶

70. Kathleen Hamilton, *Re: E-Sign Study Comment P004102*, at <http://www.ftc.gov/bcp/workshops/esign/comments/cca.htm> (Mar. 9, 2001).

71. Michael E. Arruda & Irian A. Shestakova, *US Enacts E-Sign: The Electronic Signatures in Global and National Commerce Act*, at <http://www.cla.org/usenacts.pdf> (last visited Nov. 2, 2002).

72. E-Sign Act, *supra* note 41 at § 101(c)(1)(3).

73. Thomas J. Greco, *the E-Sign Act in General*, Digital Signature Trust Co., at <http://www.ftc.gov/bcp/workshops/esign/comments/dstc.htm> (Mar. 27, 2001).

74. *Id.*

75. *Id.*

76. *Id.*

Demonstration of capacity to access online information on the website is established when the applicant enters his or her activation code.⁷⁷

According to Economic and Statistics Administration & National Telecommunications and Information Administration, the percentage of Americans who have no access to the Internet in their home or elsewhere is over 55 percent.⁷⁸ Only 41.5 percent of all U.S. users can access the Internet from their home. Eight percent of Americans rely on public access, and the percentage of elderly and poor who do not have access to the Internet is much higher. There is a need for additional consumer protection, such as electronic delivery assurance. In order to provide stronger protection to consumers, the notices transmitted to a consumer should be considered received only when the notice itself is opened, acknowledged, or automatically acknowledged by a flag that indicates the recipient has opened it.⁷⁹

In Thailand, the percentage of Thais who have access to the Internet is relatively low. Almost all Thais rely on traditional means of communication, such as mails, telegrams, and faxes. Although the E-Transactions Act is more comprehensive than the E-Sign Act in terms of specific duties imposed upon parties involved in online transactions, it does not address mechanisms for protection of consumers as the E-Sign Act does.

The Thai E-Transactions Act does not incorporate affirmative consumer consent provisions. This will allow unscrupulous businesses to take advantage of relatively unsophisticated consumers by encouraging them to consent to receive electronic documents even though these are beyond that consumers' needs or ability to use. For example, businesses may incorporate terms that allow them to send information to consumers who provide their e-mail addresses. Having an e-mail address does not mean that the consumer has the ability to access and use electronic records.

Lack of provisions regarding prior consent puts the consumer in danger without means of protection. Consumers may not wish to enter into electronic contracts because they distrust the transactions, or they do not have confidence in the use of electronic media. But some websites may not allow consumers to conduct transactions with them through conventional paper means. This means consumers may not get

77. *Id.*

78. U.S. Department of Commerce, Economic and Statistics Administration & National Telecommunications and Information Administration, "Falling Through the Net: Toward Digital Inclusion" A Report on Americans' Access to Technology Tools, October 2000. Figure II-13.

79. *The Dynamics of Consumer Protection in Light of UETA and E-Sign*, *supra* note 40, at 8.

notification if they cannot access the Internet. Thus, requirements for prior consent are indispensable if businesses wish to provide electronic documents to consumers.

C. PAPER BACKUP

Although the E-Sign Act and E-Transactions Act allow certain transactions to be made electronically, there is the potential risk of alteration and modification because the E-Sign Act does not require that the process of electronically signing the records itself would prevent alteration of that record.⁸⁰ Even though most transactions are electronically stored, back up on paper is vital for online commerce since any alteration of paper-based documents is more easily noticed than on electronic records.⁸¹ When electronic records may have been exposed to modifications which have left no trace, without proper detection technology it will be hard to prove that the consumers agreed.

Some vendors may encourage consumers to agree to receive copies of concluded contracts in electronic form. Proof of agreement may be files attached to e-mails, or a showing that the cost of the product was discounted because the consumer chose to receive an electronic copy. Vendors may also provide computers for consumers to electronically sign electronic contracts at the vendor's office, and inform the consumer that they will receive a copy of the signed contract in a paper form later. This provides opportunities for vendors to alter electronic records after signatures have been affixed.⁸² Without an accurate, secure means of detecting changes, fraud and the potential for alteration or modification of the agreement are potential sources of exposure for consumers.

This issue can be resolved by requiring that in transactions where the seller provides the electronic equipment, the consumer must be given a written, non-electronic copy of the contract. If the consumer wishes to receive notices electronically in the future, they may consent to do so on the condition that the consent must be made or confirmed on electronic equipment not provided by the seller.⁸³ To protect consumers and provide primary evidence of their transactions, consumers should be entitled to have a paper back up from the businesses for a nominal fee. The danger

80. The National Consumer Law Center, *Electronic Signatures in Global and National Commerce Act: E-Sign Study- Comment P004102*, 7 (2001), at <http://www.ftc.gov/bcp/workshops/esign/comments/nclc.pdf> (last visited Nov. 2, 2002).

81. Angel, *supra* note 13, at 2.

82. The National Consumer Law Center, *supra* note 80, at 7.

83. Margot Saunders & Gail Hillebrand, *E-Sign and UETA: What Should States Do Now?* available at <http://www.consumerlaw.org/e-sign.html> (n.d.).

here is that the fee might provide a disincentive for consumers to obtain paper back up. This paper back up requirement not only provides consumers with solid record for their consummated transactions, but also proof of non-alteration as laid out in the contents and terms set forth in the agreement.

D. RIGHT OF ACCESS TO READABLE AND NON-REPUDIABLE ELECTRONIC DOCUMENTS

The E-Sign Act has as strong a provision for electronic record integrity as in the Thai E-Transactions Act. Record keeping processes are a key concern in consumer protection. When online merchants attempt to prove the integrity of electronic documents, courts may deny legal effect to electronic record on the grounds that they are not in an accurately reproducible form capable of use for later reference. Both Acts require that records of online transactions be capable of being retained and accurately reproduced for subsequently reference regardless of whether the parties actually retained it.⁸⁴

There must be measures to protect consumers and provide them with access to the records by any means provided by the businesses. The problem that needs to be addressed is how consumers can be assured that the electronic document is the one that they signed or agreed with. Although businesses are by law mandated to maintain and store electronic records in a retrievable form and without modification,⁸⁵ neither Act specifies which or what kind of technology be used to maintain record integrity.

To comply with the requirements, records must be preserved in locked formats that cannot be modified, such as Portable Document Format (.pdf – an Adobe Corporation trademarked but freely available format able to be used on nearly all recent computer systems) to prevent innocent or deliberate alteration whenever the document is read.⁸⁶ To prevent changes or repudiation and to protect consumers, they should be able to request the businesses to provide electronic records that were stored or kept in non-alterable form. To provide preventive measures, the consumer should be able to request businesses to digitally sign document because digital signatures are able to detect modifications after signature. This is the best solution for both modification prevention and non-repudiation.

84. MICHAEL D. SCOTT, SCOTT ON COMPUTER LAW 7-132 (2d ed. 2002).

85. Inslee, *supra* note 52.

86. The National Consumer Law Center, *supra* note 80, at 5.

E. DISCLOSURE

The best and most common means of consumer protection is to educate consumers about the legal effects of the use of electronic signature technology, and to warn them against signing electronic documents without fully understanding that they have legally binding force. Without knowing how to use proper technology consumers may end up being bound to online contracts without intending to. Since many consumers lack legal and technological awareness, they may not know that their actions, such as typing their names at the end of an e-mail message, clicking a check box, or leaving a voice message, can bind them. There is a need for disclosure about the risk of being legally bound.

Neither the E-Sign Act nor the E-Transactions Act requires businesses to disclose information indicating that clicking an agreement button constitutes consumer acceptance. The disclosure notifies consumers that a binding contract will be formed if they intentionally click on the “I agree” icon.⁸⁷ Disclosure encourages consumers to read the terms carefully and be alert before taking steps that bind them to electronic transactions.

It is necessary that mandatory disclosure be among the duties placed upon businesses in consumer transactions. Such notification must be presented in a clear and conspicuous manner.⁸⁸ This will ensure that consumers signing electronic messages by clicking “I agree” buttons or typing their names in blanks have been given necessary notice prior to doing so.

F. BURDEN OF PROOF

Neither the E-Sign Act nor E-Transactions Act addresses the issue of the burden of proof in cases of lost, stolen, unauthorized use of, or technical failure of applications of electronic signatures. A typed name at the end of e-mails, one simple form of electronic signatures, is easily forged. The application of a more secure electronic signature, such as a digital signature, is preferable in order to lessen or eliminate risks.⁸⁹

For repudiation of traditional handwritten signatures, persons who assert forgery as a defense must present some proof that the signature is not authentic.⁹⁰ Holders of signed documents are not required to prove the

87. Ballon, *supra* note 38, at 935.

88. *Id.* at 932.

89. GRAHAM J H SMITH, INTERNET LAW AND REGULATION 462 (3d ed. 2001).

90. The National Consumer Law Center, *supra* note 80, at 11.

signature's authenticity because they have the right to rely upon the presumption of authenticity.⁹¹ Proof of forgery in a physical signature is not difficult because fake signatures may be compared with authentic ones. On the other hand, proving forgery in digital signatures is much more difficult, such that a computer expert witness is usually needed.

For credit card systems, Congress passed the Fair Credit Billing Act that provides consumers with high protection in the event of unauthorized use of credit cards, fraud, theft or system failure by transferring risk of loss to the industry creating and maintaining the credit card system.⁹² In Thailand, the use of credit card is not as stringently regulated as in the United States. Even though the Consumer Protection Committee has declared that the credit card business is a regulated business, only terms in the credit card agreements are highly regulated by the Committee. For instance, the credit card issuers cannot force consumers to pay for any transaction that occurs after the consumer has notified the issuers to temporarily suspend the credit card, unless the credit card issuers can prove that the credit card holder in fact made such transaction.⁹³ It is clear that any transaction made after the notification may not be enforced against the credit card holder. But for transactions that occurred before the notification, even if they were unauthorized, the credit card holder is still responsible unless he or she can prove that the signature is forged.

The use of digital signatures is similar to the use of credit cards since credit cards are electronic devices binding holders of credit cards to a promise to pay.⁹⁴ Digital signatures are in effect electronically generated promises to pay that can bind the owner.⁹⁵ Because of the technological characteristics, unauthorized use and misuse of a digital signatures is likely feasible. Thus, the consumers will bear great burdens if the rules for traditional handwritten signatures apply to the issue of proof in unauthorized use of electronically signed transactions.

In transactions between consumers and technology service providers, the burden of proof of reliability of digital signature technology should be placed on the technology service providers. The law should place a burden of proof of unauthorized use of digital signature on the merchant in merchant to consumer transaction.⁹⁶ This will force the electronic

91. *Id.* at 12.

92. *Id.*

93. PIROJ ARTRUKSA, LAW OF CONSUMER PROTECTION 69 (2000).

94. The National Consumer Law Center, *supra* note 80, at 12.

95. *Id.*

96. *House Subcommittee Questions Preemption Language in Electronic Signatures Bill*, Tech Law Journal, at <http://www.techlawjournal.com/internet/19991002.htm> (last visited Nov. 2, 2002).

commerce industry to create systems for using and accepting electronic signatures that limit losses from fraud, mistake, theft and system breakdown.⁹⁷

G. SELF-EDUCATION

Education is the most effective form of consumer protection.⁹⁸ The government has to alert consumers to possible online fraudulent activities, the significance of privacy in the information age, and other critical consumer protection issues.⁹⁹ Dissemination of information regarding legal effect of consumers' actions is also a key strategy to prevent consumers from entering into online contract without sufficient knowledge. The government has to educate consumers on how they can protect themselves from fraud and how to be smart and careful online shoppers.

Government has to produce publications in electronic and non-electronic forms to provide consumers with consumer protection information. Publications include consumer alert websites, online and paper-based newsletters. Government has to provide guidelines to online marketers on how to assure that fundamental principles for consumer protection apply in Internet commerce as well as in traditional commerce.¹⁰⁰ A wide variety of approaches should be used to disseminate principles of consumer protection to business and industry. These approaches include guidelines, brochures, speeches at industry and academic meetings and conferences.¹⁰¹

H. MINIMUM STANDARDS OF PRIVACY

On the issue of personal data protection, government has to lay out minimum privacy standards in order to protect consumers who provide personal data for certification service providers to issue digital certificates. Such personal data should be protected and may not be used without authorization or consent from consumers. The certification service providers are not allowed to use such data for other purposes than to verify the identity of consumers who applied for a digital certificate.

97. The National Consumer Law Center, *supra* note 80, at 12.

98. FEDERAL TRADE COMMISSION STAFF, A REPORT OF THE FTC'S FIRST FIVE YEARS PROTECTING CONSUMERS ONLINE 16 (1999), available at <http://www.ftc.gov>.

99. *Id.*

100. *Id.* at 18.

101. *Id.*

I. ACCREDITATION SYSTEM FOR ELECTRONIC SIGNATURE SERVICE PROVIDERS

The Royal Thai government has to form an accreditation system to form a single standard for electronic signature service providers to be accredited. Electronic signature service providers must meet standards imposed by the government, such as for trustworthiness, as provided in § 29 of the Thai E-Transactions Act. Consumers will be confident when they conduct transactions with accredited electronic signature service providers because their systems, policies, and practices have been certified as meeting satisfactory standards.

J. UNFAIR TERMS IN CERTIFICATE PRACTICE STATEMENTS

In open PKI environments, persons who apply for online digital certificates may be required by online authentication service providers to accept or agree with terms set forth in service agreements. Online subscribers and consumers will only be able to take or leave the terms without having any capacity to negotiate¹⁰² because of the inequality of bargaining power between the parties.¹⁰³ In order to prevent certification service providers from issuing certificate practice statements unfairly favorable to themselves, the Thai government has to lay down standard clauses that certification authorities will be obligated to state in their certificate practice statements. This will include events such as where certification authorities may be entitled to limit their liability, as well as situations where they may not limit liability. Enacting specific laws to deal with this issue can be an effective means of consumer protection.¹⁰⁴

In Thailand, when the Consumer Protection Committee regards terms set forth in certification service agreements as unfair, it may require certification authorities to repeal or exclude those terms. To determine the unfairness of terms, the Consumer Protection Committee may define terms that are contrary to the requirement of good faith as unfair. The Committee may also judge terms incorporated in service agreements as unfair if such terms cause significant imbalances in the parties' rights, obligations, provide unfair advantages,¹⁰⁵ or are harmful to consumers.¹⁰⁶ Other examples of unfair contract terms are exclusionary, limited

102. DARAPORN THIRAWAT, *CONTRACT LAW: NEW STATUS OF CURRENT CONTRACT AND UNFAIR CONTRACT TERMS* 35 (1995).

103. BRIAN W. HARVEY, *THE LAW OF CONSUMER PROTECTION AND FAIR TRADING* 105 (2d ed. 1982).

104. THIRAWAT, *supra* note 102, at 35.

105. *Id.* at 50.

106. G. STEPHENSON & P. CLARK, *COMMERCIAL & CONSUMER LAW* 94 (4th ed. 1998).

liability, arbitrary unilateral termination clauses.¹⁰⁷ With the exclusion of such unfair terms, online consumers will be better protected.

III. ELECTRONIC NOTARIZATION

Unlike the E-Sign Act, the E-Transactions Act does not address the issue of electronic notarization. E-Sign Act §101(g) provides:

If a statute, regulation, or other rule of law requires a signature or record relating to a transaction in or affecting interstate or foreign commerce to be notarized, acknowledged, verified, or made under oath, that requirement is satisfied if the electronic signature of the person authorized to perform those acts, together with all other information required to be included by other applicable statute, regulation, or rule of law, is attached to or logically associated with the signature or record.

The E-Sign Act allows electronic signatures to be notarized, acknowledged, and verified by affixing the electronic signature of persons authorized to do so for the basic information normally required by state laws, such as names, date of commission expiration.¹⁰⁸ In Thailand, the Civil and Commercial Code, §9, requires persons affixing fingerprints, crosses, and other such marks to paper documents, to be certified by the signatures of two witnesses. After enactment of the E-Transactions Act, the use of typed names, fingerprints, crosses and other such marks are equivalent to traditional handwritten signatures and there is no need for certification.

In some cases, where the identity of a signatory of an electronic signature is determined to be material, such as in transactions where witnesses are needed, electronic or digital signatures may be notarized, acknowledged, and verified by affixing another electronic or digital signature of witnesses. The notary's signature and stamp provide concrete means of locating witnesses.¹⁰⁹ Certification authorities and trusted third parties are able to authenticate legally significant transactions in order to increase confidence in the integrity and authenticity of the transactions.¹¹⁰ Even

107. CHAIWAT WONGWATTANASART, LAW OF CONSUMER PROTECTION 29 (2000).

108. Arruda & Shestakova, *supra* note 71.

109. PERRITT, *supra* note 10, at 588.

110. CHAIWAT WONGWATANASAN ET AL., EXPLANATION OF THE ELECTRONIC TRANSACTIONS ACT, B.E. 2544 136 (2002). The Singapore Evidence Act (Chapter 97) § 35 provides that "where computer output is tendered in evidence for any purpose whatsoever, such output shall be admissible if it is relevant or otherwise admissible according to... any other written law, and it is... produced in an approved process..." The law also provides presumptions of accuracy and reliability by

though the E-Transactions Act does not address this issue specifically, the concept of signature verification may be applied in order to provide proof of signing electronic documents.

IV. ONLINE ALTERNATIVE DISPUTE RESOLUTION

To encourage consumers to conduct online transactions, one strategy is to make them feel confident that if there is any dispute, they will have access to a resolution mechanism.¹¹¹ Online disputes are defined as any dispute that arises in the course of electronic commerce, including disagreements over the rights of domain names, qualities of goods traded through the Internet¹¹², unauthorized orders, and mistaken identity. If disputes arise from online consumer transactions conducted between online merchants and consumers, there should be alternative means of out-of-court dispute settlements, because filing legal actions can be complicated, costly and time-consuming. It is imperative that the government initiates primary remedies in the form of effective out-of-court systems for dispute settlement¹¹³ in order to prevent otherwise resolvable issues from unnecessarily taking up court system time.

Alternative dispute resolution (ADR) refers to approaches for determining and settling disputes that do not involve the traditional judicial system. Possibilities include negotiation, mediation and arbitration.¹¹⁴ Mediation is a dispute mechanism where neutral mediators are appointed.¹¹⁵ This is effective in some cases because the appointed mediator will assist and encourage the parties in reaching a mutually satisfactory settlement.¹¹⁶ Mediators play vital roles in providing advice

specifying that "output certified by a designated authority as produced in accordance with an approved process will be presumed to be accurate and reliable."

111. Federal Trade Commission, *Summary of Public Workshop: Alternative Dispute Resolution for Consumer Transactions in the Borderless Online Marketplace*, at 1, available at <http://www.ftc.gov/bcp/altdisresolution/summary.htm> (June 6-7, 2000).

112. ROGER LEROY MILLER & GAYLORD A. JENTZ, *MANAGEMENT AND E-COMMERCE: THE ONLINE LEGAL ENVIRONMENT* 60 (2001).

113. IAN LLOYD, *LEGAL ASPECTS OF THE INFORMATION SOCIETY* 279 (2000). According to Electronic Commerce Directive, Article 17 provides that "member states shall ensure that, in the event of disagreement between an Information Society service provider and the recipient of the service, their legislation does not hamper the use of out-of-court schemes, available under national law, for dispute settlement, including appropriate electronic means."

114. MILLER & JENTZ, *supra* note 112, at 50.

115. RAY AUGUST, *INTERNATIONAL BUSINESS LAW: TEXT, CASES, AND READINGS* 93 (1993). Mediation involves the use of a third party who transmits and interprets the proposals of the principal parties. When mediators provide a channel of communication only, they are offering their "good offices."

116. DAVID I. BAINBRIDGE, *INTRODUCTION TO COMPUTER LAW* 187 (4th ed. 1999). *See also* 13th Annual Fulbright Symposium on International Legal Problems, Milena Petrovic: Mediation and Conciliation, Golden Gate University (2003). Benefits of mediation are: fast settlement; safe environment for negotiation; flexibility and informality; privacy and confidentiality.

and clarifying issues in order for the parties to achieve plausible and fair compromises.¹¹⁷

The mediation process is based on mutual consent, which may be withdrawn or abandoned at any time.¹¹⁸ Even though the mediation process itself does not legally bind the parties, it is considered to be a highly successful means of settling disputes, with an estimated settlement rate of 90 per cent.¹¹⁹

Government and private sectors have to cooperate in developing fair and effective alternative dispute resolutions for online consumer transactions in order to encourage online parties to attempt some forms of dispute settlement mechanisms prior to trial. Dispute mechanism alternatives must be disclosed to online consumers in order for them to know where and how to file their claims. Establishing alternative dispute resolution possibilities, nevertheless, does not prevent consumers from pursuing legal remedies.¹²⁰

Due to online environment characteristics, traditional alternative dispute mechanisms may not be appropriate for settling all online disputes. Innovative online dispute mechanisms have been created. Unlike traditional court proceedings, online alternative dispute resolution provides better solutions for parties located in different or distant jurisdictions.¹²¹ Taking part in online alternative dispute resolution can be simple, quicker, less complicated and less expensive than lawsuits in a court of law.¹²² The government and private sector should develop various types of online dispute resolution in order to facilitate a variety of possibilities for online dispute resolution, such as online mediation and online arbitration.

Online Mediators, eResolution, and Square Trade are examples of online alternative dispute resolution providers developing online complaint forms and providing online mediator to reconcile disputes between

117. MILLER & JENTZ, *supra* note 112, at 52.

118. BAINBRIDGE, *supra* note 116. *See also* AUGUST, *supra* note 115. All parties to a dispute must consent to mediation.

119. *Id.* at 187.

120. According to 15 U.S.C § 2310(a)(3) (1982) (Magnuson Moss Act), if a warrantor establishes an informal dispute settlement procedures, that procedure must be used by the consumer prior to commencing any legal remedy and the consumer may not bring a law suit unless it initially resorts to the informal procedure.

121. Federal Trade Commission, *supra* note 111, at 2.

122. *Id.*

parties.¹²³ Others, such as *CyberSettle*, *ClicknSettle*, *CyberSolve*, and *Settlement Now* have developed systems for negotiating and settling monetary disputes.¹²⁴ *Online Disputes.org* provides settlement dispute services based on automated rules. *Icourthouse*, an online jury trial system, allows parties to choose a jury to try their case in an entirely virtual courtroom.¹²⁵

The issue of substantive rules to be used in deciding online disputes is still controversial, but online alternative dispute mechanisms are helping to identify and develop rules that may eventually serve as codes of conduct for parties conducting online business battling over jurisdiction issues.¹²⁶ Online alternative dispute resolution providers may apply different rules in resolving the disputes as long as they are fair and effective.¹²⁷ These rules may include the development of a system of precedents.¹²⁸ For example, in the domain name dispute context, online alternative dispute resolution providers have decided over 400 cases, and new cases are now often based on precedent.¹²⁹ Thus, the determination of disputes regarding the use of digital signatures in terms of consumer protection could also rely on a system of precedent.

Online alternative dispute resolution means handling online disputes in a cost-effective manner because complaints can be filed by e-mail.¹³⁰ Online alternative dispute resolution also assures consumers that companies are who they say they are.¹³¹ These online alternative dispute mechanisms may be appropriate for resolving small-to-medium sized liability claims¹³² since filing civil actions may not be cost-effective

123. *Id.* See also, *Mediation: How the Online Mediation Process Works*, at <http://www.onlinerresolution.com/om-how.cfm> (last visited Mar. 25, 2003).

124. MILLER & JENTZ, *supra* note 112, at 69.

125. Federal Trade Commission, *supra* note 111, at 5.

126. MILLER & JENTZ, *supra* note 112, at 61.

127. See *Mediation: How the Online Mediation Process Works*, at <http://www.onlinerresolution.com/om-how.cfm> (last visited Mar. 25, 2003). There are the standards of mediation practice jointly defined by the American Bar Association (ABA), Society of Professionals in Dispute Resolution (SPIDR) and the American Arbitration Association (AAA) and are generally applicable to the mediation of legal disputes. See also *Model Standards of Practice for Mediators*, at <http://www.mediate.com/articles/spidrstds.cfm> (Aug. 1998). The standards of mediation practice recognize the principle of "self-determination." A mediator shall recognize that mediation is based on the principle of self-determination by the parties, therefore the parties may mutually agree to specify a particular law to be applied by the mediator.

128. *Id.*

129. Federal Trade Commission, *supra* note 111, at 4.

130. *Id.* at 5.

131. *Id.*

132. MILLER & JENTZ, *supra* note 112, at 69.

solutions. Application of online alternative dispute resolution lessens the tension level between the parties.¹³³

Apportionment of costs for settling online disputes should depend on which party filing an online complaint had the position of bargaining power.¹³⁴ Fees for addressing business-to-consumer disputes should be minimal in order to encourage consumers to seek these remedies since traditional court system is more costly. For disputes involving business-to-business transactions, both parties should bear the cost equally. For instance, *Online Disputes.org* and *Online Mediators* have provided dispute settlement services to consumers for free, but charge a set fee for businesses.¹³⁵ Online dispute resolution seems to be more practical in settling disputes on the Internet because everything can be done electronically, services are available around the clock, and fees are lower or nominal.¹³⁶ Online dispute resolution has not yet been widely accepted.¹³⁷ Satisfaction depends on the cooperation of both parties and there is no way to enforce it if one party refuses to comply with the settlement agreement.¹³⁸

Another way of resolving online disputes includes credit card charge backs, escrow arrangements, complaint bulletin boards¹³⁹ and special governmental online consumer protection agencies. The credit card charge back system seems to be highly practical¹⁴⁰ and the most attractive means for dispute settlement between online purchasers and merchants. Since most online transactions are paid by credit cards, the credit card charge back scheme is the best solution to resolve consumer's dispute when online merchants have charged consumers, but failed to deliver the ordered product or perform their obligations.

In the United States, a credit card charge back mechanism is one form of alternative dispute resolution that works efficiently for online consumers. Credit card issuers are required to conduct investigations when cardholders file claims of billing errors, according to the Fair Credit Billing Act.¹⁴¹ Disputes in billing statements include non-acceptance of goods or services in compliance with the agreement consummated at the

133. Federal Trade Commission, *supra* note 111, at 5.

134. *Id.* at 6.

135. *Id.*

136. MILLER & JENTZ, *supra* note 112, at 73.

137. *Id.* at 73.

138. *Id.*

139. PERRITT, *supra* note 10, at 826.

140. *Id.*

141. *Id.*

time of a transaction.¹⁴² This protection is provided only for consumers, not businesses.

In the event of non-acceptance or non-delivery, the Fair Credit Billing Act also requires card issuers to determine whether such goods or services were actually mailed and delivered.¹⁴³ The consumer needs to be alert when receiving monthly credit card statements. If they find any suspicious transactions, they must contact the card issuers and protest the charges either by phones or letters, and there is a limit on how long they can wait before they are prevented from doing so. This form of dispute resolution is provided without cost so that the merchant and the consumer can reach a compromise. This mechanism provides dual advantages. First, it provides a primary remedy for online consumers. Secondly, dishonest online merchants will be excluded from the credit card network.¹⁴⁴

In Thailand, credit card charge back measures are based on the Consumer Protection Law. The Consumer Protection Act, B.E. 2522 (1979) came into force on 4th May 1979¹⁴⁵ and was amended in 1998 by adding provisions on the establishment of the Consumer Protection Board, consisting of the Prime Minister as Chairman.¹⁴⁶ The Board is vested with powers to consider complaints from consumers who suffer hardship or injury resulting from the conduct of businesses.¹⁴⁷ It has a duty to disseminate information to public and educate consumers about necessary consumer protection measures.

The Committee, which is subject to the Thai Consumer Protection Act of 1979, and is appointed by the Board, may review contractual terms set forth in sales or service contracts where the law or custom requires evidence in writing.¹⁴⁸ The Committee is empowered to declare that such businesses be regulated in areas of contractual matters.¹⁴⁹ All terms stipulated in contracts provided by these controlled business are subject to change or modification. The Committee may order businesses to

142. *Id.*

143. 12 C.F.R. § 226.13 (e) (1977).

144. PERRITT, *supra* note 10, at 828.

145. The Consumer Protection Act 1979 of Thailand, at <http://www.ciroap.org/apcl/countries/thailand.overview.html>.

146. *Id.*

147. *Id.*

148. The Consumer Protection Act 1979 of Thailand, *supra* note 145 at § 35 bis. provides that "In any business in connection with the sale of any goods or the provision of services if contract of sale or such contract service required by law or the custom to be made in writing, the committee on Contract shall have the power to provide such business to be a controlled business with respect to contract."

149. The Consumer Protection Act 1979 of Thailand, *supra* note 145.

incorporate terms that are necessary for consumer protection and exclude any unreasonably disadvantageous terms to the consumers.¹⁵⁰ The Consumer Protection Act defines consumers as buyers or persons obtaining services from businesses or who are offered or invited by business to buy a product or obtain services, including any lawful product users or service users with or without consideration.¹⁵¹ The concept of consumer protection is granted to only private consumers, not for members of the business sector.

In Thailand, there are no specific laws regulating the use of credit cards as in the United States. The Committee has declared that credit card businesses whose terms of contractual agreement are regulated. According to the Royal Decree Promulgating the Protection of Consumer via Contracts B.E. 2542 (1999), credit card issuers are obligated to provide prior notice in writing to their consumers if there is any change in any term of credit card agreements, including interest rates, late fees, fees, other service charges.¹⁵² The proclamation also requires credit card issuers to include that in the event of an unauthorized use of credit card, liability for unauthorized transactions will be immediately suspended pending resolution. If the consumers have paid for those transactions, the credit card issuers have to credit the funds back to the cardholders immediately, unless the issuers can prove that those transactions were in fact made by the cardholders.

The current credit card charge back mechanism in Thailand is not as strong as in the United States because there are no specific laws which impose a duty upon card issuers to conduct investigations as the United States Fair Credit Billing Act does. It is thus necessary for the Thai government to provide the credit card charge back mechanism in order to protect online consumers by imposing a duty upon card issuers to conduct investigations in the event of non-acceptance or non-delivery. Protection of consumers by controlling credit card agreements may provide them a better level of protection since they will at least have some protection. In online disputes between online merchants and consumers, the consumers will be able to report such unauthorized transactions to the credit card issuers who, according to the credit card agreements, are not entitled to demand the consumers pay those reported unauthorized transactions. Credit card issuers have to credit the charges back to the cardholders' accounts right away. This measure provides a primary remedy for online

150. The Consumer Protection Act 1979 of Thailand, *supra* note 145 at § 35 ter.

151. The Consumer Protection Act 1979 of Thailand, *supra* note 145 at § 4.

152. ARTRUKSA, *supra* note 93, at 68.

consumers and they will not need to use other legal remedies unless the disputes have become more complicated.

Since sanctions and penalties for non-conformance with such proclamations are not strong or severe enough, businesses may simply choose to ignore Royal Decrees. The Thai Consumer Protection Act, §57 provides that the business that has failed to incorporate such required terms in the credit card agreement may be fined up to 100,000 Baht, or imprisoned up to one year, or both. The penalty for failure to comply with this proclamation has to be much stronger, perhaps by doubling the amount of fines. Sanctions other than imprisonment should be imposed. For instance, business licenses could be suspended, or other means of injunctive protection may be used to force businesses to strictly comply with the proclamations and follow consumer protection policies. With strong sanctions, consumers will be adequately protected in the online environment.

Another mechanism for resolving an online dispute regarding the reliability of electronic signatures, including digital signatures, is to establish an autonomous agency that performs a function of determining whether an electronic signature satisfies the requirements of reliability imposed in section 26 of the Thai E-Transactions Act. A Royal Decree may provide that a particular State agency is competent to determine the reliability of electronic signatures.¹⁵³ It is extremely useful to have this agency perform a primary investigation and determination of the reliability features of electronic signatures when the parties are in dispute on the reliability of electronic signatures. They may be able to settle the dispute before bringing a claim to a court of law if the agency is of the opinion that such signed electronic signatures are not trustworthy and unreliable. The party intending to enforce the signed agreement may withdraw his or her claim. This will lessen the number of cases to be adjudicated by means of judicial system in which the legal processes are sophisticated and time-consuming.

On the contrary, if the agency is of the opinion that a signed electronic signature is trustworthy and reliable, the party against whom the enforcement is sought may comply with the agreement and settle the dispute with enforcing party. If a settlement could not be reached, the enforcing party may institute an action before the courts. To adjudicate the case, courts may summon a competent officer who determined the

153. Uncitral Model Law on Electronic Signatures art. 7 (2001) provides that any person, organ or authority, whether public or private, specified by the enacting State as competent, may determine which electronic signatures satisfy the provisions of article 6 of this Law.

trustworthiness and reliability of the electronic signature to testify on behalf of the agency before the court. Any party in legal proceedings may adduce a statement of determination issued by the agency to support his or her claim. The courts may adjudicate the case regarding the trustworthiness of the signed electronic signature appeared in the electronic document by relying upon the opinion of the agency because such agency does not have any interest in the dispute or, in the case where the courts think fit, the courts may also summon a computer expertise to testify against the opinion of the agency.

Establishing this agency provides several benefits to both online parties and courts. A small claim may be settled before being brought to a court of law. Online parties, in addition, can be assured that in the case of disagreement as to the reliability of electronic signatures, the issue can be primarily investigated and determined by a competent and trustworthy State agency.

V. CONCLUSION

The Internet technology has provided substantial benefits for both online merchants and consumers, but the development of online commerce depends on security and trust. Without proper security mechanisms, the commission of fraud is a possibility. The use of digital signatures is not mandatory, but it is an option. The online businesses may ensure consumer confidence in transaction security by the use of digital signatures. The author is of the opinion that additional mechanisms for the protection of consumers should be provided. The author, thus, suggests various mechanisms for the protection of consumers to be later enacted in a Royal Decree. These mechanisms are as follows: caps on consumer liability, consumer consent, paper back up, right of access to readable and non-repudiable documents, disclosure, burden of proof, self-education, minimum standard of privacy, accreditation system, and unfair terms. The author, eventually, recommends the use of electronic notarization, credit card charge back measures, and the establishment of an autonomous agency for the determination of reliability of electronic signatures.

