



“Implementing Electronic Records and Signatures:
Strategies Developed by the Financial Services Industry”

Testimony of the

Electronic Financial Services Council

Before the

National Committee on
Vital and Health Statistics

Jeremiah S. Buckley
Buckley Kolar LLP

December 8, 2004

Testimony of the Electronic Financial Services Council
By Jeremiah S. Buckley¹

I am pleased to have been asked to speak with you today regarding the development of electronic records and signatures. I act as General Counsel of the Electronic Financial Services Council, an organization of leading companies in the financial services industry dedicated to the advancement of electronic commerce. I have been invited to share with you our experiences working in the financial services industry to develop standards and guidelines for the use of electronic records and signatures. I hope these experiences will be helpful to your panel as it considers the use of electronic signatures and records to facilitate pharmaceutical prescriptions.

1) Electronic Records and Signatures

a) Overview

Use of the Internet presents both hazards and opportunities. The rise of Ecommerce has been credited with significant advances in productivity, in customer service and in reductions in the cost of providing goods and services. As businesses moved online, they often were required, or thought it prudent, to obtain a signature as part of the transaction process.

Under the common law, a signature can be any sort of symbol, even an “X,” if it is placed or adopted by a competent signer with the intent to sign a record. Nevertheless, as business moved online, there was concern that signatures obtained through electronic means would not be valid and that records that were created or stored electronically would not be legally enforceable. Moreover, in industries that must provide disclosures to consumers or other business partners, there was concern that those disclosures could not be provided electronically and still comply with the law.

To help address these concerns and allow businesses and consumers to reap the benefits of electronic commerce, two laws were passed: The Uniform Electronic Transactions Act (“UETA”) at the state level and the federal Electronic Signatures in Global and National Commerce Act (“ESIGN”). ESIGN and the UETA apply to “transactions” in commerce. Both statutes cover consumer and commercial transactions, and the UETA has an additional clause, broadening its scope to apply to government transactions at the state level. These laws have had, and will continue to have, a profound impact on how businesses utilize the online environment.

¹ Jeremiah S. Buckley is General Counsel of the Electronic Financial Services Council, a trade group of national companies dedicated to facilitating electronic commerce. EFSC Members include: AIG, Fannie Mae, Freddie Mac, GE Mortgage Holdings, Intuit Inc., Principal Financial Group, and Wells Fargo. For more information on EFSC please see www.efscouncil.org. Mr. Buckley also is counsel to the Drafting Committee of Standards and Procedures for Electronic Records and Signatures (“SPeRS”). Mr. Buckley is a partner of Buckley Kolar LLP, a Washington, DC law firm, and co-author of The Law of Electronic Signatures and Records (Glasser LegalWorks 2004).

b) The Uniform Electronic Transactions Act

Although before adoption of the UETA some states had enacted electronic signature laws, these laws lacked uniformity. This disparity in state laws spurred concerns about the risks and efficiencies of transacting business online in what is essentially a borderless medium. In response, the National Conference of Commissioners on Uniform State Laws (“NCCUSL”) established a committee to draft a uniform electronic records and signature act. Working on a fast track, NCCUSL approved the UETA’s final draft in 1999. Since that time, approximately 47 jurisdictions have enacted the UETA in some form. Some states, however, have enacted non-uniform versions of the UETA. The differences range from minor typographical changes to significant variations from the NCCUSL text.

c) The Electronic Signatures in Global and National Commerce Act

Due in part to concerns about non-uniform UETA enactments and the potential for slow state adoption of the UETA, Congress passed a federal electronic signature and record statute. Enacted in 2000, ESIGN borrowed many concepts from the UETA. It also contained some significant differences from the UETA. Most importantly, ESIGN places special obligations on those who wish to electronically provide disclosures to a consumer, if the disclosures are otherwise required to be provided to the consumer “in writing.”

d) Significant Features of ESIGN and the UETA

Both UETA and ESIGN are technology neutral statutes designed to put electronic records and signatures on equal footing with their paper counterparts. Accordingly, they both operate as “overlay” statutes amending thousands of state and federal laws. Neither statute changes the substance of underlying laws. For example, all of the elements of a contract (such as offer, acceptance, capacity and consideration) must be present in an electronic context. UETA and ESIGN also do not change the standards for validity of a signature, except to allow the signature to be in electronic form.

Moreover, ESIGN and the UETA do not change disclosure requirements other than to allow electronic delivery. If, for example, a law requires that a disclosure be made at a certain time, then it must still be provided at that time. If a law requires that a disclosure be presented in a certain format, such as 12-point bold face type, it must be presented electronically in the same font. ESIGN and UETA allow the form of the disclosure to change from paper to electronic, but do not alter other aspects of the disclosure requirement.

The UETA and ESIGN have three main precepts:

- Electronic records and signatures cannot be denied legal effect or enforceability solely because they are in electronic form;

- If a law requires a record to be in writing, an electronic record satisfies the law; and
- If a law requires a signature, an electronic signature satisfies the law.

Together, these principles provide for the equality of electronic and non-electronic records and signatures.

Both UETA and E-SIGN only allow for the use of electronic records and signatures when both parties to the transaction agree to their use. In other words, one party to a transaction cannot unilaterally decide to do business electronically.

Second, the elements of an electronic signature are the same under both statutes. An electronic signature is any: a) sound, symbol or process; b) that is made or adopted by the signer; c) where the signer has the capacity and authority to sign; and d) the signer intends to sign (or adopt the signature).

Third, in order to have the benefit of equivalence to non-electronic records or signatures, both laws require electronic records to be able to be reproduced accurately and be accessible to all those who have a right to access them. For example, one cannot inhibit printing of such records. Not only will underlying statutory writing requirements not be met, but the admissibility of an electronic record may be adversely affected if one provides an electronic record in a manner that impedes the other party from retaining or being able to access a copy.

e) Preemption

The relationship between the preemption provisions of E-SIGN and the provisions of the UETA is worth noting. E-SIGN was passed by Congress before most states had enacted the UETA. Congress sought to jump start the e-signature process by preempting any state laws that were inconsistent with E-Sign, thus amending thousands of state laws as well as federal laws. However, Congress did not want to discourage the states from adopting the UETA, and therefore exempted from preemption any state enactment of the UETA as reported by NCCUSL. It continued, however, to preempt any state enactment of the UETA that varied from the reported version and any other state law that was inconsistent with the E-SIGN Act.

Of course, with respect to federally regulated records such as federally mandated disclosures that must be in writing and are required to be provided by private parties, the only general federal law that applies to private transactions is E-SIGN. While Congress may grant authority to Federal agencies to establish specific rules for electronic records that go beyond or vary from the E-SIGN rules, this would require a specific legislative grant of authority. Otherwise federal regulators may only vary from the E-SIGN in very limited ways as described in Section 104 of the E-SIGN Act.

Of course, the E-SIGN rules are designed to apply only to “transactions,” not to government filings or other relationships with the federal or state government. Where the

government is itself a party to the transaction, it may set the rules under which it will use or allow the use of electronic media even if those rules differ from the requirements set out in the ESIGN Act.

2) Standards and Procedures for electronic Records and Signatures

a) Overview

The UETA and ESIGN have wide application across many areas of the law and most transactions. To accomplish this goal, they are necessarily broadly worded. However, this flexibility comes at the price of concrete guidance. The Ecommerce laws tell you that you can do business electronically, but with very rare exceptions, they deliberately do not tell you how to do business electronically.

To try to develop some implementation guidelines, the financial services industry developed Standards and Procedures for electronic Records and Signatures, commonly referred to as SPeRSSM. SPeRS is a cross industry initiative created by a variety of leading companies in the financial services and technology industries.

Rather than providing normative rules that must be followed by all entities, such as specifying a certain type of encryption or a given type of server communication, SPeRS provides “rules of the road” that system design teams – ideally an interdisciplinary team of business, technical and legal personnel – can follow when designing, building and deploying Ecommerce applications.

SPeRS: 1) permits businesses to establish a common understanding with internal team members and outside vendors concerning the methodology for designing eCommerce systems; 2) assists in establishing industry standards for commercially reasonable, enforceable structures and processes; and 3) helps provide the customer with a “common experience” across various online transactions.

In keeping with SPeRS’ inclusive goals, it has attracted a wide variety of organizations and points of view. SPeRS members include government sponsored entities such as Fannie Mae and Freddie Mac, leading industry corporations such as Wells Fargo, Citigroup, AIG, Charles Schwab, Genworth Financial, MassMutual and Verisign, and influential trade organizations such as the American Council of Life Insurers and American Bankers’ Association. This variety ensures that all angles of a problem are covered and contributes to lively and informative discussions.

b) Main Features of SPeRS

To provide useful guidance for Ecommerce applications, SPeRS is divided into five sections:

- 1) Authentication;
- 2) Consent to use electronic records and signatures;

- 3) Agreements, notices and disclosures;
- 4) Electronic signatures; and
- 5) Record retention.

Each of these sections provides several high-level standards, and I have attached copies of these standards in my written testimony. Each standard, in turn, provides checklists to guide the organization's decision process, along with legal commentary and, where appropriate, sample forms that can be used to speed the development process.

Today I will give a brief overview of each SPeRS section. Hopefully some of what we have done in the financial services sector will be of assistance to your committee as it develops its recommendations for the Secretary.

SPeRS § 1: Authentication

The first section of SPeRS addresses the problem of authenticating persons online. How do you know that somebody is who he or she claims to be? To address this problem, SPeRS presents four main development guidelines. These guidelines are found on pages A-1 through A-3 of the appendix to my prepared comments. You will note that each SPeRS standard contains several bullet points, each providing more detailed guidance on the issues to be addressed. The SPeRS manual provides additional legal discussion of the principles, along with checklists that can be used to fully explore each issue.

As you will note from the Appendix, there are four SPeRS standards addressing the following authentication issues:

- Identifying and evaluating the appropriate authentication strategy when creating a relationship;
- Identifying and evaluating the appropriate authentication strategy when selecting a credential method. SPeRS provides a chart comparing authentication methods including self-authentication, third party authentication and positive authentication and compares the strengths and weaknesses of each method;
- Providing consumers information concerning the distribution of risk of unauthorized transactions; and
- Establishing the authority of representatives to act electronically.

In the context of authentication, a common problem that may apply in the electronic prescription context is the risk of fraud. Authentication strategies can be used to positively identify all parties involved in the transaction. However, it will also be important to consider how the risk of loss will be distributed among the parties. There also may be important questions regarding the use of credentials by representatives – for example, in your context will physicians be allowed to provide their credentials to their office personnel to transmit prescriptions that they have written, and if so (or if not), how will the system validate those transactions? As with many activities, resolving authentication questions will be a balancing act between competing priorities. The

system will need to be accessible and easy to use, while still maintaining security and integrity.

i) SPeRS § 2: Consent to Use Electronic Records and Signatures

SPeRS' second section addresses issues involved with obtaining consent to use electronic records and signatures. Located at pages A-4 and A-5 of Appendix A, the six standards are:

- Obtaining a general agreement to use electronic records and signatures;
- The applicability of the ESIGN consumer consent process;
- Content of the ESIGN consumer consent disclosures;
- Formatting and timing of presenting the ESIGN consumer consent disclosures;
- The method and timing of obtaining the consumer's affirmative consent to using electronic records and signatures; and
- Methods of satisfying ESIGN's "reasonable demonstration" test.

Both the UETA and ESIGN require that the parties agree to use electronic records and signatures for a particular transaction or set of transactions. Under the UETA, that agreement can be express or implied, proven by the facts and circumstances surrounding the transaction. Consumer transactions covered by ESIGN, however, require that the consumer, after receive appropriate disclosures, provide his or her affirmative consent to the transaction and provide a reasonable demonstration of his or her ability to access the electronic disclosures before the underlying disclosures are provided.

In the electronic prescription context, it may be critical to ensure that all parties understand that they are electronically entering into agreements to dispense prescription drugs. State regulations governing physicians and pharmacists may play a part in any standards that are adopted. If the standards will govern transactions directly involving the consumer (for example, electronic requests for refills of previously authorized prescriptions), there may be a need to obtain consumer consent to do business electronically.

ii) SPeRS § 3: Agreements, Notices and Disclosures

SPeRS' third section deals with the methods of providing notices, disclosures and agreements. As I noted earlier, the UETA's and ESIGN's status as "overlay" statutes does not change the substantive requirements of underlying law with respect to the method and nature of displaying required information. However, providing such information in compliant electronic form is sometimes challenging. To help the system design team create a compliant system, SPeRS has seven main guidelines, found in the appendix at pages A-6 through A-10:

- General principles for display and presentation of information;
- Methods of delivering and displaying records and information;
- Retention of records and information by other transaction participants;

- Methods of indicating agreement to those disclosures;
- Methods of expressing and acknowledging access or delivery;
- Creating clear and conspicuous disclosures; and
- Strategies for the use of hyperlinks and other navigational cues.

An issue that may be of interest and importance to electronic prescriptions is the presentation of disclosures that are required by law or regulation. How will such disclosures be delivered: via email or Internet? In PDF format or Word? How can you ensure that they are reliably sent? How will you determine that the disclosures are viewed? Might it be desirable to force the recipients to view a certain disclosure every time they access a system, or should the process be designed to permit regular users to bypass disclosures that the recipient has previously viewed?

The method of displaying information online is an area of particular interest. While the Internet allows for quick and efficient transmission of large amounts of data, an unintelligible flood of information should be avoided. When used thoughtfully, navigational tools such as hyperlinks can highlight important information.

iii) SPeRS § 4: Electronic Signatures

Electronic signatures are the heart of many electronic commerce applications, and I understand that to be an important issue in the context of electronic prescriptions. To assist users in developing Ecommerce applications, the SPeRS guidelines listed on pages A-11 through A-13 of my prepared comments address:

- Selecting a signature process;
- Providing information on the signing process to transaction participants;
- Establishing the intent to sign;
- Associating an electronic signature with a record;
- Attributing a signature; and
- Special rules for creating signatures with electronic agents.

Selecting a signature process is an important decision. An electronic signature can be any sound, symbol or process, attached to or logically associated with the record and executed or adopted by a person with the intent to sign. This is a broad definition, as the examples on the screen demonstrate. SPeRS provides an extensive chart presenting an analytic tool for assessing which signature process to use.

An electronic signature also requires that the signature be attached to or logically associated with the contract or other record that is signed. Satisfying this requirement can have a significant impact on records management systems, a topic we will touch on in more detail later.

iv) SPeRS § 5: Record Retention

After a signer has been authenticated and issued a credential, all information has been provided and the parties have validly executed a contract or other record, the final step is record retention. The EFSC and SPeRS have found that this is an area that has not been fully explored by American businesses and is of increasing importance. The goals are to retain records in compliance with legal and regulatory requirements, to maintain them for the proper length of time, to store them so that they are accessible to all those who are legally entitled to access, and to keep them in a manner that ensures that they will be admissible evidence if they are ever needed in a dispute.

To provide guidance in developing an effective document retention program, SPeRS has developed seven record retention principles thus far, which are reprinted in the appendix to my written testimony at pages A-14 through A-16:

- Meeting accuracy, accessibility and retention requirements;
- Verifying the integrity and accuracy of electronic records through design of the physical and logical environment as the system is established;
- Verifying the consistency and integrity of electronic records on an ongoing basis;
- Document conversion;
- Vendor relationships;
- Interaction with government agencies; and
- Transferable records and rules applicable to electronic chattel paper.

Electronic record retention is a critical aspect of electronic operations. Setting aside the obvious operational inefficiencies that can arise if records are not kept in an orderly and reliable fashion, there are significant legal repercussions that should be kept in mind. At a conference sponsored by the EFSC several weeks ago, one of our speakers, Ken Withers of the Federal Judicial Center, pointed out that the failure to keep electronic records in a manner that helps ensure their accuracy and reliability could have significant impacts in litigation. Most records, be they accounting records or records of which medicine was prescribed and sent to a pharmacy to be filled, are not automatically admissible as evidence. In fact, they constitute “hearsay,” a category of evidence that is not admissible unless one can find an applicable exception in the rules of evidence.

One such exception is the Business Records rule. Under the Business Records exception to the hearsay rule, a business record can be admitted into evidence, even if it would otherwise constitute hearsay, if it is created and stored in the regular course of business and in a manner that indicates that it is authentic and reliable. Thus, if you are embroiled in a lawsuit and you need to prove that you sent or received a certain prescription, the court might not allow you to bring in a document that you incorrectly stored on your own system unless you can show that it was created and retained in a manner that demonstrates its reliability.

Your opponent, however, might be able to admit the same document or other documents that were incorrectly stored on your computer, on the grounds that they are party admissions, statements against interest or for purposes of cross-examining or impeaching your witnesses.

To help meet these challenges, electronic prescriptions will need to be stored in a manner that protects their authenticity, demonstrating that they are what they purport to be. Document integrity is another critical issue. Some record management solutions use electronic signatures that “wrap” the records to ensure their integrity. Others use a mixture of logical and physical controls over database access to ensure that their records are not being altered inappropriately. SPeRS contains guidance that allows organizations to parse the issues associated with safeguarding the electronic records.

Process integrity is ensuring that the entire lifecycle of the document, from presentation to ultimate destruction, is compliant with applicable regulations and other requirements. This can be particularly important if the storage duties are outsourced to third parties. SPeRS provides a checklist and guidance that can be useful in evaluating your needs in IT vendors and in evaluating the vendors that compete for your business.

c) SPeRS as a Cross Industry Resource

The SPeRS guidelines have a broad scope, and they have been put to several uses within the financial services industry. The Mortgage Bankers Association established a standards organization named MISMO, which is creating e-records standards for the mortgage industry, including document creation standards. SPeRS principles are being used in the MISMO process to create voluntary electronic standards for the mortgage industry. Similarly, the American Financial Services Association (“AFSA”) published a standard for retail contracting in the automotive finance industry using SPeRS principles. The X9 committee of the American National Standards Institute (“ANSI”) approved and accepted SPeRS as an ANSI/X9 Technical Report. Elsewhere, companies in insurance, securities and banking have used the SPeRS guidelines to develop their Ecommerce applications and deploy electronic signatures. The American Council of Life Insurers and American Bankers Association offer SPeRS to their members through their bookstores and other means.

As electronic prescriptions move forward, we hope that there may be some benefit for the pharmacy industry from the financial industry’s experience. Although the applications and context may differ, both the financial services and pharmacy industries share many of the same issues when moving their processes online. How do we make sure that persons are who they say they are, and that they have the authorization to complete a given transaction? How do we ensure that all the parties have consented to use electronic processes to prescribe the drugs? If and when consumers become part of the equation, how do we address the unique concerns and requirements of transacting business online with them? Should all, or just certain notices and disclosures be provided electronically? What type of security is needed, both in completing the transaction and in storing the records – especially given the sensitive nature of prescription or financial records? And

finally, how should records be retained in a manner that allows them to remain both secure and accessible, and to be reliable evidence in the event that they are needed for regulatory or other purposes?

In my presentation today, I have only been able to hit the highlights of SPeRS, but the SPeRS manual contains over 400 pages, including detailed checklists, to guide users in establishing and evaluating e-signature and e-record technologies. I have attached a copy of the SPeRS Guidelines as an appendix to my prepared testimony to provide insight into their operation. You can obtain a copy of the entire manual by going to the website www.spers.org.

While SPeRS was developed primarily by participants in the financial services industry, its principles are of general applicability, we believe. It sets out behavioral, legal and regulatory issues that need to be considered in developing any e-signature or e-records process. These guidelines do not claim to be the only or best way of creating electronic records, but they will help anyone designing or evaluating an e-records system. They are deliberately open standards, not endorsing any technology solution, but providing ways to measure the legal efficacy of any specific e-records system. If the issues raised by SPeRS are not addressed, then there is some risk that the e-records system is flawed.

By developing these guidelines, the financial services industry had provided participants in the e-records marketplace with a common reference point. Rather than each company or industry incurring the not insignificant expense of developing the criteria it will use to evaluate its and vendors' e-records solutions, SPeRS gives the company and its internal and external e-records system providers a common reference point and a common language to evaluate whether any e-records process properly addresses the requirements to create and maintain legally enforceable and binding records.

SPeRS for the most part deals with what I would call umbrella issues, that is issues that are relevant not only to the financial services business, but to any business in which e-records are used. For this reason, it may prove to be helpful to you in your work. SPeRS will give you the questions you may want to ask about any e-prescriptions proposals and provide the basis for open, technology neutral criteria to be developed in the e-prescription context.

APPENDIX A – SPeRS STANDARDS

Section 1 Summary Statement of Standards to Guide Systems Design Teams

STANDARD 1-1. IDENTIFYING AND EVALUATING THE APPROPRIATE AUTHENTICATION STRATEGY – CREATING THE RELATIONSHIP

SPERS STANDARD 1-1

The System Design Team should determine the appropriate Authentication Process for establishing a Relationship with each Transaction Participant. The assessment and selection Process should include:

- Assessing the legal liability and Transaction risk associated with failing to correctly identify the Transaction Participant,
- Assessing the practical and system considerations that may affect the choice of an Authentication Process,
- Determining whether the Authentication Process for the Transaction must comply with specific legal or regulatory requirements,
- Selecting an Authentication strategy that provides an appropriate level of security and certainty, based on the preceding considerations, and
- Determining what information will be required in order to implement the selected Authentication strategy.

STANDARD 1-2. IDENTIFYING AND EVALUATING THE APPROPRIATE AUTHENTICATION STRATEGY – CREDENTIALS

SPERS STANDARD 1-2

The System Design Team should determine the appropriate Credential for a Participant conducting a Transaction as part of an established Relationship. The process for selecting a Credential should include:

- Assessing the risks associated with unauthorized access to conduct the Transaction,
- Determining whether there are specific legal or regulatory requirements for a Credential associated with the Transaction;
- Determining the types of Credentials appropriate to the Transaction based on the risk assessment and any applicable legal or regulatory requirements,
- Determining the cost of establishing and using a particular Credential,
- Assessing the relative speed with which the Credential may be established and used,
- Assessing any specific hardware or software requirements to use a particular Credential and whether such requirements are appropriate to the Transaction, and
- Evaluating the information that needs to be obtained from, and provided to, the Transaction Participant to implement and maintain a particular Credential.

STANDARD 1-3. PROVIDING CONSUMERS INFORMATION CONCERNING THE DISTRIBUTION OF RISK OF UNAUTHORIZED TRANSACTIONS

SPERS STANDARD 1-3

Where appropriate, and particularly in Consumer Transactions, the System Design Team should consider providing a Transaction Participant with an opportunity to obtain information concerning the risks associated with unauthorized Transactions, including:

- The Transaction Participant's responsibilities with respect to protecting Credentials,
- The potential consequences of unauthorized use of Credentials, and
- The procedure for giving notice that a Credential has been stolen or compromised.

STANDARD 1-4. ESTABLISHING THE AUTHORITY OF REPRESENTATIVES

SPERS STANDARD 1-4

Where appropriate, the System Design Team should consult with legal counsel or compliance personnel to determine whether it is likely that individuals will be representing Transaction Participants (either individuals or legal entities such as corporations or trusts) other than themselves, and if so:

- Determine whether it is advisable to obtain some representation or evidence of the individual's authority to act as a representative, and
- Establish appropriate methods for obtaining representations or evidence of the representative's authority.

Section 2 Summary of Statement of Standards

STANDARD 2-1. GENERAL AGREEMENT TO USE ELECTRONIC RECORDS AND SIGNATURES

SPERS STANDARD 2-1

Systems should be designed to obtain either:

- The Transaction Participants' express Agreement to use Electronic Records and Signatures; or
- The Transaction Participants' implied Agreement in a fashion that allows a reasonable inference that Transaction Participants have assented to use Electronic Records and Signatures.

STANDARD 2-2. APPLICABILITY OF THE ESIGN CONSUMER CONSENT PROCESS

SPERS STANDARD 2-2

With respect to business to-Consumer Transactions, the System Design Team should consult with legal counsel or a compliance officer concerning application of the ESIGN Consumer Consent Process. The ESIGN Consumer Consent Process should be used if:

- The Consent Process is required by any Rule of Law, or
- The System Design Team determines that its voluntary use would be beneficial and its use would not hamper, confuse or unduly complicate the Transaction.²

STANDARD 2-3. THE ESIGN CONSUMER CONSENT DISCLOSURES

SPERS STANDARD 2-3

When the System Design Team has determined that the ESIGN Consumer Consent Process should be employed, it should implement the Consent Process:

- In compliance with the requirements of the ESIGN Consumer Consent Disclosures; and
- With the goal of providing the Consumer with information designed to assist the Consumer in making an informed choice with respect to the use of Electronic Records and Signatures.

² "Voluntary use" refers to the use of all, or part of the ESIGN Consumer Consent Process.

STANDARD 2-4. THE ESIGN CONSUMER CONSENT DISCLOSURES –
FORMAT AND TIMING

SPERS STANDARD 2-4

When presenting the ESIGN Consumer Consent Disclosures to the Consumer they must be provided:

- In a clear and conspicuous format;
- At a meaningful time in the Transaction; and
- Prior to the Consumer providing his or her affirmative consent to engage in business electronically.³

STANDARD 2-5. OBTAINING THE CONSUMER’S AFFIRMATIVE CONSENT -
METHODS AND TIMING

SPERS STANDARD 2-5

When employing the Consumer Consent Process systems will need to be designed to obtain the Consumer’s affirmative consent to access Required Consumer Information. Providers should obtain the Consumer’s affirmative consent either::

- Prior to, or at the time Required Consumer Information is presented, or
- After Required Consumer Information is presented but before the time when the Consumer becomes obligated on the Transaction.

STANDARD 2-6. REASONABLE DEMONSTRATION OF ACCESS

SPERS STANDARD 2-6

If the ESIGN Consumer Consent Process will be employed, the System Design Team should create a mechanism, method of process that enables a Consumer’s provision of consent to Reasonably Demonstrate that the Consumer can access the electronic method(s) and format(s) the system will use to provide or make available Electronic Records such as notices, disclosures, and agreements over the course of the Transaction.

³ The methods for, and the timing of obtaining the Consumer’s affirmative consent are discussed in SPeRS Standard 2-5.

Section 3 Summary Statement of Standards

STANDARD 3-1. GENERAL PRINCIPLES FOR DISPLAY AND PRESENTATION OF INFORMATION

SPERS STANDARD 3-1

The System should be designed to display and present information efficiently and effectively. Absent special circumstances, the System Design Team should provide a reasonable opportunity to access information, whether it is part of an agreement, Notice or Disclosure, so that:

- The information is displayed or made available in a manner and/or format that complies with any applicable Rule of Law.
- The opportunity to access the information occurs:
 - At the point in the Transaction required by an applicable Rule of Law, or
 - If there is no applicable Rule of Law, at or before the point in the Transaction where having access to the information is appropriate for the recipient, but not later than the point at which the recipient is asked to indicate agreement with, or acknowledge access to, the information.
- During the course of the Transaction, the information may be retained by the recipient, or accessed by the recipient at a later time, consistent with the purpose of the Transaction, the nature of the information and applicable Rule of Law (See SPeRS Section 5).

STANDARD 3-2. DELIVERING AND DISPLAYING RECORDS AND INFORMATION

SPERS STANDARD 3-2

When developing a process that includes the electronic display and delivery of Agreements, Notices or Disclosures, the System Design Team should:

- Identify the Records and information that will be delivered electronically to each Transaction Participant in the course of the Transaction;
- Consult with legal counsel or compliance personnel to determine whether any of the Records or information to be provided are subject to any specific delivery requirements under an applicable Rule of Law;
- Accomplish delivery by providing access or the opportunity to access the Record, as applicable;
- Determine the appropriate method(s) for providing access to the Records and information, taking into account:
 - The nature of the Transaction and the intended audience,
 - Whether the Records and information will be provided or made available as part of an interactive session with the recipient, as part of a unilateral transmission to the recipient, some combination of the two, or through other means,
 - Whether the Records and information to be provided or made available include sensitive or confidential information,
 - The time period for which the Records and information should remain available for access by the recipient during the course of the Transaction, and
 - Whether the recipient should be required to access any of the Records and information in order to proceed with the Transaction.

STANDARD 3-3. DELIVERING AND DISPLAYING RECORDS AND INFORMATION – RETENTION OF RECORDS BY OTHER TRANSACTION PARTICIPANTS

SPERS STANDARD 3-3

For Electronic Records that must be signed, or that contain Required Information, the System Design Team:

- Should provide the Transaction Participant signing or accessing an Electronic Record with:
 - An explanation of the options that the Transaction Participant will have during the Transaction to retain a copy of the Record, including any Disclosure or explanation required by the E-SIGN Consumer Consent Process (*See* SPeRS Standard 2-2), and
 - A reasonable opportunity to retain a copy of the Record for later reference.
- May wish to provide the Transaction Participant with an opportunity to agree to the methods being provided for retaining a copy of the Record.

STANDARD 3-4. INDICATING AGREEMENT

SPERS STANDARD 3-4

When developing a process that includes the electronic delivery or display of agreements to Transaction Participants, the System Design Team should:

- Consult with legal counsel or compliance personnel to determine:
 - Which Records or information being delivered or displayed require some indication of agreement by a Transaction Participant
 - The level of formality or ceremony required for each indication of agreement
- Implement a process design which, in the context of the Transaction and the particular information or Record in question:
 - Offers the Transaction Participant:
 - A clear choice to either agree or decline to agree, and
 - A clear method to express agreement or decline to agree
 - Provides an explanation of the consequences are inherently obvious in the context of the Transaction, and
 - When appropriate, offers the Transaction Participant an opportunity to correct an election to assent or refuse assent made in error except when impractical or unnecessary.

SECTION 3-5: ACKNOWLEDGING ACCESS OR DELIVERY

SPERS STANDARD 3-5

When developing a process that includes the electronic display and of and opportunity to access Disclosures and Notices to Transaction Parties, the System Design Team should:

- Consult with legal counsel or compliance personnel to determine:
 - Which Records or information being displayed or provided require some acknowledgement of access or opportunity to access by a Transaction Participant, and
 - The level of formality or ceremony required for each acknowledgement of access or opportunity to access.
- For Records that require acknowledgement of access or delivery, implement a process design which, in the context of the Transaction and the particular information or Record in question, offers the Transaction Participant a clear method to acknowledge access or opportunity to access.

STANDARD 3-6. CLEAR AND CONSPICUOUS DISCLOSURE

SPERS STANDARD 3-6

When developing a process that includes the electronic display of or access to agreements, Notices or Disclosures to Transaction Parties, the System Design Team should:

- Consult with legal counsel or compliance personnel to determine whether any of the Records or information to be provided are subject to “conspicuous disclosure” requirements under an applicable Rule of Law, and
- If “conspicuous disclosure” is required:
 - Implement a process design which, in the context of the Transaction and the particular information or Record in question, delivers the required Record or information in a form which is:
 - Reasonably understandable, and
 - Designed to call attention to the information that must be disclosed.
 - Employ electronic tools and display techniques so as to effectively convey the information.

STANDARD 3-7. USING HYPERLINKS AND OTHER NAVIGATIONAL CUES

SPERS STANDARD 3-7

When displaying information electronically, the System Design Team should consider using navigational cues in order to better organize, enhance or protect the presentation of information.

When using a navigational cue, the System Design Team should label or title the navigational cue, or provide explanatory information for use of the navigational cue, reasonably sufficient to permit the Transaction Participant to understand the general nature of the Records or information associated with the navigational cue.

Section 4 Summary Statement of Standards

STANDARD 4-1. SELECTING A SIGNATURE PROCESS

SPERS STANDARD 4-1

The selection of an appropriate signature technology for a particular application should be based on a determination of the relevant factors and circumstances, including:

- Applicable hardware and software requirements
- Any Rule of Law limiting the type of Electronic Signature that may be used
- Characteristics of the signer
- Susceptibility of the technology to repudiation
- Ability of the signature to protect the Record from undetected alteration after signing
- Portability of the signature process
- Suitability of the signature for:
 - non-repetitive in-person Transactions
 - repetitive in-person Transactions
 - non-repetitive remote Transactions
 - repetitive remote Transactions
 - Ease of use for multiple signatures by same signer in one Record
 - Ease of use for multiple signers in one Record

STANDARD 4-2. PROVIDING INFORMATION ON THE SIGNING PROCESS

SPERS STANDARD 4-2

The execution of an Electronic Signature should be preceded by an opportunity for the signer to review:

- A description and explanation of the procedure used to create the Electronic Signature, and
- A description of the sequence of events that will result in the signature becoming final and effective.

Provided, however, that the signature process may be sufficiently familiar or self-explanatory that a description is superfluous or would be repetitive.

STANDARD 4-3. ESTABLISHING THE INTENT TO SIGN

SPERS STANDARD 4-3

The process used to create an Electronic Signature should be designed so that:

- It is clear that the signer intended to create a signature, and
- When not reasonably apparent under the circumstances, the signer is advised that the signature fulfills one or more purposes:
 - Affirming the accuracy of information in the record
 - Affirming assent or agreement with the information in the Record
 - Affirming the signer's opportunity to become familiar with information in the Record,
 - Affirming the source of the information in the record, or
 - Other specified purposes.

STANDARD 4-4. ASSOCIATING A ELECTRONIC SIGNATURE WITH A RECORD

SPERS STANDARD 4-4

A process for signing records should be designed so that:

- The Record is presented for signature before the signature becomes effective, and
- The signature is attached to, or logically associated with, the Record presented.

STANDARD 4-5. ATTRIBUTING A SIGNATURE

SPERS STANDARD 4-5

A process for signing Records should be designed so that either:

- The signature itself provides evidence of the signer's identity, or
- The process surrounding creation or affirmation of the signature:
 - provides evidence of the signer's identity, and
 - is in some manner preserved, evidenced, or capable of recall or recreation during the life of the Transaction.

STANDARD 4-6. ELECTRONIC AGENTS

SPERS STANDARD 4-6

A system designed to implement an agreement and signature by an Electronic Agent:

- Should require a clear and detailed definition of the parameters of the electronic agent's authority to form an agreement and sign on behalf of the represented Participant, and
- May either reflect the use of an electronic agent in the signature information provided as part of the signed Record, or present the signature as the act of the represented Participant without reference to the use of an electronic agent.

Section 5 Summary Statement of Standards

STANDARD 5-1. MEETING ACCURACY, ACCESSIBILITY AND RETENTION REQUIREMENTS

SPERS STANDARD 5-1

Electronic Record retention systems should be designed to ensure the information contained in the Electronic Records remain:

- Protected from undetected and unauthorized alteration, and
- Accessible to the Record Holder and others entitled by Rule of Law or Agreement to access, or obtain a copy of, the Record Holder's copy of the Record

See also SPeRS Standard 3-3 for the Record Provider's obligation to provide access or copies of Records to other Transaction Participants (e.g., Consumers).

STANDARD 5-2. VERIFYING THE INTEGRITY AND ACCURACY OF ELECTRONIC RECORDS/THE PHYSICAL AND LOGICAL ENVIRONMENT

SPeRS STANDARD 5-2

As part of the infrastructure necessary to protect the integrity of Electronic Records, the System Design Team should establish a commercially reasonable design for:

- The physical environment in which the records are maintained that takes into account:
 - The types of transactions evidenced by the Electronic Records,
 - The value of the transactions evidenced by the Electronic Records,
 - The value or confidentiality of the information contained in the Electronic Records, including whether the record is subject to state or federal privacy laws, and
 - The impact of loss, destruction or theft of the Electronic Records on the operations of the Record Holder.
- The technical environment in which the records are maintained that takes into account:
 - · Network controls,
 - · Hardware controls, and
 - · Software controls.

STANDARD 5-3. VERIFYING THE CONSISTENCY AND INTEGRITY OF ELECTRONIC RECORDS

SPERS STANDARD 5-3

When appropriate, the System Design Team should consider including in the process for creating, delivering and submitting Electronic Records commercially reasonable checks to confirm that:

- The Record:
 - Contains information that is both internally consistent and consistent with other Transaction Records;
 - For signed Electronic Records, the Record appears to have been electronically signed by each of the targeted signers before being accepted as final and complete;
 - Has not been altered without authorization once it is effective; and
 - Is retrievable in a form perceivable by an individual.
- Any set of Transaction documents intended to be reviewed, completed, and/or signed as a group is complete and that all necessary tasks have been performed before being submitted and/or accepted in final form.

STANDARD 5-4. DOCUMENT CONVERSION

SPERS STANDARD 5-4

System design teams should develop guidelines and procedures for the preservation and conversion of paper to electronic documents to meet the following objectives:

- Promote cost and organizational efficiency;
- Ensure safekeeping of documents;
- Ensure compliance with state and federal requirements regarding Record retention, access to Records, and document destruction;
- Maintain secure, reliable, long-term access to Records; and
- Establish data integrity to satisfy the Rules of Evidence.

STANDARD 5-5. VENDOR RELATIONSHIPS

SPERS STANDARD 5-5

When using third party vendors to perform Record retention functions, Providers should adopt a risk management process that includes:

- Proper due diligence to identify and select a third-party provider;
- Contracts that outline duties, obligations, and responsibilities of the parties involved; and
- Ongoing oversight of the third parties and third-party activities.

STANDARD 5-6. INTERACTION WITH GOVERNMENTAL AGENCIES

SPERS STANDARD 5-6

The System Design Team should consult with legal counsel or compliance personnel to determine whether there are any state or federal regulatory requirements that may affect the for or methods used to create, file or maintain the Records.

STANDARD 5-7. TRANSFERABLE RECORDS AND ELECTRONIC CHATTEL PAPER

SPERS STANDARD 5-7

If the system is intended to manage the creation, execution, transfer and/or storage of electronic equivalents of negotiable promissory notes, bills of lading, warehouse receipts, retail installments sales contracts, debt obligations secured by personal property, or leases of tangible personal property, the System Design Team should consult with legal counsel or compliance personnel to determine the special requirements for:

- Controlling the transfer of ownership of the Electronic Record,
- Storing the Electronic Record, and
- Protecting the Electronic Record from unauthorized alteration.