January 6, 2006 . Workshop 9:00am-2:00pm

Present: Lee Alley (SCS), Steve Zink (UNR), Steve Zideck (TMCC), Jeff Cox (GBC), Lori Temple (UNLV), Brian Chongtai (NSC), Sally Phares (SCS). Absent: Lyle Pritchett (DRI), Don Moxley (WNCC)

Presenters: Ed Anderson, Jana Dunn, Annie Macias, Annie McDonald

1. Draft Security Recommendations

Ed Anderson and Jana Dunn presented materials prepared by the Connectivity Ad Hoc group with proposals on how to formalize this process.

Decision: Each CTO will send the name of a representative for Security recommendations to Ed Anderson. The CTO will make the final endorsement.

Click [here] to see attached documents.

2. RIAA-Survey Summary

Decision: Each institution will review the summary and send changes/ additions to Sally Phares by January 31, 2006. Each institution is at liberty to distribute only their campus' information.

Click [here] to see attached documents.

3. AUP

Discussion: Conversation about distinction between monitoring vs. examining "content of files". The main area that could require addressing involves using security software tools. This item will continue to be discussed.

4. Digital Signatures

A presentation of background material regarding the federal act, the State of Nevada statute, other institutions using this technology and vendor information was made by Annie Macias.

Decision: Sally Phares and staff will prepare an RFI , circulate it for review before the next meeting. The RFI will be on the next agenda for final decision.

Click [here] to see attached documents.

5. Organizational Changes

Lee shared with the group how SCS is approaching inventorying the various areas for discussion/resolution with Mark Bordwine, the new CCSN CIO. He suggested the other institutions may want to use a similar approach. Sally will send the template SCS is using.

Lee also shared some ideas on approaching changes at SCS including the role the Data Administrator will play.

Thank you Lori Temple for the Tour of UNLV's NOC.

6. 1/10/06 Council of Presidents Meeting

This was a discussion of how they expect the meeting to go and who will present the funding model. Steve Zink provided some insight as to how the model was developed and how it's likely to be received.

7. iNtegrate Project Update

Lee asked Annie McDonald to go over the timeline for the January and February activities:

* Response opening process
* Worksheets
* Reference lists
* Site visits
* Evaluation of bids
* Nevada Student Association presentations
* Bid clarification teleconference
    - Vendor/subject matter expert meeting

The question was asked about the data clean-up process. Lee described his expectations for this activity.

Lori Temple shared how her campus has organized for this project. The group is addressing data administration issues, has conducted a server survey and supplemental systems survey and is working on the issues related to records retention. Lori will provide a description to share with everyone else.

Steve Zideck reported that TMCC has recently started a similar group.

8. Core Data Survey

Lori brought up the new area in the survey that requires assistance from SCS. She brought the pages with her highlighting the specific areas. Lee asked that all institutions participate in the survey. He assured Lori that Glenda Krietlow will provide the needed information.

9. Preview of IT Budget Requests 07-09

Discussion of how the budget requests are presented and the timing of the various stages of the budget process.

10. Other

Discussion of the face to face meeting led to setting new dates, times and places for future meetings as follows:

* February 15, 2006 – via video
* March 15, 2006 – via video
* April 14, 2006 – group
* May 17, 2006 – via video
* June 21, 2006 – via video
* July 7, 2006 – group in Elko
* August 16, 2006 – via video
* September 20, 2006 – via video
* October 13, 2006 – group in Reno
* November 15, 2006 – via video
* December 20, 2006 – via video

Access and Authentication Guidelines
For Information Resources
NSHE Security Interest Group

Scope
These guidelines are a series of recommended general best practices pertaining to network and resource access, authentication, and logging.

We encourage campuses to survey their information and infrastructure assets. A thorough understanding of the degree of sensitivity of data or resources can guide the selection of appropriate security controls to protect those assets. More critical resources require more extensive protection; simpler scenarios may be acceptable for less critical resources. For example, a multilevel authentication scheme with detailed logging may be a good choice for protecting certain financial or medical information, but a very simple, easy-to-use authentication method may be acceptable for a student lab.

End-User Passwords and Account Security

1. Authorized users are responsible for the security of their accounts and passwords. Account credentials may not be shared with anyone, including family members and trusted associates. Account holders should keep passwords secure; users should not write down passwords, should not e-mail passwords, and should not store passwords in a means readily accessible by other users. Account holders may be held liable for any inappropriate activity tied to their accounts, such as copyright violations or other illegal activity, exposure of confidential or proprietary information, or harassment of other users.
2. Because information contained on portable devices is especially vulnerable, special care should be exercised; this could include the use of passwords and the encryption of data.

Guidelines for Device/System Configuration and System Administration

1. System-level passwords and passwords for privileged access should be changed on a regular basis; where practical, systems should be configured to enforce expiration periods for passwords.
2. When possible, software should be configured to enforce passwords of reasonable complexity and an appropriate minimum length, while maintaining a realistic ease of use.
3. Account sharing is discouraged. Where shared accounts are necessary for technical or logistical reasons, passwords should be changed regularly. Resource access for the shared account should be limited to strictly what is necessary. For example, a shared account password should be changed when a user who knows the password no longer requires access.
4. Student computing labs should require authentication in order to manage access to copyrighted materials, licensed software, and for potential legal reasons, e.g. minors participating in a campus program.

Review and Removal of Accounts and Related Access
When possible, account creation, deactivation, and removal should be automated and synchronized with information from enrollment and/or employment systems.

Institutions should generate documented procedures for the creation, removal, activation or deactivation, and any other processes involved with accounts.

Authentication Logs
Logging levels should be commensurate with the sensitivity of the resource to be accessed. For most resources and systems, this entails logging both successful and unsuccessful authentication attempts. Where DHCP is used, logging should allow the association of an IP assignment with the corresponding user. Campuses should create log review and retention procedures. Member institutions should be aware of the laws and policies that may affect their own campuses, departments, and programs (i.e., HIPAA, Sarbanes-Oxley, etc.).

Remote Access and Authentication
Remote (off-campus) access to resources should be formalized and managed per campus or institution. Access should be restricted to secured protocols (i.e., those that encrypt their traffic--SSH, POP3 secure, IMAP secure, etc.). Where authentication credentials must pass over possibly-insecure network segments, we recommend the use of highly secure protocols, such as NTLM v2, Kerberos, or LDAP over SSL. Where practical, legacy or unencrypted authentication protocols should be disabled on both clients and servers.

Guest Accounts and Temporary Access
When campus guests require network or system access, their needs should be met with temporary guest accounts with limited resource access. Account activity should be regulated, and these guest accounts should be managed according to established procedures. Institutions must be aware of licensing implications of guest accounts with respect to systems, devices, software, and information services.

Centralized Authentication
Campuses are encouraged to develop centralized authentication systems. When appropriately planned and implemented, centralized systems can provide better services to users, reduce support costs, and improve security. Systems administrators, software developers, and data stewards should make use of centralized authentication system where it is possible and prudent to do so.

Recommendations for a centralized authentication system include secure data transmission, cross-platform compatibility, and the use of standards (i.e., LDAP, Kerberos, etc.). Automation is highly recommended in order to create, expire, and delete accounts. The system should also provide the ability to manually create accounts for the exceptions, and incorporate tools for managing the exceptions.

Review and Approval

Revision History

Institutional Policies and Practices Addressing Digital Management Survey
Summary-**DRAFT** for Review

Question	Joint Comm. Institutional Recommendation	CCSN	GBC	DRI	NSC
1. Most important measures being taken at your institution to educate the campus community about the illegality of file sharing (peer-to-peer) related to copyright infringement	Required Policy signature, required online quiz, poster campaigns, paid ads in school newspaper, email messages, informational brochure to all students, video clips, student government forum, orientation week presentation, guest speaker in academic courses	Has not taken measures to educate the campus community about the legal issues associated with file sharing in relation to copyright infringement		Not Surveyed	Website, campus-wide e-mails, one-on-one basis if we find a user who may be participating in illegal file sharing
2. What network management technologies and related procedures your institution uses to address possible copyright infringement?	Bandwidth shaping, firewalls restricting file transfers, network management tools	Uses packet shaping on academic network	network appliance software	Not Surveyed	Student workstations utilize security software that will erase any changes made to the machines after a reboot
3. Most important policies your institution has in place to address computer use as it relates to digital rights management and potential copyright infringement?	Acceptable use policy, specific copyright policy, references for more information, description of how abusers would be caught	Do not have a companion policy to NSHE Computer Resource Policy		Not Surveyed	System Computer Usage Policy; NSC Fair Use Guidelines
4. What types of mechanisms do you rely on most for enforcing the policies above?	Make penalty structure known, shut down offender access, use other disciplinary processes in place	Lab managers announcements in Computer Labs; Disabling violators' account		Not Surveyed	IT staff scans the public network shared areas, cleans, notifies
5. Do you provide *or recommend* any major alternate options to the campus community that support legal file sharing?		No		Not Surveyed	Shared network drive space that is accessible to all NSC enrolled students
6. What avenues for disseminating information on institutional policies and practices on copyrights does your institution rely on most?	Multiple means of conveyence, web site, email, student newspaper, flyers	Institutional website	everytime a person turns on the computer, the policy is displayed on the screen for the user to agree to	Not Surveyed	Website and internal e-mails
7. Are there other ways in which your institution has addressed possible digital copyright infringements such as illegal music downloads?		No		Not Surveyed	

Institutional Policies and Practices Addressing Digital Management Survey
Summary-**DRAFT** for Review

Question	Joint Comm. Institutional Recommendation	TMCC	UNLV	UNR	WNCC
1. Most important measures being taken at your institution to educate the campus community about the illegality of file sharing (peer-to-peer) related to copyright infringement	Required Policy signature, required online quiz, poster campaigns, paid ads in school newspaper, email messages, informational brochure to all students, video clips, student government forum, orientation week presentation, guest speaker in academic courses	Website, discussions in committees when college looks at the academic software requests and when the college puts together the academic computer lab software image	ResNet policy; UNLV copyright policy; UNLV Campus Housing Network and Computer Lab Use Policies; "Think before you Click" campaign	No Response	Presented in the college policies via the college website
2. What network management technologies and related procedures your institution uses to address possible copyright infringement?	Bandwidth shaping, firewalls restricting file transfers, network management tools	Blocks P2P only. In addition faculty and staff do not have admin rights on their TMCC owned computers	NOC monitors network traffic patterns; no traffic shaping; no port blocking at this time	No Response	P2P is blocked at the workstation level; ability to change setting taken away from the student and faculty/staff user; network level firewalls installed
3. Most important policies your institution has in place to address computer use as it relates to digital rights management and potential copyright infringement?	Acceptable use policy, specific copyright policy, references for more information, description of how abusers would be caught	TMCC Copyright Infringement Procedures	General policy on Copyright; Student Computer Use policy; faculty/staff Acceptable Use policy in draft ready for campus process	No Response	Computing and Network Use Agreement
4. What types of mechanisms do you rely on most for enforcing the policies above?	Make penalty structure known, shut down offender access, use other disciplinary processes in place	Constant network scanning to track violations	NOC monitors “top talkers”; notifies ResNet staff or computer lab staff; disables network port temporarily	No Response	Workstation imaging and firewall policies
5. Do you provide *or recommend* any major alternate options to the campus community that support legal file sharing?		No	No	No Response	None
6. What avenues for disseminating information on institutional policies and practices on copyrights does your institution rely on most?	Multiple means of conveyence, web site, email, student newspaper, flyers	TMCC Website	Web sites; required residence hall policy sign-off; computer lab posters; "Think Before You Click" campaign	No Response	Website
7. Are there other ways in which your institution has addressed possible digital copyright infringements such as illegal music downloads?		No		No Response	Typically we have responded to warnings passed on to us from SCS

	DEFINITIONS	EXAMPLE
Electronic Signature	ESIGN 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." Thus, an "electronic signature" can come in many forms, including PIN numbers, passwords, or even clicking an icon.	"I accept" button Digitized version of handwritten signature Anything that can be construed as 'intent to sign'
Digital Signature (one type of Electronic Signature)	An electronic identifier created by computer, intended by the party to be the same as manual signature. It is one type of electronic signature if "intent to sign is present".	Data field on database that says "I accept" button was pushed
Federal Acts	Electronic Signatures in Global and National Commerce Act (S.761) (E-SIGN) Uniform Electronic Transaction Act (UETA)	
Nevada Revised Statutes	NRS 719 Electronic Transactions (Uniform Act) NRS 720 Digital Signatures NAC 720 Digital Signatures	
	Dean Heller Nevada Secretary of State Nevada Digital Signature Project Notary Division 102 North Carson Street, Suite 3 Carson City, NV. 89701-3714 **Phone:** 775-684-5708 **Email:** nvnotary@sos.nv.gov	

Frequently Asked Questions

What does ESIGN do?	Some courts have ruled that electronic signatures are valid, and several states have passed laws validating electronic signatures. These rulings and statutes differed in their requirements and application, resulting in continued uncertainty regarding the validity of electronic contracts. ESIGN addresses this problem. ESIGN provides a uniform federal law that validates electronic signatures, effectively allowing parties to enter into a contract on the Internet without wondering which state law applies. ESIGN also allows businesses to keep electronic records, and to send electronic records and documents to consumers. ESIGN does contain exceptions that prevent the use of electronic signatures and records in some areas, including the use of official court documents, notice of cancellation of utility services, health insurance or life insurance, and recalling products.
What does ESIGN say about business-to-consumer transactions?	ESIGN provides that specific disclosures must be made to consumers: Consumers must be provided with "clear and conspicuous" statements regarding certain procedures involved with using electronic data. Consumers must affirmatively consent to the use of electronic signatures or records. The consumer must be supplied with information regarding the hardware and software used in the process, and the consumer must consent in a way that demonstrates that they have access to the information in the electronic form that will be used. Businesses are not required to use any specific type of technology to verify the electronic signature or the consent.
-What effect does ESIGN have on state “electronic signature” laws?	Before ESIGN, several states had their own electronic signature laws. These laws varied greatly from state to state, causing confusion when parties from different states were involved in business transactions. ESIGN effectively preempts state laws on electronic signatures, ensuring that states are under a uniform law and that parties have certainty when dealing within different jurisdictions. ESIGN does not, however, completely preempt state electronic signature laws. States may modify, limit, or supersede ESIGN if they are consistent with the Uniform Electronic Transactions Act, which was approved by the National Conference of Commissioners on Uniform State Laws.
What are the advantages of ESIGN?	ESIGN has paved the way for businesses and consumers to do business online. The bill provides enough flexibility to allow technology to change and still be in step with the law. ESIGN also creates a more predictable e-commerce market because it relieves parties of choice of law dilemmas that were once prevalent with the advent of various state laws. The law also provides certainty that contracts formed over the Internet will be valid and enforceable, an issue that

What are the advantages of ESIGN? (cont.)	was once unclear. ESIGN has also been touted as a way for businesses to save an enormous amount of money and time. The cost of paper correspondence and storage may be reduced. Businesses will no longer have to use the mail to send documents, a process that costs businesses time and money. ESIGN is largely symbolic because electronic signatures have been used by many businesses in the past. The symbolic nature of ESIGN is important, however, because the bill will create greater confidence in businesses and consumers when doing transactions online.
What are the disadvantages of ESIGN?	ESIGN signifies the beginning of a new frontier in business. New frontiers invariably involve some uncertainty and unanswered questions. For example, the definition of "electronic signature" will most likely be an issue in the future. The status of electronic signatures in business-to-business transactions is also left in the hands of businesses. The need for protection of consumers may force businesses to invest in expensive technology that will ensure that the party signing the contract is authorized. The cost and sophistication of this technology is still indefinite for businesses and consumers. Technology such as thumbscanners and eye sensors are viable options for big companies, but small to medium size businesses may not be able to afford such amenities.
What are the FERPA electronic signature regulations?	"Signed and written consent to release student record information" may include a record and signature in electronic form. It must: - identify and authenticate a person as the source of the consent and – indicate the person's approval. Does not require institutions to ask the student for consent to do the transaction electronically.
What are the rules for Federal Student Aid?	Issued by the Department of Education in 2001. Creates standards for electronic signatures in student loan transactions: - Do not permit administrator's access to PIN. - Allow students to change PIN -PINs and passwords should be kept in a secure database -PINs and passwords should be encrypted when stored. Created a FAFSA-PIN service (Free Application for Federal Student Aid)

UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

Drafted by the

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

and by it

APPROVED AND RECOMMENDED FOR ENACTMENT

IN ALL THE STATES

at its

ANNUAL CONFERENCE

MEETING IN ITS ONE-HUNDRED-AND-EIGHTH YEAR

IN DENVER, COLORADO

JULY 23 - 30, 1999

WITH PREFATORY NOTE AND COMMENTS

By

NATIONAL CONFERENCE OF COMMISSIONERS

ON UNIFORM STATE LAWS

1/20/00

UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

The Committee that acted for the National Conference of Commissioners on Uniform State Laws in preparing the Uniform Electronic Transactions Act (1999) was as follows:

PATRICIA BRUMFIELD FRY, University of North Dakota, School of Law, P.O. Box 9003,

Grand Forks, ND 58201, *Chair*

STEPHEN Y. CHOW, 30th Floor, One Beacon St., Boston, MA 02108

KENNETH W. ELLIOTT, City Place Building, 22nd Floor, 204 N. Robinson Avenue,

Oklahoma City, OK 73102

HENRY DEEB GABRIEL, JR., Loyola University, School of Law, 526 Pine Street, New Orleans,

LA 70118

BION M. GREGORY, Office of Legislative Counsel, State Capitol, Suite 3021, Sacramento,

CA 95814-4996

JOSEPH P. MAZUREK, Office of the Attorney General, P.O. Box 201401, 215 N. Sanders,

Helena, MT 59620

PAMELA MEADE SARGENT, P.O. Box 846, Abingdon, VA 24212

D. BENJAMIN BEARD, University of Idaho, College of Law, 6th and Rayburn, Moscow,

ID 83844-2321, *Reporter*

EX OFFICIO

GENE N. LEBRUN, P.O. Box 8250, 9th Floor, 909 St. Joseph Street, Rapid City, SD 57709,

President

HENRY M. KITTLESON, P.O. Box 32092, 92 Lake Wire Drive, Lakeland, FL 33802,

Division Chair

AMERICAN BAR ASSOCIATION ADVISORS

C. ROBERT BEATTIE, Plaza VII, 45 S. 7th Street, Suite 3400, Minneapolis, MN 55402-1609,

Business Law Section

AMELIA H. BOSS, Tmple University, School of Law, 1719 N. Broad Street, Philadelphia,

PA 19122, *Advisor*

THOMAS J. SMEDINGHOFF, 130 E. Randolph Drive, Suite 3500, Chicago, IL 60601,

Science and Technology Section

EXECUTIVE DIRECTOR

FRED H. MILLER, University of Oklahoma, College of Law, 300 Timberdell Road, Norman,

OK 73019, *Executive Director*

WILLIAM J. PIERCE, 1505 Roxbury Road, Ann Arbor, MI 48104, *Executive Director Emeritus*

Copies of this Act may be obtained from:

NATIONAL CONFERENCE OF COMMISSIONERS
ON UNIFORM STATE LAWS
211 E. Ontario Street, Suite 1300
Chicago, Illinois 60611
312/915-0195

UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

TABLE OF CONTENTS

UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

PREFATORY NOTE

With the advent of electronic means of communication and information transfer, business models and methods for doing business have evolved to take advantage of the speed, efficiencies, and cost benefits of electronic technologies. These developments have occurred in the face of existing legal barriers to the legal efficacy of records and documents which exist solely in electronic media. Whether the legal requirement that information or an agreement or contract must be contained or set forth in a pen and paper writing derives from a statute of frauds affecting the enforceability of an agreement, or from a record retention statute that calls for keeping the paper record of a transaction, such legal requirements raise real barriers to the effective use of electronic media.

One striking example of electronic barriers involves so called check retention statutes in every State. A study conducted by the Federal Reserve Bank of Boston identified more than 2500 different state laws which require the retention of canceled checks by the issuers of those checks. These requirements not only impose burdens on the issuers, but also effectively restrain the ability of banks handling the checks to automate the process. Although check truncation is validated under the Uniform Commercial Code, if the bank's customer must store the canceled paper check, the bank will not be able to deal with the item through electronic transmission of the information. By establishing the equivalence of an electronic record of the information, the Uniform Electronic Transactions Act (UETA) removes these barriers without affecting the underlying legal rules and requirements.

It is important to understand that the purpose of the UETA is to remove barriers to electronic commerce by validating and effectuating electronic records and signatures. It is NOT a general contracting statute - the substantive rules of contracts remain unaffected by UETA. Nor is it a digital signature statute. To the extent that a State has a Digital Signature Law, the UETA is designed to support and compliment that statute.

A. Scope of the Act and Procedural Approach. The scope of this Act provides coverage which sets forth a clear framework for covered transactions, and also avoids unwarranted surprises for unsophisticated parties dealing in this relatively new media.

The clarity and certainty of the scope of the Act have been obtained while still providing a solid legal framework that allows for the continued development of innovative technology to facilitate electronic transactions.

With regard to the general scope of the Act, the Act's coverage is inherently limited by the definition of "transaction." The Act does not apply to *all* writings and signatures, but only to electronic records and signatures relating to a transaction, defined as those interactions between people relating to business, commercial and governmental affairs. In general, there are few writing or signature requirements imposed by law on many of the "standard" transactions that had been considered for exclusion. A good example relates to trusts, where the general rule on creation of a trust imposes no formal writing requirement. Further, the writing requirements in other contexts derived from governmental filing issues. For example, real estate transactions were considered potentially troublesome because of the need to file a deed or other instrument for protection against third parties. Since the efficacy of a real estate purchase contract, or even a deed, between the parties is not affected by any sort of filing, the question was raised why these transactions should not be validated by this Act if done via an electronic medium. No sound reason was found. Filing requirements fall within Sections 17-19 on governmental records. An exclusion of all real estate transactions would be particularly unwarranted in the event that a State chose to convert to an electronic recording system, as many have for Article 9 financing statement filings under the Uniform Commercial Code.

The exclusion of specific Articles of the Uniform Commercial Code reflects the recognition that, particularly in the case of Articles 5, 8 and revised Article 9, electronic transactions were addressed in the specific contexts of those revision processes. In the context of Articles 2 and 2A the UETA provides the vehicle for assuring that such transactions may be accomplished and effected via an electronic medium. At such time as Articles 2 and 2A are revised the extent of coverage in those Articles/Acts may make application of this Act as a gap-filling law desirable. Similar considerations apply to the recently promulgated Uniform Computer Information Transactions Act ("UCITA").

The need for certainty as to the scope and applicability of this Act is critical, and makes any sort of a broad, general exception based on notions of inconsistency with existing writing and signature requirements unwise at best. The uncertainty inherent in leaving the applicability of the Act to judicial construction of this Act with other laws is unacceptable if electronic transactions are to be facilitated.

Finally, recognition that the paradigm for the Act involves two willing parties conducting a transaction electronically, makes it necessary to expressly provide that some form of acquiescence or intent on the part of a person to conduct transactions electronically is necessary before the Act can be invoked. Accordingly, Section 5 specifically provides that the Act only applies between parties that have agreed to conduct transactions electronically. In this context, the construction of the term agreement must be broad in order to assure that the Act applies whenever the circumstances show the parties intention to transact electronically, regardless of whether the intent rises to the level of a formal agreement.

B. Procedural Approach. Another fundamental premise of the Act is that it be minimalist and procedural. The general efficacy of existing law in an electronic context, so long as biases and barriers to the medium are removed, validates this approach. The Act defers to existing substantive law. Specific areas of deference to other law in this Act include: (1) the meaning and effect of "sign" under existing law, (2) the method and manner of displaying, transmitting and formatting information in Section 8, (3) rules of attribution in Section 9, and (4) the law of mistake in Section 10.

The Act's treatment of records and signatures demonstrates best the minimalist approach that has been adopted. Whether a record is attributed to a person is left to law outside this Act. Whether an electronic signature has any effect is left to the surrounding circumstances and other law. These provisions are salutary directives to assure that records and signatures will be treated in the same manner, under currently existing law, as written records and manual signatures.

The deference of the Act to other substantive law does not negate the necessity of setting forth rules and standards for using electronic media. The Act expressly validates electronic records, signatures and contracts. It provides for the use of electronic records and information for retention purposes, providing certainty in an area with great potential in cost savings and efficiency. The Act makes clear that the actions of machines ("electronic agents") programmed and used by people will bind the user of the machine, regardless of whether human review of a particular transaction has occurred. It specifies the standards for sending and receipt of electronic records, and it allows for innovation in financial services through the implementation of transferable records. In these ways the

Act permits electronic transactions to be accomplished with certainty under existing substantive rules of law.

UNIFORM ELECTRONIC TRANSACTIONS ACT (1999)

SECTION 1. SHORT TITLE. This [Act] may be cited as the Uniform Electronic Transactions Act.

SECTION 2. DEFINITIONS. In this [Act]:

(1) "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations, and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(2) "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by an individual in the ordinary course in forming a contract, performing under an existing contract, or fulfilling an obligation required by the transaction.

(3) "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(4) "Contract" means the total legal obligation resulting from the parties' agreement as affected by this [Act] and other applicable law.

(5) "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic, or similar capabilities.

(6) "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by an individual.

(7) "Electronic record" means a record created, generated, sent, communicated, received, or stored by electronic means.

(8) "Electronic signature" means an electronic sound, symbol, or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(9) " Governmental agency" means an executive, legislative, or judicial agency, department, board, commission, authority, institution, or instrumentality of the federal government or of a State or of a county, municipality, or other political subdivision of a State.

(10) "Information" means data, text, images, sounds, codes, computer programs, software, databases, or the like.

(11) "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying, or processing information.

(12) "Person" means an individual, corporation, business trust, estate, trust, partnership, limited liability company, association, joint venture, governmental agency, public corporation, or any other legal or commercial entity.

(13) "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(14) "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record, or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption, or callback or other acknowledgment procedures.

(15) "State" means a State of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands, or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a State.

(16) "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial, or governmental affairs.

Sources: UNICTRAL Model Law on Electronic Commerce; Uniform Commercial Code; Uniform Computer Information Transactions Act; Restatement 2d Contracts.

Comment

1. **"Agreement."**

Whether the parties have reached an agreement is determined by their express language and all surrounding circumstances. The Restatement 2d Contracts § 3 provides that, "An agreement is a manifestation of mutual assent on the part of two or more persons." See also Restatement 2d Contracts, Section 2, Comment b. The Uniform Commercial Code specifically includes in the circumstances from which an agreement may be inferred "course of performance, course of dealing and usage of trade . . ." as defined in the UCC. Although the definition of agreement in this Act does not make specific reference to usage of trade and other party conduct, this definition is not intended to affect the construction of the parties' agreement under the substantive law applicable to a particular transaction. Where that law takes account of usage and conduct in informing the terms of the parties' agreement, the usage or conduct would be relevant as "other circumstances" included in the definition under this Act.

Where the law applicable to a given transaction provides that system rules and the like constitute part of the agreement of the parties, such rules will have the same effect in determining the parties agreement under this Act. For example, UCC Article 4 (Section 4-103(b)) provides that Federal Reserve regulations and operating circulars and clearinghouse rules have the effect of agreements. Such agreements by law properly would be included in the definition of agreement in this Act.

The parties' agreement is relevant in determining whether the provisions of this Act have been varied by agreement. In addition, the parties' agreement may establish the parameters of the parties' use of electronic records and signatures, security procedures and similar aspects of the transaction. See Model Trading Partner Agreement, 45 Business Lawyer Supp. Issue (June 1990). See Section 5(b) and Comments thereto.

2. **"Automated Transaction."**

An automated transaction is a transaction performed or conducted by electronic means in which machines are used without human intervention to form contracts and perform

obligations under existing contracts. Such broad coverage is necessary because of the diversity of transactions to which this Act may apply.

As with electronic agents, this definition addresses the circumstance where electronic records may result in action or performance by a party although no human review of the electronic records is anticipated. Section 14 provides specific rules to assure that where one or both parties do not review the electronic records, the resulting agreement will be effective.

The critical element in this definition is the lack of a human actor on one or both sides of a transaction. For example, if one orders books from Bookseller.com through Bookseller's website, the transaction would be an automated transaction because Bookseller took and confirmed the order via its machine. Similarly, if Automaker and supplier do business through Electronic Data Interchange, Automaker's computer, upon receiving information within certain pre-programmed parameters, will send an electronic order to supplier's computer. If Supplier's computer confirms the order and processes the shipment because the order falls within pre-programmed parameters in Supplier's computer, this would be a fully automated transaction. If, instead, the Supplier relies on a human employee to review, accept, and process the Buyer's order, then only the Automaker's side of the transaction would be automated. In either case, the entire transaction falls within this definition.

3. **"Computer program."** This definition refers to the functional and operating aspects of an electronic, digital system. It relates to operating instructions used in an electronic system such as an electronic agent. (See definition of "Electronic Agent.")

4. **"Electronic."** The basic nature of most current technologies and the need for a recognized, single term warrants the use of "electronic" as the defined term. The definition is intended to assure that the Act will be applied broadly as new technologies develop. The term must be construed broadly in light of developing technologies in order to fulfill the purpose of this Act to validate commercial transactions regardless of the medium used by the parties. Current legal requirements for "writings" can be satisfied by almost any tangible media, whether paper, other fibers, or even stone. The purpose and applicability of this Act covers intangible media which are technologically capable of

storing, transmitting and reproducing information in human perceivable form, but which lack the tangible aspect of paper, papyrus or stone.

While not all technologies listed are technically "electronic" in nature (e.g., optical fiber technology), the term "electronic" is the most descriptive term available to describe the majority of current technologies. For example, the development of biological and chemical processes for communication and storage of data, while not specifically mentioned in the definition, are included within the technical definition because such processes operate on electromagnetic impulses. However, whether a particular technology may be characterized as technically "electronic," i.e., operates on electromagnetic impulses, should not be determinative of whether records and signatures created, used and stored by means of a particular technology are covered by this Act. This Act is intended to apply to all records and signatures created, used and stored by any medium which permits the information to be retrieved in perceivable form.

5. **"Electronic agent."** This definition establishes that an electronic agent is a machine. As the term "electronic agent" has come to be recognized, it is limited to a tool function. The effect on the party using the agent is addressed in the operative provisions of the Act (e.g., Section 14)

An electronic agent, such as a computer program or other automated means employed by a person, is a tool of that person. As a general rule, the employer of a tool is responsible for the results obtained by the use of that tool since the tool has no independent volition of its own. However, an electronic agent, by definition, is capable within the parameters of its programming, of initiating, responding or interacting with other parties or their electronic agents once it has been activated by a party, without further attention of that party.

While this Act proceeds on the paradigm that an electronic agent is capable of performing only within the technical strictures of its preset programming, it is conceivable that, within the useful life of this Act, electronic agents may be created with the ability to act autonomously, and not just automatically. That is, through developments in artificial intelligence, a computer may be able to "learn through experience, modify the instructions in their own programs, and even devise new instructions." Allen and

Widdison, "Can Computers Make Contracts?" *9 Harv. J.L.&Tech 25* (Winter, 1996). If such developments occur, courts may construe the definition of electronic agent accordingly, in order to recognize such new capabilities.

The examples involving Bookseller.com and Automaker in the Comment to the definition of Automated Transaction are equally applicable here. Bookseller acts through an electronic agent in processing an order for books. Automaker and the supplier each act through electronic agents in facilitating and effectuating the just-in-time inventory process through EDI.

6. **"Electronic record."** An electronic record is a subset of the broader defined term "record." It is any record created, used or stored in a medium other than paper (see definition of electronic). The defined term is also used in this Act as a limiting definition in those provisions in which it is used.

Information processing systems, computer equipment and programs, electronic data interchange, electronic mail, voice mail, facsimile, telex, telecopying, scanning, and similar technologies all qualify as electronic under this Act. Accordingly information stored on a computer hard drive or floppy disc, facsimiles, voice mail messages, messages on a telephone answering machine, audio and video tape recordings, among other records, all would be electronic records under this Act.

7. **"Electronic signature."**

The idea of a signature is broad and not specifically defined. Whether any particular record is "signed" is a question of fact. Proof of that fact must be made under other applicable law. This Act simply assures that the signature may be accomplished through electronic means. No specific technology need be used in order to create a valid signature. One's voice on an answering machine may suffice if the requisite intention is present. Similarly, including one's name as part of an electronic mail communication also may suffice, as may the firm name on a facsimile. It also may be shown that the requisite

intent was not present and accordingly the symbol, sound or process did not amount to a signature. One may use a digital signature with the requisite intention, or one may use the private key solely as an access device with no intention to sign, or otherwise accomplish a legally binding act. In any case the critical element is the intention to execute or adopt the sound or symbol or process for the purpose of signing the related record.

The definition requires that the signer execute or adopt the sound, symbol, or process with the intent to sign the record. The act of applying a sound, symbol or process to an electronic record could have differing meanings and effects. The consequence of the act and the effect of the act as a signature are determined under other applicable law. However, the essential attribute of a signature involves applying a sound, symbol or process with an intent to do a legally significant act. It is that intention that is understood in the law as a part of the word "sign", without the need for a definition.

This Act establishes, to the greatest extent possible, the equivalency of electronic signatures and manual signatures. Therefore the term "signature" has been used to connote and convey that equivalency. The purpose is to overcome unwarranted biases against electronic methods of signing and authenticating records. The term "authentication," used in other laws, often has a narrower meaning and purpose than an electronic signature as used in this Act. However, an authentication under any of those other laws constitutes an electronic signature under this Act.

The precise effect of an electronic signature will be determined based on the surrounding circumstances under Section 9(b).

This definition includes as an electronic signature the standard webpage click through process. For example, when a person orders goods or services through a vendor's website, the person will be required to provide information as part of a process which will result in receipt of the goods or services. When the customer ultimately gets to the last step and clicks "I agree," the person has adopted the process and has done so with the intent to associate the person with the record of that process. The actual effect of the electronic signature will be determined from all the surrounding circumstances, however, the person adopted a process which the circumstances indicate s/he intended to have the effect of

getting the goods/services and being bound to pay for them. The adoption of the process carried the intent to do a legally significant act, the hallmark of a signature.

Another important aspect of this definition lies in the necessity that the electronic signature be linked or logically associated with the record. In the paper world, it is assumed that the symbol adopted by a party is attached to or located somewhere in the same paper that is intended to be authenticated, e.g., an allonge firmly attached to a promissory note, or the classic signature at the end of a long contract. These tangible manifestations do not exist in the electronic environment, and accordingly, this definition expressly provides that the symbol must in some way be linked to, or connected with, the electronic record being signed. This linkage is consistent with the regulations promulgated by the Food and Drug Administration. 21 CFR Part 11 (March 20, 1997).

A digital signature using public key encryption technology would qualify as an electronic signature, as would the mere inclusion of one's name as a part of an e-mail message - so long as in each case the signer executed or adopted the symbol with the intent to sign.

8. **"Governmental agency."** This definition is important in the context of optional Sections 17-19.

9. **"Information processing system."** This definition is consistent with the UNCITRAL Model Law on Electronic Commerce. The term includes computers and other information systems. It is principally used in Section 15 in connection with the sending and receiving of information. In that context, the key aspect is that the information enter a system from which a person can access it.

10. **"Record."** This is a standard definition designed to embrace all means of communicating or storing information except human memory. It includes any method for storing or communicating information, including "writings." A record need not be indestructible or permanent, but the term does not include oral or other communications which are not stored or preserved by some means. Information that has not been retained

other than through human memory does not qualify as a record. As in the case of the terms "writing" or "written," the term "record" does not establish the purposes, permitted uses or legal effect which a record may have under any particular provision of substantive law. ABA Report on Use of the Term "Record," October 1, 1996.

11. **"Security procedure."**

A security procedure may be applied to verify an electronic signature, verify the identity of the sender, or assure the informational integrity of an electronic record. The definition does not identify any particular technology. This permits the use of procedures which the parties select or which are established by law. It permits the greatest flexibility among the parties and allows for future technological development.

The definition in this Act is broad and is used to illustrate one way of establishing attribution or content integrity of an electronic record or signature. The use of a security procedure is not accorded operative legal effect, through the use of presumptions or otherwise, by this Act. In this Act, the use of security procedures is simply one method for proving the source or content of an electronic record or signature.

A security procedure may be technologically very sophisticated, such as an asymetric cryptographic system. At the other extreme the security procedure may be as simple as a telephone call to confirm the identity of the sender through another channel of communication. It may include the use of a mother's maiden name or a personal identification number (PIN). Each of these examples is a method for confirming the identity of a person or accuracy of a message.

12. **"Transaction."** The definition has been limited to actions between people taken in the context of business, commercial or governmental activities. The term includes all interactions between people for business, commercial, including specifically consumer, or governmental purposes. However, the term does not include unilateral or non-

transactional actions. As such it provides a structural limitation on the scope of the Act as stated in the next section.

It is essential that the term commerce and business be understood and construed broadly to include commercial and business transactions involving individuals who may qualify as "consumers" under other applicable law. If Alice and Bob agree to the sale of Alice's car to Bob for $2000 using an internet auction site, that transaction is fully covered by this Act. Even if Alice and Bob each qualify as typical "consumers" under other applicable law, their interaction is a transaction in commerce. Accordingly their actions would be related to commercial affairs, and fully qualify as a transaction governed by this Act.

Other transaction types include:

1. A single purchase by an individual from a retail merchant, which may be accomplished by an order from a printed catalog sent by facsimile, or by exchange of electronic mail.

2. Recurring orders on a weekly or monthly basis between large companies which have entered into a master trading partner agreement to govern the methods and manner of their transaction parameters.

3. A purchase by an individual from an online internet retail vendor. Such an arrangement may develop into an ongoing series of individual purchases, with security procedures and the like, as a part of doing ongoing business.

4. The closing of a business purchase transaction via facsimile transmission of documents or even electronic mail. In such a transaction, all parties may participate through electronic conferencing technologies. At the appointed time all electronic records are

executed electronically and transmitted to the other party. In such a case, the electronic records and electronic signatures are validated under this Act, obviating the need for " in person" closings.

A transaction must include interaction between two or more persons. Consequently, to the extent that the execution of a will, trust, or a health care power of attorney or similar health care designation does not involve another person and is a unilateral act, it would not be covered by this Act because not occurring as a part of a transaction as defined in this Act. However, this Act *does* apply to all electronic records and signatures *related* to a transaction, and so does cover, for example, internal auditing and accounting records related to a transaction.

SECTION 3. SCOPE.

(a) Except as otherwise provided in subsection (b), this [Act] applies to electronic records and electronic signatures relating to a transaction.

(b) This [Act] does not apply to a transaction to the extent it is governed by:

(1) a law governing the creation and execution of wills, codicils, or testamentary trusts;

(2) [The Uniform Commercial Code other than Sections 1-107 and 1-206, Article 2, and Article 2A];

(3) [the Uniform Computer Information Transactions Act]; and

(4) [other laws, if any, identified by State].

(c) This [Act] applies to an electronic record or electronic signature otherwise excluded from the application of this [Act] under subsection (b) to the extent it is governed by a law other than those specified in subsection (b).

(d) A transaction subject to this [Act] is also subject to other applicable substantive law.

See Legislative Note below - Following Comments.

Comment

1. The scope of this Act is inherently limited by the fact that it only applies to transactions related to business, commercial (including consumer) and governmental matters. Consequently, transactions with no relation to business, commercial or governmental transactions would not be subject to this Act. Unilaterally generated electronic records and signatures which are not part of a transaction also are not covered by this Act. See Section 2, Comment 12.

2. This Act affects the medium in which information, records and signatures may be presented and retained under current legal requirements. While this Act covers all electronic records and signatures which are used in a business, commercial (including consumer) or governmental transaction, the operative provisions of the Act relate to requirements for writings and signatures under other laws. Accordingly, the exclusions in subsection (b) focus on those legal rules imposing certain writing and signature requirements which will ***not*** be affected by this Act.

3. The exclusions listed in subsection (b) provide clarity and certainty regarding the laws which are and are not affected by this Act. This section provides that transactions subject to specific laws are unaffected by this Act and leaves the balance subject to this Act.

4. Paragraph (1) excludes wills, codicils and testamentary trusts. This exclusion is largely salutary given the unilateral context in which such records are generally created and the unlikely use of such records in a transaction as defined in this Act (i.e., actions taken by two or more persons in the context of business, commercial or governmental affairs). Paragraph (2) excludes all of the Uniform Commercial Code other than UCC Sections 1-107 and 1-206, and Articles 2 and 2A. This Act does not apply to the excluded UCC articles, whether in "current" or "revised" form. The Act does apply to UCC Articles 2 and 2A and to UCC Sections 1-107 and 1-206.

5. Articles 3, 4 and 4A of the UCC impact payment systems and have specifically been removed from the coverage of this Act. The check collection and electronic fund transfer systems governed by Articles 3, 4 and 4A involve systems and relationships involving numerous parties beyond the parties to the underlying contract. The impact of validating electronic media in such systems involves considerations beyond the scope of this Act. Articles 5, 8 and 9 have been excluded because the revision process relating to those

Articles included significant consideration of electronic practices. Paragraph 4 provides for exclusion from this Act of the Uniform Computer Information Transactions Act (UCITA) because the drafting process of that Act also included significant consideration of electronic contracting provisions.

6. The very limited application of this Act to Transferable Records in Section 16 does not affect payment systems, and the section is designed to apply to a transaction only through express agreement of the parties. The exclusion of Articles 3 and 4 will not affect the Act's coverage of Transferable Records. Section 16 is designed to allow for the development of systems which will provide "control" as defined in Section 16. Such control is necessary as a substitute for the idea of possession which undergirds negotiable instrument law. The technology has yet to be developed which will allow for the possession of a unique electronic token embodying the rights associated with a negotiable promissory note. Section 16's concept of control is intended as a substitute for possession.

The provisions in Section 16 operate as free standing rules, establishing the rights of parties using Transferable Records *under this Act*. The references in Section 16 to UCC Sections 3-302, 7-501, and 9-308 (R9-330(d)) are designed to incorporate the substance of those provisions into this Act for the limited purposes noted in Section 16(c). Accordingly, an electronic record which is also a Transferable Record, would not be used for purposes of a transaction governed by Articles 3, 4, or 9, but would be an electronic record used for purposes of a transaction governed by Section 16. However, it is important to remember that those UCC Articles will still apply to the transferable record in their own right. Accordingly any other substantive requirements, e.g., method and manner of perfection under Article 9, must be complied with under those other laws. See Comments to Section 16.

7. This Act does apply, *in toto*, to transactions under unrevised Articles 2 and 2A. There is every reason to validate electronic contracting in these situations. Sale and lease transactions do not implicate broad systems beyond the parties to the underlying transaction, such as are present in check collection and electronic funds transfers. Further sales and leases generally do not have as far reaching effect on the rights of third parties beyond the contracting parties, such as exists in the secured transactions system. Finally, it is in the area of sales, licenses and leases that electronic commerce is occurring to its greatest extent today. To exclude these transactions would largely gut the purpose of this Act.

In the event that Articles 2 and 2A are revised and adopted in the future, UETA will only apply to the extent provided in those Acts.

8. An electronic record/signature may be used for purposes of more than one legal requirement, or may be covered by more than one law. Consequently, it is important to make clear, despite any apparent redundancy, in subsection (c) that an electronic record used for purposes of a law which is ***not*** affected by this Act under subsection (b) may nonetheless be used and validated for purposes of other laws not excluded by subsection (b). For example, this Act does not apply to an electronic record of a check when used for purposes of a transaction governed by Article 4 of the Uniform Commercial Code, i.e., the Act does not validate so-called electronic checks. However, for purposes of check retention statutes, the same electronic record of the check is covered by this Act, so that retention of an electronic image/record of a check will satisfy such retention statutes, so long as the requirements of Section 12 are fulfilled.

In another context, subsection (c) would operate to allow this Act to apply to what would appear to be an excluded transaction under subsection (b). For example, Article 9 of the Uniform Commercial Code applies generally to any transaction that creates a security interest in personal property. However, Article 9 excludes landlord's liens. Accordingly, although this Act excludes from its application transactions subject to Article 9, this Act would apply to the creation of a landlord lien if the law otherwise applicable to landlord's liens did not provide otherwise, because the landlord's lien transaction is excluded from Article 9.

9. Additional exclusions under subparagraph (b)(4) should be limited to laws which govern electronic records and signatures which may be used in transactions as defined in Section 2(16). Records used unilaterally, or which do not relate to business, commercial (including consumer), or governmental affairs are not governed by this Act in any event, and exclusion of laws relating to such records may create unintended inferences about whether other records and signatures are covered by this Act.

It is also important that additional exclusions, if any, be incorporated under subsection (b)(4). As noted in Comment 8 above, an electronic record used in a transaction excluded under subsection (b), e.g., a check used to pay one's taxes, will nonetheless be validated for purposes of other, non-excluded laws under subsection (c), e.g., the check when used as proof of payment. It is critical that additional exclusions, if any, be incorporated into subsection (b) so that the salutary effect of subsection (c) apply to validate those records in other, non-excluded transactions. While a legislature may determine that a particular notice, such as a utility shutoff notice, be provided to a person in writing on paper, it is difficult to see why the utility should not be entitled to use electronic media for storage and evidentiary purposes. ***Legislative Note Regarding Possible Additional Exclusions under Section 3(b)(4).***

The following discussion is derived from the Report dated September 21, 1998 of The Task Force on State Law Exclusions (the "Task Force") presented to the Drafting Committee. After consideration of the Report, the Drafting Committee determined that exclusions other than those specified in the Act were not warranted. In addition, other inherent limitations on the applicability of the Act (the definition of transaction, the requirement that the parties acquiesce in the use of an electronic format) also militate against additional exclusions. Nonetheless, the Drafting Committee recognized that some legislatures may wish to exclude additional transactions from the Act, and determined that guidance in some major areas would be helpful to those legislatures considering additional areas for exclusion.

Because of the overwhelming number of references in state law to writings and signatures, the following list of possible transactions is not exhaustive. However, they do represent those areas most commonly raised during the course of the drafting process as areas that might be inappropriate for an electronic medium. It is important to keep in mind however, that the Drafting Committee determined that exclusion of these additional areas was not warranted.

1. **Trusts** (other than testamentary trusts). Trusts can be used for both business and personal purposes. By virtue of the definition of transaction, trusts used outside the area of business and commerce would not be governed by this Act. With respect to business or commercial trusts, the laws governing their formation contain few or no requirements for paper or signatures. Indeed, in most jurisdictions trusts of any kind may be created orally. Consequently, the Drafting Committee believed that the Act should apply to any transaction where the law leaves to the parties the decision of whether to use a writing.

Thus, in the absence of legal requirements for writings, there is no sound reason to exclude laws governing trusts from the application of this Act.

2. **Powers of Attorney.** A power of attorney is simply a formalized type of agency agreement. In general, no formal requirements for paper or execution were found to be applicable to the validity of powers of attorney.

Special health powers of attorney have been established by statute in some States. These powers may have special requirements under state law regarding execution, acknowledgment and possibly notarization. In the normal case such powers will not arise in a transactional context and so would not be covered by this Act. However, even if such a record were to arise in a transactional context, this Act operates simply to remove the barrier to the use of an electronic medium, and preserves other requirements of applicable substantive law, avoiding any necessity to exclude such laws from the operation of this Act. Especially in light of the provisions of Sections 8 and 11, the substantive requirements under such laws will be preserved and may be satisfied in an electronic format.

3. **Real Estate Transactions.** It is important to distinguish between the efficacy of paper documents involving real estate between the parties, as opposed to their effect on third parties. As between the parties it is unnecessary to maintain existing barriers to electronic contracting. There are no unique characteristics to contracts relating to real property as opposed to other business and commercial (including consumer) contracts. Consequently, the decision whether to use an electronic medium for their agreements should be a matter for the parties to determine. Of course, to be effective against third parties state law generally requires filing with a governmental office. Pending adoption of electronic filing systems by States, the need for a piece of paper to file to perfect rights against third parties, will be a consideration for the parties. In the event notarization and acknowledgment are required under other laws, Section 11 provides a means for such actions to be accomplished electronically.

With respect to the requirements of government filing, those are left to the individual States in the decision of whether to adopt and implement electronic filing systems. (See optional Sections 17-19.) However, government recording systems currently require

paper deeds including notarized, manual signatures. Although California and Illinois are experimenting with electronic filing systems, until such systems become widespread, the parties likely will choose to use, at the least, a paper deed for filing purposes. Nothing in this Act precludes the parties from selecting the medium best suited to the needs of the particular transaction. Parties may wish to consummate the transaction using electronic media in order to avoid expensive travel. Yet the actual deed may be in paper form to assure compliance with existing recording systems and requirements. The critical point is that nothing in this Act prevents the parties from selecting paper or electronic media for all or part of their transaction.

4. **Consumer Protection Statutes.** Consumer protection provisions in state law often require that information be disclosed or provided to a consumer in writing. Because this Act does apply to such transactions, the question of whether such laws should be specifically excluded was considered. Exclusion of consumer transactions would eliminate a huge group of commercial transactions which benefit consumers by enabling the efficiency of the electronic medium. Commerce over the internet is driven by consumer demands and concerns and must be included.

At the same time, it is important to recognize the protective effects of many consumer statutes. Consumer statutes often require that information be provided in writing, or may require that the consumer separately sign or initial a particular provision to evidence that the consumer's attention was brought to the provision. Subsection (1) requires electronic records to be retainable by a person whenever the law requires information to be delivered in writing. The section imposes a significant burden on the sender of information. The sender must assure that the information system of the recipient is compatible with, and capable of retaining the information sent by, the sender's system. Furthermore, nothing in this Act permits the avoidance of legal requirements of separate signatures or initialing. The Act simply permits the signature or initialing to be done electronically.

Other consumer protection statutes require (expressly or implicitly) that certain information be presented in a certain manner or format. Laws requiring information to be presented in particular fonts, formats or in similar fashion, as well as laws requiring conspicuous displays of information are preserved. Section 8(b)(3) specifically preserves the applicability of such requirements in an electronic environment. In the case of legal requirements that information be presented or appear conspicuous, the determination of what is conspicuous will be left to other law. Section 8 was included to specifically

preserve the protective functions of such disclosure statutes, while at the same time allowing the use of electronic media if the substantive requirements of the other laws could be satisfied in the electronic medium.

Formatting and separate signing requirements serve a critical purpose in much consumer protection legislation, to assure that information is not slipped past the unsuspecting consumer. Not only does this Act not disturb those requirements, it preserves those requirements. In addition, other bodies of substantive law continue to operate to allow the courts to police any such bad conduct or overreaching, e.g., unconscionability, fraud, duress, mistake and the like. These bodies of law remain applicable regardless of the medium in which a record appears.

The requirement that both parties agree to conduct a transaction electronically also prevents the imposition of an electronic medium on unwilling parties See Section 5(b). In addition, where the law requires inclusion of specific terms or language, those requirements are preserved broadly by Section 5(e).

Requirements that information be sent to, or received by, someone have been preserved in Section 15. As in the paper world, obligations to send do not impose any duties on the sender to assure receipt, other than reasonable methods of dispatch. In those cases where receipt is required legally, Sections 5, 8, and 15 impose the burden on the sender to assure delivery to the recipient if satisfaction of the legal requirement is to be fulfilled.

The preservation of existing safeguards, together with the ability to opt out of the electronic medium entirely, demonstrate the lack of any need generally to exclude consumer protection laws from the operation of this Act. Legislatures may wish to focus any review on those statutes which provide for post-contract formation and post-breach notices to be in paper. However, any such consideration must also balance the needed protections against the potential burdens which may be imposed. Consumers and others will not be well served by restrictions which preclude the employment of electronic technologies sought and desired by consumers.

SECTION 4. PROSPECTIVE APPLICATION. This [Act] applies to anyelectronic record or electronic signature created, generated, sent, communicated, received, or stored on or after the effective date of this [Act].

Comment

This section makes clear that the Act only applies to validate electronic records and signatures which arise subsequent to the effective date of the Act. Whether electronic records and electronic signatures arising before the effective date of this Act are valid is left to other law.

SECTION 5. USE OF ELECTRONIC RECORDS AND ELECTRONIC SIGNATURES; VARIATION BY AGREEMENT.

(a) This [Act] does not require a record or signature to be created, generated, sent, communicated, received, stored, or otherwise processed or used by electronic means or in electronic form.

(b) This [Act] applies only to transactions between parties each of which has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

(c) A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

(d) Except as otherwise provided in this [Act], the effect of any of its provisions may be varied by agreement. The presence in certain provisions of this [Act] of the words "unless otherwise agreed", or words of similar import, does not imply that the effect of other provisions may not be varied by agreement.

(e) Whether an electronic record or electronic signature has legal consequences is determined by this [Act] and other applicable law.

Comment

This section limits the applicability of this Act to transactions which parties have agreed to conduct electronically. Broad interpretation of the term agreement is necessary to assure that this Act has the widest possible application consistent with its purpose of removing barriers to electronic commerce.

1. This section makes clear that this Act is intended to facilitate the use of electronic means, but does not require the use of electronic records and signatures. This fundamental principle is set forth in subsection (a) and elaborated by subsections (b) and (c), which require an intention to conduct transactions electronically and preserve the right of a party to refuse to use electronics in any subsequent transaction.

2. The paradigm of this Act is two willing parties doing transactions electronically. It is therefore appropriate that the Act is voluntary and preserves the greatest possible party autonomy to refuse electronic transactions. The requirement that party agreement be found from all the surrounding circumstances is a limitation on the scope of this Act.

3. If this Act is to serve to facilitate electronic transactions, it must be applicable under circumstances not rising to a full fledged contract to use electronics. While absolute certainty can be accomplished by obtaining an explicit contract before relying on electronic transactions, such an explicit contract should not be necessary before one may feel safe in conducting transactions electronically. Indeed, such a requirement would itself be an unreasonable barrier to electronic commerce, at odds with the fundamental purpose of this Act. Accordingly, the requisite agreement, express or implied, must be determined from all available circumstances and evidence.

4. Subsection (b) provides that the Act applies to transactions in which the parties have agreed to conduct the transaction electronically. In this context it is essential that the parties' actions and words be broadly construed in determining whether the requisite agreement exists. Accordingly, the Act expressly provides that the party's agreement is to be found from all circumstances, including the parties' conduct. The critical element is the intent of a party to conduct a transaction electronically. Once that intent is established, this Act applies. See Restatement 2d Contracts, Sections 2, 3, and 19.

Examples of circumstances from which it may be found that parties have reached an agreement to conduct transactions electronically include the following:

A. Automaker and supplier enter into a Trading Partner Agreement setting forth the terms, conditions and methods for the conduct of business between them electronically.

B. Joe gives out his business card with his business e-mail address. It may be reasonable, under the circumstances, for a recipient of the card to infer that Joe has agreed to communicate electronically for business purposes. However, in the absence of additional facts, it would not necessarily be reasonable to infer Joe's agreement to communicate electronically for purposes outside the scope of the business indicated by use of the business card.

C. Sally may have several e-mail addresses - home, main office, office of a non-profit organization on whose board Sally sits. In each case, it may be reasonable to infer that Sally is willing to communicate electronically with respect to business related to the business/purpose associated with the respective e-mail addresses. However, depending on the circumstances, it may not be reasonable to communicate with Sally for purposes other than those related to the purpose for which she maintained a particular e-mail account.

D. Among the circumstances to be considered in finding an agreement would be the time when the assent occurred relative to the timing of the use of electronic communications. If one orders books from an on-line vendor, such as Bookseller.com, the intention to conduct that transaction and to receive any correspondence related to the transaction electronically can be inferred from the conduct. Accordingly, as to information related to that transaction it is reasonable for Bookseller to deal with the individual electronically.

The examples noted above are intended to focus the inquiry on the party's agreement to conduct a transaction electronically. Similarly, if two people are at a meeting and one tells the other to send an e-mail to confirm a transaction - the requisite agreement under subsection (b) would exist. In each case, the use of a business card, statement at a meeting, or other evidence of willingness to conduct a transaction electronically must be viewed in light of all the surrounding circumstances with a view toward broad validation of electronic transactions.

5. Just as circumstances may indicate the existence of agreement, express or implied from surrounding circumstances, circumstances may also demonstrate the absence of true agreement. For example:

A. If Automaker, Inc. were to issue a recall of automobiles via its Internet website, it would not be able to rely on this Act to validate that notice in the case of a person who never logged on to the website, or indeed, had no ability to do so, notwithstanding a clause in a paper purchase contract by which the buyer agreed to receive such notices in such a manner.

B. Buyer executes a standard form contract in which an agreement to receive all notices electronically in set forth on page 3 in the midst of other fine print. Buyer has never communicated with Seller electronically, and has not provided any other information in the contract to suggest a willingness to deal electronically. Not only is it unlikely that any but the most formalistic of agreements may be found, but nothing in this Act prevents courts from policing such form contracts under common law doctrines relating to contract formation, unconscionability and the like.

6. Subsection (c) has been added to make clear the ability of a party to refuse to conduct a transaction electronically, even if the person has conducted transactions electronically in the past. The effectiveness of a party's refusal to conduct a transaction electronically will be determined under other applicable law in light of all surrounding circumstances. Such circumstances must include an assessment of the transaction involved.

A party's right to decline to act electronically under a specific contract, on the ground that each action under that contract amounts to a separate "transaction," must be considered in light of the purpose of the contract and the action to be taken electronically. For example, under a contract for the purchase of goods, the giving and receipt of notices electronically, as provided in the contract, should not be viewed as discreet transactions. Rather such notices amount to separate actions which are part of the "transaction" of purchase evidenced by the contract. Allowing one party to require a change of medium in the middle of the transaction evidenced by that contract is not the purpose of this subsection. Rather this subsection is intended to preserve the party's right to conduct the next purchase in a non-electronic medium.

7. Subsection (e) is an essential provision in the overall scheme of this Act. While this Act validates and effectuates electronic records and electronic signatures, the legal effect of such records and signatures is left to existing substantive law outside this Act except in very narrow circumstances. See, e.g., Section 16. Even when this Act operates to validate records and signatures in an electronic medium, it expressly preserves the substantive rules of other law applicable to such records. See, e.g., Section 11.

For example, beyond validation of records, signatures and contracts based on the medium used, Section 7 (a) and (b) should not be interpreted as establishing the legal effectiveness of any given record, signature or contract. Where a rule of law requires that the record contain minimum substantive content, the legal effect of such a record will depend on whether the record meets the substantive requirements of other applicable law.

Section 8 expressly preserves a number of legal requirements in currently existing law relating to the presentation of information in writing. Although this Act now would allow such information to be presented in an electronic record, Section 8 provides that the other substantive requirements of law must be satisfied in the electronic medium as well.

SECTION 6. CONSTRUCTION AND APPLICATION. This [Act] must be construed and applied:

(1) to facilitate electronic transactions consistent with other applicable law; (2) to be consistent with reasonable practices concerning electronic transactions and with the continued expansion of those practices; and

(3) to effectuate its general purpose to make uniform the law with respect to the subject of this [Act] among States enacting it.

Comment

1. The purposes and policies of this Act are

(a) to facilitate and promote commerce and governmental transactions by validating and authorizing the use of electronic records and electronic signatures;

(b) to eliminate barriers to electronic commerce and governmental transactions resulting from uncertainties relating to writing and signature requirements;

(c) to simplify, clarify and modernize the law governing commerce and governmental transactions through the use of electronic means;

(d) to permit the continued expansion of commercial and governmental electronic practices through custom, usage and agreement of the parties;

(e) to promote uniformity of the law among the States (and worldwide) relating to the use of electronic and similar technological means of effecting and performing commercial and governmental transactions;

(f) to promote public confidence in the validity, integrity and reliability of electronic commerce and governmental transactions; and

(g) to promote the development of the legal and business infrastructure necessary to implement electronic commerce and governmental transactions.

2. This Act has been drafted to permit flexible application consistent with its purpose to validate electronic transactions. The provisions of this Act validating and effectuating the employ of electronic media allow the courts to apply them to new and unforeseen technologies and practices. As time progresses, it is anticipated that what is new and unforeseen today will be commonplace tomorrow. Accordingly, this legislation is intended to set a framework for the validation of media which may be developed in the future and which demonstrate the same qualities as the electronic media contemplated and validated under this Act.

SECTION 7. LEGAL RECOGNITION OF ELECTRONIC RECORDS, ELECTRONIC SIGNATURES, AND ELECTRONIC CONTRACTS.

(a) A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

(b) A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

(c) If a law requires a record to be in writing, an electronic record satisfies the law.

(d) If a law requires a signature, an electronic signature satisfies the law.

Source: UNCITRAL Model Law on Electronic Commerce, Articles 5, 6, and 7.

Comment

1. This section sets forth the fundamental premise of this Act: namely, that the medium in which a record, signature, or contract is created, presented or retained does not affect it's legal significance. Subsections (a) and (b) are designed to eliminate the single element of medium as a reason to deny effect or enforceability to a record, signature, or contract. The fact that the information is set forth in an electronic, as opposed to paper, record is irrelevant.

2. Under Restatement 2d Contracts Section 8, a contract may have legal effect and yet be unenforceable. Indeed, one circumstance where a record or contract may have effect but be unenforceable is in the context of the Statute of Frauds. Though a contract may be unenforceable, the records may have collateral effects, as in the case of a buyer that insures goods purchased under a contract unenforceable under the Statute of Frauds. The insurance company may not deny a claim on the ground that the buyer is not the owner, though the buyer may have no direct remedy against seller for failure to deliver. See Restatement 2d Contracts, Section 8, Illustration 4.

While this section would validate an electronic record for purposes of a statute of frauds, if an agreement to conduct the transaction electronically cannot reasonably be found (See Section 5(b)) then a necessary predicate to the applicability of this Act would be absent and this Act would not validate the electronic record. Whether the electronic record might be valid under other law is not addressed by this Act.

3. Subsections (c) and (d) provide the positive assertion that electronic records and signatures satisfy legal requirements for writings and signatures. The provisions are limited to requirements in laws that a record be in writing or be signed. This section does not address requirements imposed by other law in addition to requirements for writings and signatures See, e.g., Section 8.

Subsections (c) and (d) are particularized applications of subsection (a). The purpose is to validate and effectuate electronic records and signatures as the equivalent of writings, subject to all of the rules applicable to the efficacy of a writing, except as such other rules are modified by the more specific provisions of this Act.

Illustration 1: A sends the following e-mail to B: "I hereby offer to buy widgets from you, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to buy widgets for delivery next Tuesday. /s/ B." The e-mails may not be denied effect solely because they are electronic. In addition, the e-mails do qualify as records under the Statute of Frauds. However, because there is no quantity stated in either record, the parties' agreement would be unenforceable under existing UCC Section 2-201(1).

Illustration 2: A sends the following e-mail to B: "I hereby offer to buy 100 widgets for $1000, delivery next Tuesday. /s/ A." B responds with the following e-mail: "I accept your offer to purchase 100 widgets for $1000, delivery next Tuesday. /s/ B." In this case the analysis is the same as in Illustration 1 except that here the records otherwise satisfy the requirements of UCC Section 2-201(1). The transaction may not be denied legal effect solely because there is not a pen and ink "writing" or "signature".

4. Section 8 addresses additional requirements imposed by other law which may affect the legal effect or enforceability of an electronic record in a particular case. For example, in Section 8(a) the legal requirement addressed is *the provision of information* in writing. The section then sets forth the standards to be applied in determining whether the provision of information by an electronic record is the equivalent of the provision of information in writing. The requirements in Section 8 are in addition to the bare validation that occurs under this section.

5. Under the substantive law applicable to a particular transaction within this Act, the legal effect of an electronic record may be separate from the issue of whether the record contains a signature. For example, where notice must be given as part of a contractual obligation, the effectiveness of the notice will turn on whether the party provided the notice regardless of whether the notice was signed (See Section 15). An electronic record attributed to a party under Section 9 and complying with the requirements of Section 15 would suffice in that case, notwithstanding that it may not contain an electronic signature.

SECTION 8. PROVISION OF INFORMATION IN WRITING; PRESENTATION OF RECORDS.

(a) If parties have agreed to conduct a transaction by electronic means and a law requires a person to provide, send, or deliver information in writing to another person, the requirement is satisfied if the information is provided, sent, or delivered, as the case may be, in an electronic record capable of retention by the recipient at the time of receipt. An electronic record is not capable of retention by the recipient if the sender or its information processing system inhibits the ability of the recipient to print or store the electronic record.

(b) If a law other than this [Act] requires a record (i) to be posted or displayed in a certain manner, (ii) to be sent, communicated, or transmitted by a specified method, or (iii) to contain information that is formatted in a certain manner, the following rules apply:

(1) The record must be posted or displayed in the manner specified in the other law.

(2) Except as otherwise provided in subsection (d)(2), the record must be sent, communicated, or transmitted by the method specified in the other law.

(3) The record must contain the information formatted in the manner specified in the other law.

(c) If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

(d) The requirements of this section may not be varied by agreement, but:

(1) to the extent a law other than this [Act] requires information to be provided, sent, or delivered in writing but permits that requirement to be varied by agreement, the requirement under subsection (a) that the information be in the form of an electronic record capable of retention may also be varied by agreement; and

(2) a requirement under a law other than this [Act] to send, communicate, or transmit a record by [first-class mail, postage prepaid] [regular United States mail], may be varied by agreement to the extent permitted by the other law.

Source: Canadian - Uniform Electronic Commerce Act

Comment

1. This section is a savings provision, designed to assure, consistent with the fundamental purpose of this Act, that otherwise applicable substantive law will not be overridden by this Act. The section makes clear that while the pen and ink provisions of such other law

may be satisfied electronically, nothing in this Act vitiates the other requirements of such laws. The section addresses a number of issues related to disclosures and notice provisions in other laws.

2. This section is independent of the prior section. Section 7 refers to legal requirements for a writing. This section refers to legal requirements for the provision of information in writing or relating to the method or manner of presentation or delivery of information. The section addresses more specific legal requirements of other laws, provides standards for satisfying the more particular legal requirements, and defers to other law for satisfaction of requirements under those laws.

3. Under subsection (a), to meet a requirement of other law that information be provided in writing, the recipient of an electronic record of the information must be able to get to the electronic record and read it, and must have the ability to get back to the information in some way at a later date. Accordingly, the section requires that the electronic record be capable of retention for later review.

The section specifically provides that any inhibition on retention imposed by the sender or the sender's system will preclude satisfaction of this section. Use of technological means now existing or later developed which prevents the recipient from retaining a copy the information would result in a determination that information has not been provided under subsection (a). The policies underlying laws requiring the provision of information in writing warrant the imposition of an additional burden on the sender to make the information available in a manner which will permit subsequent reference. A difficulty does exist for senders of information because of the disparate systems of their recipients and the capabilities of those systems. However, in order to satisfy the *legal requirement* of other law to make information available, the sender must assure that the recipient receives and can retain the information. However, it is left for the courts to determine whether the sender has complied with this subsection if evidence demonstrates that it is something peculiar the recipient's system which precludes subsequent reference to the information.

4. Subsection (b) is a savings provision for laws which provide for the means of delivering or displaying information and which are not affected by the Act. For example,

if a law requires delivery of notice by first class US mail, that means of delivery would not be affected by this Act. The information to be delivered may be provided on a disc, i.e., in electronic form, but the particular means of delivery must still be via the US postal service. Display, delivery and formatting requirements will continue to be applicable to electronic records and signatures. If those legal requirements can be satisfied in an electronic medium, e.g., the information can be presented in the equivalent of 20 point bold type as required by other law, this Act will validate the use of the medium, leaving to the other applicable law the question of whether the particular electronic record meets the other legal requirements. If a law requires that particular records be delivered together, or attached to other records, this Act does not preclude the delivery of the records together in an electronic communication, so long as the records are connected or associated with each other in a way determined to satisfy the other law.

5. Subsection (c) provides incentives for senders of information to use systems which will not inhibit the other party from retaining the information. However, there are circumstances where a party providing certain information may wish to inhibit retention in order to protect intellectual property rights or prevent the other party from retaining confidential information about the sender. In such cases inhibition is understandable, but if the sender wishes to enforce the record in which the information is contained, the sender may not inhibit its retention by the recipient. Unlike subsection (a), subsection (c) applies in all transactions and simply provides for unenforceability against the recipient. Subsection (a) applies only where another law imposes the writing requirement, and subsection (a) imposes a broader responsibility on the sender to assure retention capability by the recipient.

6. The protective purposes of this section justify the non-waivability provided by subsection (d). However, since the requirements for sending and formatting and the like are imposed by other law, to the extent other law permits waiver of such protections, there is no justification for imposing a more severe burden in an electronic environment.

SECTION 9. ATTRIBUTION AND EFFECT OF ELECTRONIC RECORD AND ELECTRONIC SIGNATURE.

(a) An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of

the efficacy of any security procedure applied to determine the person to which the electronic record or electronic signature was attributable.

(b) The effect of an electronic record or electronic signature attributed to a person under subsection (a) is determined from the context and surrounding circumstances at the time of its creation, execution, or adoption, including the parties' agreement, if any, and otherwise as provided by law.

Comment

1. Under subsection (a), so long as the electronic record or electronic signature resulted from a person's action it will be attributed to that person - the legal effect of that attribution is addressed in subsection (b). This section does not alter existing rules of law regarding attribution. The section assures that such rules will be applied in the electronic environment. A person's actions include actions taken by human agents of the person, as well as actions taken by an electronic agent, i.e., the tool, of the person. Although the rule may appear to state the obvious, it assures that the record or signature is not ascribed to a machine, as opposed to the person operating or programing the machine.

In each of the following cases, both the electronic record and electronic signature would be attributable to a person under subsection (a):

A. The person types his/her name as part of an e-mail purchase order;

B. The person's employee, pursuant to authority, types the person's name as part of an e-mail purchase order;

C. The person's computer, programmed to order goods upon receipt of inventory information within particular parameters, issues a purchase order which includes the person's name, or other identifying information, as part of the order.

In each of the above cases, law other than this Act would ascribe both the signature and the action to the person if done in a paper medium. Subsection (a) expressly provides that the same result will occur when an electronic medium is used.

2. Nothing in this section affects the use of a signature as a device for attributing a record to a person. Indeed, a signature is often the primary method for attributing a record to a person. In the foregoing examples, once the electronic signature is attributed to the person, the electronic record would also be attributed to the person, unless the person established fraud, forgery, or other invalidating cause. However, a signature is not the only method for attribution.

3. The use of facsimile transmissions provides a number of examples of attribution using information other than a signature. A facsimile may be attributed to a person because of the information printed across the top of the page that indicates the machine from which it was sent. Similarly, the transmission may contain a letterhead which identifies the sender. Some cases have held that the letterhead actually constituted a signature because it was a symbol adopted by the sender with intent to authenticate the facsimile. However, the signature determination resulted from the necessary finding of intention in that case. Other cases have found facsimile letterheads NOT to be signatures because the requisite intention was not present. The critical point is that with or without a signature, information within the electronic record may well suffice to provide the facts resulting in attribution of an electronic record to a particular party.

In the context of attribution of records, normally the content of the record will provide the necessary information for a finding of attribution. It is also possible that an established course of dealing between parties may result in a finding of attribution Just as with a paper record, evidence of forgery or counterfeiting may be introduced to rebut the evidence of attribution.

4. Certain information may be present in an electronic environment that does not appear to attribute but which clearly links a person to a particular record. Numerical codes, personal identification numbers, public and private key combinations all serve to establish the party to whom an electronic record should be attributed. Of course security procedures will be another piece of evidence available to establish attribution.

The inclusion of a specific reference to security procedures as a means of proving attribution is salutary because of the unique importance of security procedures in the electronic environment. In certain processes, a technical and technological security procedure may be the best way to convince a trier of fact that a particular electronic record or signature was that of a particular person. In certain circumstances, the use of a security procedure to establish that the record and related signature came from the person's business might be necessary to overcome a claim that a hacker intervened. The reference to security procedures is not intended to suggest that other forms of proof of attribution should be accorded less persuasive effect. It is also important to recall that the particular strength of a given procedure does not affect the procedure's status as a security procedure, but only affects the weight to be accorded the evidence of the security procedure as tending to establish attribution.

5. This section does apply in determining the effect of a "click-through" transaction. A "click-through" transaction involves a process which, if executed with an intent to "sign," will be an electronic signature. See definition of Electronic Signature. In the context of an anonymous "click-through," issues of proof will be paramount. This section will be relevant to establish that the resulting electronic record is attributable to a particular person upon the requisite proof, including security procedures which may track the source of the click-through.

6. Once it is established that a record or signature is attributable to a particular party, the effect of a record or signature must be determined in light of the context and surrounding circumstances, including the parties' agreement, if any. Also informing the effect of any attribution will be other legal requirements considered in light of the context. Subsection (b) addresses the effect of the record or signature once attributed to a person.

SECTION 10. EFFECT OF CHANGE OR ERROR. If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

(1) If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

(2) In an automated transaction involving an individual, the individual may avoid the effect of an electronic record that resulted from an error made by the individual in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the individual learns of the error, the individual:

(A) promptly notifies the other person of the error and that the individual did not intend to be bound by the electronic record received by the other person;

(B) takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(C) has not used or received any benefit or value from the consideration, if any, received from the other person.

(3) If neither paragraph (1) nor paragraph (2) applies, the change or error has the effect provided by other law, including the law of mistake, and the parties' contract, if any.

(4) Paragraphs (2) and (3) may not be varied by agreement.

Source: Restatement 2d Contracts, Sections 152-155.

Comment

1. This section is limited to changes and errors occurring in transmissions between parties - whether person-person (paragraph 1) or in an automated transaction involving an individual and a machine (paragraphs 1 and 2). The section focuses on the effect of changes and errors occurring when records are exchanged between parties. In cases where changes and errors occur in contexts other than transmission, the law of mistake is expressly made applicable to resolve the conflict.

The section covers both changes and errors. For example, if Buyer sends a message to Seller ordering 100 widgets, but Buyer's information processing system changes the order to 1000 widgets, a "change" has occurred between what Buyer transmitted and what

Seller received. If on the other hand, Buyer typed in 1000 intending to order only 100, but sent the message before noting the mistake, an error would have occurred which would also be covered by this section.

2. Paragraph (1) deals with any transmission where the parties have agreed to use a security procedure to detect changes and errors. It operates against the non-conforming party, i.e., the party in the best position to have avoided the change or error, regardless of whether that person is the sender or recipient. The source of the error/change is not indicated, and so both human and machine errors/changes would be covered. With respect to errors or changes that would not be detected by the security procedure even if applied, the parties are left to the general law of mistake to resolve the dispute.

3. Paragraph (1) applies only in the situation where a security procedure would detect the error/change but one party fails to use the procedure and does not detect the error/change. In such a case, consistent with the law of mistake generally, the record is made avoidable at the instance of the party who took all available steps to avoid the mistake. See Restatement 2d Contracts Sections 152-154.

Making the erroneous record avoidable by the conforming party is consistent with Sections 153 and 154 of the Restatement 2d Contracts because the non-conforming party was in the best position to avoid the problem, and would bear the risk of mistake. Such a case would constitute mistake by one party. The mistaken party (the conforming party) would be entitled to avoid any resulting contract under Section 153 because s/he does not have the risk of mistake and the non-conforming party had reason to know of the mistake.

4. As with paragraph (1), paragraph (2), when applicable, allows the mistaken party to avoid the effect of the erroneous electronic record. However, the subsection is limited to human error on the part of an individual when dealing with the electronic agent of the other party. In a transaction between individuals there is a greater ability to correct the error before parties have acted on it. However, when an individual makes an error while dealing with the electronic agent of the other party, it may not be possible to correct the error before the other party has shipped or taken other action in reliance on the erroneous record.

Paragraph (2) applies only to errors made by individuals. If the error results from the electronic agent, it would constitute a system error. In such a case the effect of that error would be resolved under paragraph (1) if applicable, otherwise under paragraph (3) and the general law of mistake.

5. The party acting through the electronic agent/machine is given incentives by this section to build in safeguards which enable the individual to prevent the sending of an erroneous record, or correct the error once sent. For example, the electronic agent may be programed to provide a "confirmation screen" to the individual setting forth all the information the individual initially approved. This would provide the individual with the ability to prevent the erroneous record from ever being sent. Similarly, the electronic agent might receive the record sent by the individual and then send back a confirmation which the individual must again accept before the transaction is completed. This would allow for correction of an erroneous record. In either case, the electronic agent would "provide an opportunity for prevention or correction of the error," *and the subsection would not apply*. Rather, the affect of any error is governed by other law.

6. Paragraph (2) also places additional requirements on the mistaken individual before the paragraph may be invoked to avoid an erroneous electronic record. The individual must take prompt action to advise the other party of the error and the fact that the individual did not intend the electronic record. Whether the action is prompt must be determined from all the circumstances including the individual's ability to contact the other party. The individual should advise the other party both of the error and of the lack of intention to be bound (i.e., avoidance) by the electronic record received. Since this provision allows avoidance by the mistaken party, that party should also be required to expressly note that it is seeking to avoid the electronic record, i.e., lacked the intention to be bound.

Second, restitution is normally required in order to undo a mistaken transaction. Accordingly, the individual must also return or destroy any consideration received, adhering to instructions from the other party in any case. This is to assure that the other party retains control over the consideration sent in error.

Finally, and most importantly in regard to transactions involving intermediaries which may be harmed because transactions cannot be unwound, the individual cannot have received any benefit from the transaction. This section prevents a party from unwinding a transaction after the delivery of value and consideration which cannot be returned or destroyed. For example, if the consideration received is information, it may not be possible to avoid the benefit conferred. While the information itself could be returned, mere access to the information, or the ability to redistribute the information would constitute a benefit precluding the mistaken party from unwinding the transaction. It may also occur that the mistaken party receives consideration which changes in value between the time of receipt and the first opportunity to return. In such a case restitution cannot be made adequately, and the transaction would not be avoidable. In each of the foregoing cases, under subparagraph (2)(c), the individual would have received the benefit of the consideration and would NOT be able to avoid the erroneous electronic record under this section.

7. In all cases not covered by paragraphs (1) or (2), where error or change to a record occur, the parties contract, or other law, specifically including the law of mistake, applies to resolve any dispute. In the event that the parties' contract and other law would achieve different results, the construction of the parties' contract is left to the other law. If the error occurs in the context of record retention, Section 12 will apply. In that case the standard is one of accuracy and retrievability of the information.

8. Paragraph (4) makes the error correction provision in paragraph (2) and the application of the law of mistake in paragraph (3) non-variable. Paragraph (2) provides incentives for parties using electronic agents to establish safeguards for individuals dealing with them. It also avoids unjustified windfalls to the individual by erecting stringent requirements before the individual may exercise the right of avoidance under the paragraph. Therefore, there is no reason to permit parties to avoid the paragraph by agreement. Rather, parties should satisfy the paragraph's requirements.

SECTION 11. NOTARIZATION AND ACKNOWLEDGMENT. If a law requires a signature or record to be notarized, acknowledged, verified, or made under oath, the 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 law, is attached to or logically associated with the signature or record.

Comment

This section permits a notary public and other authorized officers to act electronically, effectively removing the stamp/seal requirements. However, the section does not eliminate any of the other requirements of notarial laws, and consistent with the entire thrust of this Act, simply allows the signing and information to be accomplished in an electronic medium.

For example, Buyer wishes to send a notarized Real Estate Purchase Agreement to Seller via e-mail. The notary must appear in the room with the Buyer, satisfy him/herself as to the identity of the Buyer, and swear to that identification. All that activity must be reflected as part of the electronic Purchase Agreement and the notary's electronic signature must appear as a part of the electronic real estate purchase contract.

As another example, Buyer seeks to send Seller an affidavit averring defects in the products received. A court clerk, authorized under state law to administer oaths, is present with Buyer in a room. The Clerk administers the oath and includes the statement of the oath, together with any other requisite information, in the electronic record to be sent to the Seller. Upon administering the oath and witnessing the application of Buyer's electronic signature to the electronic record, the Clerk also applies his electronic signature to the electronic record. So long as all substantive requirements of other applicable law have been fulfilled and are reflected in the electronic record, the sworn electronic record of Buyer is as effective as if it had been transcribed on paper.

SECTION 12. RETENTION OF ELECTRONIC RECORDS; ORIGINALS.

(a) If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(1) accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(2) remains accessible for later reference.

(b) A requirement to retain a record in accordance with subsection (a) does not apply to any information the sole purpose of which is to enable the record to be sent, communicated, or received.

(c) A person may satisfy subsection (a) by using the services of another person if the requirements of that subsection are satisfied.

(d) If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection (a).

(e) If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection (a).

(f) A record retained as an electronic record in accordance with subsection (a) satisfies a law requiring a person to retain a record for evidentiary, audit, or like purposes, unless a law enacted after the effective date of this [Act] specifically prohibits the use of an electronic record for the specified purpose.

(g) This section does not preclude a governmental agency of this State from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.

Source: UNCITRAL Model Law On Electronic Commerce Articles 8 and 10.

Comment

1. This section deals with the serviceability of electronic records as retained records and originals. So long as there exists reliable assurance that the electronic record accurately reproduces the information, this section continues the theme of establishing the functional equivalence of electronic and paper-based records. This is consistent with Fed.R.Evid. 1001(3) and Unif.R.Evid. 1001(3) (1974). This section assures that information stored electronically will remain effective for all audit, evidentiary, archival and similar purposes.

2. In an electronic medium, the concept of an original document is problematic. For example, as one drafts a document on a computer the "original" is either on a disc or the hard drive to which the document has been initially saved. If one periodically saves the draft, the fact is that at times a document may be first saved to disc then to hard drive, and at others vice versa. In such a case the "original" may change from the information on the disc to the information on the hard drive. Indeed, it may be argued that the

"original" exists solely in RAM and, in a sense, the original is destroyed when a "copy" is saved to a disc or to the hard drive. In any event, in the context of record retention, the concern focuses on the integrity of the information, and not with its "originality."

3. Subsection (a) requires accuracy and the ability to access at a later time. The requirement of accuracy is derived from the Uniform and Federal Rules of Evidence. The requirement of continuing accessibility addresses the issue of technology obsolescence and the need to update and migrate information to developing systems. It is not unlikely that within the span of 5-10 years (a period during which retention of much information is required) a corporation may evolve through one or more generations of technology. More to the point, this technology may be incompatible with each other necessitating the reconversion of information from one system to the other.

For example, certain operating systems from the early 1980's, e.g., memory typewriters, became obsolete with the development of personal computers. The information originally stored on the memory typewriter would need to be converted to the personal computer system in a way meeting the standards for accuracy contemplated by this section. It is also possible that the medium on which the information is stored is less stable. For example, information stored on floppy discs is generally less stable, and subject to a greater threat of disintegration, that information stored on a computer hard drive. In either case, the continuing accessibility issue must be satisfied to validate information stored by electronic means under this section.

This section permits parties to convert original written records to electronic records for retention so long as the requirements of subsection (a) are satisfied. Accordingly, in the absence of specific requirements to retain written records, written records may be destroyed once saved as electronic records satisfying the requirements of this section.

The subsection refers to the information contained in an electronic record, rather than relying on the term electronic record, as a matter of clarity that the critical aspect in retention is the information itself. What information must be retained is determined by the purpose for which the information is needed. If the addressing and pathway information regarding an e-mail is relevant, then that information should also be retained. However if it is the substance of the e-mail that is relevant, only that information need be

retained. Of course, wise record retention would include all such information since what information will be relevant at a later time will not be known.

4. Subsections (b) and (c) simply make clear that certain ancillary information or the use of third parties, does not affect the serviceability of records and information retained electronically. Again, the relevance of particular information will not be known until that information is required at a subsequent time.

5. Subsection (d) continues the theme of the Act as validating electronic records as originals where the law requires retention of an original. The validation of electronic records and electronic information as originals is consistent with the Uniform Rules of Evidence. See Uniform Rules of Evidence 1001(3), 1002, 1003 and 1004.

6. Subsection (e) specifically addresses particular concerns regarding check retention statutes in many jurisdictions. A Report compiled by the Federal Reserve Bank of Boston identifies hundreds of state laws which require the retention or production of original canceled checks. Such requirements preclude banks and their customers from realizing the benefits and efficiencies related to truncation processes otherwise validated under current law. The benefits to banks and their customers from electronic check retention are effectuated by this provision.

7. Subsections (f) and (g) generally address other record retention statutes. As with check retention, all businesses and individuals may realize significant savings from electronic record retention. So long as the standards in Section 12 are satisfied, this section permits all parties to obtain those benefits. As always the government may require records in any medium, however, these subsections require a governmental agency to specifically identify the types of records and requirements that will be imposed.

SECTION 13. ADMISSIBILITY IN EVIDENCE. In a proceeding, evidence of a record or signature may not be excluded solely because it is in electronic form.

Source: UNCITRAL Model Law on Electronic Commerce Article 9.

Comment

Like Section 7, this section prevents the nonrecognition of electronic records and signatures solely on the ground of the media in which information is presented.

Nothing in this section relieves a party from establishing the necessary foundation for the admission of an electronic record. See Uniform Rules of Evidence 1001(3), 1002,1003 and 1004.

SECTION 14. AUTOMATED TRANSACTION. In an automated transaction, the following rules apply:

(1) A contract may be formed by the interaction of electronic agents of the parties, even if no individual was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.

(2) A contract may be formed by the interaction of an electronic agent and an individual, acting on the individual's own behalf or for another person, including by an interaction in which the individual performs actions that the individual is free to refuse to perform and which the individual knows or has reason to know will cause the electronic agent to complete the transaction or performance.

(3) The terms of the contract are determined by the substantive law applicable to it.

Source: UNICTRAL Model Law on Electronic Commerce Article 11.

Comment

1. This section confirms that contracts can be formed by machines functioning as electronic agents for parties to a transaction. It negates any claim that lack of human intent, at the time of contract formation, prevents contract formation. When machines are involved, the requisite intention flows from the programing and use of the machine. As in other cases, these are salutary provisions consistent with the fundamental purpose of the Act to remove barriers to electronic transactions while leaving the substantive law, e.g., law of mistake, law of contract formation, unaffected to the greatest extent possible.

2. The process in paragraph (2) validates an anonymous click-through transaction. It is possible that an anonymous click-through process may simply result in no recognizable legal relationship, e.g., A goes to a person's website and acquires access without in any way identifying herself, or otherwise indicating agreement or assent to any limitation or obligation, and the owner's site grants A access. In such a case no legal relationship has been created.

On the other hand it may be possible that A's actions indicate agreement to a particular term. For example, A goes to a website and is confronted by an initial screen which advises her that the information at this site is proprietary, that A may use the information for her own personal purposes, but that, by clicking below, A agrees that any other use without the site owner's permission is prohibited. If A clicks "agree" and downloads the information and then uses the information for other, prohibited purposes, should not A be bound by the click? It seems the answer properly should be, and would be, yes.

If the owner can show that the only way A could have obtained the information was from his website, and that the process to access the subject information required that A must have clicked the "I agree" button after having the ability to see the conditions on use, A has performed actions which A was free to refuse, which A knew would cause the site to grant her access, i.e., "complete the transaction." The terms of the resulting contract will be determined under general contract principles, but will include the limitation on A's use of the information, as a condition precedent to granting her access to the information.

3. In the transaction set forth in Comment 2, the record of the transaction also will include an electronic signature. By clicking "I agree" A adopted a process with the intent to "sign," i.e., bind herself to a legal obligation, the resulting record of the transaction. If

a "signed writing" were required under otherwise applicable law, this transaction would be enforceable. If a "signed writing" were not required, it may be sufficient to establish that the electronic record is attributable to A under Section 9. Attribution may be shown in any manner reasonable including showing that, of necessity, A could only have gotten the information through the process at the website.

SECTION 15. TIME AND PLACE OF SENDING AND RECEIPT.

(a) Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

(1) is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(2) is in a form capable of being processed by that system; and

(3) enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

(b) Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

(1) it enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(2) it is in a form capable of being processed by that system.

(c) Subsection (b) applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under subsection (d).

(d) Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this subsection, the following rules apply:

(1) If the sender or recipient has more than one place of business, the place of business of that person is the place having the closest relationship to the underlying transaction.

(2) If the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as the case may be.

(e) An electronic record is received under subsection (b) even if no individual is aware of its receipt.

(f) Receipt of an electronic acknowledgment from an information processing system described in subsection (b) establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

(g) If a person is aware that an electronic record purportedly sent under subsection (a), or purportedly received under subsection (b), was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection may not be varied by agreement.

Source: UNCITRAL Model Law on Electronic Commerce Article 15.

Comment

1. This section provides default rules regarding when and from where an electronic record is sent and when and where an electronic record is received. This section does not address the efficacy of the record that is sent or received. That is, whether a record is unintelligible or unusable by a recipient is a separate issue from whether that record was sent or received. The effectiveness of an illegible record, whether it binds any party, are questions left to other law.

2. Subsection (a) furnishes rules for determining when an electronic record is sent. The effect of the sending and its import are determined by other law once it is determined that a sending has occurred.

In order to have a proper sending, the subsection requires that information be properly addressed or otherwise directed to the recipient. In order to send within the meaning of this section, there must be specific information which will direct the record to the intended recipient. Although mass electronic sending is not precluded, a general

broadcast message, sent to systems rather than individuals, would not suffice as a sending.

The record will be considered sent once it leaves the control of the sender, or comes under the control of the recipient. Records sent through e-mail or the internet will pass through many different server systems. Accordingly, the critical element when more than one system is involved is the loss of control by the sender.

However, the structure of many message delivery systems is such that electronic records may actually never leave the control of the sender. For example, within a university or corporate setting, e-mail sent within the system to another faculty member is technically not out of the sender's control since it never leaves the organization's server. Accordingly, to qualify as a sending, the e-mail must arrive at a point where the recipient has control. This section does not address the effect of an electronic record that is thereafter "pulled back," e.g., removed from a mailbox. The analog in the paper world would be removing a letter from a person's mailbox. As in the case of providing information electronically under Section 8, the recipient's ability to receive a message should be judged from the perspective of whether the sender has done any action which would preclude retrieval. This is especially the case in regard to sending, since the sender must direct the record to a system designated or used by the recipient.

3. Subsection (b) provides simply that when a record enters the system which the recipient has designated or uses and to which it has access, in a form capable of being processed by that system, it is received. Keying receipt to a system accessible by the recipient removes the potential for a recipient leaving messages with a server or other service in order to avoid receipt. However, the section does not resolve the issue of how the sender proves the time of receipt.

To assure that the recipient retains control of the place of receipt, subsection (b) requires that the system be specified or used by the recipient, and that the system be used or designated for the type of record being sent. Many people have multiple e-mail addresses for different purposes. Subsection (b) assures that recipients can designate the e-mail address or system to be used in a particular transaction. For example, the recipient retains the ability to designate a home e-mail for personal matters, work e-mail for official

business, or a separate organizational e-mail solely for the business purposes of that organization. If A sends B a notice at his home which relates to business, it may not be deemed received if B designated his business address as the sole address for business purposes. Whether actual knowledge upon seeing it at home would qualify as receipt is determined under the otherwise applicable substantive law.

4. Subsections (c) and (d) provide default rules for determining where a record will be considered to have been sent or received. The focus is on the place of business of the recipient and not the physical location of the information processing system, which may bear absolutely no relation to the transaction between the parties. It is not uncommon for users of electronic commerce to communicate from one State to another without knowing the location of information systems through which communication is operated. In addition, the location of certain communication systems may change without either of the parties being aware of the change. Accordingly, where the place of sending or receipt is an issue under other applicable law, e.g., conflict of laws issues, tax issues, the relevant location should be the location of the sender or recipient and not the location of the information processing system.

Subsection (d) assures individual flexibility in designating the place from which a record will be considered sent or at which a record will be considered received. Under subsection (d) a person may designate the place of sending or receipt unilaterally in an electronic record. This ability, as with the ability to designate by agreement, may be limited by otherwise applicable law to places having a reasonable relationship to the transaction.

5. Subsection (e) makes clear that receipt is not dependent on a person having notice that the record is in the person's system. Receipt occurs when the record reaches the designated system whether or not the recipient ever retrieves the record. The paper analog is the recipient who never reads a mail notice.

6. Subsection (f) provides legal certainty regarding the effect of an electronic acknowledgment. It only addresses the fact of receipt, not the quality of the content, nor whether the electronic record was read or "opened."

7. Subsection (g) limits the parties' ability to vary the method for sending and receipt provided in subsections (a) and (b), when there is a legal requirement for the sending or receipt. As in other circumstances where legal requirements derive from other substantive law, to the extent that the other law permits variation by agreement, this Act does not impose any additional requirements, and provisions of this Act may be varied to the extent provided in the other law.

SECTION 16. TRANSFERABLE RECORDS.

(a) In this section, "transferable record" means an electronic record that:

(1) would be a note under [Article 3 of the Uniform Commercial Code] or a document under [Article 7 of the Uniform Commercial Code] if the electronic record were in writing; and

(2) the issuer of the electronic record expressly has agreed is a transferable record.

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

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

(1) a single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (4), (5), and (6), unalterable;

(2) the authoritative copy identifies the person asserting control as:

(A) the person to which the transferable record was issued; or

(B) if the authoritative copy indicates that the transferable record has been transferred, the person to which the transferable record was most recently transferred;

(3) the authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(4) copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(5) each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(6) any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

(d) Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in [Section 1-201(20) of the Uniform Commercial Code], of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under [the Uniform Commercial Code], including, if the applicable statutory requirements under [Section 3-302(a), 7-501, or 9-308 of the Uniform Commercial Code] are satisfied, the rights and defenses of a holder in due course, a holder to which a negotiable document of title has been duly negotiated, or a purchaser, respectively. Delivery, possession, and indorsement are not required to obtain or exercise any of the rights under this subsection.

(e) Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under [the Uniform Commercial Code].

(f) If requested by a person against which enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that the person is in control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

Source: Revised Article 9, Section 9-105.

Comment

1. Paper negotiable instruments and documents are unique in the fact that a tangible token - a piece of paper - actually embodies intangible rights and obligations. The extreme difficulty of creating a unique electronic token which embodies the singular attributes of a paper negotiable document or instrument dictates that the rules relating to negotiable documents and instruments not be simply amended to allow the use of an electronic record for the requisite paper writing. However, the desirability of establishing rules by which business parties might be able to acquire some of the benefits of negotiability in an electronic environment is recognized by the inclusion of this section on Transferable Records.

This section provides legal support for the creation, transferability and enforceability of electronic note and document equivalents, as against the issuer/obligor. The certainty created by the section provides the requisite incentive for industry to develop the systems and processes, which involve significant expenditures of time and resources, to enable the use of such electronic documents.

The importance of facilitating the development of systems which will permit electronic equivalents is a function of cost, efficiency and safety for the records. The storage cost and space needed for the billions of paper notes and documents is phenomenal. Further, natural disasters can wreak havoc on the ability to meet legal requirements for retaining, retrieving and delivering paper instruments. The development of electronic systems meeting the rigorous standards of this section will permit retention of copies which reflect the same integrity as the original. As a result storage, transmission and other costs will be reduced, while security and the ability to satisfy legal requirements governing such paper records will be enhanced.

Section 16 provides for the creation of an electronic record which may be controlled by the holder, who in turn may obtain the benefits of holder in due course and good faith purchaser status. If the benefits and efficiencies of electronic media are to be realized in this industry it is essential to establish a means by which transactions involving paper promissory notes may be accomplished completely electronically. Particularly as other aspects of such transactions are accomplished electronically, the drag on the transaction of requiring a paper note becomes evident. In addition to alleviating the logistical problems of generating, storing and retrieving paper, the mailing and transmission costs associated with such transactions will also be reduced.

2. The definition of transferable record is limited in two significant ways. First, only the equivalent of paper promissory notes and paper documents of title can be created as transferable records. Notes and Documents of Title do not impact the broad systems that relate to the broader payments mechanisms related, for example, to checks. Impacting the check collection system by allowing for "electronic checks" has ramifications well beyond the ability of this Act to address. Accordingly, this Act excludes from its scope transactions governed by UCC Articles 3 and 4. The limitation to promissory note

equivalents in Section 16 is quite important in that regard because of the ability to deal with many enforcement issues by contract without affecting such systemic concerns.

Second, not only is Section 16 limited to electronic records which would qualify as negotiable promissory notes or documents if they were in writing, but the issuer of the electronic record must expressly agree that the electronic record is to be considered a transferable record. The definition of transferable record as "an electronic record that...the issuer of the electronic record expressly has agreed is a transferable record" indicates that the electronic record itself will likely set forth the issuer's agreement, though it may be argued that a contemporaneous electronic or written record might set forth the issuer's agreement. However, conversion of a paper note issued as such would not be possible because the issuer would not be the issuer, in such a case, of an electronic record. The purpose of such a restriction is to assure that transferable records can only be created at the time of issuance by the obligor. The possibility that a paper note might be converted to an electronic record and then intentionally destroyed, and the effect of such action, was not intended to be covered by Section 16.

The requirement that the obligor expressly agree in the electronic record to its treatment as a transferable record does not otherwise affect the characterization of a transferable record (i.e., does not affect what would be a paper note) because it is a statutory condition. Further, it does not obligate the issuer to undertake to do any other act than the payment of the obligation evidenced by the transferable record. Therefore, it does not make the transferable record "conditional" within the meaning of Section 3-104(a)(3) of the Uniform Commercial Code.

3. Under Section 16 acquisition of "control" over an electronic record serves as a substitute for "possession" in the paper analog. More precisely, "control" under Section 16 serves as the substitute for delivery, indorsement and possession of a negotiable promissory note or negotiable document of title. Section 16(b) allows control to be found so long as "a system employed for evidencing the transfer of interests in the transferable record reliably establishes [the person claiming control] as the person to which the transferable record was issued or transferred." The key point is that a system, whether involving third party registry or technological safeguards, must be shown to reliably establish the identity of *the* person entitled to payment. Section 16(c) then sets forth a safe harbor list of very strict requirements for such a system. The specific provisions listed in Section 16(c) are derived from Section 105 of Revised Article 9 of the Uniform Commercial Code. Generally, the transferable record must be unique, identifiable, and

except as specifically permitted, unalterable. That "authoritative copy" must (i) identify the person claiming control as the person to whom the record was issued or most recently transferred, (ii) be maintained by the person claiming control or its designee, and (iii) be unalterable except with the permission of the person claiming control. In addition any copy of the authoritative copy must be readily identifiable as a copy and all revisions must be readily identifiable as authorized or unauthorized.

The control requirements may be satisfied through the use of a trusted third party registry system. Such systems are currently in place with regard to the transfer of securities entitlements under Article 8 of the Uniform Commercial Code, and in the transfer of cotton warehouse receipts under the program sponsored by the United States Department of Agriculture. This Act would recognize the use of such a system so long as the standards of subsection (c) were satisfied. In addition, a technological system which met such exacting standards would also be permitted under Section 16.

For example, a borrower signs an electronic record which would be a promissory note or document if it were paper. The borrower specifically agrees in the electronic record that it will qualify as a transferable record under this section. The lender implements a newly developed technological system which dates, encrypts, and stores all the electronic information in the transferable record in a manner which lender can demonstrate reliably establishes lender as the person to which the transferable record was issued. In the alternative, the lender may contract with a third party to act as a registry for all such transferable records, retaining records establishing the party to whom the record was issued and all subsequent transfers of the record. An example of this latter method for assuring control is the system established for the issuance and transfer of electronic cotton warehouse receipts under 7 C.F.R. section 735 et seq.

Of greatest importance in the system used is the ability to securely and demonstrably be able to transfer the record to others in a manner which assures that only one "holder" exists. The need for such certainty and security resulted in the very stringent standards for a system outlined in subsection (c). A system relying on a third party registry is likely the most effective way to satisfy the requirements of subsection (c) that the transferable record remain unique, identifiable and unalterable, while also providing the means to assure that the transferee is clearly noted and identified.

It must be remembered that Section 16 was drafted in order to provide sufficient legal certainty regarding the rights of those in control of such electronic records, that legal incentives would exist to warrant the development of systems which would establish the requisite control. During the drafting of Section 16, representatives from the Federal Reserve carefully scrutinized the impact of any electronicization of any aspect of the national payment system. Section 16 represents a compromise position which, as noted, serves as a bridge pending more detailed study and consideration of what legal changes, if any, are necessary or appropriate in the context of the payment systems impacted. Accordingly, Section 16 provides limited scope for the attainment of important rights derived from the concept of negotiability, in order to permit the development of systems which will satisfy its strict requirements for control.

4. It is important to note what the section does not provide. Issues related to enforceability against intermediate transferees and transferors (i.e., indorser liability under a paper note), warranty liability that would attach in a paper note, and issues of the effect of taking a transferable record on the underlying obligation, are NOT addressed by this section. Such matters must be addressed, if at all, by contract between and among the parties in the chain of transmission and transfer of the transferable record. In the event that such matters are not addressed by the contract, the issues would need to be resolved under otherwise applicable law. Other law may include general contract principles of assignment and assumption, or may include rules from Article 3 of the Uniform Commercial Code applied by analogy.

For example, Issuer agrees to pay a debt by means of a transferable record issued to A. Unless there is agreement between issuer and A that the transferable record "suspends" the underlying obligation (see Section 3-310 of the Uniform Commercial Code), A would not be prevented from enforcing the underlying obligation without the transferable record. Similarly, if A transfers the transferable record to B by means granting B control, B may obtain holder in due course rights against the obligor/issuer, but B's recourse against A would not be clear unless A agreed to remain liable under the transferable record. Although the rules of Article 3 may be applied by analogy in an appropriate context, in the absence of an express agreement in the transferable record or included by applicable system rules, the liability of the transferor would not be clear.

5. Current business models exist which rely for their efficacy on the benefits of negotiability. A principal example, and one which informed much of the development of Section 16, involves the mortgage backed securities industry. Aggregators of commercial

paper acquire mortgage secured promissory notes following a chain of transfers beginning with the origination of the mortgage loan by a mortgage broker. In the course of the transfers of this paper, buyers of the notes and lenders/secured parties for these buyers will intervene. For the ultimate purchaser of the paper, the ability to rely on holder in due course and good faith purchaser status creates the legal security necessary to issue its own investment securities which are backed by the obligations evidenced by the notes purchased. Only through their HIDC status can these purchasers be assured that third party claims will be barred. Only through their HIDC status can the end purchaser avoid the incredible burden of requiring and assuring that each person in the chain of transfer has waived any and all defenses to performance which may be created during the chain of transfer.

6. This section is a stand-alone provision. Although references are made to specific provisions in Article 3, Article 7, and Article 9 of the Uniform Commercial Code, these provisions are incorporated into this Act and made the applicable rules for purposes of this Act. The rights of parties to transferable records are established under subsections (d) and (e). Subsection (d) provides rules for determining the rights of a party in control of a transferable record. The subsection makes clear that the rights are determined under this section, and not under other law, by incorporating the rules on the manner of acquisition into this statute. The last sentence of subsection (d) is intended to assure that requirements related to notions of possession, which are inherently inconsistent with the idea of an electronic record, are not incorporated into this statute.

If a person establishes control, Section 16(d) provides that that person is the "holder" of the transferable record which is equivalent to a holder of an analogous paper negotiable instrument. More importantly, if the person acquired control in a manner which would make it a holder in due course of an equivalent paper record, the person acquires the rights of a HIDC. The person in control would therefore be able to enforce the transferable record against the obligor regardless of intervening claims and defenses. However, by pulling these rights into Section 16, this Act does NOT validate the wholesale electrification of promissory notes under Article 3 of the Uniform Commercial Code.

Further, it is important to understand that a transferable record under Section 16, while having no counterpart under Article 3 of the Uniform Commercial Code, would be an "account," "general intangible," or "payment intangible" under Article 9 of the Uniform Commercial Code. Accordingly, two separate bodies of law would apply to that asset of

the obligee. A taker of the transferable record under Section 16 may acquire purchaser rights under Article 9 of the Uniform Commercial Code, however, those rights may be defeated by a trustee in bankruptcy of a prior person in control unless perfection under Article 9 of the Uniform Commercial Code by filing is achieved. If the person in control also takes control in a manner granting it holder in due course status, of course that person would take free of any claim by a bankruptcy trustee or lien creditor.

7. Subsection (e) accords to the obligor of the transferable record rights equal to those of an obligor under an equivalent paper record. Accordingly, unless a waiver of defense clause is obtained in the electronic record, or the transferee obtains HDC rights under subsection (d), the obligor has all the rights and defenses available to it under a contract assignment. Additionally, the obligor has the right to have the payment noted or otherwise included as part of the electronic record.

8. Subsection (f) grants the obligor the right to have the transferable record and other information made available for purposes of assuring the correct person to pay. This will allow the obligor to protect its interest and obtain the defense of discharge by payment or performance. This is particularly important because a person receiving subsequent control under the appropriate circumstances may well qualify as a holder in course who can enforce payment of the transferable record.

9. Section 16 is a singular exception to the thrust of this Act to simply validate electronic media used in commercial transactions. Section 16 actually provides a means for expanding electronic commerce. It provides certainty to lenders and investors regarding the enforceability of a new class of financial services. It is hoped that the legal protections afforded by Section 16 will engender the development of technological and business models which will permit realization of the significant cost savings and efficiencies available through electronic transacting in the financial services industry. Although only a bridge to more detailed consideration of the broad issues related to negotiability in an electronic context, Section 16 provides the impetus for that broader consideration while allowing continuation of developing technological and business models.

[**SECTION 17. CREATION AND RETENTION OF ELECTRONIC RECORDS AND CONVERSION OF WRITTEN RECORDS BY GOVERNMENTAL AGENCIES.** [Each governmental agency] [The [designated state officer]] of this State shall determine whether, and the extent to which, [it] [a governmental agency] will create and retain electronic records and convert written records to electronic records.]

Comment

See Comments following Section 19.

[**SECTION 18. ACCEPTANCE AND DISTRIBUTION OF ELECTRONIC RECORDS BY GOVERNMENTAL AGENCIES.**

(a) Except as otherwise provided in Section 12(f), [each governmental agency] [the [designated state officer]] of this State shall determine whether, and the extent to which, [it] [a governmental agency] will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use, and rely upon electronic records and electronic signatures.

(b) To the extent that a governmental agency uses electronic records and electronic signatures under subsection (a), the [governmental agency] [designated state officer], giving due consideration to security, may specify:

(1) the manner and format in which the electronic records must be created, generated, sent, communicated, received, and stored and the systems established for those purposes;

(2) if electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;

(3) control processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality, and auditability of electronic records; and

(4) any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

(c) Except as otherwise provided in Section 12(f), this [Act] does not require a governmental agency of this State to use or permit the use of electronic records or electronic signatures.]

Source: Illinois Act Section 25-101; Florida Electronic Signature Act, Chapter 96-324, Section 7 (1996).

Comment

See Comments following Section 19.

[**SECTION 19. INTEROPERABILITY.** The [governmental agency] [designated officer] of this State which adopts standards pursuant to Section 18 may encourage and promote consistency and interoperability with similar requirements adopted by other governmental agencies of this and other States and the federal government and nongovernmental persons interacting with governmental agencies of this State. If appropriate, those standards may specify differing levels of standards from which governmental agencies of this State may choose in implementing the most appropriate standard for a particular application.]

Source: Illinois Act Section 25-115.

See Legislative Note below - Following Comments.

Comment

1. Sections 17-19 have been bracketed as optional provisions to be considered for adoption by each State. Among the barriers to electronic commerce are barriers which exist in the use of electronic media by state governmental agencies - whether among themselves or in external dealing with the private sector. In those circumstances where the government acts as a commercial party, e.g., in areas of procurement, the general validation provisions of this Act will apply. That is to say, the government must agree to conduct transactions electronically with vendors and customers of government services.

However, there are other circumstances when government ought to establish the ability to proceed in transactions electronically. Whether in regard to records and communications within and between governmental agencies, or with respect to information and filings which must be made with governmental agencies, these sections allow a State to establish the ground work for such electronicization.

2. The provisions in Sections 17-19 are broad and very general. In many States they will be unnecessary because enacted legislation designed to facilitate governmental use of electronic records and communications is in place. However, in many States broad validating rules are needed and desired. Accordingly, this Act provides these sections as a baseline.

Of paramount importance in all States however, is the need for States to assure that whatever systems and rules are adopted, the systems established are compatible with the systems of other governmental agencies and with common systems in the private sector. A very real risk exists that implementation of systems by myriad governmental agencies and offices may create barriers because of a failure to consider compatibility, than would be the case otherwise.

3. The provisions in Section 17-19 are broad and general to provide the greatest flexibility and adaptation to the specific needs of the individual States. The differences and variations in the organization and structure of governmental agencies mandates this approach. However, it is imperative that each State always keep in mind the need to prevent the erection of barriers through appropriate coordination of systems and rules within the parameters set by the State.

4. Section 17 authorizes state agencies to use electronic records and electronic signatures generally for intra-governmental purposes, and to convert written records and manual signatures to electronic records and electronic signatures. By its terms the section gives enacting legislatures the option to leave the decision to use electronic records or convert written records and signatures to the governmental agency or assign that duty to a designated state officer. It also authorizes the destruction of written records after conversion to electronic form.

5. Section 18 broadly authorizes state agencies to send and receive electronic records and signatures in dealing with non-governmental persons. Again, the provision is permissive and not obligatory (see subsection (c)). However, it does provide specifically that with respect to electronic records used for evidentiary purposes, Section 12 will apply unless a particular agency expressly opts out.

6. Section 19 is the most important section of the three. It requires governmental agencies or state officers to take account of consistency in applications and interoperability to the extent practicable when promulgating standards. This section is critical in addressing the concern that inconsistent applications may promote barriers greater than currently exist. Without such direction the myriad systems that could develop independently would be new barriers to electronic commerce, not a removal of barriers. The key to interoperability is flexibility and adaptability. The requirement of a single system may be as big a barrier as the proliferation of many disparate systems.

Legislative Note Regarding Adoption of Sections 17-19

1. Sections 17-19 are optional sections for consideration by individual legislatures for adoption, and have been bracketed to make this clear. The inclusion or exclusion of Sections 17-19 will not have a detrimental impact on the uniformity of adoption of this Act, so long as Sections 1-16 are adopted uniformly as presented. In some States Sections 17-19 will be unnecessary because legislation is already in place to authorize and implement government use of electronic media. However, the general authorization provided by Sections 17-19 may be critical in some States which desire to move forward in this area.

2. In the event that a state legislature chooses to adopt Sections 17-19, a number of issues must be addressed:

A. Is the general authorization to adopt electronic media, provided by Sections 17-19 sufficient for the needs of the particular jurisdiction, or is more detailed and specific authorization necessary? This determination may be affected by the decision regarding the appropriate entity or person to oversee implementation of the use of electronic media (See next paragraph). Sections 17-19 are broad and general in the authorization granted. Certainly greater specificity can be added subsequent to adoption of these sections. The question for the legislature is whether greater direction and specificity is needed at this time. If so, the legislature should not enact Sections 17-19 at this time.

B. Assuming a legislature decides to enact Sections 17-19, what entity or person should oversee implementation of the government's use of electronic media? As noted in each of Sections 17-19, again by brackets, a choice must be made regarding the entity to make critical decisions regarding the systems and rules which will govern the use of electronic media by the State. Each State will need to consider its particular structure and administration in making this determination. However, legislatures are strongly encouraged to make compatibility and interoperability considerations paramount in making this determination.

C. Finally, a decision will have to be made regarding the process by which coordination of electronic systems will occur between the various branches of state government and among the various levels of government within the State. Again this will require consideration of the unique situation in each State.

3. If a State chooses not to enact Sections 17-19, UETA Sections 1-16 will still apply to governmental entities when acting as a "person" engaging in "transactions" within its scope. The definition of transaction includes "governmental affairs." Of course, like any other party, the circumstances surrounding a transaction must indicate that the governmental actor has agreed to act electronically (See Section 5(b)), but otherwise all the provisions of Sections 1-16 will apply to validate the use of electronic records and signatures in transactions involving governmental entities.

If a State does choose to enact Sections 17-19, Sections 1-16 will continue to apply as above. In addition, Sections 17-19 will provide authorization for intra-governmental uses of electronic media. Finally, Sections 17-19 provide a broader authorization for the State

to develop systems and procedures for the use of electronic media in its relations with non-governmental entities and persons.

SECTION 20. SEVERABILITY CLAUSE. If any provision of this [Act] or its application to any person or circumstance is held invalid, the invalidity does not affect other provisions or applications of this [Act] which can be given effect without the invalid provision or application, and to this end the provisions of this [Act] are severable.

SECTION 21. EFFECTIVE DATE. This [Act] takes effect .....

DISCUSSION DRAFT ONLY
SUBJECT TO REVISION

Electronic Signatures in Global and National Commerce Act of 2000:
Effect on State Laws

Raymond T. Nimmer

I. Introduction

In the summer of the year 2000, Congress enacted the Electronic Signatures in Global and National Commerce Act (Federal Act). The Federal Act establishes a national principle that, subject to listed exceptions, electronic signatures and records cannot be denied legal effect solely because they are electronic as compared to being on paper. This paper focuses on the relationship of the Federal Act to state law and, particularly, on the extent to which the Federal Act preempts state law.

Notably, the Federal Act contains no general statement about the scope of its preemption. Rather, the preemptive effect of the Act must be discerned from the terms and scope of the provisions of the Act that specifically invalidate contrary state law, and from the underlying purpose of the statute. As we see below, there are several preemptive rules in Section 101 of the Federal Act and these constitute the relevant essence of the preemption under this statute. Section 102 of the Act, however, allows states to step away from those preemptive effects by following one of two approaches under which they can modify or supersede the effects of Section 101. There is no general preemption of substantive state law, including any law that deals with establishing obligations or attribution to a party.

II. Barriers and Statutory Focus

The Federal Act stems from a broad consensus since at least the mid-1990's that electronic commerce should be promoted. An early U.S. governmental report described the relationship between contract law, e-commerce and that goal in the following terms:

> The challenge for commercial law [is] to adapt to the reality of the NII [National Information Infrastructure] by providing clear guidance as to the rights and responsibilities of those using the NII. Without certainty in electronic contracting, the NII will not fulfill its commercial potential. [Regardless] of the type of transaction, where parties wish to contract electronically, they should be able to form a valid contract on-line. In particular, on-line licenses should be encouraged because they offer efficiency for both licensors and licensees.[1]

[1] Report of the Working Group on Intellectual Property Rights, Intellectual Property and the National Informaton Infrastructure 58-59 (1995).

While there are many other fundamental contract law issues that must be resolved in order to facilitate electronic commerce, many have focused on a perceived need to remove technical *barriers* to electronic commerce. Two goals often dominate the discussion or barriers: 1) prevent burdensome local regulation (*regulation issues*) and 2) establish that electronic technology satisfies traditional requirements associated with paper writings (*technology adequacy issues*).

The Federal Act narrowly focuses on the latter of these two goals. We can see this in Congressional Record statements by primary legislators involved in enactment of the Federal Act.[2] For example, one sponsor commented:

> [This Federal Act] is founded on a simple premise. Any requirement in law that a contract be signed or that a document be in writing can be met by an electronically signed contract or an electronic document. We are simply giving the electronic medium the same legal effect and enforceability as the medium of paper.[3]

The statement of another leading legislative figure in enactment likewise carves out a narrow but important, focused goal for the Federal Act:

> [The Federal Act] will eliminate the single most significant vulnerability of electronic commerce, which is the fear that everything it revolves around - electronic signatures, contracts, and other records - could be rendered invalid solely by virtue of their being in "electronic" form, rather than in a tangible, ink and paper format. This [Act] will literally supply the pavement for the e-commerce lane of the information superhighway.[4]

It is quite clear that the basic rule should be that, except in limited cases, electronic records and signatures should fulfill former legal requirements of a writing so long as the content, timing and the intent underlying these electronics corresponds to other requirements in law.

Section 101(a), the primary substantive provision, corresponds to these statements. It provides:

> Notwithstanding any statute, regulation, or other rule of law … with respect to any transaction in or affecting interstate or foreign commerce:
>
> (1) a signature, contract, or other record relating to such transaction may not be denied legal effect, validity, or enforceability solely because it is in electronic form; and

[2] The Federal Act does not have official commentary or an official explanatory statement by the Conference Committee, but was accompanied by prepared statements in Congress by sponsors and members of the conference committee.

[3] Statement by Representative Bliley, 146 Cong.Rec. H4352 (June 14, 2000).

[4] Statement by Senator Abraham, 146 Cong. Rec. S5223 (June 15, 2000).

(2) a contract relating to such transaction may not be denied legal effect, validity, or enforceability solely because an electronic signature or electronic record was used in its formation.[5]

This language states the basic principle of technology adequacy. That rule and the underlying premise are, indeed, quite simple: law should not deny effect to a signature, record or contract solely because it is electronic.

What we have, then, is a statute directed to eliminating barriers in the form of obstacles e-commerce through rules that prevent a state from denying legal effect to electronics simply because they are electronic in nature. Consistent with that focused goal, Section 101(c) establishes various disclosure and consent standards that apply to consumer protection laws that require disclosure or provision of information in writing to a consumer. These are described as exceptions to the general rule of Section 101(a) (which requires not preconditions to establish application of its basic rule). Whether the consumer disclosure rules are mandatory (e.g., the only method available to use electronic disclosures) is not clear from the statute, but that does not directly bear on preemption as discussed here.

Section 101 contains four additional rules that alter contrary state law. These are:

- Section 101(h): a state cannot deny effect to contracts involving electronic agents solely because of electronic character.
- Section 101(d): certain electronic records meet any rule that requires retention of a record or production of an original.
- Section 101(g): changes rules on use of electronic signatures in notarization and the like.
- Section 101(j): places limits under other law on the liability risk for insurance agents from use of electronic procedures.

In addition, Section 101 contains various rules concerning electronic records and signatures that support, rather than supplant state sovereignty. These include rules that exclude any intended effect on notice or similar requirements, exclude any effect on state or other law creating or excluding obligations, and permit a state to deny effect to an electronic record that was not retainable.[6]

[5] Federal Act § 101. The Act contains a number of exclusions from this principle which, in the interests of space, I will not discuss in this context.

[6] Federal Act § 101(e). Federal Act 101(b) states: "This title does not …limit, alter, or otherwise affect any requirement imposed by a statute, regulation, or rule of law relating to the rights and obligations of persons under such statute, regulation, or rule of law other than a requirement that contracts or other records be written, signed, or in non-electronic form." The Federal Act contains other specific but seemingly redundant rules. For example, it states that its provisions do not alter the required content or timing of any disclosure or other record required to be provided or made available to any consumer under any other law. Similarly, in a consumer context, the Act does not alter a requirement that the record be made available in a form or method that requires verification or acknowledgment of receipt.

III. Preemption

Before Congress adopted the Federal Act, numerous states had adopted rules dealing with electronic records and signatures. Of course, an appropriately enacted and applicable federal statute can preempt contrary state law. On the other hand, federal statutes often coexist with state law on the same subject. While some might argue that the Federal Act preempts all state law other than UETA and several listed exceptions dealing with electronic records and signatures, the Federal Act does not say that. Indeed, it stops far short of widespread preemption.

The issues are two-fold.

- First, what is the scope of preemption to begin with?
- Second, what is the meaning of the rule in Section 102 of the Federal Act that allows certain state laws to modify or supersede Section 101 rules?

1. *Scope of Affirmative Preemption*

Federal law does not preempt state law unless (1) it expressly does so, (2) the state law conflicts with, and will frustrate a clear policy in the federal law, or (3) the federal law precludes state laws in an area because it occupies the entire field..

As I have said, the Federal Act does not contain any statement of preemption of state law, other than in the specifically preemptive rules in Section 101. There is no general statement that preempts other state law. There is a provision (Section 102) that which cuts back on preemption of state law, but that provision reduces preemption, it does not create independent preemptive effect. I discuss that rule below.

There is clearly no effort in the Federal Act to fully occupy the field in a way the precludes all other state action. Statutes that seek this effect, such as the federal Bankruptcy Code, are typically far more extensive in their coverage of topics within the field. Instead, the Federal Act, by its language and content, is a narrow statute that does not occupy the entire field concerning the legal efficacy of electronic records. The statutory rules are premised generally on the simple policy premise that any "requirement in law that a contract be signed or that a document be in writing can be met by an electronically signed contract or an electronic document."[7] State laws that conflict with or frustrate *that* policy and that are not authorized by the Federal Act itself are preempted.

Consistent with this policy focus, the primary mandatory (preemptive) rules deal with altering existing legal requirements (and preventing future requirements) that hinge the validity of a record or signature on the existence (or non-existence) of a writing. For these, the Act forbids any law that *denies effect* to electronics *solely* because they are electronic except as allowed in the Act itself.[8] This preserves state choices, but leaves no room to impose restrictions on the fundamental *technology adequacy* rule.

[7] For purposes of this statement, I ignore the treatment of insurance agent liability in Section 101.
[8] Obviously, a similarly preclusive effect arises for the other mandatory rules.

To understand the scope of preemption, consider several hypothetical state laws:

No Writing Required. *A state law provides that no writing of any type is required to form a particular contract or give a particular notice.*

The Federal Act does not apply since Section 101 concerns only state (or federal) laws that require writings. That same result governs for the disclosure and consent procedures with respect to consumers in cases where consumer protection law does not require disclosures or notices in writing. The Federal Act consumer rules only apply when a law requires information to be in a writing. They do not prevent a state from deciding that no writing is required.

Law Equates Electronics with Writings: *A state law provides that a statute of frauds rule can be met by either a signed writing or an authenticated electronic record*.

Does the Federal Act preempt? No. This law does not trigger Section 101 because it does not deny enforceability solely because the record or contract is electronic and does not require a writing or a written signature. Indeed, the state law has the opposite effect. This result is not affected by, and has no relationship to, the so-called back-in rule in Section 102 which, as discussed later, allows states to reassert control over electronics as satisfying writing requirements in some cases.

Mandatory Digital Signature Law: *A state law provides that electronic records and signatures will be recognized only if they use a particular, designated technology*.

This is a "mandatory digital signature law." Is that law preempted? Yes. By validating *only* one type of electronic record or signature *and* denying all other electronic records, it denies effect to the other electronics *solely* because they are electronic. Section 101(a) bans that. The result is that electronics using the designated technology and electronics using any other technology are enforceable under law as altered by the Federal Act.

Optional Digital Signature Law (Secure Signatures): *A state law provides that, if the parties opt to use a specific technology, the results of using that technology 1) satisfy the signature and the writing requirement, and 2) create a presumption that the party identified by the technology was the party actually using it.*

This is an "optional law" since it does not preclude use of other electronics or require parties to use on method. This approach describes most modern secure signature or digital signature statutes. Does the Federal Act preempt such statutes? No, but it does change part of the framework in which this law applies.

The Federal Act does not deal with state law on when or whether a signature or record is *attributed* to a person and does not deal with state laws that determine whether obligations exist that are chargeable to a person. Indeed, the Federal Act expressly

excludes any change in the law on rights or obligations of persons under other law.[9] That rule clearly preserves the second part of the hypothetical law stated above. Even without that rule, attribution, obligations and the like are not covered by the Federal Act. A statute does not preempt rules outside its coverage unless the Act specifically so provides or purports to entirely dominate the entire field. The Federal Act does not do so. The only way to argue for a different result under the Act would be to argue that the Federal Act rule that on its face merely bars state laws that invalidate electronic records actually contains an implied invalidation or policy that invalidates any state law that gives enhanced effect to certain technologies the Federal Act itself does not establish. But that ignores preemption jurisprudence and the simple purpose of the Federal Act: to validate electronics. It attempts to read in preemptive coverage of a topic that the Act specifically does not address.

However, the Federal Act does supplant rules that deny enforcement of electronic records solely because they are electronic. Thus, in our "optional digital signature" illustration, the Federal Act converts any underlying state statute of frauds into a rule that requires a writing *or* an electronic record. This precludes any part of the hypothetical statute that implicitly gave effect *only* to signatures or records created with a particular technology. It renders the first statement in the hypothetical (which validates the electronics) irrelevant. The result: electronic and written records are equivalent, but procedures recognized in state law which give presumptions to users of particular procedures are not disturbed.

2. *The "Back in" Rule.*

Section 102 of the Federal Act, entitled "exemption to preemption," contains a curious rule which I will describe as a "back-in rule" because its effect is to allow states back into the business of determining when or whether electronics satisfy requirements of a writing. The section reads as follows:

> (a) …. A State [law] may modify, limit, or supersede … section 101 with respect to State law only if such [law]:
>
> (1) [enacts UETA] as approved … by the National Conference of Commissioners on Uniform State Laws in 1999, except that any exception to the scope of [UETA is] preempted to the extent such exception is inconsistent with this title … or would not be permitted under paragraph (2)(A)(ii) of this subsection; **or**
>
> (2)(A) specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures to establish the legal effect, validity, or enforceability of contracts or other records, if—
>
> (i) such alternative procedures or requirements are consistent with this [Act]; and

[9] Federal Act § 101(b)(1).

(ii) such alternative procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology …; and

(B) if enacted or adopted after the date of the enactment of this Act, makes specific reference to this Act.[10]

This language is curious because it implies that state law can modify federal law.[11] That is never true. Also, it is curious because some read into it a broad, preemptive policy that this section simply do not address.

On its face, Section 102 simply states that a state can "modify, limit, or supersede Section 101" in one of two ways. Before jumping to the ways this can be done, a focus on the language of the rule itself is needed: a state may modify, limit or supersede *provisions of Section 101*. This rule only applies to changing (or superseding) the effect of Section 101, but many of the rules of Section 101 in themselves permit state law to control. Section 101 contains only a few mandatory rules and has no other mandatory effect.

The rules in Section 102 thus mean that, unless a state enactment meets the conditions in Section 102, it cannot alter the effect of the mandatory Section 101 rules. Thus, a state cannot limit or supersede the rule that precludes a law from denying effect to electronics solely because they are electronic except by complying with one of the options in Section 102. It cannot deny effect to contracts by electronic agents except as permitted by Section 102.

a. Clean Version of UETA

Federal Act Section 102 permits a state to supersede Section 101 by adopting UETA as proposed by the National Conference of Commissioners on Uniform State Laws (NCCUSL) and without changes. The legislative history refers to this as a right to "opt-out" of the federal scheme and replace it with UETA.[12] Enactment of UETA in its pure form supersedes the Federal Act and excludes its impact. To produce that outcome, the enactment must be pure and most likely should express an intent to supersede the Federal Act. Otherwise, the fact that UETA is limited to transactions in which use of electronics is agreed to leaves the Federal Act governing cases where no assent was obtained.

Prior to the Federal Act, a number of states enacted UETA (and a variety of other electronic validation laws), but in many cases the UETA enactment made significant modifications in the statute, ranging from the wholesale changes in California, to relatively minor adjustments, to circumstances where a state adopted attribution rules rejected in UETA.

---

[10] Federal Act § 102(a).

[11] What is meant here apparently is that a state can modify, limit or supersede the effect of Section 101 on transactions in the state.

[12] "The conference report adopts a substitute provision. Section 102 of the conference report provides a conditioned process for States to enact their own statutes, regulations or other rules of law dealing with the use and acceptance of electronic signatures and records and thus opt-out of the federal regime." Statement by Senator Abraham.

These variant statutes do not meet the requirement of a *clean* enactment of UETA and, thus, do not fall within the first standard for modifying the effect of the Federal Act. As the legislative history comments: "Any variation or derivation from the exact UETA document reported and recommended for enactment by NCCUSL shall not qualify under subsection (a)(1). Instead, such efforts and any other effort may or may not be eligible under subsection (a)(2)." This seemingly takes not only the modifications out of the scope of Section 102(a)(1), but the entire enactment, placing it under Section 102(a)(2).[13]

There are many differences between UETA and the Federal Act. Thus, the federal policy regarding UETA does not mean that UETA and the Federal Act are identical. Rather, the federal policy here entails a narrow deference to state sovereignty on matters involving electronic records and signatures. Congress elected to permit adoption of a uniform state law, even though it differs significantly from the Federal Act in important ways. This presents a significant policy choice to the states: a state may rely on the enabling rules of the Federal Act or exclude and replace them by adopting UETA in pure form. To date, no states have considered that choice. As it relates to preemption, however, the choice centers only on modifying, limiting, or superseding Section 101 of the Federal Act. Neither the Federal Act nor UETA preclude other laws that do not conflict with the core validation principles of Section 101.

b. Consistent Other Laws.

The second back-in rule permits states to modify, limit or supersede the terms of Section 101 if the state law specifies the alternative procedures or requirements for the use or acceptance (or both) of electronic records or electronic signatures and:

- the alternative procedures or requirements are *consistent* with the Federal Act;
- do not require, or accord 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; and
- if enacted after enactment of the Federal Act, the statute makes specific reference to the Federal Act.

Of these three conditions, the only clear rule requires that new laws make a specific reference to the Federal Act if they are to modify or supersede the provisions of Section 101.

(i) <u>Technology Neutrality</u>. Section 102(a)(2) disallows any state law that modifies, limits or supersedes Section 101 of the Federal Act by a law that does not maintain technology neutrality, that is, by a law that requires or gives greater legal status or effect to a specific technology. Some may claim that this back-in rule precludes any state law that hinges any

[13] There are two exceptions to this: 1) the Federal Act specifically disallows modifications of the scope of UETA that are not *consistent* with the provisions of the Federal Act scope, and 2) the Federal Act disallows use of the unusual UETA rule on mail delivery as a means to circumvent the policy of the Federal Act that electronics are to be treated as equivalent to paper. In both cases, efforts to do either of these apparently leaves the remainder of a clean UETA enactment intact.

beneficial effect on complying with a particular type of technology, but that seems well beyond the scope of this rule.

The rule only precludes superseding or modifying *Section 101 rules* (e.g., rules that bar invalidation of records or signatures solely because they are electronic and the other Section 101 preemptive rules) with a law that validates a particular technology and not others. The rule of neutrality thus functions within Section 102 as a whole and, as a result, only is relevant with respect to the effects of Section 101.

There is understandable confusion on this issue because the language of Section 102(a)(2) states that it applies only if the alternative state "procedures or requirements do not require, or accord greater legal status or effect to, the implementation or application of a specific technology …" The troublesome language here is the reference to giving "greater legal status" to a specific technology. The uncertainty about this language and the neutrality rule is buttressed by some references in the legislative history of the Federal Act to preventing state laws from "favoring" certain technologies. Thus, the argument goes, the Federal Act precludes and preempts any state law that, through certification or other means, gives enhanced effect to any particular technology whether that effect extends to satisfying a writing or signature requirement, to establishing in law the identity of a party (attribution), to creating or foreclosing obligations on the part of a service provider, or any other issue.

That argument is flawed. A basic principle of statutory interpretation is that the language of the statute and comments made in reference to it must be interpreted in their statutory context. Legislative history cannot rewrite statutory text and statutory text cannot be pulled out of the context in which it is placed in the statute. The statutory context of the neutrality rule is Section 102 and Section 102 only refers to allowing (or disallowing) a state from altering the effect of Section 101. As we have seen, Section 101 does not deal with questions about attribution, obligations, or other substantive rules. It precludes state laws that deny validity to electronics solely because they are electronic or to contracts solely because they are created through electronic agents. In that context, the neutrality rule states simply that a state cannot circumvent the Federal Act by a state law that gives legal validity as supplanting a writing only to electronics executed through a designated technology. A state cannot enact a law that validates *only* a particular type of technology. That is preempted. But the requirement of neutrality on its face goes no further.[14]

This view of the statutory language is fully consistent with comments in the legislative history about not favoring a particular technology. What is precluded is favoring a technology by making it the only one (or one of only several) that fulfills a requirement of a writing or a

[14] A similar interpretations appears appropriate for Section 301 which states a federal position that, internationally, electronic record and signature rules should conform to four stated principles. Describing the type of approaches to be resisted, the legislative history focuses on the German Digital Signature law and German policy characterized as allowing an electronic signature to be valid *only* if it conforms to reglated technology standards. The key fact once again is the mandatory and preclusive nature of the technology requirement. Statement by Senator Abraham, 146 Cong. Rec. S5281-06 (Senate Proceedings and Debate of the 106th Congress, 2d Sess. (June 16, 2000).

signature. But the comments must be read in context of the language and effect of the statute itself. The statement of Senator Abraham puts this in the right context: "[Inclusion] of the 'or accord greater legal status or effect to' is intended to prevent a state from giving a leg-up or impose an additional burden on one technology or technical specification that is not applicable to all others, and is not intended to prevent a state or its subdivisions from developing, establishing, using or certifying a certificate authority system."[15]

Assume the following two hypothetical statutes enacted after the adoption of the Federal Act and specifically referring to it:

> **Statute 1:** "In this state, electronic records and signatures satisfy existing laws requiring a written signature or paper record only if they use "XYZ" technology."
>
> **Statute 2:** "In this state, electronic records and signatures satisfy requirements of a writing or signature. In addition, if the parties choose to use them, signatures that use XYZ technology and certification procedures establish a presumption that they are the records or signatures of the person identified by the technology."

Statute 1 is not technologically neutral. It cannot modify, limit or supersede the federal rule in Section 101 on questions dealt with on a mandatory basis in Section 101. The federal rule continues to over-ride on topics it addresses and a wide range of technologies suffice to meet writing and signature requirements.

Statute 2 is technology neutral on questions addressed in Section 101 of the Federal Act (see the first sentence of the statute). Indeed, on questions about the adequacy of electronics, this statute arguably precludes any application of the Section 101 rules that apply only if a law otherwise *requires* a writing or a written signature. Under the first sentence, state law no longer requires a writing. Statute 2, however, also goes beyond adequacy and other Section 101 issues, and establishes a presumption about the attribution of a signature or message. The Federal Act does not deal with this issue. So long as the attribution rule does not modify the basic rule in Section 101, the Federal Act does not apply. That aspect of Statute 2 is not affected by Section 102, nor is it affected by enactment of UETA.

(ii) Consistency. The third condition requires that, in order to limit, modify or supersede the effect of Section 101, the state law must be *consistent* with the Federal Act. The legislative history gives no guidance on what is meant by "consistent."

The provision clearly allows state laws substantively identical to the Federal Act. Thus, a state might supersede Section 101 by adopting the federal provisions in full as state law. This would allow state courts to rule on the relevant issues and return the subject matter to state law control. Of course, a clean UETA enactment can supersede Section 101 of the Federal Act even though UETA is not consistent with it on many issues, but that is under a separate rule.

[15] 146 Cong.Rec. S5281-06.

A state law can be "consistent" with the Federal Act if it is identical to the Federal Act on issues covered in the federal law, but also deals with additional issues (e.g., attribution, timing of notice, etc.) or with issues permitted by the Federal Act to be handled as a matter of state law (assuming that it does so in a manner that does not conflict with the Federal Act).

Arguably, a state law may be consistent with the Federal Act if it is "substantively identical" to the Act. If, however, the idea of consistency goes beyond that it means "substantively identical" on issues covered by the Federal Act, we will be open to a large array of uncertainty and litigation.

Throughout, it is important to recognize that the rule requires consistency with the Federal Act. It does not refer to state laws "consistent" with UETA. While the Federal Act allows a clean UETA to supersede the provisions of Section 101, both the statutory language and the legislative comments indicate that a modified UETA enactment is judged under a standard of consistency with the Federal Act, not whether the modification is consistent with the official UETA draft.

IV. Summary

The Federal Act sets a strong basis for eliminating the issues encountered in rationalizing the idea of *electronic* commerce with laws centered on and developed for paper commerce. The Act is "founded on a simple premise. Any requirement in law that a contract be signed or that a document be in writing can be met by an electronically signed contract or an electronic document. We are simply giving the electronic medium the same legal effect and enforceability as the medium of paper." This policy, along with the preemptive rules of Section 101, sets parameters of federal preemption. As a basic principle, except as such preconditions are permitted in the Act, the Federal Act only precludes state laws that place mandatory conditions on the adequacy of electronics to meet existing writing requirements or that conflict with the other preemptive rules of Section 101.

Introduction
Information Technology
Security Guidelines
NSHE Security Interest Group

Overview
The NSHE SIG guidelines are intended to assist member institutions with the application of current NSHE program policy. The guidelines are not policies in themselves; they are recommendations concerning the application of technical and other controls.

Effective security is a team effort involving the participation and support of all member institutions. All NSHE employees, students, and institutional affiliates have the potential to negatively affect the security, functionality and integrity of NSHE computing and network resources. These guideline documents can define shared goals and guide in the efficient application of limited technical/security staff time and resources. The SIG intends that these guidelines will result in improved levels of security and efficiency for all NSHE institutions.

Scope
These guidelines are intended to be consistent with existing NSHE system-wide program policy. Institutions should use these general guidelines to assist in the production of baselines, minimum standards, documentation, training plans, checklists, and procedures tailored to the needs of the individual institutions.

These guidelines should apply to all employees, students, guests, visitors, consultants, temporaries, and other workers at the member institutions, including all personnel affiliated with third parties (e.g., contractors and subcontractors). These recommendations also apply to all equipment used by NSHE or NSHE member institutions, and apply to any equipment connected to an NSHE network. Certain sensitive or critical systems may be covered by program-specific or system-specific policies and procedures, may be affected by contractual obligations, or may be covered by state or federal legislation that mandates stricter or more extensive controls than are detailed in these guidelines.

Audience
The bulk of the recommendations in these guidelines are directed at institutional information security staff, and system and network administrators. The guidelines also contain recommendations for end-users.

Related Documents
See the NSHE Computing Resource Policy and the NevadaNet policies for details on appropriate usage of computing equipment and NSHE networks. Also see the appropriate related institutional policies and procedures.

Exceptions
For technical or other reasons, institutions may support systems or networks that substantially deviate from best practice. Institutions should develop documented procedures for reviewing, documenting, and managing these situations.

Training and Security Awareness
Institutions should develop communication, training, and security awareness programs or procedures tailored to their needs and constituencies. For example, staff members who have privileged system access or who have access to sensitive or confidential information should be reminded of their responsibilities regarding the special access they have. All account holders and NevadaNet users should be aware of NSHE and NevadaNet policy and of their responsibilities as end users.

Review
These guidelines are written and approved by members of the NSHE Security Interest Group. The guidelines strongly reflect industry best practice and also reflect a strong consensus among the NSHE SIG group members.

Teams of volunteers from the NSHE Security Interest Group write these guidelines. Each team consists of, at a minimum, a lead author, an editor, and at least one technical reviewer. Once the team has composed a draft, the team forwards it to the SIG for review and revision.

Endorsement
Each institutional Chief Technical Officer will designate a representative to review and endorse the guidelines. These representatives vote on the guidelines via email. Voting is on a simple majority system. Once approved by the institutional representatives, the guidelines will then go to the Chief Technical Officers for final endorsement.

The guideline drafting process may be altered by consensus of the SIG members or by the SCS System Security Officer. The endorsement process may be amended by the SIG in conjunction with the institutional Chief Technical Officers and/or the System Security Officer.

NEVADA ADMINISTRATIVE CODE

Containing All Permanent Regulations of State Agencies
Adopted under chapter 233B of NRS

Classified, Arranged, Revised, Indexed and Published
(Pursuant to NRS 233B.062 to 233B.065 inclusive)

by the
LEGISLATIVE COUNSEL
STATE OF NEVADA

Please direct any questions or suggestions
pertaining to NAC to:

Legislative Counsel Bureau
401 S. Carson St.
Carson City, Nevada 89701
(775) 684-6830

CHAPTER 720 - DIGITAL SIGNATURES

GENERAL PROVISIONS

LICENSING AND OPERATION OF CERTIFICATION AUTHORITY

CERTIFICATE: ISSUANCE AND PUBLICATION

CERTIFICATE: REVOCATION, SUSPENSION AND EXPIRATION

RECOGNIZED REPOSITORIES

USE AND EFFECT OF DIGITAL SIGNATURE

ENFORCEMENT

PROCEEDINGS

GENERAL PROVISIONS

NAC 720.010 Definitions. (NRS 720.150) As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 720.020 to 720.130, inclusive, and NAC 720.015 to 720.175, inclusive, have the meanings ascribed to them in those sections.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.015 "Accept a certificate" defined. (NRS 720.150) "Accept a certificate" means to manifest approval of a certificate by using the certificate or otherwise, with knowledge or notice of its contents.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.020 "Certification practice statement" defined. (NRS 720.150) "Certification practice statement" means a declaration that complies with the requirements of NAC 720.360.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.025 "Certify" defined. (NRS 720.150) "Certify" means, with reference to a certificate, to declare with ample opportunity to reflect after apprising oneself of all material facts.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.030 "Confirm" defined. (NRS 720.150) "Confirm" means to ascertain through appropriate inquiry and investigation.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.035 "Disclosure record" defined. (NRS 720.150) "Disclosure record" means a publicly accessible record maintained by the Secretary of State concerning a licensee that is available on-line through the Internet.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.040 "Electronic" defined. (NRS 720.150) "Electronic" means an electrical, digital, magnetic, optical, electromagnetic or similar form of technology.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.045 "Electronic message" defined. (NRS 720.150) "Electronic message" means a record that is generated, communicated, received or stored by electronic means for use in an information system or transmission between separate information systems.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.050 "Foreign license" defined. (NRS 720.150) "Foreign license" means a license to conduct business as a certification authority issued by a governmental entity outside of this State.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.055 "Hearing officer" defined. (NRS 720.150) "Hearing officer" means the Secretary of State or a hearing officer designated by the Secretary of State.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.060 "Incorporate by reference" defined. (NRS 720.150) "Incorporate by reference" means to make a message a part of another message by identifying the message to be incorporated and expressing the intention that it be incorporated.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.065 "Issue a certificate" defined. (NRS 720.150) "Issue a certificate" means the creation of a certificate and notification of the subscriber identified in the certificate of the contents of the certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.070 "License" defined. (NRS 720.150) "License" means a license to conduct business as a certification authority issued by the Secretary of State.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.075 "Licensee" defined. (NRS 720.150) "Licensee" means a certification authority who holds a license.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.080 "Notify" defined. (NRS 720.150) "Notify" means to communicate a fact to a person in a manner reasonably likely under the circumstances to impart knowledge of the information to that person.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.085 "Official public business" defined. (NRS 720.150) "Official public business" means any legally authorized transaction or communication between a public agency and any other person.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.090 "Operative personnel" defined. (NRS 720.150) "Operative personnel" means one or more natural persons acting as a certification authority or his agent, or in the employment of or under contract with a certification authority, who have:

1. Duties directly involving the issuance of certificates or the creation of private keys;

2. Responsibility for the secure operation of the system of computer hardware and software used by the certification authority to conduct business as a certification authority or to operate a recognized repository;

3. Direct responsibility, other than general supervisory authority, for the establishment or adoption of policies regarding the operation and security of the certification authority; or

4. Such other duties or responsibilities as the Secretary of State determines to be significant to the operation of a certification authority.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.095 "Person" defined. (NRS 720.150) "Person" means a natural person, any organization that is capable of signing a document, either legally or as a matter of fact, a government, a governmental agency or a political subdivision of a government.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.100 "Public agency" defined. (NRS 720.150) "Public agency" has the meaning ascribed to it in NRS 720.170.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.105 "Publish" defined. (NRS 720.150) "Publish" means to make information publicly available.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.110 "Recipient" defined. (NRS 720.150) "Recipient" means a person who:

1. Has received a certificate and a digital signature that is verifiable with reference to the public key set forth in the certificate; and

2. Is in a position to rely on the digital signature.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.115 "Recognized certification authority" defined. (NRS 720.150) "Recognized certification authority" means the Secretary of State, a licensee or a certification authority whose foreign license is recognized by the Secretary of State pursuant to NAC 720.420.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.120 "Recognized repository" defined. (NRS 720.150) "Recognized repository" means the state repository or a repository designated by the Secretary of State pursuant to NAC 720.650.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.125 "Recommended limit of reliance" defined. (NRS 720.150) "Recommended limit of reliance" means the monetary amount that a certification authority recommends is the maximum amount upon which a certificate may be relied.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.130 "Repository" defined. (NRS 720.150) "Repository" means a system for storing and retrieving certificates and other information relevant to digital signatures.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.135 "Revoke a certificate" defined. (NRS 720.150) "Revoke a certificate" means to make a certificate ineffective permanently from a specified time forward through means of a notation on the certificate or the inclusion of the certificate in a set of revoked certificates.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.140 "Rightfully hold a private key" defined. (NRS 720.150) "Rightfully hold a private key" means to hold a private key that:

1. Has not been disclosed by the holder of the key or his agents to any person who is not authorized to use the key; and
2. Has not been obtained by the holder of the key through theft, deceit, eavesdropping or other unlawful means.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.145 "State repository" defined. (NRS 720.150) "State repository" means a repository operated pursuant to NAC 720.700.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.150 "Suitable insurance" defined. (NRS 720.150) "Suitable insurance" means insurance that satisfies the requirements of NAC 720.290.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.155 "Suspend a certificate" defined. (NRS 720.150) "Suspend a certificate" means to make a certificate ineffective temporarily for a specified time forward.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.160 "Time stamp" defined. (NRS 720.150) "Time stamp" means:

1. A notation that:
   (a) Is digitally signed by a certification authority;
   (b) Is appended or attached to a message, digital signature or certificate; and
   (c) Indicates at least:
      (1) The date and time the notation was appended or attached; and
      (2) The identity of the person appending or attaching the notation; or
2. To append or attach such a notation to a message, digital signature or certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.165 "Transactional certificate" defined. (NRS 720.150) "Transactional certificate" means a certificate that is effective only for a specific transaction or series of transactions specified or incorporated by reference in the certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.170 "Trustworthy system" defined. (NRS 720.150) "Trustworthy system" means a system of computer hardware and software that complies with the requirements of NAC 720.300.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.175 "Valid certificate" defined. (NRS 720.150) "Valid certificate" means a certificate that:

1. Has been issued by a recognized certification authority;
2. Has been accepted by the subscriber identified in the certificate;
3. Has not been suspended or revoked; and
4. Has not expired.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.180 Purposes of chapter. (NRS 720.150) The purposes of this chapter are to:

1. Ensure that electronic messages with digital signatures are not denied legal recognition solely because they are in electronic form;
2. Facilitate commerce by means of reliable electronic messages;
3. Establish procedures for the use of digital signatures for official public business;
4. Provide persons who engage in commerce or official public business with reasonable assurance of the integrity and authenticity of electronic messages with digital signatures and that those messages will not be repudiated;
5. Provide a mechanism for the licensing of certification authorities and the recognition of repositories;
6. Minimize the incidence of forged digital signatures and fraud in electronic commerce;
7. Provide for the legal implementation of technical standards relating to electronic messages with digital signatures; and
8. Coordinate, with other states and jurisdictions, the establishment of uniform provisions regarding the authentication and reliability of electronic messages.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.185 Construction. (NRS 720.150) The provisions of this chapter:

1. Must be construed in a manner that:

(a) Is commercially reasonable under the circumstances; and

(b) Carries out the purposes of this chapter.

2. Must not be construed in such a manner as to:

(a) Require the Secretary of State to conduct any business or take any other action as a certification authority;

(b) Preclude a licensee from conforming to any standards or requirements that are more stringent than, but nevertheless consistent with, those provisions; or

(c) Authorize the award of any punitive or exemplary damages.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.190 Variation of certain provisions by agreement; remedies not exclusive. (NRS 720.150)

1. Except as otherwise provided by a specific provision of this chapter, the provisions of this chapter regarding the issuance, acceptance, publication and use of a certificate may be varied by agreement between the certification authority who issues the certificate and the subscriber identified in the certificate.

2. The remedies provided pursuant to this chapter are not exclusive and are in addition to any other remedies provided by law, including, without limitation, any criminal prosecution pursuant to the laws of this State or of the United States. Injunctive relief must not be denied to a person regarding any conduct governed by the provisions of this chapter solely because the conduct is or may be subject to criminal prosecution.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.195 Severability of provisions. (NRS 720.150) The provisions of this chapter are hereby declared to be severable. If any of the provisions of this chapter is held invalid, or if the application of any of those provisions to any person, thing or circumstance is held invalid, that invalidity does not affect any other provision of this chapter that can be given effect without the invalid provision or application.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.200 Adoption by reference of standards. (NRS 720.150) The Secretary of State hereby adopts by reference:

1. The technical standards designated as *X.509, Version 3*, as adopted by the International Telecommunication Union. A copy of those standards may be obtained from the Office of the Secretary of State, 101 North Carson Street, Suite 3, Carson City, Nevada 89701-4786, for the price of $22.50.

2. The provisions of the *CSPP - Guidance for COTS Security Protection Profiles, Version 1.0*, as developed by the National Institute of Standards and Technology of the Technology Administration of the United States Department of Commerce. A copy of those provisions may be obtained from the Office of the Secretary of State, 101 North Carson Street, Suite 3, Carson City, Nevada 89701-4786, for the price of $9.50.

3. The provisions of the *WebTrust Program for Certification Authorities, Version 1.0*, as developed by the American Institute of Certified Public Accountants and the Canadian Institute of Chartered Accountants. A copy of those provisions may be obtained from the Office of the Secretary of State, 101 North Carson Street, Suite 3, Carson City, Nevada 89701-4786, for the price of $9.50.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99; A by R040-03, 12-4-2003)

NAC 720.205 Confidentiality of information. (NRS 720.150)

1. Except as otherwise provided in subsection 2 or required by a court order, any:

(a) Trade secret, as that term is defined in NRS 600A.030;

(b) Information regarding the design, security or programming of a computer system used for the licensing or operation of a certification authority or repository pursuant to this chapter; or

(c) Information that identifies a private key held by a subscriber,

➥ which is in the possession of the Secretary of State or Department of Information Technology for the purposes of this chapter, or an auditor conducting an audit pursuant to NAC 720.320, shall be deemed confidential and must not be made available for public disclosure, inspection or copying.

2. For the purposes of an audit conducted pursuant to NAC 720.320, a licensee shall provide the auditor with any information in his possession that is relevant to the audit, including any information that is deemed confidential pursuant to subsection 1.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

LICENSING AND OPERATION OF CERTIFICATION AUTHORITY

NAC 720.250 Qualifications for license; period of validity of license. (NRS 720.150**)**

1. To qualify for a license, a certification authority must:

(a) Use a secure method for limiting access to his private key;

(b) Maintain an office or registered agent for service of process in this State; and

(c) Comply with the provisions of this chapter and chapter 720 of NRS.

2. The issuance or renewal of a license is valid for 1 year unless the license is suspended, revoked or otherwise terminated at an earlier date. The Secretary of State may notify a licensee before his license is due to expire, but any failure to do so does not excuse a licensee from failing to renew the license within that period.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.260 Issuance of license to governmental entity. (NRS 720.150**)**

1. Except as otherwise provided in this section, the Secretary of State will not issue a license to any governmental entity.

2. The Secretary of State may issue a license to the Department of Information Technology. For the purposes of this chapter, the Department of Information Technology is not required to:

(a) Obtain or submit proof that the Department has suitable insurance; or

(b) Pay any of the amounts otherwise required pursuant to NAC 720.430, 720.810 or 720.840.

3. If the Department of Information Technology obtains a license, the Department may issue a certificate only:

(a) For a subscriber who is a public agency; or

(b) For the conduct of official public business by any other person.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.270 Prerequisites to issuance and renewal of license. (NRS 720.150**)** Except as otherwise provided in NAC 720.260, the Secretary of State may issue a license to, or renew the license of, a certification authority who meets the qualifications for a license set forth in NAC 720.250 and submits to the Secretary of State:

1. A completed application that complies with the requirements of NAC 720.280.

2. The amounts required pursuant to NAC 720.430 and 720.810.

3. Proof of his identity or, if the certification authority is a business entity, proof of existence and good standing of the certification authority in the following form:

(a) If the certification authority is formed, incorporated, organized, registered, qualified to transact business or otherwise created in the State of Nevada pursuant to the provisions of title 7 of NRS, a certificate of existence and good standing from the Secretary of State. To comply with the provisions of this paragraph, the certification authority must submit a separate application to the Secretary of State to receive a certificate of existence and good standing.

(b) If the certification authority is formed, incorporated, organized, registered, qualified to transact business or otherwise created in a state or territory other than the State of Nevada, in the District of Columbia, in a possession of the United States or in a foreign country, a certificate of existence and good standing if the jurisdiction has such a certificate, or an equivalent form signifying that the certification authority has been formed, incorporated, organized, registered, qualified to transact business or otherwise created in that jurisdiction from the appropriate governmental agency of each jurisdiction in which the certification authority is formed, incorporated, organized, registered, qualified to transact business or otherwise created.

4. Proof that he has suitable insurance.

5. A report of an audit of the policies, practices, procedures, facilities and computer hardware and software of the applicant which:

(a) Establishes that the applicant operates a trustworthy system; and

(b) Was obtained pursuant to an audit performed in compliance with the requirements of NAC 720.320 and 720.330, except that the audit and report required for the initial issuance of a license is not required to include any matters other than compliance with the requirements of paragraph (a).

6. The documentation required pursuant to NAC 720.340.

7. A certification practice statement that complies with the requirements of NAC 720.360.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99; A by R040-03, 12-4-2003)

NAC 720.280 Application for license. (NRS 720.150**)** An application for the issuance or renewal of a license must be on a form prescribed by the Secretary of State and include:

1. The name of the applicant;
2. The mailing address and, if different, the physical address of the applicant;
3. The telephone number of the applicant;
4. The electronic mail address of the applicant;
5. The name and address of the registered agent in this State for service of process upon the applicant, including the physical address and, if different, the mailing address; and
6. The names of all operative personnel of the applicant.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.290 Insurance: Minimum requirements; proof. (NRS 720.150**)**

1. Except as otherwise provided in NAC 720.260, a licensee shall maintain a policy of insurance issued by an insurance company authorized to do business in this State, which:

(a) Provides the licensee with coverage for:

(1) Professional liability in an amount of not less than $5,000,000; and

(2) Commercial general liability in an amount of not less than $10,000,000; and

(b) Contains a provision that requires the insurance company to notify the Secretary of State at least 30 days before cancellation or nonrenewal of the policy.

2. For the purposes of this chapter, proof of the policy of insurance required by subsection 1 must:

(a) Be in a form that is prescribed or approved by the Secretary of State;

(b) Identify the insurance company by name, mailing address and physical address, and include the number or a copy of the document authorizing the insurance company to do business in this State; and

(c) Identify the licensee for whom the policy is issued.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.300 Trustworthy system: Minimum requirements. (NRS 720.150**)** A licensee shall maintain such policies, practices, procedures and facilities as are necessary to ensure that his system of computer hardware and software:

1. Is reasonably secure from intrusion and misuse;

2. Provides a reasonable level of availability, reliability and correct operation;

3. Is reasonably suited to performing its intended functions; and

4. Is in material compliance with the provisions of the *CSPP - Guidance for COTS Security Protection Profiles, Version 1.0* and the *WebTrust Program for Certification Authorities, Version 1.0*, as adopted by reference pursuant to NAC 720.200. The Secretary of State will determine whether compliance is material:

(a) In accordance with the provisions of this chapter; and

(b) In a manner that is consistent with state and federal law and reasonable for the context in which the system is used.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99; A by R040-03, 12-4-2003)

NAC 720.310 Trustworthy system: Use. (NRS 720.150**)** A licensee shall use only a trustworthy system to:

1. Issue, suspend or revoke a certificate; and

2. Publish in a recognized repository or otherwise give notice of the issuance, suspension or revocation of a certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.320 Compliance audit: Performance; report to Secretary of State. (NRS 720.150**)**

1. A licensee shall obtain an audit at least once each year to receive an opinion as to whether the licensee is in material compliance with the requirements of this chapter. If the Secretary of State has designated a repository operated by the licensee as a recognized repository, the audit must include the operation of the recognized repository.

2. The auditor shall exercise reasonable professional judgment in determining whether a condition that is not in strict compliance with the requirements of this chapter is material, taking into consideration the particular circumstances and context. In addition to any other conditions the auditor determines to be material, the auditor shall consider as material:

(a) Any condition relating to the validity of a certificate that does not comply with the requirements of this chapter.

(b) Noncompliance with the requirements of NAC 720.350.

(c) Noncompliance with the provisions of this chapter regarding the use of a trustworthy system.

3. The licensee must file a copy of the audit report with the Secretary of State before his license may be renewed. The report may be filed electronically if the electronic message complies with the requirements of this chapter. The licensee is not required to file the complete audit report if he files a summary of the report that:

(a) States the target of evaluation of the audit;

(b) Describes all audit exceptions and conditions of noncompliance included in the complete report, including, without limitation, any conditions described in subsection 2; and

(c) Bears the signature of the auditor.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.330 Compliance audit: Qualifications of auditor. (NRS 720.150**)** Each audit required pursuant to NAC 720.320 must be performed by a certified public accountant who:

1. Is certified pursuant to chapter 628 of NRS or a similar law of another jurisdiction; and

2. Holds or, for the purpose of the audit, employs, contracts with or associates with a person who holds a current certification as:

(a) A certified information systems auditor issued by the Information Systems Audit and Control Association; or

(b) A certified information systems security professional issued by the International Information Systems Security Certification Consortium.

➥ The audit report or a letter accompanying that report must disclose the name of each person who possesses the certification required pursuant to this section.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.340 Qualifications of operative personnel. (NRS 720.150**)**

1. An applicant for the issuance or renewal of a license must submit to the Secretary of State such documentation as the Secretary of State requires to ensure that all operative personnel of the applicant are qualified to act in that capacity. The documentation must include, for each person who acts in that capacity:

(a) A declaration, executed by the person under penalty of perjury, that:

(1) Specifies his name, including all names by which he has been known in the past, his date of birth and his business address; and

(2) Specifies each country, other than the United States, in which the person resided during the past 5 years and states the period of that residency;

(b) Two sets of fingerprint cards that have been completed by a recognized law enforcement agency;

(c) An executed Law Enforcement Record Form No. 3321-SA or equivalent authorization for the release of information contained in records of law enforcement;

(d) Written authorization for the Secretary of State to submit the fingerprint cards to the Central Repository for Nevada Records of Criminal History for further submission to

the Federal Bureau of Investigation and to receive reports regarding the criminal histories of the subjects of the fingerprint cards; and

(e) The amount of the fees charged by any local agencies of law enforcement, the Central Repository for Nevada Records of Criminal History and the Federal Bureau of Investigation for the handling of the fingerprint cards and issuance of the reports of criminal histories.

2. For the issuance or renewal of a license, the reports received pursuant to subsection 1 must indicate that the applicant and all operative personnel of the applicant:

(a) Have not been convicted in any jurisdiction during the 7 years immediately preceding the date the application for the issuance or renewal of a license is submitted of any felony; and

(b) Have never been convicted in any jurisdiction of a crime involving fraud, deception or a false statement.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99; A by R040-03, 12-4-2003)

NAC 720.350 Persons convicted of certain crimes not to act as operative personnel. (NRS 720.150**)**

1. A licensee shall not allow any person to undertake any of the responsibilities or duties of his operative personnel if the licensee knows or, based upon the records provided to the Secretary of State pursuant to NAC 720.340, should know that the person:

(a) Has been convicted in any jurisdiction during the 7 years immediately preceding the date the application for the issuance or renewal of a license is submitted of any felony; or

(b) Has ever been convicted in any jurisdiction of a crime involving fraud, deception or a false statement.

2. If a licensee discovers that a person who has undertaken any of the responsibilities or duties of his operative personnel has been convicted as described in subsection 1, the licensee shall:

(a) Immediately remove the person from that position; and

(b) Within 3 business days after making that discovery, notify the Secretary of State of his action to remove the person from that position.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99; A by R040-03, 12-4-2003)

NAC 720.360 Certification practice statement: Filing and publication; contents. (NRS 720.150**)** A licensee shall file with the Secretary of State and publish a certification practice statement that includes, without limitation:

1. A description of the policies, practices and procedures of the licensee for the creation, issuance, distribution, management, storage, suspension, revocation and renewal of certificates;

2. If certificates are issued by class, the necessary criteria for each class, including the methods for identifying subscribers applicable to each class;

3. A written description of all representations required by the licensee from a subscriber regarding the responsibility of the subscriber to protect his private key; and

4. A disclosure of any:

(a) Warnings, limitations on liability, disclaimers of warranty and provisions for indemnity and holding harmless upon which the licensee intends to rely;

(b) Disclaimers and limitations on obligations, losses or damages to be asserted by the licensee; and

(c) Mandatory procedures for the resolution of disputes, including any provisions regarding the choice of forum or applicable law.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.370 Disclosure records: Publication and updating by Secretary of State. (NRS 720.150**)**

1. The Secretary of State will publish a disclosure record for each licensee that includes, without limitation:

(a) The name, mailing address, telephone number and electronic mail address of the insurance company that issued suitable insurance for the licensee;

(b) A copy of the most recent certification practice statement filed with the Secretary of State by the licensee pursuant to this chapter;

(c) A copy of the summary or report of the most recent audit of the licensee filed with the Secretary of State pursuant to this chapter;

(d) Information regarding the current status of the license, including a disclosure of any suspension or revocation and, if a suspension or revocation is currently pending proceedings for administrative or judicial review, a statement of that fact;

(e) A statement of whether a repository operated by the licensee has been designated as a recognized repository and information sufficient to locate or identify any repository the licensee operates or otherwise uses;

(f) A list of all judgments regarding the licensee filed with the Secretary of State pursuant to NAC 720.410 within the past 5 years; and

(g) Any other information required by this chapter.

2. The Secretary of State will update a disclosure record when he discovers that any information contained in the disclosure record has changed or is no longer accurate.

3. In carrying out this section, the Secretary of State will rely on records received by his office and is not obligated to conduct any investigation or other inquiry regarding the information contained in those records.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.380 Imposition of restrictions on operation of licensee. (NRS 720.150**)** The Secretary of State may:

1. As a condition to the issuance and retention of a license, impose any restrictions on the operation of the licensee as he deems appropriate; and

2. Maintain in his file for the licensee a written record of the basis for imposing the restrictions.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.390 Creation and retention of records by licensee. (NRS 720.150**)**

1. A licensee shall:

(a) Create and retain such records as are necessary for the licensee to demonstrate compliance with this chapter.

(b) Retain each notice of the suspension or revocation of a certificate given by the licensee pursuant to NAC 720.600.

(c) Create and retain a database that contains a record of the identity of each subscriber named in a certificate issued by the licensee, which must include the number and date of issuance of the certificate and each fact represented in the certificate.

(d) Create and retain a database that contains a record of each time stamp the licensee appends or attaches to a message, digital signature or certificate, which must include sufficient information to identify the relevant subscriber and message, digital signature or certificate.

2. The records required pursuant to:

(a) Paragraphs (a) and (b) of subsection 1 must be retained for not less than 5 years.

(b) Paragraph (c) of subsection 1 must be retained for not less than 10 years after the date the certificate expires or is revoked.

(c) Paragraph (d) of subsection 1 must be retained for not less than 10 years after the date the time stamp is appended or attached.

3. The records required pursuant to subsection 1 must be:

(a) Set forth on paper, retrievable from a computer or created and retained in any other form authorized by the State Library and Archives Administrator pursuant to NRS 378.255 or 378.280 for the retention of records; and

(b) Indexed, stored, preserved and reproduced in such a manner as to remain accurate, complete and accessible to an auditor.

4. This section does not require the inclusion of:

(a) Any of the extensions of data specified in section 4.2 of the technical standards designated as *X.509, Version 3*, as adopted by reference pursuant to NAC 720.200; or

(b) Any information that would compromise the security of the licensee, in any record that is publicly accessible.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.400 Duties of licensee discontinuing services as certification authority. (NRS 720.150**)** A licensee who intends to discontinue providing services as a certification authority shall:

1. Before discontinuing those services, notify the subscribers identified in all valid certificates issued by the licensee;

2. Take such commercially reasonable efforts as are necessary to minimize disruption to those subscribers and to persons who rely on those certificates; and

3. Make reasonable arrangements for the preservation of his records relating to his services as a certification authority. If the licensee is unable to make other reasonable arrangements for the preservation of those records, the licensee shall:

(a) Revoke all valid certificates he has issued and return all his records regarding those certificates to the appropriate subscribers; or

(b) Submit those records to such other licensees as the Secretary of State designates for that purpose.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.410 Filing of judgments against licensees; scope of liability of recognized certification authority. (NRS 720.150**)**

1. A licensee shall file with the Secretary of State a certified copy of each judgment entered against the licensee for damages resulting from any acts of the licensee within the scope of his activities as a certification authority.

2. Except as otherwise provided in this chapter, a recognized certification authority is not liable for:

(a) Any damages incurred by a person who relies on a certificate issued by the certification authority, or on any representation contained in the certificate which the certification authority is required to confirm, that exceed any recommended limit of reliance clearly specified in the certificate and in the last certification practice statement filed by the certification authority with the Secretary of State pursuant to this chapter before the reliance occurred.

(b) Any loss caused by the failure of the certification authority to comply with any provision of this chapter regarding the issuance of a certificate, in excess of any recommended limit of reliance specified in the certificate.

(c) Any loss caused by the reliance of a person on a false or forged digital signature of a subscriber identified in a certificate issued by the certification authority if the certification authority complied with all the material requirements of this chapter regarding the certificate. This subsection does not relieve a certification authority from liability for any failure to act in good faith or for the breach of any promise, warranty or certification provided pursuant to NAC 720.480 or 720.490.

(d) Any punitive or exemplary damages resulting from the reliance of a person on a certificate issued by the certification authority.

(e) Any damages for pain and suffering resulting from the reliance of a person on a certificate issued by the certification authority.

3. A recognized certification authority may waive any of the provisions of subsection 2.

4. A recognized certification authority may liquidate, limit, alter or exclude liability for any consequential or incidental damages resulting from the reliance of a person on a certificate issued by the certification authority by:

(a) Agreement with the person who incurs the loss; or

(b) Notification of the person who incurs the loss, before he relies on the certificate, of the liquidation, limitation, alteration or exclusion,

➥ if the liquidation, limitation, alteration or exclusion is not unconscionable.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.420 Recognition of foreign license. (NRS 720.150)

1. The Secretary of State may recognize a foreign license, in whole or in part, if:

(a) The certification authority who holds the foreign license, in addition to complying with any other legal requirements for the transaction of business in this State, submits to the Secretary of State:

(1) An application for the recognition of his foreign license;

(2) A certified copy of his foreign license; and

(3) The amounts required pursuant to NAC 720.430 and 720.810; and

(b) The Secretary of State determines that the governmental entity that issued the foreign license imposes requirements substantially similar to the requirements of this chapter.

2. The Secretary of State will determine that the requirements of a governmental entity are substantially similar to the requirements of this chapter if, in addition to any other factors the Secretary of State deems to be material, the governmental entity requires that a certification authority must, as a condition to holding the foreign license:

(a) Issue certificates:

(1) Based upon an asymmetric cryptosystem; and

(2) Using a trustworthy system;

(b) Maintain a policy of insurance which provides not less than the minimum amounts of coverage required by NAC 720.290;

(c) Employ as operative personnel only persons who have not been convicted of a felony within the past 7 years and have never been convicted of a crime involving fraud, deception or a false statement; and

(d) Comply with a legally established system for the enforcement of the requirements of that governmental entity regarding digital signatures.

3. The Secretary of State will:

(a) Make available, upon request, a list of the governmental entities that the Secretary of State has determined meet the requirements of subsection 2; and

(b) Consider a governmental entity for addition to that list upon:

(1) The request of the governmental entity or a certification authority licensed by the governmental entity; and

(2) The receipt of a copy of the licensing requirements of the governmental entity, together with an English translation if it is in a foreign language.

4. The recognition of a foreign license pursuant to this section is valid:

(a) Until the foreign license expires or otherwise becomes invalid; or

(b) For 1 year,

➥ whichever period is less.

5. The provisions of this section do not prohibit a certification authority who holds a foreign license from obtaining a license pursuant to the other provisions of this chapter.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.430 Licensing fees. (NRS 720.150**,** 720.180**)** The Secretary of State will charge, in addition to any other amounts required pursuant to this chapter, the following licensing fees:

1. For the issuance or renewal of a license, $1,000.

2. For the recognition of a foreign license, $1,000.

3. For the designation of a repository as a recognized repository, $1,000.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

CERTIFICATE: ISSUANCE AND PUBLICATION

NAC 720.450 Prerequisites to issuance of certificate to subscriber. (NRS 720.150**)**

1. A certification authority may issue a certificate to a subscriber only after the certification authority has:

(a) Received a request for the issuance of a certificate signed by the prospective subscriber; and

(b) Confirmed, which must include requiring a subscriber and his agent or agents to certify the accuracy of relevant information under penalty of perjury, that:

(1) The prospective subscriber is the person to be identified in the requested certificate;

(2) The prospective subscriber rightfully holds a private key which:

(I) Is capable of creating a digital signature; and

(II) Corresponds to the public key to be set forth in the requested certificate;

(3) The public key to be set forth in the requested certificate can be used to verify a digital signature affixed by the private key held by the prospective subscriber;

(4) The information to be included in the requested certificate is accurate;

(5) The requested certificate provides sufficient information to locate or identify one or more repositories in which the certificate will be stored and, if the certificate is suspended or revoked, notice of the suspension or revocation will be published; and

(6) If the prospective subscriber is acting through one or more agents, the prospective subscriber has:

(I) Authorized the agent or agents to have custody of his private key, to request the issuance of a certificate setting forth the corresponding public key and to sign digitally on behalf of the prospective subscriber; and

(II) Ensured that adequate safeguards exist to prevent the creation of a digital signature that exceeds any limitations on the authority of the agent or agents.

2. A certification authority shall, when seeking to obtain any other information material to the issuance of a certificate, require the subscriber and his agent or agents to certify the accuracy of relevant information under penalty of perjury.

3. The provisions of this section may not be waived, disclaimed or otherwise limited by agreement.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.460 Confirmation of identity of prospective subscriber. (NRS 720.150)

1. When carrying out the provisions of NAC 720.450 requiring a certification authority to confirm that a prospective subscriber is the person to be identified in a requested certificate, a certification authority shall make such an inquiry into the identity of the prospective subscriber as is reasonable based upon:

(a) Any representations the certification authority will make regarding the reliability of the certificate, including any recommended limit of reliance;

(b) Any recommendations the certification authority will make regarding the use or application of the certificate; and

(c) Whether the certificate will be a transactional certificate.

2. If the prospective subscriber appears before the certification authority and presents a current:

(a) Identifying document issued by or under the authority of the United States or another country; or

(b) Driver's license or other identifying document issued by a state of the United States,

➥ which is reviewed and accepted by a notary public or any operative personnel of the certification authority, there is a rebuttable presumption that the certification authority has confirmed that the prospective subscriber is the person to be identified in the requested certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.470 Contents of certificate. (NRS 720.150) A certificate:

1. Must indicate the date upon which the certificate expires.

2. May include, without limitation, any disclaimers and limitations on obligations, losses or damages to be asserted by the certification authority who issues the certificate.

3. Must comply with the standards for basic certificate fields specified in section 4.1 of the technical standards designated as *X.509, Version 3,* as adopted by reference pursuant to NAC 720.200, except that fields are not required for extensions of data. If fields are used for extensions of data:

(a) The use must conform to the guidelines specified in sections 4.1.2.1 and 4.2 of the technical standards designated as *X.509, Version 3,* as adopted by reference pursuant to NAC 720.200; and

(b) The fields may be displayed on the certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.480 Warranties, promises and certifications by Secretary of State. (NRS 720.150) Except as otherwise provided in NAC 720.610, if the Secretary of State:

1. Issues a certificate, the Secretary of State:

(a) Warrants to the subscriber named in the certificate that the certificate:

(1) Contains no information known by the Secretary of State to be false; and

(2) Satisfies all material requirements of this chapter.

(b) Promises to the subscriber named in the certificate:

(1) To act promptly to suspend or revoke a certificate in accordance with this chapter; and

(2) To notify the subscriber within a reasonable time of any facts known to the Secretary of State that significantly affect the validity or reliability of the certificate after issuance.

2. Issues and publishes a certificate, the Secretary of State certifies to all persons who reasonably rely on the information contained in the certificate or on a digital signature verifiable by the public key set forth in the certificate that:

(a) The Secretary of State has issued the certificate to the subscriber;

(b) The subscriber has accepted the certificate;

(c) The information in the certificate identified as confirmed by the Secretary of State was accurate when the certificate was issued; and

(d) All information foreseeably material to the reliability of the certificate is stated or incorporated by reference in the certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.490 Warranties, promises and certifications by other certification authorities. (NRS 720.150)

1. Except as otherwise provided in NAC 720.480 and 720.610, a certification authority:

(a) By issuing a certificate:

(1) Warrants to the subscriber named in the certificate that:

(I) The certificate contains no information known by the certification authority to be false;

(II) The certificate satisfies all material requirements of this chapter; and

(III) The certification authority has not exceeded any limitations on his authority in issuing the certificate.

(2) Promises to the subscriber named in the certificate, unless the certification authority and subscriber agree otherwise:

(I) To act promptly to suspend or revoke a certificate in accordance with this chapter; and

(II) To notify the subscriber within a reasonable time of any facts known to the certification authority that significantly affect the validity or reliability of the certificate after issuance.

(3) Certifies to all persons who reasonably rely on the information contained in the certificate or on a digital signature verifiable by the public key set forth in the certificate that:

(I) The subscriber has accepted the certificate;

(II) The information in the certificate identified as confirmed by the certification authority was accurate when the certificate was issued;

(III) All information foreseeably material to the reliability of the certificate is stated or incorporated by reference in the certificate; and

(IV) The certification authority has complied with all applicable laws and regulations of this State governing the issuance of the certificate.

(b) By publishing a certificate, certifies to the repository where the certificate is published and to all persons who reasonably rely on the information contained in the certificate that the certification authority has issued the certificate to the subscriber.

2. Except as otherwise provided in this section, the provisions of this section may not be waived, disclaimed or otherwise limited by agreement.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.500 Certification of authority of person requesting certificate. (NRS 720.150**)**

1. Except as otherwise provided in NAC 720.610, by requesting the issuance of a certificate as an agent of the subscriber to be identified in the certificate, the person requesting the certificate certifies to all persons who reasonably rely on the information contained in the certificate that he has the legal authority to:

(a) Apply for the issuance of the certificate; and

(b) Sign digitally on behalf of the subscriber and that, if this authority is limited in any way, adequate safeguards exist to prevent the creation of a digital signature that exceeds the limitations on his authority.

2. No person may waive, disclaim or otherwise limit by agreement or obtain indemnity from the provisions of this section in such a manner as to limit his liability for any misrepresentation of fact to any person who reasonably relies on a certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.510 Certifications by subscriber. (NRS 720.150**)**

1. Except as otherwise provided in NAC 720.610, by accepting a certificate, the subscriber identified in the certificate certifies to all persons who reasonably rely on the information contained in the certificate that:

(a) The subscriber rightfully holds the private key that corresponds to the public key set forth in the certificate;

(b) All representations made by the subscriber to the certification authority who issued the certificate which are material to the information set forth in the certificate are true; and

(c) All material representations included in the certificate and not confirmed by the certification authority are true.

2. No person may waive, disclaim or otherwise limit by agreement or obtain indemnity from the provisions of this section in such a manner as to limit his liability for any misrepresentation of fact to any person who reasonably relies on a certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.520 Indemnification of certification authority for certain losses or damages. (NRS 720.150**)**

1. Except as otherwise provided in NAC 720.610, by accepting a certificate, the subscriber identified in the certificate and any agent of the subscriber who requested the issuance of the certificate promise to indemnify the certification authority who issued the certificate for any loss or other damage resulting from the issuance or publication of the certificate in reliance upon any:

(a) Misrepresentation of a material fact by the subscriber or his agent; or

(b) Failure by the subscriber or his agent to disclose a material fact,

➥ if the misrepresentation or failure to disclose was negligent or intended to deceive the certification authority or a person relying on the certificate.

2. The provisions of this section may not be waived, disclaimed or otherwise limited by agreement, but consistent, additional terms may be provided by agreement.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.530 Private key: Promises and property right of subscriber. (NRS 720.150**)**

1. Except as otherwise provided in subsection 2, by accepting a certificate, the subscriber identified in the certificate promises to exercise reasonable care to retain control of the corresponding private key and prevent its disclosure to any person who is not authorized to create the digital signature of the subscriber until:

(a) The expiration of the certificate;

(b) Notice of the revocation of the certificate is published pursuant to NAC 720.600; or

(c) One business day after the subscriber has submitted to the certification authority who issued the certificate a written request for the revocation of the certificate and such evidence as is reasonably sufficient to confirm that the person requesting the revocation is the subscriber or an agent of the subscriber who is authorized to make the request,

➥ whichever occurs first.

2. By accepting a transactional certificate, the subscriber identified in the certificate promises to exercise reasonable care to retain control of the corresponding private key and prevent its disclosure to any person who is not authorized to create the digital signature of the subscriber until:

(a) The expiration of the certificate; or

(b) Notice of the revocation of the certificate is published pursuant to NAC 720.600,

➥ whichever occurs first.

3. The provisions of subsections 1 and 2 may not be waived, disclaimed or otherwise limited by agreement.

4. A private key is the personal property of the subscriber who rightfully holds the private key.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.540 Publication of certificate by Secretary of State or licensee. (NRS 720.150**)**

1. If the Secretary of State issues a certificate and:

(a) The subscriber accepts the certificate, the Secretary of State will publish a signed copy of the certificate in a recognized repository.

(b) The subscriber does not accept the certificate, the Secretary of State will not publish the certificate or, if the Secretary of State has already published the certificate, will cancel that publication.

2. If a licensee issues a certificate and:

(a) The subscriber accepts the certificate, the licensee shall, except as otherwise provided by agreement between the licensee and subscriber:

(1) Publish the certificate in compliance with any applicable policies for the publication of certificates contained in the certification practice statement of the licensee; or

(2) If the licensee has not included in his certification practice statement any applicable policies for the publication of certificates, publish a signed copy of the certificate in a recognized repository agreed upon by the licensee and subscriber.

(b) The subscriber does not accept the certificate, the licensee shall not publish the certificate or, if the licensee has already published the certificate, shall cancel that publication.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

CERTIFICATE: REVOCATION, SUSPENSION AND EXPIRATION

NAC 720.550 Revocation of certificate not issued in accordance with requirements; suspension to conduct investigation; notification of subscriber. (NRS 720.150**)**

1. If a certification authority confirms that a certificate he has issued was not issued in accordance with the requirements of NAC 720.450, the certification authority shall immediately revoke the certificate.

2. A certification authority may suspend a certificate he has issued for such a period, not to exceed 5 business days, as is necessary for him to conduct an investigation to confirm any grounds for revocation of the certificate pursuant to subsection 1.

3. A certification authority shall notify the subscriber as soon as practicable after the certification authority determines to suspend or revoke a certificate pursuant to this section.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.560 Order by Secretary of State to revoke or suspend certificate; notification; compliance with order. (NRS 720.150**)**

1. The Secretary of State may:

(a) Order a certification authority to revoke a certificate the certification authority has issued if, after providing the certification authority and subscriber with notice of the proposed order and an opportunity to be heard on the matter, the Secretary of State determines that:

(1) The certificate was issued without substantial compliance with the provisions of this chapter; and

(2) The noncompliance poses a significant risk to persons who may reasonably rely on the certificate.

(b) Without a prior hearing, order a certification authority to suspend, for not more than 5 business days, a certificate the certification authority has issued if the Secretary of State determines that an emergency requires an immediate remedy. If the certification authority:

(1) Is a licensee, the Secretary of State will mail a copy of the order, together with a summary of the facts upon which he based his determination, to the licensee at the mailing address or electronic mail address of the licensee specified on the application for the license; or

(2) Is not a licensee, the Secretary of State will provide the certification authority with notice of the order in such a manner as is reasonable under the circumstances.

➥ After issuing an order pursuant to this paragraph, the Secretary of State will proceed as quickly as feasible to complete the proceedings in the manner otherwise provided pursuant to the provisions of chapter 233B of NRS.

2. A certification authority shall comply with any order issued by the Secretary of State pursuant to this section within 24 hours after the certification authority receives the order.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.570 Suspension upon request by appropriate person. (NRS 720.150)

1. Except as otherwise provided in this section, a certification authority shall, within 24 hours after the receipt of all information he requires pursuant to this subsection, suspend a certificate he has issued, for not more than 5 business days, if the suspension is requested by a person whom the certification authority reasonably believes to be an appropriate person. The certification authority is not required to confirm that the person requesting the suspension is an appropriate person, but may require the person to provide evidence, which may include a statement given under oath or affirmation, that the person is an appropriate person.

2. A person who requests the suspension of a certificate pursuant to subsection 1 shall not misrepresent his identity or authority to request the suspension.

3. The subscriber identified in a certificate may agree with the certification authority who issues the certificate to limit or preclude the suspension of the certificate pursuant to subsection 1, except that such an agreement is effective only if notice of the agreement is published in the certificate or in the certification practice statement of the certification authority.

4. A certification authority may not suspend a transactional certificate pursuant to this section.

5. As used in this section, "appropriate person" means the subscriber named in a certificate or a person authorized to act on his behalf.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.580 Termination of requested suspension. (NRS 720.150) Except as otherwise agreed by a subscriber and certification authority, the certification authority shall terminate the suspension of a certificate pursuant to NAC 720.570 if:

1. The termination is requested by a person who the certification authority confirms is the subscriber named in the suspended certificate or an agent of the subscriber who is authorized to request the termination; or

2. The certification authority discovers and confirms that the request for suspension was made without the authorization of the subscriber. This subsection does not require a certification authority to confirm a request for the suspension of a certificate pursuant to NAC 720.570.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.590 Revocation of certificate by certification authority upon receipt of request or certain information. (NRS 720.150)

1. Except as otherwise provided in subsection 2, a certification authority shall revoke a certificate he has issued:

(a) Within 1 business day after he receives:

(1) A written request for the revocation from the subscriber named in the certificate or an agent of the subscriber who is authorized to request the revocation; and

(2) Such evidence as is reasonably sufficient to confirm that the person requesting the revocation is the subscriber or an agent of the subscriber who is authorized to make the request;

(b) Upon receiving a certified copy of the death certificate of the subscriber or confirming by other evidence that the subscriber is dead; or

(c) Upon receiving documents effecting the dissolution of the subscriber or confirming by other evidence that the subscriber has been dissolved or otherwise ceases to exist, except that the certification authority is not required to revoke the certificate if he ascertains, before completing the revocation of the certificate, that the dissolution has been rescinded or that the existence of the subscriber has otherwise been restored.

2. A certification authority may not revoke a transactional certificate pursuant to subsection 1.

3. A certification authority may revoke a certificate he has issued if the certificate is or becomes unreliable, regardless of whether the subscriber consents to the revocation and notwithstanding any agreement to the contrary between the certification authority and subscriber.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.600 Notice of suspension or revocation. (NRS 720.150)

1. Immediately upon the suspension or revocation of a certificate pursuant to this chapter, the certification authority who issued the certificate shall, except as otherwise provided in subsection 2, give notice of the suspension or revocation in such a manner as is specified in the certificate. If the certificate specifies that the notice must be given in one or more repositories, the certification authority shall publish a signed notice of the suspension or revocation:

(a) In each of the specified repositories that will accept publication; and

(b) In a recognized repository if:

(1) Any of the specified repositories refuse to accept publication or have ceased to exist; or

(2) None of the specified repositories is a recognized repository.

2. The Secretary of State will not give notice of a suspension requested pursuant to NAC 720.570 unless the person requesting the suspension pays in advance any fee for publication required by each repository where the notice is to be published.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.610 Discharge of certification authority or subscriber from responsibility for certain transactions. (NRS 720.150)

1. Upon giving notice of the revocation of a certificate as required pursuant to NAC 720.600, the certification authority who issued the certificate is discharged from any liability or other responsibility, with regard to any transactions occurring after the notice is given, for any promise, warranty or certification provided pursuant to NAC 720.480 or 720.490 regarding the certificate.

2. When a certificate expires, the certification authority who issued the certificate, the subscriber identified in the certificate and the agents of that subscriber are discharged from any liability or other responsibility, with regard to any transactions occurring after the expiration occurs, for any promise, warranty or certification provided pursuant to NAC 720.480, 720.490, 720.500, 720.510 or 720.520 regarding the certificate.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

RECOGNIZED REPOSITORIES

NAC 720.650 Designation. (NRS 720.150)

1. The Secretary of State may designate a repository as a recognized repository after he:

(a) Receives:

(1) An application for such a designation submitted by a licensee;

(2) Such evidence as he deems sufficient to determine that the licensee and repository meet the requirements of this chapter; and

(3) Except as otherwise provided in NAC 720.260, the amounts required pursuant to NAC 720.430 and 720.810; and

(b) Determines, if the repository will publish certificates that are not issued by recognized certification authorities, that the certification authorities issuing those certificates conform to legally binding requirements that the Secretary of State determines to be substantially similar to or more stringent than the requirements of this chapter.

2. The designation of a repository as a recognized repository is valid for 1 year unless the designation is revoked or otherwise terminated at an earlier date.

3. The operator of a recognized repository may discontinue its designation as such by:

(a) Filing a notice of discontinuance with the Secretary of State at least 30 days before the date of discontinuance; and

(b) Complying with NAC 720.690.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.660 Application for designation. (NRS 720.150**)** An application for designation as a recognized repository must be on a form prescribed by the Secretary of State and include:

1. The name of the licensee or applicant for a license who will operate the repository;
2. The mailing address and, if different, the physical address of the applicant;
3. The telephone number of the applicant;
4. The electronic mail address of the applicant;
5. The electronic mail address of the repository; and
6. A description of the computer hardware, software and database of the repository that demonstrates compliance with the requirements of this chapter.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.670 Operation. (NRS 720.150**)** A recognized repository:

1. Must be operated by a licensee;
2. Must operate by means of a trustworthy system that:

(a) Provides access to the repository on-line through the Internet on a continuous basis, except for such periods as are reasonably required for scheduled maintenance;

(b) Has the capacity to process transactions in a reasonably adequate manner for the anticipated volume of transactions; and

(c) Provides for the periodic reproduction and secure storage of data, in accordance with NRS 239.051, in a location other than the location of the principal system of the repository;

3. Must include a database that contains:

(a) Certificates that are published in the repository;

(b) Notices of suspended or revoked certificates that are published by recognized certification authorities;

(c) A record of certificates that have expired or been suspended or revoked pursuant to this chapter; and

(d) Any other information required by the Secretary of State; and

4. Must not contain a significant amount of information that is known or reasonably likely to be untrue, inaccurate or unreliable.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.680 Revocation of designation; notice to licensee. (NRS 720.150**)**

1. The designation of a repository as a recognized repository shall be deemed revoked immediately upon the expiration or revocation of the license of the licensee who operates the repository.
2. The Secretary of State may, in accordance with subsection 3 and without revoking the license of the licensee who operates a recognized repository, revoke the designation of the repository as a recognized repository if the Secretary of State determines that the licensee or repository is not in compliance with all the provisions of this chapter.
3. The Secretary of State will inform a licensee who operates a recognized repository of his determination to revoke that designation by mailing a written notice to the mailing address and electronic mail address of the licensee specified on the application for the designation of the repository as a recognized repository. The notice must state the date when the revocation becomes effective, which must not occur until at least 30 days after the mailing of the notice. If the licensee files an application for a hearing on the matter

before the effective date specified in the notice, the revocation does not become effective until so ordered by the hearing officer.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.690 Cessation of operation. (NRS 720.150**)** If a repository of a licensee ceases to operate as a recognized repository, the licensee shall publish the information maintained in the repository in another recognized repository.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.700 State repository. (NRS 720.150**)**

1. The Secretary of State may operate or contract for the operation of a state repository. If the Secretary of State contracts for the operation of the repository by an entity other than the Department of Information Technology, the contractor must be a licensee and agree to operate the repository in compliance with the provisions of this chapter. The Secretary of State may rescind a contract for the operation of the state repository for:

(a) Any ground that would be sufficient for the revocation of the designation of the repository as a recognized repository; or

(b) Any other legally recognized ground for rescission.

2. If a state repository is operated pursuant to subsection 1, the repository must include:

(a) A disclosure record for each licensee;

(b) A list of all judgments filed with the Secretary of State pursuant to NAC 720.410 within the past 5 years;

(c) Each advisory statement published by the Secretary of State pursuant to NAC 720.800; and

(d) Any other information the Secretary of State deems appropriate for inclusion in the state repository.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.710 Liability of licensee. (NRS 720.150**)**

1. Except as otherwise provided in this section, a licensee who operates a recognized repository shall agree to pay for any loss incurred by a person who reasonably relies on a digital signature that is verified by the public key set forth in a suspended or revoked certificate, if the reliance occurs:

(a) More than 1 business day after the licensee receives from a recognized certification authority a request to publish notice of the suspension or revocation; and

(b) Before the licensee has published the notice in the recognized repository it operates.

2. Subsection 1 does not require a licensee to agree to pay any:

(a) Punitive or exemplary damages or damages for pain or suffering; or

(b) Amount in excess of any limitations on obligations, losses or damages listed in the suspended or revoked certificate.

3. A licensee may liquidate, limit, alter or exclude liability for any consequential or incidental damages resulting from the requirements of subsection 1 by:

(a) Agreement with the person who incurs the loss; or

(b) Notification of the person who incurs the loss, before he relies on the digital signature, of the liquidation, limitation, alteration or exclusion,

➥ if the liquidation, limitation, alteration or exclusion is not unconscionable.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

USE AND EFFECT OF DIGITAL SIGNATURE

NAC 720.750 General provisions. (NRS 720.150)

1. Except as otherwise provided by a specific statute, regulation or contract:

(a) An electronic message that bears in its entirety a digital signature which is verified by the public key set forth in a certificate that was a valid certificate when the digital signature was created, is as valid, enforceable and effective as a record set forth on paper.

(b) An electronic message that is digitally signed shall be deemed to be an original of the message.

(c) A digital signature may be accepted in any manner that is reasonable under the circumstances.

2. Except as otherwise provided by a specific statute or regulation:

(a) An electronic message that bears a digital signature does not constitute an instrument pursuant to chapter 104 of NRS unless all the parties to the transaction agree, including any financial institutions affected by the transaction.

(b) In any action for the adjudication of a dispute involving a digital signature, issues regarding jurisdiction, venue and choice of law must be determined in the same manner as if all transactions had been effected through documents set forth on paper.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.760 Public agency: Acceptance and use of digital signature; confidentiality of private key. (NRS 720.150)

1. Except as otherwise provided by a specific statute or regulation, a public agency shall not accept a digital signature as a substitute for a handwritten or facsimile signature unless the digital signature is verified by a valid certificate.

2. Except as otherwise provided in subsection 3 or by a specific statute or regulation, a public agency shall not use a digital signature to conduct official public business unless the digital signature is verifiable with reference to a public key set forth in a valid certificate that identifies the public agency as the subscriber. A public agency may become the subscriber of a certificate issued by a recognized certification authority to conduct through electronic messages any official public business for which any statute or regulation requires the signature of an officer, employee or other agent of the public agency.

3. Subsection 2 does not apply to the use of a digital signature for internal procedures of a public agency unless otherwise required by a specific statute, regulation or court rule, or by the office of financial management, training and controls of the Department of Administration.

4. A private key held by a public agency or any person on behalf of a public agency, and any information that identifies such a private key are confidential.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.770 Acceptance of digital signature as acknowledgment; liability of certification authority. (NRS 720.150)

1. Except as otherwise provided by a specific statute, regulation or contract, a digital signature that is verifiable with reference to the public key set forth in a valid certificate shall be deemed to satisfy the requirements for an acknowledgment, regardless of whether the person who executed the digital signature appeared before the certification authority or a person who is authorized to take acknowledgments in this State, if:

(a) The digitally signed message includes a statement that the digital signature is intended as an acknowledgment;

(b) The digital signature is verified by the public key set forth in the certificate;

(c) The certificate was a valid certificate when the digital signature was affixed; and

(d) The certificate provides that the digital signature satisfies the requirements for an acknowledgment.

2. If a certificate provides that a digital signature satisfies the requirements for an acknowledgment, the certification authority who issued the certificate is liable for the digital signature to the same extent as if the certification authority was a notary public who had acknowledged the signature, except that his liability must not exceed any recommended limit of reliance set forth in the certificate. No certification authority may waive, disclaim or otherwise limit by agreement the provisions of this subsection.

3. As used in this section, "acknowledgment" has the meaning ascribed to it in NRS 240.002.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.780 Reasonable reliance on digital signature or certificate. (NRS 720.150)

1. Except as otherwise provided by a specific statute, regulation or contract, if reliance on a digital signature is not reasonable under the circumstances, the recipient of the digital signature assumes the risk that the digital signature was forged.

2. Any determination of whether it is reasonable to rely upon a certificate or a digital signature verifiable with reference to the public key set forth in a certificate must include, without limitation, an evaluation of:

(a) The facts known to the relying person or of which he has notice, including all the facts stated or incorporated by reference in the certificate;

(b) The value or relative importance of the digitally signed message, if known;

(c) The course of dealing between the relying person and the subscriber, and any available indicia of reliability or unreliability other than the digital signature; and

(d) The usage of the trade, particularly trade conducted by trustworthy systems or other computer systems.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.790 Good faith of certification authority, subscriber and recipient of digital signature. (NRS 720.150)

1. A certification authority, a subscriber and a recipient of a digital signature shall use good faith in the use of a digital signature and in conducting any activities governed by the provisions of this chapter.

2. The provisions of subsection 1 may not be waived, disclaimed or otherwise limited by agreement, except that the parties to an agreement may establish the standards by

which their good faith with regard to one another will be measured if those standards are not manifestly unreasonable.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

ENFORCEMENT

NAC 720.800 Activities of certification authority that create unreasonable risk prohibited; advisory statement from Secretary of State. (NRS 720.150**)**

1. A certification authority shall not conduct any activities as a certification authority in any manner that creates an unreasonable risk of loss to any subscriber of the certification authority, any person relying on a certificate issued by the certification authority or any repository.

2. If the Secretary of State determines that the activities of a certification authority create a risk of loss to any subscriber of the certification authority, any person relying on a certificate issued by the certification authority or any repository, the Secretary of State may publish a brief statement generally advising subscribers, persons who rely on digital signatures and repositories about those activities.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.810 Investigation of applicant; payment of costs of investigation. (NRS 720.150**,** 720.180**)**

1. The Secretary of State may conduct such an investigation of an applicant as he determines is necessary to determine the qualifications of the applicant and whether the applicant is in compliance with the provisions of this chapter and chapter 720 of NRS. Except as otherwise provided in NAC 720.260 or unless waived by the Secretary of State, all fees and other costs incurred by the Secretary of State to conduct the investigation must be paid by the applicant.

2. Before commencing the investigation of an applicant, the Secretary of State may require the applicant to deposit such an amount as the Secretary of State estimates will be necessary to pay the fees and other costs of that investigation. Upon taking final action on the application, the Secretary of State will provide the applicant with an itemized statement of the fees and other costs incurred and refund any unexpended portion of the amount deposited.

3. As used in this section, "applicant" means a person who submits an application pursuant to NAC 720.270, 720.420 or 720.650.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.820 Examination and copying of records of licensee. (NRS 720.150**)** To determine compliance with this chapter and chapter 720 of NRS, the Secretary of State may:

1. Without prior notice, examine in any manner that is reasonable under the circumstances the records of a licensee, whether maintained within or outside of this State. The licensee shall make his records available to the Secretary of State in legible form.

2. Copy any records of a licensee or require the licensee to provide the Secretary of State with copies of any of his records, to such an extent and in such a manner as is reasonable under the circumstances.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.830 Investigatory authority of Secretary of State. (NRS 720.150)

1. The Secretary of State may conduct any investigation, whether within or outside of this State, as he determines is necessary to ascertain whether a person has violated or is about to violate this chapter or chapter 720 of NRS, or to aid in the enforcement of this chapter or chapter 720 of NRS.

2. To carry out subsection 1, the Secretary of State or any employee designated by the Secretary of State may conduct hearings, administer oaths and affirmations, render findings of fact and conclusions of law, subpoena witnesses, compel their attendance, take evidence and require the production, by subpoena or otherwise, of books, papers, correspondence, memoranda, agreements or other documents or records which the Secretary of State determines to be relevant or material to the investigation. A person whom the Secretary of State does not consider to be the subject of an investigation is entitled to reimbursement at the rate of 25 cents per page for copies of documents which he is required by subpoena to produce. The Secretary of State may require or permit a person to file a statement, under oath or otherwise as the Secretary of State determines, as to the facts and circumstances concerning the matter to be investigated.

3. If the activities constituting an alleged violation for which the information is sought would be a violation of this chapter or chapter 720 of NRS had the activities occurred in this State, the Secretary of State may issue and apply to enforce subpoenas in this State at the request of a comparable licensing agency of another state.

4. If a person does not testify or produce any documents as required by a subpoena issued pursuant to this section, the Secretary of State may apply to the court for an order compelling compliance. A request for such an order may be addressed to:

(a) The district court in and for the county where service may be obtained on the person refusing to testify or produce, if the person is subject to service of process in this State; or

(b) A court of another state having jurisdiction over the person refusing to testify or produce, if the person is not subject to service of process in this State.

5. Not later than the time the Secretary of State requests an order for compliance, he shall:

(a) Send notice of the request by certified mail, return receipt requested, to the respondent at the last known address of the respondent; or

(b) Take other steps reasonably calculated to give the respondent actual notice.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.840 Payment of costs of investigation of licensee. (NRS 720.150, 720.180)

1. Except as otherwise provided in NAC 720.260, a licensee shall pay all proper costs incurred by the Secretary of State to conduct an investigation of the licensee pursuant to NAC 720.830.

2. The Secretary of State may require the licensee to deposit such an amount as the Secretary of State estimates will be necessary to pay those costs. The licensee shall remit:

(a) The deposit within 15 days after the Secretary of State provides the licensee with a statement of that estimate; and

(b) Any other balance due for the investigation within 45 days after the Secretary of State provides the licensee with a bill for that amount.

➥ The Secretary of State may issue an order for the denial, suspension or revocation of the license of a licensee who fails to comply with the provisions of this subsection.

3. For the purposes of this section, "proper costs" includes, without limitation:

(a) Not less than $500 for the compensation of employees of the Secretary of State for time spent:

(1) Traveling to and from the site of the investigation;

(2) Conducting the investigation; and

(3) Preparing a report of the investigation,

➥ at a rate of $50 per hour for each employee;

(b) The per diem allowance and travel expenses of the employees of the Secretary of State conducting the investigation, as provided for state officers and employees generally; and

(c) The cost of supplies, materials, photocopying and postage incurred in conducting the investigation.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.850 Issuance of orders for enforcement. (NRS 720.150**,** 720.190**)**

1. Except as otherwise provided in this section, the Secretary of State may, as appropriate, issue an order denying, suspending or revoking a license, limiting any of the activities as a certification authority in this State of a licensee or an applicant for a license or imposing a civil penalty on a licensee if the Secretary of State determines that the order is in the public interest and that the licensee or applicant for a license has:

(a) Filed with the Secretary of State an application for a license which, on the effective date of the application or, in the case of an order denying a license any date after the filing of the application, was incomplete in a material respect or contained a statement that was, in light of the circumstances under which the statement was made, false or misleading with regard to a material fact;

(b) Violated or failed to comply with a provision of this chapter or chapter 720 of NRS;

(c) Within the last 10 years been convicted of a felony or misdemeanor that the Secretary of State determines to have:

(1) Arisen out of the conduct of business as a certification authority or repository; or

(2) Involved larceny, theft, robbery, extortion, forgery, counterfeiting, fraudulent concealment, embezzlement, fraudulent conversion, misappropriation of money, or any similar offense or conspiracy to commit such an offense;

(d) Been temporarily or permanently enjoined by any court of competent jurisdiction, from:

(1) Performing any activity as a certification authority or repository;

(2) Performing any activity as an affiliated person or employee of a certification authority or repository; or

(3) Engaging in or continuing any conduct or practice in connection with an activity described in subparagraph (1) or (2),

➥ unless the order has been vacated;

(e) Been or is the subject of an order of the Secretary of State for the denial, suspension or revocation of a license, unless the order has been vacated;

(f) Been or is the subject of an order issued within the last 5 years under the authority of another country or state or a Canadian province or territory, after the provision of notice and an opportunity for a hearing:

(1) For the denial, suspension or revocation of a license as a certification authority; or

(2) To cease and desist any activity as a certification authority,

➥ unless the order has been vacated; or

(g) Become insolvent. For the purposes of this paragraph, "insolvent" means that:

(1) The liabilities of a person exceed his assets; or

(2) A person is unable to meet his obligations as they mature.

2. If the Secretary of State, when a license becomes effective, has knowledge of any fact or transaction for which he may issue an order pursuant to subsection 1, he must commence proceedings for the issuance of the order within 90 days after the issuance of the license.

3. If the Secretary of State determines that a licensee or an applicant for a license has ceased to exist or to do business as a certification authority, the Secretary of State may issue an order revoking the license or denying the application for a license.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

PROCEEDINGS

NAC 720.900 Applicability of chapter 233B of NRS; request for administrative hearing. (NRS 720.150)

1. Except as otherwise provided in this chapter, the provisions of this chapter must be carried out in accordance with the provisions of chapter 233B of NRS.

2. A person affected by a determination or action of the Secretary of State made pursuant to this chapter may request an administrative hearing on the matter before a hearing officer by submitting an application for such a hearing to the Secretary of State. The application:

(a) May be submitted on a form provided by the Secretary of State, or on another document or in an electronic message signed by the applicant or his representative; and

(b) Must specify each issue to be considered at the hearing.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.910 Persons permitted to appear in representative capacity. (NRS 720.150) No person may appear in a representative capacity in an administrative hearing conducted pursuant to this chapter except:

1. An attorney who is admitted to practice law in this State.

2. An authorized officer, manager, partner or full-time employee of an organization or governmental entity who appears on behalf of the organization or governmental entity.

3. A natural person who represents himself.

4. An interpreter for a person who:

(a) Speaks a language other than English and does not know the English language; or

(b) Is a handicapped person, as that term is defined in NRS 50.050.

5. Such other persons as the hearing officer allows, based upon his determination that it would be unduly burdensome to require a person to use one of the representatives identified in subsections 1 and 2.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.920 Rebuttable presumptions. (NRS 720.150**)** For the purposes of an administrative hearing conducted pursuant to this chapter or any other adjudication of a dispute involving a digital signature, there is a rebuttable presumption that:

1. A certificate that has been:

(a) Digitally signed by a recognized certification authority; and

(b) Published in a recognized repository or otherwise made available by the certification authority who issued the certificate or the subscriber identified in the certificate,

➥ has been issued by that certification authority and accepted by that subscriber.

2. The information set forth in a valid certificate and confirmed by the certification authority who issued the certificate is accurate.

3. If a digital signature is verified by the public key set forth in a valid certificate:

(a) The digital signature is the digital signature of the subscriber identified in that certificate;

(b) The digital signature was affixed by that subscriber with the intention of signing the message;

(c) The message associated with the digital signature has not been altered since the signature was affixed; and

(d) The recipient of that digital signature has no notice or knowledge that:

(1) The subscriber has breached any term of his promise pursuant to NAC 720.530; or

(2) The signer does not rightfully hold the private key used to create the digital signature.

4. A digital signature was created before it was time stamped by a disinterested person using a trustworthy system.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.930 Filing of documents in electronic form; service by electronic transmission. (NRS 720.150**)** In an administrative hearing conducted pursuant to this chapter:

1. A party to the hearing may, unless the hearing officer directs otherwise, file any pleading or other document in electronic form.

2. If a pleading or other document that is filed electronically must be signed, it must be signed with a digital signature that is verifiable by a valid certificate issued by a certification authority who is not a party to the hearing.

3. The service of a pleading or other document by electronic transmission shall be deemed effective upon receipt, except that such an electronic transmission which is sent after 5 p.m. on a business day or at any time on a weekend or state holiday shall be deemed effective at 8 a.m. on the next business day.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.940 Summary proceeding. (NRS 720.150**)**

1. As an alternative to any other authorized procedure, the Secretary of State may commence a proceeding under this chapter or chapter 720 of NRS by entering a summary order pursuant to this section. The order must be in writing and may be entered without providing any prior notice or opportunity for a hearing, and need not be supported by findings of fact or conclusions of law.

2. Upon the entry of a summary order pursuant to subsection 1, the Secretary of State will promptly notify in writing all persons against whom action is taken or contemplated that the summary order has been entered and the reasons therefor. The Secretary of State will send all persons against whom action is taken a notice of an opportunity for a hearing on the matters set forth in the order. The notice must state that the persons have 15 calendar days after receipt of the notice to mail a written request for a hearing to the Secretary of State.

3. The Secretary of State will set the matter for a hearing on a date not more than 60 or less than 15 calendar days after the receipt of the request for a hearing, and will promptly notify the parties of the time and place for the hearing. The time of the hearing may be continued upon the written request of a party for good cause shown.

4. The Secretary of State may issue an order that makes a summary order final:

(a) Fifteen days after a person against whom action is taken or contemplated receives notice of the right to request a hearing, if that person fails to request a hearing; or

(b) If a party fails to appear at a hearing, on the date set for the hearing.

5. If a hearing is requested, the Secretary of State may:

(a) Extend the summary order until final determination of the matter; or

(b) After providing further notice of an opportunity for a prior hearing to all parties against whom action is taken or contemplated, modify or vacate the summary order.

6. For the purposes of this section, notice is complete:

(a) Upon delivery personally to a person;

(b) By mailing by certified mail to the last known address of a person; or

(c) By mailing by electronic mail to the address of a person specified on an application submitted by the person pursuant to this chapter to the Secretary of State.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NAC 720.950 Emergency administrative proceeding. (NRS 720.150)

1. To carry out the provisions of this chapter or chapter 720 of NRS and as an alternative to any other authorized procedure, the Secretary of State may use an emergency administrative proceeding pursuant to this section if there is an immediate danger to the public welfare requiring immediate action.

2. The Secretary of State may take only such action pursuant to this section as is necessary to prevent or avoid the immediate danger to the public welfare that justifies the use of an emergency administrative proceeding.

3. An order issued pursuant to this section will include a brief statement of:

(a) Findings of fact;

(b) Conclusions of law; and

(c) The reasons for:

(1) Determining that there is an immediate danger to the public welfare; and

(2) The decision of the Secretary of State to take the specific action ordered.

4. The Secretary of State will give such notice as is practicable to persons who are required to comply with the order. The order is effective when issued.

5. After issuing an order pursuant to this section, the Secretary of State will proceed as quickly as feasible to complete the proceedings in the manner otherwise provided pursuant to the provisions of chapter 233B of NRS.

6. The record of the Secretary of State consists of the documents regarding the matter that were considered or prepared by him. The Secretary of State will maintain these documents as the official record.

7. Except as otherwise required by law, the official record need not constitute the exclusive basis for his action in an emergency administrative proceeding or for judicial review of the action.

8. An order issued pursuant to this section is subject to judicial review in the manner provided in chapter 233B of NRS for the final decision in a contested case.

(Added to NAC by Sec'y of State by R155-98, eff. 12-2-99)

NEVADA REVISED STATUTES

Title 59 - ELECTRONIC RECORDS AND TRANSACTIONS

CHAPTER 719
ELECTRONIC TRANSACTIONS (UNIFORM ACT)

NRS 719.350 **Acceptance and distribution of electronic records by governmental agencies.**

_____

NRS 719.010 Short title. This chapter may be cited as the Uniform Electronic Transactions Act.

(Added to NRS by 2001, 2714)

NRS 719.020 Definitions. As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 719.030 to 719.180, inclusive, have the meanings ascribed to them in those sections.

(Added to NRS by 2001, 2714)

NRS 719.030 "Agreement" defined. "Agreement" means the bargain of the parties in fact, as found in their language or inferred from other circumstances and from rules, regulations and procedures given the effect of agreements under laws otherwise applicable to a particular transaction.

(Added to NRS by 2001, 2714)

NRS 719.040 "Automated transaction" defined. "Automated transaction" means a transaction conducted or performed, in whole or in part, by electronic means or electronic records, in which the acts or records of one or both parties are not reviewed by a natural person in the ordinary course in forming a contract, performing under an existing contract or fulfilling an obligation required by the transaction.

(Added to NRS by 2001, 2714)

NRS 719.050 "Computer program" defined. "Computer program" means a set of statements or instructions to be used directly or indirectly in an information processing system in order to bring about a certain result.

(Added to NRS by 2001, 2715)

NRS 719.060 "Contract" defined. "Contract" means the total legal obligation resulting from the parties' agreement as affected by this chapter and other applicable law.

(Added to NRS by 2001, 2715)

NRS 719.070 "Electronic" defined. "Electronic" means relating to technology having electrical, digital, magnetic, wireless, optical, electromagnetic or similar capabilities.

(Added to NRS by 2001, 2715)

NRS 719.080 "Electronic agent" defined. "Electronic agent" means a computer program or an electronic or other automated means used independently to initiate an action or respond to electronic records or performances in whole or in part, without review or action by a natural person.

(Added to NRS by 2001, 2715)

NRS 719.090 "Electronic record" defined. "Electronic record" means a record created, generated, sent, communicated, received or stored by electronic means.

(Added to NRS by 2001, 2715)

NRS 719.100 "Electronic signature" defined. "Electronic signature" means an electronic sound, symbol or process attached to or logically associated with a record and executed or adopted by a person with the intent to sign the record.

(Added to NRS by 2001, 2715)

NRS 719.110 "Governmental agency" defined. "Governmental agency" means an executive, legislative or judicial agency, department, board, commission, authority, institution or instrumentality of the Federal Government or of a state or of a county, municipality or other political subdivision of a state.

(Added to NRS by 2001, 2715)

NRS 719.120 "Information" defined. "Information" means data, text, images, sounds, codes, computer programs, software, databases or the like.

(Added to NRS by 2001, 2715)

NRS 719.130 "Information processing system" defined. "Information processing system" means an electronic system for creating, generating, sending, receiving, storing, displaying or processing information.

(Added to NRS by 2001, 2715)

NRS 719.140 "Person" defined. "Person" includes a governmental agency and a public corporation.

(Added to NRS by 2001, 2715)

NRS 719.150 "Record" defined. "Record" means information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form.

(Added to NRS by 2001, 2715)

NRS 719.160 "Security procedure" defined. "Security procedure" means a procedure employed for the purpose of verifying that an electronic signature, record or performance is that of a specific person or for detecting changes or errors in the information in an electronic record. The term includes a procedure that requires the use of algorithms or other codes, identifying words or numbers, encryption or callback, or other acknowledgment procedures.

(Added to NRS by 2001, 2715)

NRS 719.170 "State" defined. "State" means a state of the United States, the District of Columbia, Puerto Rico, the United States Virgin Islands or any territory or insular possession subject to the jurisdiction of the United States. The term includes an Indian tribe or band, or Alaskan native village, which is recognized by federal law or formally acknowledged by a state.

(Added to NRS by 2001, 2715)

NRS 719.180 "Transaction" defined. "Transaction" means an action or set of actions occurring between two or more persons relating to the conduct of business, commercial or governmental affairs.

(Added to NRS by 2001, 2715)

NRS 719.200 Scope.

1. Except as otherwise provided in subsection 2, the provisions of this chapter apply to electronic records and electronic signatures relating to a transaction.

2. The provisions of this chapter do not apply to a transaction to the extent it is governed by:

(a) A law governing the creation and execution of wills, codicils or testamentary trusts; or

(b) The Uniform Commercial Code other than NRS 104.1107, 104.1206 and 104.2101 to 104.2725, inclusive, and 104A.2101 to 104A.2532, inclusive.

3. The provisions of this chapter apply to an electronic record or electronic signature otherwise excluded from the application of this chapter under subsection 2 to the extent it is governed by a law other than those specified in subsection 2.

4. A transaction subject to the provisions of this chapter is also subject to other applicable substantive law.

(Added to NRS by 2001, 2715)

NRS 719.210 Prospective application; application of Electronic Signatures in Global and National Commerce Act.

1. The provisions of this chapter apply to any electronic record or electronic signature created, generated, sent, communicated, received or stored on or after October 1, 2001.

2. The provisions of section 101(c) of the Electronic Signatures in Global and National Commerce Act, 15 U.S.C. §§ 7001 et seq., apply under this chapter to a transaction in which a natural person acquires goods or services that are used primarily for personal, family or household purposes.

(Added to NRS by 2001, 2716)

NRS 719.220 Use of electronic records and electronic signatures; variation by agreement.

1. The provisions of this chapter do not require a record or signature to be created, generated, sent, communicated, received, stored or otherwise processed or used by electronic means or in electronic form.

2. The provisions of this chapter apply only to transactions between parties each of whom has agreed to conduct transactions by electronic means. Whether the parties agree to conduct a transaction by electronic means is determined from the context and surrounding circumstances, including the parties' conduct.

3. A party that agrees to conduct a transaction by electronic means may refuse to conduct other transactions by electronic means. The right granted by this subsection may not be waived by agreement.

4. Except as otherwise provided in this chapter, the effect of any of the provisions of this chapter may be varied by agreement. The presence in certain provisions of this chapter of the words "unless otherwise agreed" or words of similar import does not imply that the effect of other provisions may not be varied by agreement.

5. Whether an electronic record or electronic signature has legal consequences is determined by the provisions of this chapter and other applicable law.

(Added to NRS by 2001, 2716)

NRS 719.230 Application and construction: Promotion of uniformity. In applying and construing this uniform act, consideration must be given to the need to promote uniformity of the law with respect to its subject matter among states that enact it.

(Added to NRS by 2001, 2721)

NRS 719.240 Legal recognition of electronic records, electronic signatures and electronic contracts.

1. A record or signature may not be denied legal effect or enforceability solely because it is in electronic form.

2. A contract may not be denied legal effect or enforceability solely because an electronic record was used in its formation.

3. If a law requires a record to be in writing, an electronic record satisfies the law.

4. If a law requires a signature, an electronic signature satisfies the law.

(Added to NRS by 2001, 2716)

NRS 719.250 Provision of information in writing; presentation of records.

1. If parties have agreed to conduct a transaction by electronic means and a law requires that a contract or other record relating to the transaction be in writing, the legal effect, validity or enforceability of the contract or other record may be denied if an electronic record of the contract or other record is not in a form that is capable of being retained and accurately reproduced for later reference by all parties or other persons who are entitled to retain the contract or record.

2. If a law other than this chapter requires a record to be posted or displayed in a certain manner, to be sent, communicated or transmitted by a specified method or to contain information that is formatted in a certain manner, the following rules apply:

(a) The record must be posted or displayed in the manner specified in the other law.

(b) Except as otherwise provided in paragraph (b) of subsection 6, the record must be sent, communicated or transmitted by the method specified in the other law.

(c) The record must contain the information formatted in the manner specified in the other law.

3. If a sender inhibits the ability of a recipient to store or print an electronic record, the electronic record is not enforceable against the recipient.

4. A requirement that a notice be in writing is not satisfied by providing or delivering the notice electronically if the notice is a notice of:

(a) The cancellation or termination of service by a public utility;

(b) Default, acceleration, repossession, foreclosure or eviction, or the right to cure, under a credit agreement secured by, or a rental agreement for, a primary residence of a natural person;

(c) The cancellation or termination of a policy of health insurance, benefits received pursuant to a policy of health insurance or benefits received pursuant to a policy of life insurance, excluding annuities; or

(d) The recall of a product, or material failure of a product, that risks endangering the health or safety of a person.

5. A requirement that a document be in writing is not satisfied by providing or delivering the document electronically if the document is required to accompany any transportation or handling of hazardous materials, pesticides, or other toxic or dangerous materials.

6. The requirements of this section may not be varied by agreement, but:

(a) To the extent a law other than this chapter requires that a contract or other record relating to a transaction be in writing but permits that requirement to be varied by agreement, the provisions of subsection 1 concerning the denial of the legal effect, validity or enforceability of a contract or other record relating to a transaction may also be varied by agreement; and

(b) A requirement under a law other than this chapter to send, communicate or transmit a record by first-class mail, postage prepaid, regular United States mail, may be varied by agreement to the extent permitted by the other law.

(Added to NRS by 2001, 2716)

NRS 719.260 Attribution and effect of electronic record and electronic signature.

1. An electronic record or electronic signature is attributable to a person if it was the act of the person. The act of the person may be shown in any manner, including a showing of the efficacy of any security procedure applied to determine the person to whom the electronic record or electronic signature was attributable.

2. The effect of an electronic record or electronic signature attributed to a person under subsection 1 is determined from the context and surrounding circumstances at the time of its creation, execution or adoption, including the parties' agreement, if any, and otherwise as provided by law.

(Added to NRS by 2001, 2717)

NRS 719.270 Effect of change or error. If a change or error in an electronic record occurs in a transmission between parties to a transaction, the following rules apply:

1. If the parties have agreed to use a security procedure to detect changes or errors and one party has conformed to the procedure, but the other party has not, and the nonconforming party would have detected the change or error had that party also conformed, the conforming party may avoid the effect of the changed or erroneous electronic record.

2. In an automated transaction involving a natural person, the natural person may avoid the effect of an electronic record that resulted from an error made by him in dealing with the electronic agent of another person if the electronic agent did not provide an opportunity for the prevention or correction of the error and, at the time the natural person learns of the error, the natural person:

(a) Promptly notifies the other person of the error and that the natural person did not intend to be bound by the electronic record received by the other person;

(b) Takes reasonable steps, including steps that conform to the other person's reasonable instructions, to return to the other person or, if instructed by the other person, to destroy the consideration received, if any, as a result of the erroneous electronic record; and

(c) Has not used or received any benefit or value from the consideration, if any, received from the other person.

3. If neither subsection 1 nor subsection 2 applies, the change or error has the effect provided by other law, including the law of mistake and the parties' contract, if any.

4. Subsections 2 and 3 may not be varied by agreement.

(Added to NRS by 2001, 2718)

NRS 719.280 Notarization and acknowledgment. If a law requires a signature or record to be notarized, acknowledged, verified or made under oath, the 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 law, is attached to or logically associated with the signature or record.

(Added to NRS by 2001, 2718)

NRS 719.290 Retention of electronic records; originals.

1. If a law requires that a record be retained, the requirement is satisfied by retaining an electronic record of the information in the record which:

(a) Accurately reflects the information set forth in the record after it was first generated in its final form as an electronic record or otherwise; and

(b) Remains accessible to all persons who are legally entitled to access to the record, for the period required by law, in a form that is capable of being accurately reproduced for later reference.

2. A requirement to retain a record in accordance with subsection 1 does not apply to any information the sole purpose of which is to enable the record to be sent, communicated or received.

3. A person may satisfy subsection 1 by using the services of another person if the requirements of that subsection are satisfied.

4. If a law requires a record to be presented or retained in its original form, or provides consequences if the record is not presented or retained in its original form, that law is satisfied by an electronic record retained in accordance with subsection 1.

5. If a law requires retention of a check, that requirement is satisfied by retention of an electronic record of the information on the front and back of the check in accordance with subsection 1.

6. A record retained as an electronic record in accordance with subsection 1 satisfies a law requiring a person to retain a record for evidentiary, audit or like purposes, unless a law enacted after October 1, 2001, specifically prohibits the use of an electronic record for the specified purpose.

7. This section does not preclude a governmental agency of this state from specifying additional requirements for the retention of a record subject to the agency's jurisdiction.

(Added to NRS by 2001, 2718)

NRS 719.300 Admissibility in evidence. In a proceeding, evidence of a record or signature must not be excluded solely because it is in electronic form.

(Added to NRS by 2001, 2719)

NRS 719.310 Automated transaction. In an automated transaction, the following rules apply:

1. A contract may be formed by the interaction of electronic agents of the parties, even if no natural person was aware of or reviewed the electronic agents' actions or the resulting terms and agreements.

2. A contract may be formed by the interaction of an electronic agent and a natural person, acting on his own behalf or for another person, as by an interaction in which the natural person performs actions that he is free to refuse to perform and which he knows or has reason to know will cause the electronic agent to complete the transaction or performance.

3. The terms of the contract are determined by the substantive law applicable to it.

(Added to NRS by 2001, 2719)

NRS 719.320 Time and place of sending and receipt.

1. Unless otherwise agreed between the sender and the recipient, an electronic record is sent when it:

(a) Is addressed properly or otherwise directed properly to an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record;

(b) Is in a form capable of being processed by that system; and

(c) Enters an information processing system outside the control of the sender or of a person that sent the electronic record on behalf of the sender or enters a region of the information processing system designated or used by the recipient which is under the control of the recipient.

2. Unless otherwise agreed between a sender and the recipient, an electronic record is received when:

(a) It enters an information processing system that the recipient has designated or uses for the purpose of receiving electronic records or information of the type sent and from which the recipient is able to retrieve the electronic record; and

(b) It is in a form capable of being processed by that system.

3. Subsection 2 applies even if the place the information processing system is located is different from the place the electronic record is deemed to be received under subsection 4.

4. Unless otherwise expressly provided in the electronic record or agreed between the sender and the recipient, an electronic record is deemed to be sent from the sender's place of business and to be received at the recipient's place of business. For purposes of this subsection, the following rules apply:

(a) If the sender or recipient has more than one place of business, his place of business is the place having the closest relationship to the underlying transaction.

(b) If the sender or the recipient does not have a place of business, the place of business is the sender's or recipient's residence, as the case may be.

5. An electronic record is received under subsection 2 even if no natural person is aware of its receipt.

6. Receipt of an electronic acknowledgment from an information processing system described in subsection 2 establishes that a record was received but, by itself, does not establish that the content sent corresponds to the content received.

7. If a person is aware that an electronic record purportedly sent under subsection 1, or purportedly received under subsection 2, was not actually sent or received, the legal effect of the sending or receipt is determined by other applicable law. Except to the extent permitted by the other law, the requirements of this subsection may not be varied by agreement.

(Added to NRS by 2001, 2719)

NRS 719.330 Transferable records.

1. In this section, "transferable record" means an electronic record that:

(a) Would be a note under NRS 104.3101 to 104.3605, inclusive, or a document under NRS 104.7101 to 104.7603, inclusive, if the electronic record were in writing; and

(b) The issuer of the electronic record expressly has agreed is a transferable record.

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

3. A system satisfies subsection 2, and a person is deemed to have control of a transferable record, if the transferable record is created, stored and assigned in such a manner that:

(a) A single authoritative copy of the transferable record exists which is unique, identifiable, and, except as otherwise provided in paragraphs (d), (e) and (f), unalterable;

(b) The authoritative copy identifies the person asserting control as:

(1) The person to whom the transferable record was issued; or

(2) If the authoritative copy indicates that the transferable record has been transferred, the person to whom the transferable record was most recently transferred;

(c) The authoritative copy is communicated to and maintained by the person asserting control or its designated custodian;

(d) Copies or revisions that add or change an identified assignee of the authoritative copy can be made only with the consent of the person asserting control;

(e) Each copy of the authoritative copy and any copy of a copy is readily identifiable as a copy that is not the authoritative copy; and

(f) Any revision of the authoritative copy is readily identifiable as authorized or unauthorized.

4. Except as otherwise agreed, a person having control of a transferable record is the holder, as defined in subsection 20 of NRS 104.1201, of the transferable record and has the same rights and defenses as a holder of an equivalent record or writing under the Uniform Commercial Code, including, if the applicable statutory requirements under NRS 104.7501, 104.9308 or subsection 1 of NRS 104.3302 are satisfied, the rights and defenses of a holder to whom a negotiable document of title has been duly negotiated, a purchaser, or a holder in due course, respectively. Delivery, possession and endorsement are not required to obtain or exercise any of the rights under this subsection.

5. Except as otherwise agreed, an obligor under a transferable record has the same rights and defenses as an equivalent obligor under equivalent records or writings under the Uniform Commercial Code.

6. If requested by a person against whom enforcement is sought, the person seeking to enforce the transferable record shall provide reasonable proof that he is in

control of the transferable record. Proof may include access to the authoritative copy of the transferable record and related business records sufficient to review the terms of the transferable record and to establish the identity of the person having control of the transferable record.

(Added to NRS by 2001, 2720)

NRS 719.340 Creation and retention of electronic records and conversion of written records by governmental agencies. Each governmental agency of this State shall determine whether, and the extent to which, it will create and retain electronic records and convert written records to electronic records.

(Added to NRS by 2001, 2721)

NRS 719.350 Acceptance and distribution of electronic records by governmental agencies.

1. Except as otherwise provided in subsection 6 of NRS 719.290, each governmental agency of this state shall determine whether, and the extent to which, it will send and accept electronic records and electronic signatures to and from other persons and otherwise create, generate, communicate, store, process, use and rely upon electronic records and electronic signatures.

2. To the extent that a governmental agency uses electronic records and electronic signatures under subsection 1, the governmental agency, giving due consideration to security, may specify:

(a) The manner and format in which the electronic records must be created, generated, sent, communicated, received and stored and the systems established for those purposes;

(b) If electronic records must be signed by electronic means, the type of electronic signature required, the manner and format in which the electronic signature must be affixed to the electronic record, and the identity of, or criteria that must be met by, any third party used by a person filing a document to facilitate the process;

(c) Processes and procedures as appropriate to ensure adequate preservation, disposition, integrity, security, confidentiality and auditability of electronic records; and

(d) Any other required attributes for electronic records which are specified for corresponding nonelectronic records or reasonably necessary under the circumstances.

3. Except as otherwise provided in subsection 6 of NRS 719.290, the provisions of this chapter do not require a governmental agency of this state to use or permit the use of electronic records or electronic signatures.

(Added to NRS by 2001, 2721)

NEVADA REVISED STATUTES

Title 59 - ELECTRONIC RECORDS AND TRANSACTIONS

CHAPTER 720
DIGITAL SIGNATURES

NRS 720.010 Definitions. As used in this chapter, unless the context otherwise requires, the words and terms defined in NRS 720.020 to 720.130, inclusive, have the meanings ascribed to them in those sections.

(Added to NRS by 1999, 1953; A 2001, 2722)

NRS 720.020 “Asymmetric cryptosystem” defined. “Asymmetric cryptosystem” means an algorithm or series of algorithms that provide a secure key pair.

(Added to NRS by 1999, 1953)

NRS 720.030 “Certificate” defined. “Certificate” means a computer-based record that:

1. Identifies the certification authority using it;
2. Identifies a subscriber;
3. Sets forth the public key of the subscriber; and
4. Is digitally signed by the certification authority issuing it.

(Added to NRS by 1999, 1953)

NRS 720.040 "Certification authority" defined. "Certification authority" means a person who issues a certificate.

(Added to NRS by 1999, 1953)

NRS 720.050 "Correspond" defined. "Correspond" means, with reference to keys, belonging to the same key pair.

(Added to NRS by 1999, 1953)

NRS 720.060 "Digital signature" defined. "Digital signature" means an electronic signature that transforms a message by using an asymmetric cryptosystem. As used in this section, "electronic signature" has the meaning ascribed to it in NRS 719.100.

(Added to NRS by 1999, 1953; A 2001, 2722)

NRS 720.070 "Hold a private key" defined. "Hold a private key" means to be authorized to use a private key.

(Added to NRS by 1999, 1954)

NRS 720.080 "Key pair" defined. "Key pair" means a private key and its corresponding public key in an asymmetric cryptosystem, which may be used in such a manner that the public key can verify a digital signature created by the private key.

(Added to NRS by 1999, 1954)

NRS 720.090 "Message" defined. "Message" means a digital representation of information.

(Added to NRS by 1999, 1954)

NRS 720.100 "Private key" defined. "Private key" means the key of a key pair used to create a digital signature.

(Added to NRS by 1999, 1954)

NRS 720.110 "Public key" defined. "Public key" means the key of a key pair used to verify a digital signature.

(Added to NRS by 1999, 1954)

NRS 720.115 "Record" defined. "Record" has the meaning ascribed to it in NRS 719.150.

(Added to NRS by 2001, 2721)

NRS 720.120 "Subscriber" defined. "Subscriber" means a person who:

1. Is identified as such in a certificate;
2. Accepts the certificate; and
3. Holds the private key that corresponds to the public key set forth in the certificate.

(Added to NRS by 1999, 1954)

NRS 720.130 "Verify a digital signature" defined. "Verify a digital signature" means, in relation to a given digital signature, message and public key, to determine accurately that:

1. The digital signature was created by the private key corresponding to the public key; and

2. The message has not been altered since the digital signature was created.

(Added to NRS by 1999, 1954)

NRS 720.140 Applicability of chapter.

1. The provisions of this chapter apply to any transaction for which a digital signature is used to sign an electronic record.

2. As used in this section, "electronic record" has the meaning ascribed to it in NRS 719.090.

(Added to NRS by 1999, 1954; A 2001, 2722)

NRS 720.150 Adoption of regulations by Secretary of State. The Secretary of State shall adopt regulations regarding digital signatures, including, without limitation, regulations pertaining to:

1. The use of a digital signature, including, without limitation, standards for the commercial use of a digital signature;

2. Licensure of a certification authority, including, without limitation, professional standards that a certification authority must meet in conducting its business;

3. The verification of a digital signature;

4. The liability that may be incurred by a subscriber, certification authority or recipient of a message transformed by a digital signature, including, without limitation, the limitation of such liability;

5. The use of a digital signature as an acknowledgment, as that term is defined in NRS 240.002;

6. The issuance of injunctions and orders and the imposition of civil penalties pursuant to NRS 720.190;

7. The status of a private key as personal property;

8. The responsibilities of a subscriber with respect to the use and handling of a private key;

9. The confidentiality of information represented in a message that is transformed by a digital signature; and

10. Any other aspect of the use or verification of digital signatures that the Secretary of State determines to be necessary.

(Added to NRS by 1999, 1955)

NRS 720.160 Use of digital signature.

1. Except as otherwise provided in this section, if each person who will be involved in the submission and acceptance of a record agrees to the use of a digital signature, the use of a message which:

(a) Represents the record; and

(b) Is transformed by a digital signature,

constitutes a sufficient signing of the record.

2. The provisions of this section do not apply with respect to:

(a) A record that is required to be signed in the presence of a third party; or

(b) A record with respect to which the requirement that the record must be signed is accompanied by an additional qualifying requirement.

(Added to NRS by 1999, 1954; A 2001, 2722)

NRS 720.180 Licensure of certification authorities: Requirement; fee.

1. A person shall not conduct business as a certification authority without first obtaining a license as a certification authority from the Secretary of State.

2. The Secretary of State may charge a reasonable fee for such licensure.

(Added to NRS by 1999, 1955)

NRS 720.190 Enforcement of chapter: Injunctions and other orders; civil penalty. The Secretary of State may:

1. Issue injunctions and orders to enforce the provisions of this chapter and any regulations adopted by the Secretary of State pursuant thereto.

2. Impose a civil penalty not to exceed $10,000 for a willful violation of a provision of this chapter or a regulation adopted by the Secretary of State pursuant thereto.

(Added to NRS by 1999, 1955)

NRS 720.200 Unlawful acts; penalty.

1. It is unlawful for a person to:

(a) Forge a digital signature; or

(b) Provide false information knowingly to the Secretary of State with respect to any provision of this chapter or a regulation adopted pursuant thereto that requires such a person to provide information to the Secretary of State.

2. A person who violates the provisions of subsection 1 is guilty of a gross misdemeanor.

3. As used in this section, “forge a digital signature” means to create a digital signature that:

(a) Is not authorized by the person who holds the private key used to create the digital signature; or

(b) Although verifiable by a public key, the certificate that contains the public key identifies a subscriber who:

(1) Does not exist; or

(2) Does not hold the private key that corresponds to the public key contained in the certificate.

(Added to NRS by 1999, 1955)

Electronic Signatures – Some Leading Higher Education Institutions

University of Alabama at Birmingham http://oit.ua.edu/

Dartmouth College http://www.dartmouth.edu/comp/

University of California

University of Wisconsin – Madison

University of Texas – Houston Health Science Center

University of Virginia

Georgetown University http://www.georgetown.edu/

Electronic Signatures – Some Leading Higher Education Institutions

University of Alabama at Birmingham http://oit.ua.edu/

Dartmouth College http://www.dartmouth.edu/comp/

University of California

University of Wisconsin – Madison

University of Texas – Houston Health Science Center

University of Virginia

Georgetown University http://www.georgetown.edu/

Vendors

AlphaTrust Corporation	www.alphatrust.com Ben Woodard AlphaTrust 8409 Pickwick Lane #252 Dallas, Texas 75225, USA Voice 214.828.9853
Topaz Systems, Inc.	www.topazsystems.com Matt Leitch Account Executive 10772 Indian Head Ind. Blvd. St. Louis, MO 63132 Phone: 800.423.8826 x1205 Fax: 314.428.0314
IntegriSign Digital Signatures	www.integrisign.com Karie Miller Inside Sales Manager eTransactions Interlink Electronics Phone: 805.484.8855 x134 Fax: 805.484.8380 kmiller@interlinkelec.com
Verisign	www.verisign.com Frank Machado Sales Engineer II VeriSign, Inc. Phone: 650.426.3684 fmachado@verisign.com
Yozons Technology	www.yozons.com Lee Falco, Sales Manager Yozons Executive Management Team Member Phone: 425.558.9333 lee.falco@verizon.net