In this chapter, I define the scope of electronic commerce law and discuss how law can evolve in response to rapid change in social and business practices. I summarize how commercial law has adapted to electronic sales of goods using EDI and Internet distribution systems, discuss the strengths and weaknesses from a legal perspective of a new technology-based model for electronic commerce – digital signatures and public key infrastructure – and compare that model with others for managing the legal risks of electronic sales of foods. I also summarize how changes in payment systems; and how financial markets have moved to electronic systems for transferring investment securities.

**Keywords:** Electronic Contracting; Electronic Data Interchange, Public Key Infrastructure; Digital Signature; Certificate Authority; Trusted Third Party; Risk Management; Authentication Security Procedure

## 1 Introduction

Doing business over the Internet may seem to raise breathtakingly novel issues in business law, but the law of electronic commerce is actually as old as the telegraph. It was not long after the telegraph entered into widespread use that the first case was litigated in which party tried to avoid liability by claiming that an agreement reached by an exchange of telegrams could not constitute a valid and binding contract (Wright and Winn, 1998). Most courts in the US have risen to the challenge to book beyond form and evaluate the substance of the transaction, whether the new form of agreement legal effect, and in other instances, courts have been distracted or confused by new technologies, and refused to validate the parties’ agreement. The question how commercial law will adapt to the new business realities of Internet electronic commerce can best be answered by looking at how the law adapted to earlier iterations of electronic commerce – in particular, electronic data interchange electronic contracting conducted over closed, propriety networks, electronic funds transfer systems used by banks, and electronic settlement and clearing systems used in Wall Street.

This chapter will deal with the law of commercial transactions conducted electronically, whether done over open or closed networks. A commercial transaction in this context refers to a business transaction of a type normally conducted on standardized terms and in high volume. For example, a sale of goods, including the payment for those goods, is a classic example of a commercial transaction. In the US, a large part of commercial law is contained within the Uniform Commercial Code, a model statute which has been adopted as law in all fifty states with minor local variations, which has been supplemented by various state and federal laws and
regulations. The analysis of commercial law issues in this chapter will take the provisions of the UCC as the starting point, and add reference to other courses and bodies of law as necessary.

This chapter will not give a comprehensive overview of all the issues raised by doing business over the Internet. For example, an audit of all the legal issues raised by doing business from an Internet site might include not just a review of commercial law issues but also patent, trademark and copyright law issues; advertising and consumer protection regulations including privacy law issues; antitrust and deceptive trade practices law issues; record retention and email policies; the design of security procedures and access controls; and tax law issues. Nor does this chapter provide any legal advice; specific questions of electronic commerce law should be pursued with qualified legal personnel.

While many of the issues raised by Internet electronic commerce closely resemble issues raised by earlier generations of technology such as teleflexes and faxes, what may be unprecedented is the degree to which electronic commerce is changing some of the basic principles upon which business administration has been based for decades. The volume and magnitude of changes in business practice that are occurring now as a result of adopting electronic commerce systems are putting tremendous pressure on traditional commercial law doctrines to adapt and evolve. Legal institutions can respond to these pressures in a variety of ways, and this chapter will consider the costs and benefits associated with different techniques for adapting law to new business practices.

This chapter will begin with a brief sketch of the methods for adapting commercial law to changing business realities in Section 2. Section 3 first analyzes the legal issues raised by selling goods using electronic contracting systems such as electronic data interchange, which have been extensively debated for over a decade. Legal issues raised by selling goods over open networks such as the Internet are considered next in Section 3, with a discussion of how new electronic commerce systems such as digital signatures and public key infrastructure may help reduce legal risks. Section 4 looks at electronic payment systems, including credit cards and wire transfers, and the law governing them. This section analyzes the significance consumer protection law in contributing to the current dominance of credit cards as the payment system for Internet retail commerce. Section 5 looks at the process by which financial institutions replaced stock certificates and bonds with electronic settlement and clearing systems, and how commercial law adapted to those changes. The law governing transactions in financial assets was first reformed during the 1970s when computers were first introduced into the process. When those reforms proved unsuccessful, lawyers revised the law again during the 1990s, but only after undertaking a careful study of actual Wall Street business practices. Section 6 presents conclusions that can be drawn from the analysis of these examples of how commercial law has adapted to electronic commerce technologies.

2 Adapting Commercial Law to New Business Realities

The most elementary way for business parties to adapt commercial law to new circumstances is through the use of contracts. Parties can depart from the terms of current standard form contracts to write new contracts describing new transactions and allocating new risks between the contracting parties. Failed transactions that result in litigation produce reported legal opinions that become case law which in turn helps parties predict how effective in fact their new contract terms are at regulating innovative business practices. The process of building new law through
precedent can be slow and problematic, however, as the outcome of litigation is always somewhat uncertain. As contracts become more innovative, their enforceability becomes less predictable as a result.

When the parties are no longer confident that their contracts will produce predictable legal outcomes, they can lobby state legislatures or Congress to enact statutes to resolve the uncertain issue. While statutes may be more comprehensive and coherent than case law, the process of lobbying is also problematic as different interest groups may resist enacting legislation or may counter by offering undesirable alternative legislation. Furthermore, once a law is passed, even if it is found to be inadequate at resolving the matters it was designed to address, getting a statute repealed can be even more difficult than getting one enacted in the first place. The uniform law drafting process, coordinated by the National Conference of Commissioners on Uniform State Laws (Uniform Law Commission or ULC) is a collaborative process involving all fifty states that produces model statutes, and is an alternative route to getting legislation enacted. The ULC is supposed to reduce some of the uncertainty associated with law reform by providing a forum within which issues can be thoroughly and thoughtfully debated and consensus achieved prior to legislation actually being introduced in the states. But the uniform law drafting process may be even slower than other legislative routes and there is no guarantee any consensus or workable model will be produced. Because there are no easy solutions to the problem of adapting commercial law to meet the needs of innovative businesses early adopters of new technologies have no choice but to tolerate a degree of legal uncertainty.

Under ideal circumstances, commercial law statutes should be reformed in response to significant changes in established business practices to reduce uncertainties that arise under existing laws. Innovators start the process by using contracts to assign rights and responsibilities among themselves. Having lawyers individually negotiate and draw up contracts can be an expensive proposition, especially if the business party has to educate the lawyer about the basic business model the parties have developed as part of the drafting process, but it may be the only practical way for the parties to reduce some of the legal uncertainties arising out of innovative business practices. As experience grows and business practices that were once considered innovations become routine, parties to commercial transactions can standardize the terms of their contracts, minimizing or eliminating the role of lawyers in individual transactions. When contract terms and business practices become very standard and routine, commercial statutes can be revised to incorporate what can be thought of as default terms based on these standard contract terms. If the parties to a commercial contract fail to specify all the operative terms of their agreements, then commercial law can act as a gap-filler, providing missing terms that should be substantially the same as those the parties would have agreed routine business practice and eliminates uncertainty among parties to a transaction without requiring lawyers advise the parties on each contract.

Not all commercial law issues can be resolved through the slow accumulation of business custom and practice, however. Some issues, such as consumer protection issues, are generally resolved by legislatures acting to mandate what business parties must do in order to have legally enforceable agreements or to avoid legal sanctions. Regulatory approaches to commercial law may have a shorter incubation time than “freedom of contract” approaches that defer to standards chosen by commercial parties themselves, and often have less predictable outcomes for affected businesses as a result. Regulation often works best when it corrects market failures, such as those caused by information asymmetries or unequal bargaining power in summer transactions. The success of credit cards as a payment system for Internet retail commerce is a good example of
consumer protection regulation helping a market to work better than it would in a pure freedom of contract regime, and is discussed in Section 4 below. Commercial regulation often fails when it tries to anticipate the future development of business practices. Guessing future market developments is hard enough for entrepreneurs, so the offs are generally even worse that legislators will correctly guess the outcome of current business innovations. Once an inaccurate guess about what people in business will want to do in the future is locked into a statute, the law may become simply irrelevant, or worse, may distort the development of business practice into inefficient alternatives. The 1977 revision of Uniform Commercial Code Article 8, the law governing transfers of investment securities, is a good example of failed anticipatory regulation and is discussed in Section 5 below. This analysis may also apply to current efforts to promote the use of digital signatures through legislation, but it is too soon to draw that conclusion yet.

3 Sale of Goods Transactions

A sale of goods is a very basic, very common form of commercial transaction. Under US law, a contract is generally formed by one party making an offer and the other party accepting it. Each party must offer something of value (known as consideration) to the other and there must be a meeting other minds on what will be exchanged under the contract. Once the contract is formed by the exchange of promises, then the parties perform their obligations as defined by the contract. In a contract for the sale of goods, one party might offer goods for sale at a particular price, and the other party might accept the promise to deliver the goods, giving in exchange a promise to pay for the goods. While the theory is clear, the practice may be more ambiguous.

3.1 Signature and Writing Requirements

Contracts for the sale of goods are normally governed by Article 2 of the Uniform Commercial Code. In general, Article 2 seeks to minimize the formalities the parties must follow in order to create a binding contract so that contracts will not become unenforceable just because the parties did not comply with all manner of technical legal requirements. Even so, Article 2 cannot eliminate all uncertainty from the business contracting process about the rights and obligations of the parties. For example, it is common for a sale of goods transaction to involve the exchange of many pieces of paper between the transacting parties. These papers might include a request for a quotation, a price quote for a shipment of goods on particular terms, a purchase order, an acknowledgement of the purchase order, and an invoice. It is unclear at what point in all this exchange of papers the classic offer, acceptance and meeting of the minds occurs, especially if each of paper has boilerplate contract terms printed on it and the preprinted standard terms are mutually inconsistent. Article 2 rejects the notion that actual business practice must match classical contract law principles in order to produce a binding contract, looking instead to whether or not there is an agreement in fact between the parties as the basis for an enforceable contract (Gabriel and Rusch, 1997).

Not all provisions of Article 2 are so flexible. One rule of law governing the sale of goods is referred to as the “statute of frauds” and requires that sales of goods over a specified dollar amount must be evidenced by a writing and signed by the party against whom enforcement is sought in order to be enforceable (Gabriel and Rusch, 1997). This special rule overrides the
general rule that oral contracts are just as enforceable as written contracts (although they may be so much harder to prove that the attempt to enforce an oral contract is rendered futile). The policy behind this rule is to prevent fraud such as a party claiming a contract for the sale of goods exists when in fact no such agreement exists. Although other commercial laws exist which require a signed writing for a contract to be enforceable, the UCC Article 2 statute of frauds writing requirement is one of the most commonly encountered.

The statute of frauds raises problems for electronic commerce involving sales of goods. The party seeking to enforce the contract must show that there is a signed writing stating some of the most important terms of the contract. There is no requirement that the writing state all of the terms of the contract, but it must be sufficient to indicate that a contract has in fact been made by the parties. While a court look at the exchanges of email messages between a vendor and a purchaser might find that one of the email messages could be considered a writing signed by the party against whom enforcement is sought, it is far from clear that all court would come to that conclusion. As long as the parties cannot predict with confidence what will resist replacing paper forms with electronic messages even though the administrative expenses associated with paper processes are higher. The higher cost of paper-based administrative systems can be thought of as a sort of insurance premium paid to achieve more predictable legal outcomes.

### 3.2 EDI Trading Partner Agreements

The problem of harmonizing the exchange of email messages with the legal requirement of a signed writing was first presented in the 1980s when parties began adopting electronic data interchange contracting systems. EDI systems set up in the 1980s were often based on the use of “value added networks” (VANs) that were closes, proprietary networks with enhanced security and data integrity features. Before the exchange of electronic quotes, purchase orders, acknowledgements and invoices could begin, the parties normally had to invest considerable time and energy in reengineering their information systems to permit the exchange of messages in standardized formats to take place. In order to draw the maximum benefit from establishing an EDI trading partner relationship, each party needed to take whatever steps were necessary to permit the automated processing of standard messages. Although the parties might reach a complete meeting of the minds with regard to how different messages would be processed as a matter of information system specifications, the issue of how the exchange of messages would be interpreted by a court remained beyond the power of the parties to resolve through technical standards.

A consensus emerged among many EDI trading partners and their attorneys that the best way to reduce uncertainty about the legal status of the EDI messages they planned to exchange would be to sign a traditional contract that would set out the ground rule rules to interpreting the significance of the electronic messages (ABA Electronic Messaging Services Task Force, 1990). This contract, referred ti as an EDI trading partner agreement, reduced the uncertainty associated with how a court would treat email messages for statute of frauds purposes, because the trading partner agreement for an explanation of what legal significance the parties expected their electronic messages to have. Provided that what the parties set out in their trading partner agreement was reasonable, a court could be expected to defer to the wishes of the parties. The effectiveness of a trading partner agreement is not entirely without question, however, as a court
might nevertheless still expect to see a signed writing for each transaction that takes place within the trading partner relationship, not just for the relationship as a whole.

One strength of the trading partner agreement model for regulating electronic commerce is that it may eliminate the statute of frauds problem at the same time it defines the rights and obligations of the trading partners with regard to other issues as well. One weakness of this model is that it cannot govern the rights and obligations of anyone other than the two parties who signed the agreement, so each electronic contracting relationship must be governed by a separate contract. This administrative expense might not be significant in light of the large investments often required to harmonize the information systems of the trading partners. However, when the Internet made electronic contracting between strangers with no prior relationship a practical reality, the expense of having the parties meet face to face and take pen in hand to sign a paper contract would in many instances more than offset the cost savings associated with using the Internet as a communications medium.

Another weakness of the trading partner agreement model is that it might require a fair amount of work on the part of attorneys to negotiate and draw up, and many EDI trading partners simply never bothered to sign a trading partner agreement as a result. Yet there is no evidence available as to how a court would interpret an EDI trading partner relationship in the absence of a written contract. This is because there are no reported litigated cases involving EDI trading partner disputes, which is an astonishing fact in light of the enormous volume of EDI transactions taking place in the US today. There is no way to be sure why no disputes between EDI trading partners never reached the point of litigation. It is possible that trading partner agreements provided the parties with such clear guidance as to the rights and obligations of the parties that they felt litigation was unnecessary, although that can hardly have been the case with all the relationships that were not reduced to a written agreement. It seems more likely that the parties were unwilling to write off the large investment in information system reengineering required to establish EDI trading partner relationships, since the underlying business relationship would probably be irretrievably damaged if litigation were initiated. The absence of reported legal cases may indicate that EDI trading partners tend to work hard to find acceptable compromises to keep their relationship going when disputes arise.

3.3 Technology Neutral and Technology Promoting Legislation

For a court trying to determine whether email messages sent through an EDI system can meet the requirements of the statute of frauds, two separate issues must be resolved: whether there is a signature, and whether there is a writing. The standard for what constitutes a signature under the UCC is actually not difficult to meet any symbol executed or adopted by a party with a present intention to authenticate a writing. This definition is designed to be flexible enough to include documents marked with “X” or signed with a fingerprint, and it is approached in the general spirit of flexibility that animates the UCC, can accommodate the identification of the sender on an email message. For example, courts have held that a company’s printed letterhead can function as a signature for meeting a statute of frauds requirement.

What constitutes a writing is a harder problem. “Writing” is not a defined term in the UCC, but would seem to indicate that a piece of paper is required. In In re Kasper, a bankruptcy case 1997, the court held that a credit card application taken by the credit card issuer in a telephone call with the debtor did not meet the “writing” requirement of one section of the
The Bankruptcy Code that would have enabled the credit card issuer to prevent the debtor from discharging his obligation to pay the credit card balance in bankruptcy. The court went on to observe that the statute requires a “writing,” the court was entitled to insist on a piece of paper, and did not need be concerned by the fact that so holding might prevent businesses taking advantage of more efficient new electronic media.

Given that current laws do not generally treat electronic media as a functional substitute for paper documents, and that there is some uncertainty about how flexibly in fact a court will be in interpreting what constitutes a signature in electronic communication contexts, there has been considerable attention focused on the question of law reform in this area. One approach to the problem might be to enact legislation that merely authorizes a court to treat an electronic record as a writing and an electronic authentication as a signature under appropriate circumstances. Another approach might be to enact legislation that requires a court to so hold, unless circumstances dictate the contrary. Such legislation, since it focuses on legal outcomes and not technical processes, can be considered “technology neutral”.

This is one of the issues that has been considered at length in the context of revisiting the UCC to take account of new business practices. The outcome of that process will probably be a sort of global “search and replace” throughout the UCC that replaces references to “writing” with references to “record.” Record is defined as information that is inscribed on a tangible medium or that is stored in an electronic or other medium and is retrievable in perceivable form. This definition is designed to be broad enough to cover both paper and electronic documents. It is unclear whether the UCC definition of signature is already broad enough to encompass electronic commerce, or whether a new defined term, such as “authenticate” should be introduced to cover both manual signatures and electronic authentication processes. As of 1998, for the most part these reforms were still being debated in the uniform law drafting process. Until the official text of the UCC is released by the ULC, state legislatures do not begin to consider the proposed revisions. Once the revised text is available for state legislatures, it may take years for it to be enacted in all 50 states.

Even if the UCC is revised along these lines, and these revisions take effect in the near future, many laws relevant to commerce are not included in the UCC. The ULC has appointed a drafting committee to work on a “Uniform Electronic Transaction Act” that is designed to update other state laws in the same manner as the UCC is currently being revised. The UETA, like the UCC revisions, is a technology neutral statute that aims to enable all electronic commerce across the board by giving courts enough flexibility to accept electronic documents and signatures where appropriate.

While the uniform law drafting process grinds on, many states have leapt into the void and enacted laws in this area (McBride, Baker & Coles, undated). The result is a bewildering variety of approaches ranging from technology neutral to technology specified. A technology specific approach identifies one electronic commerce technology and provides that its use will have certain legal consequences. This has the effect of leaving other electronic commerce technologies struggling with the current uncertainty in the law, and focusing the attention of the public on one technology as having been endorsed by the state legislature. Given the current state of rapid innovation in electronic commerce, it is not clear that a technology specific approach to legislation in the US and abroad is asymmetric cryptography, which is used to produce “digital signatures” (ABA Information Security Committee, 1996).
3.4 Digital Signatures and Public Key Infrastructure

The use of the Internet for commerce changed the landscape of electronic contracting, and raised the statute if frauds in a new context. EDI standards and the use of VANs permitted one-to-one electronic contracting, while the Internet opened up the possibility of one-to-many contracting (Winn, 1998). In order to take advantage of the much wider market access the Internet offered, parties sought an electronic contracting model that did not depend on a written trading partner agreement gained by the transacting parties in a face to face meeting. The flip side of the greater access offered by the Internet was its lack of security infrastructure that the VANs had provided, however. For one part to have confidence that their electronic communications were in fact taking place with the correct counterparty, and that the content of the electronic communications could be trusted, the parties to Intent transactions themselves would have to take responsibility for security. Even if the parties were able to satisfy themselves that their Internet electronic contracting technology was as reliable as paper-based commerce or EDI contracting, until the UCC reforms were finalized and enacted by state legislatures, uncertainty remained as to the legal effect of such commercial practices.

One technology that seems to hold particular promise for resolving the technical problems associated with Internet contracting is asymmetric or public key cryptography (Ford and Baum, 1997). Parties interested in identifying each other over and open network can each generate a pair of matched keys, one to be kept private and one to be distributed publicly. When a message signed with a private key is tested with the associated public key, asymmetric cryptography can be used to determine with high degree of certainty that the message could not have been signed with any other private key than the one associated with that public key. However, merely establishing a strong association between a message signed with a private key with a particular public key is not very helpful for electronic commerce purposes unless the party using the public key is confident of the identify of the person in controls of the private key, and confident that person’s control over the key has been maintained at all times.

For public key cryptography to support electronic commerce, at a minimum a solution must be found to the problem of how to associate an online identity established through the use cryptographic keys and the identity of an actor in the material world who can be held legally responsible for performing a contract. The simplest solution is to have people meet face to face and exchange keys on floppy disks, but like the trading partner agreement, the costs associated with such a system will negate most of the benefits that the Internet can offer.

Another solution to the problem of binding real world identities with online identities that has been widely discussed is the use of “trusted third parties” to introduce parties to each other, eliminating the need for a gave to gave meeting between the parties. Such a trusted third party might issue a certificate attesting to the fact that a particular human being was in control of a particular private key at a particular time. The person using a cryptographic key as an online identity card might provide a new acquaintance with a copy of the public key and a certificate indicating that a trusted third party was willing to couch for the material world identity of the holder of the private key. A trusted third party offering which services to parties wishing to use digital signatures to form electronic contracts with strangers. This particular solution is based on the X.509 certificate standard developed as part of the X.500 directory standard. This standard was established to promote the use of distributed directories over networked computer systems. A system for coordinating the use of digital signature certificates issues by trusted third parties to
establish a system of reliable online identities is generally referred to as a public key infrastructure.

The strength of this model is the fact that it can create an environment of trust between parties with no prior relationship online or in the material world. A party considering entering into a contract based on an email communication could as the counterparty to include an identity certificate from a trusted third party with the signed email in order to establish a reliable association between the digital signature attached to the mail and a real human being that can accept legal responsibilities. If the trusted third party has reliably identified the counterparty, and the counterparty has never lost control of the private key used to sign messages, then the party considering the contract can have confidence that the signature is what it appears to be. If the only impediment to the formation of contracts over the Internet was uncertainty among the contracting parties as to their material world identities, then a public key infrastructure that distributes digital signature certificates would permit contracting to take place.

The weakness of this model is its failure to address many of the concerns that a party considering entering into an Internet transaction would have. These concerns include the need to know not simply the material world identity of the send of a particular email, but the capacity of the send to enter into a legally binding contract. The sender might be a minor, which creates problems because under US law contracts entered into by minors are generally voidable at the election of the minor. If the party expected to assume responsibility for a contract is a corporation or other legal entity such as a trust, then the other party needs to know whether a particular human being is duly authorized to act for the legal entity. The party considering entering into an Internet transaction also needs information about the ability of the other part to perform his or her promises. This includes the ability to deliver goods conform to the contract terms, or to pay for the goods as agreed. The party considering whether to go forward might also want to know the jurisdiction in which the other party is located, in order to estimate the risk of being haled into court in a remote location if the transaction goes awry. A simple binding of the human being with a digital signature provides no information about any of these issues.

The most common model of a public key infrastructure and digital signature certificates was actually designed to create online directories of names and addresses equivalent to phonebooks (Feigenblum, 1998). In the material world, parties do not make the decision whether to enter into contracts based on whether someone can be found in a telephone directory, and it is unlikely that parties will begin to do business online simply based on the proffer of an online ID certificate if there is no easy way to obtain the other information needed to make a business decision about the value of the contract.

It is possible that the basic framework of the public key infrastructure and digital signature certificate can be expanded to include the rest of the information parties need before they would be willing to enter into contracts over the Internet with strangers. Just how the basic framework should be expanded is a topic of considerable debate and what, if any solutions can be found to the problem of adapting the basic model to the complex realities of electronic commerce, will not be apparent for some time (Feigenblum, 1998).

In addition to these questions surrounding the business model within which digital signatures will be used, there are also substantial unresolved question about the design of large-scale open system public key infrastructures as a technical level. For example, before relying on a digital signature certificate, a party might want to check a certificate revocation list maintained by the certificate authority to make sure that the certificate had not been revoked, but there are many unresolved issues surrounding how a certificate revocation list can be reliably maintained.
and made accessible in an environment in which large volumes of certificates are in use simultaneously. While digital signatures certificate standards permit certificates to be adapted to specific purposes through the use of certificate policies contained in policy extension fields, it is unclear how such policies can be reliably recognized and acted upon in open network systems.

It is possible that the best application of this technology will not be in open environments in which strangers do business with strangers, but within more closed environments in which parties with prior relationships use digital signatures to permit communications to take place over insecure networks and eliminate their reliance on VANs. Many of the thorny business and technical design problems associated with creating a workable open system using digital signature are not difficult to resolve within a more limited context.

Many entrepreneurs, technologists and lawyers have been distracted from the fact that most current proposals for establishing public key infrastructures do not address basic business issues, and have rushed to embrace the idea of digital signatures as the panacea for Internet electronic commerce. Several states, including Utah, have enacted comprehensive digital signature legislation in advance of any commercial applications of this technology on the assumption that enabling legislation will accelerate adoption of this technology. The debate surrounding how to use digital signature technology to support real commercial transactions has not yet been resolved, and may not be resolved for some time. Until that debate is resolved thorough actual commercial implementations of the technology, it will not be possible to judge the success of the legislative efforts to promote this technology.

3.5 Extranets and Trading Partner Agreements

In 1998, the most successful examples of Internet electronic commerce were Cisco Systems, Inc. and Dell Computer Corporation. Cisco’s web revenue for 1998 were projected to be over $6 billion; Dell’s web revenues were projected to be in excess of $2 billion, and unlike Amazon.com, both companies are profiting from their Internet sales. Both companies use something resembling the old EDI trading partner agreement to minimize the legal uncertainty associated with Internet commerce.

Cisco uses its website to create an extranet, permitting only authorized users to access its web-based “Cisco Connection Online” service. Parties who have entered into a contractual relationship with Cisco are allowed to designate which employees or representatives are authorized to access Cisco’s website to place orders. These parties are then assigned user-IDs and passwords that they must use to log into those parts of Cisco website where product availability and prices can be checked and orders placed. These preexisting contractual relationships provide a framework, similar to that created by a trading partner agreement, within which email messages are exchanged that permit contracts to be formed for the sale of Cisco goods and services.

Dell permits credit card holders to make purchases of goods and services directly from its website. The framework of the credit card system determines the rights and obligations of the parties with regard to such possible issues as the ability of the customer to pay for the goods, liability for unauthorized use of the credit card, and the right of the customer to dispute the transaction. The Dell website uses asymmetric cryptography, not as an authentication process, but merely to establish a secure channel of communication between the Dell server and the customer’s browser using the Secure Sockets Layer (SSL) protocol. Assuming the customer’s
browser has the certificate authority’s certificate preloaded (which is true for recent releases of standard Internet browser software), then the customer’s browser can download a copy of Dell’s public key and determine that it has been certified by the certificate authority. The browser and the Dell server share a special cryptographic key, called a “session key” that has been encrypted with Dell’s public key for security. The consumer’s credit card information travels over the Internet encrypted with the session key, and so is protected from being intercepted in transit. The public key infrastructure merely reduces the risk of certain forms of fraud by third parties, while the contractual and regulatory framework of the credit card system, combines with the terms and conditions of use that Dell attaches to use of its website for electronic commerce, perform similar functions in this system as a trading partner agreement.

4 Payment Transactions

Payment systems were among the first commercial transaction systems to migrate to an electronic environment. In 1957, paper checks were first imprinted with the magnetic ink character recognition line on the bottom that permitted the check processing system to be automated. In the late 1960s, banks began experimenting with automated teller machines and secure systems for wire transfers of funds. At the same time, the use of credit cards rapidly proliferated. In 1970, in response to widespread criticism of aggressive tactics on the part of card issuers to expand rapidly the use of credit cards while at the same time severely limited card issuer liability. Congress enacted a comprehensive scheme of consumer protections for card holders that remains in effect today. The governing electronic funds transfers dates from 1978, when consumer protections were passed by Congress that applied to transactions such as ATM withdrawals. Outside the realm of consumer payment systems, in 1989, the ULC formalized a law governing wholesale wire transfers, UCC Article 4A, which has now been adopted in all 50 states.

In the late 1990’s, all large-scale payment systems in the US had been adapted to operate within secure networked mainframe computer systems operated by regulated financial institutions. As a result, Internet-based payment systems have faced formidable competition and have not been able to establish any significant market share (Winn, 1999). Many standard developing organizations and technology vendors are competing to achieve a dominant position in the Internet payment arena, but it is unclear which, if any, of the current competitors will ultimately prevail. First Virtual, the first commercial Internet e-cash system, began operations in 1995 amid great fanfare, but ceased payment system operations in 1998 due to lack of market share. Likewise, Internet micropayment technology seemed very promising in the mid 1990’s, but by 1998 commercial precuts such as Millicent were still not enjoying widespread acceptance. Just as it is hard to predict who will be the winners among these emerging technologies, it is also unclear how the existing large scale mainframe-based payment systems adapt to these new competitive forces.

4.1 Credit Card Transactions

Credit cards, used in combination with the SSL protocol supported by the end user’s browser, have proven to be the payment system of choice for retail Internet electronic commerce. The SSL protocol works within a very simple public key infrastructure, and provides a secure channel for
communication of information between the end user’s browser and the e-commerce server. (SSL
is further described in Section 3.5 above.) Early concerns over the lack of security for Internet
communications led MasterCard and Visa each to begin work on designing a much more
complex public key infrastructure that would provide digital signature certificates to card holders,
merchants, acquiring banks and issuing banks. These projects later merged into the Secure
Electronic Transaction (SET) standard. The SET standard offers a much higher level of security
than the SSL standard by adding new safeguards against fraud and unauthorized use of credit
card information. In order to do so however, it will have to place heavy demands on existing
credit card transaction processing infrastructure and may require the execution of complex
cryptographic algorithms that exceed the processing capacity of the average end user’s system.
These and other problems have slowed down the rate of adoption of the SET standard and
progress in further refining the standard. While work on the more sophisticated and complex
SET standard has progressed slowly, the SSL protocol has become the de facto standard for
security for retail Internet commerce today.

Although the SSL standard provides only minimal security for payments transactions
over the Internet, the existing legal and technical framework of the credit card system
supplements those protections to produce an Internet payment system that meets the current
minimum requirements of merchants, end users and financial institutions. The only segment of
the credit card system that uses the Internet as a medium of communication is the transmission of
the card holder’s account number to the Internet merchant. From the merchant’s e-commerce
server, information about authorized charges are to the merchant’s acquiring bank in the same
manner as they would be transmitted by a telephone or mail order merchant. The rights and
obligations between the merchant, the merchant’s acquiring bank and the cardholder’s issuing
bank are set by private contracts between the parties.

Consumers considering whether to use the Internet to make purchases can limit their risk
of loss due to fraud by using their credit card as a form of payment because federal regulations
limit consumer liability for unauthorized charges to $50. This limit applies whether the card is
used in a face-to-face transaction, in a telephone or mail order transaction, or in an Internet
transactions in which the merchant does not have the opportunity to inspect the credit card
cannot contest a consumer’s later claim that a particular charge transaction was unauthorized.
This rule was developed in the mail order and telephone order context, and applies equally to the
Internet context.

A merchant considering accepting payment by credit card from an Internet retail site
must first be satisfied that it has found a way to minimize the risk of fraud and error associated
with credit card use, because the merchant will not be allowed to pass those costs on to the
consumer, or in most cases, the merchant’s acquiring bank. A merchant may decide that it
nevertheless makes sense to accept credit cards as a payment device for Internet commerce given
the lack of practical alternatives, the increased volume of sales that are likely to result, and the
fact that the credit card issuer, not the merchant, assumes the risk of payment default by the card
holder.

Consumers also enjoy access to dispute resolution services provided by credit card
issuers in the event that the consumer has a dispute with the Internet merchant regarding the
goods or services purchased. Under certain circumstances, federal regulations require card
issuers to investigate and resolve cardholder complaints about goods and services purchased by
credit card. Current business practice among card issuers has considerably expanded the use of
this dispute resolution service to include more transactions than are covered by federal regulation.
From the consumer perspective, the use of a credit card as a payment mechanism substantially reduces the risk of being forced either to pay for unacceptable goods or services ordered over the Internet, or to submit to the jurisdiction of a remote forum in order to dispute the value of goods and services purchased over the Internet.

4.2 Electronic Funds Transfer

If some of the new technologies for payments under development are ultimately successful, it is possible they will be outside the scope of existing laws, including consumer protection regulations. Unless and until regulators intervene, such systems would be regulated by contracts among the parties. Wholesale funds transfer systems in the US evolved largely outside of any existing regulatory framework for over a decade before a formal body of law was established to govern the rights and obligations of the parties. The law that now addresses wholesale wire transfers is UCC Article 4A. Article 4A is a very significant development in the law of electronic commerce because it was one of the first bodies of law to consider in depth how the use of electronic authentication systems should be regulated.

In the US, financial institutions operate a wholesale wire transfer system for large scale business to business funds transfers. These systems, which include the Fedwire operated by the Federal Reserve system, and the New York Clearing House Interbank Payment Systems (CHIPS), transfer in excess of on trillion dollars per day. These systems began operations in the early 1970’s, and operate largely among banks and their major corporate customers. Before the adoption of Article 4A, the only law that applied to these systems beyond private contracts among the participants were Federal Reserve Board Operating Circulars, for transfers that used the Fedwire, and the operating rules of CHIPS, for transfer that used CHIPS. Many aspects of these transactions were not covered by an organized body of law, however, and it was possible for disputes to arise between parties which were not clearly governed by any contract or operating system rules.

Banks providing wire transfer services were not particularly concerned about the lack of formal law governing the wholesale funds transfer system until some litigated cases in the 1980s raised issues that the banks found troubling. One such issue that drove the banks to the ULC to support the Article 4A drafting process was a litigated case in which a bank failed to make a funds transfer on the date requested by its customer. The court suggested that a bank making an error in handling a wire transfer might be held liable for the lost profits from any business deal the transferor lost due to delay. Banks were unwilling to accept liability beyond the time value of the funds while they were delayed due to the error. Because a funds transfer might pass through several banks on the way from transferor to transferee, it was not possible for a bank to be certain that it would always be protected liability by a preexisting contractual relationship with the disgruntled transferor. The only way to guarantee a limit to the bank’s liability would be by statute. After considerable debate in the drafting process, the representatives of the banks; customers agreed to this limitation (Baxter and Heller, 1997).

Banks and their customers shared a commitment to keeping the price of funds transfer services low, and expanding liability for the banks would have a necessary consequence of forcing banks to raise the price of funds transfer services or to leave the market. Bank customers agreed that it was more efficient for customers to accept responsibility for monitoring the proper execution of funds when large profits were at stake then to put the banks in the position of
insuring all their customers against any risk of bank error in executing transfers. Many bank customers were operating at a level of sophistication that was equivalent to that of the banks themselves, and so in a context in which no consumers were involved, the customer could reasonably be expected to assume some responsibility for the operation of the system in exchange for lower prices.

Another major point of contention between the banks and their customers was how responsibility for unauthorized funds transfers should be allocated. The banks initially took the position that unauthorized funds transfers could only occur as a result of carelessness by their customers because banks had adequate security procedures in place, but their customers were unwilling to accept this analysis (Rubin, 1993). After heated debate, a complex compromise was worked out dividing liability for unauthorized funds transfers between the bank and the customer. The initial allocation of liability was on the bank, but the bank could shift the risk of liability to the customer if the bank and the customer agreed a “commercially reasonable security procedure” that would used to initiate funds transfers. A “commercially reasonable” security procedure is one that is adapted to the customer’s situation, in light of the amount, type and volume of funds transfers the customer makes, the customer’s business and other factors. If the bank can prove that it complied with the security procedure agreed upon with the customer, then the bank cannot be held liable for an unauthorized funds transfer executed from the customer’s account. The only exception to this rule arises in the unlikely event that the customer can prove that the unauthorized funds transfer did not originate with any person or facility under the customer’s control. In that case, which would include funds transfers executed by hackers penetrating the security of the system from outside the customer’s facilities, the bank must bear the risk of loss.

Article 4A takes a very different approach to liability issues than the consumer protection regulations that apply to credit card transactions. With credit cards, the consumer is presumed to be incapable of making any significant contribution to reducing the risk of loss due to unauthorized use of the card, and so is exonerated from almost all liability as a result. Card issuers, merchants and acquiring banks bear almost all risk of fraud and error, and as a result have an incentive to invest in the most sophisticated antifraud technology available. In the wholesale funds transfer environment, however, many bank customers are operating at a level of sophistication equivalent to that of the banks, and are required to be active participants in the design and maintenance of the security of the funds transfer system. Even though the loss allocation rules in each system point in opposite directions, Article 4A and the credit card system are each examples of commercial law that as been adapted very successfully to different categories of payment system.

5 Financial Asset Transactions

The depth and liquidity of US capital markets are unparalleled throughout the world today. One reason that US capital markets can operate so efficiently is that the back office clearing and settlement operations that support them is fully automated. Wall Street banks and securities firms recognized the need for automation in back office functions as early as the late 1960’s. The “paperwork crunch” caused by paper based settlement procedures was forcing the stock market to shut down at periodic intervals to permit back office operations to catch up with trading operations. At that time, the daily volume of stocks traded on the New York Stock Exchange was
around 10 million shares, a far cry from the 1 billion shares per day trading volume that occurred in 1998. By the mid-1970s, there was a recognition in Wall Street that UCC Article 8, the law that applied to transfers of ownership interests in investment securities, would have to be revised to take account of automated processes for handling transfers of stocks and bonds.

5.1 1977 Revisions to Investment Securities Law

The ULC appointed a drafting committee to review the then-existing version of Article 8, which had been drafted in 1957, in light of changing technology in capital markets. In 1977, the drafting committee produced a new Article 8 which they hoped would promote the use of automation in securities markets. The 1977 Article 8 drew on two models: the traditional paper bond or stock certificate model drawn from the 1957 law, and a new model based on innovations occurring in the US Treasury Department with regard to government securities. The Treasury was issuing “uncertificated” securities which existed only as a bookentry records in the Treasury computer system. The drafters of the 1977 revisions to Article 8 guessed that the private sector would follow the public sector’s lead in automating securities transfers, and included rules governing the transfer of uncertificated securities (Rocks and Bjerre, 1997).

In fact, the private sector was not following the lead of the public sector, but was devising a different system for automating securities transfers. Private sector securities market participants increased their reliance on existing cooperative institutions such as the Depository Trust Company (DTC), a corporate custodian collectively owned by most major Wall Street banks and brokerage firms. To eliminate transfers of individual stock certificates between firms, firms agreed to maintain accounts with common intermediaries such as DTC and transfer ownership interests in stock by bookentry adjustments with the intermediary. The paper certificates were not actually eliminated from this process. Instead, the issuer of the security would provide “jumbo” certificates to the intermediary who would keep them in a secure location. The system developed in the private sector was thus a system of immobilized paper combined with bookentry records of intermediaries rather a true certificate system.

5.2 1994 Revisions to Investment Securities Law

When state legislatures considered the 1977 revisions to Article 8, many declined to enact the revisions and retained the original 1957 text of the law. Some jurisdictions enacted the 1977 revisions, doubtless unaware that the revision did not cover the actual securities market business practices that had developed. The result was lack of uniform law throughout the US governing transfers of securities, and lack of any law corresponding to the system of indirect, immobilized securities holdings. The uncertain state of the law did not create a sense of crisis among market participants, however, until the stock market crash of 1987 and the failure of the Drexel Burnham firm in 1990. These events caused market participants to recognize that should a major market participant be unable to fulfill all of its obligations to deliver securities to other market participants, there was simply no system in place for sorting out the competing claims of ownership among all parties with rights to the securities held by the failed firm (Smith and Shupak, 1996).
The ULC appointed a new committee to revisit the provisions of Article 8 in light of actual commercial practice in securities markets. In 1994, a revised version of Article 8 was issued. This version of Article 8 recognizes three types of investment securities: paper certificates, certificateless securities such as Treasury obligations and some mutual funds, and a “security entitlement.” A security entitlement is what a customer of a brokerage firm has if the customer permits the brokerage firm to retain control of the stocks and bonds in the customer’s account. The customer has a claim against the brokerage firm for the securities held at the firm. That brokerage firm may in turn not possess any stock certificates, but may have security entitlements with another firm or an intermediary such as DTC. The 1994 revised version of Article 8 includes provisions governing transfers of ownership in security entitlements, including the use of security entitlements as collateral for loans, thus resolving the uncertainty created by failure of the 1977 revisions to provide for such commercial practices.

The failure of 1977 revisions to correctly anticipate the manner in which private sector automation occurred shows the difficulty of drafting anticipatory commercial law. The drafters of the 1977 revisions based their model on the only well established and well understood model for electronic securities transfers. Although the practice of immobilizing securities and holding through intermediaries was already taking shape in 1977, it escaped the notice of the drafters. If someone were to have suggested to the drafters of the 1977 revisions that in the future, electronic securities transfers would be possible in Wall Street because paper certificates for trillions of shares of stock would be held in vaults at DTC, the suggestions might have struck them as too ludicrous to be taken seriously. Yet that is the system that is in operation today and it is highly successful.

6 Conclusion

Existing commercial law can be adapted to new electronic commerce technologies in a manner that simplifies and supports business practice if changes are made in light of present commercial reality. There are many successful examples of technology neutral commercial law, such as the article 4A concept of a “security procedure” and the Article 8 concept of a “security entitlement,” that are flexible enough to accommodate many different forms of technology. Business practices in Internet commerce may not yet be well enough established for commercial law to capture and reflect the standard default terms the parties might expect to operate in the absence of explicit contract terms. Until a body of business practices develop to guide the direction of legislation, transacting parties should carefully consider how risks are allocated by private agreement.

If Congress and state legislature leap in too quickly to promote promising technologies, chances are great that the result will be greater inefficiency, not less. Legislators should not be in the business of trying to guess the winners in the current competition among technologies for Internet commerce. If Congress and state legislatures cannot refrain from acting in this area, however, they should limit their intervention to protecting less sophisticated parties from possible overreaching by more sophisticated parties. The model of credit card consumer protection offers a promising model for legislation that promotes electronic commerce without dictating any technological choices. Credit card consumer protection regulations shelter less sophisticated parties from fraud and error risks they cannot control while forcing more
sophisticated parties to invest in security procedures to reduce such risks as much as possible. This type of legislation can help to make the entire system operate more efficiently than it would if transactions were governed simply by standard from contracts drawn up by card issuers.

References

Uniform Law Commission website [http://www.nccusl.org](http://www.nccusl.org)