1998

Open Systems, Free Markets, and Regulation of Internet Commerce

Jane Kaufman Winn
University of Washington School of Law

Follow this and additional works at: https://digitalcommons.law.uw.edu/faculty-articles

Part of the Commercial Law Commons, Consumer Protection Law Commons, and the Internet Law Commons

Recommended Citation

This Article is brought to you for free and open access by the Faculty Publications at UW Law Digital Commons. It has been accepted for inclusion in Articles by an authorized administrator of UW Law Digital Commons. For more information, please contact cnyberg@uw.edu.
Can commercial transactions conducted over the Internet be regulated by existing commercial law doctrines? Many promoters of Internet commerce argue that business done over open computer networks such as the Internet will require a new regulatory framework. In fact, many issues raised by Internet commerce have already been considered at length in the context of electronic commerce conducted over closed computer networks, such as those used in financial markets. One of the most hotly debated issues regarding the regulation of Internet commerce is the question of what would be the online equivalent of a signature. Some have argued that, because new technology using public key cryptography is uniquely suited to resolving this issue, public key cryptography should be promoted with special legislation. These claims for preferential treatment should be viewed with skepticism, however, when they are advanced by those marketing the technology before there have been any large-scale adoptions of the technology in question. The desirability of technology-specific legislation should be especially suspect if it comes at the expense of consumer protection provisions found in the regulation of equivalent electronic financial services such as credit cards or electronic funds transfers. A technology-neutral approach to Internet commerce legislation will permit parties to commercial transactions to make up their own minds about what new business practices make sense for Internet commerce. If any special legislation is needed to promote sound business practices in Internet commerce at this early stage in its development, it would be technology-neutral consumer protection legislation, not protections for technology developers and promoters before the risks associated with their products have become apparent.

I. INTRODUCTION .................................................................................................................. 1179

II. IMPACT OF THE INTERNET ON COMMERCIAL TRANSACTIONS ........................................ 1184
A. Open Networks and Distributed Computing ................................................................. 1184
B. Trustworthy Systems and Communication Security ..................................................... 1190
C. Digital Signatures, Certificate Authorities, and Public Key Infrastructure ..................... 1198
D. How Will Internet Authentication Procedures Be Used? .............................................. 1207
   1. Closed—Bilateral ........................................................................................................... 1209
   2. Closed—Bound Community ......................................................................................... 1210
   3. Closed—Subscription .................................................................................................... 1210
   4. Open—Server Security ............................................................................................... 1211
   5. Open—Client Security ............................................................................................... 1213

* Associate Professor of Law, Southern Methodist University, <http://www.smu.edu/~jwinn> or <jwinn@mail.smu.edu>. The author gratefully acknowledges the support of the Dorothy Lee Trust, which funded the research for this Article, and the thoughtful comments of Dwight Arthur, Richard, Field, and Ronald Mann on earlier drafts of this Article.

1177
III. WHAT IS THE ELECTRONIC EQUIVALENT OF A SIGNATURE FOR INTERNET COMMERCE?

A. Common Law of Signatures
   1. What Is a Signature? ......................... 1216
   2. When Can a Signature Machine Produce a Valid and Binding Signature? .................. 1218
   3. What Is the Significance of Notarizing a Signature? ............................................. 1219
   4. What Is a Signature in Electronic Commerce? ........ 1220

B. Negotiable Instruments Law
   1. What Is a Signature? .......................... 1222
   2. When Can a Party Be Held Liable for a Signature He or She Did Not Produce? .......... 1223
   3. When Is a Signature Presumed To Be Authentic? ..................................................... 1224

C. UCC Article 4A and Commercially Reasonable Security Procedures
   2. When Can a Party Be Held Liable for a Payment Order It Did Not Originate? .......... 1229

D. Consumer Electronic Funds Transfers Under Regulations Z and E
   1. How Is a Consumer Payment or Electronic Funds Transfer Authorized? .................. 1233
   2. When Can a Party Be Held Liable for a Payment or Funds Transfer He or She Did Not Authorize? ................................................................. 1235

E. Proposed Revisions to the UCC Definition of Signature and Writing .......................... 1237

IV. HOW SHOULD AUTHENTICATION PROCEDURES USED IN INTERNET COMMERCE BE REGULATED?

A. Different Approaches to Regulating Open Network Authentication Procedures .............. 1238
   1. ABA Digital Signature Guidelines .................. 1240
   2. Minimalist Enabling Legislation .................. 1249

B. UCC Article 8 and the Danger of Drafting Technology-Specific Commercial Law .......... 1250

C. Assigning Liability for Fraud or Error in the Use of Rapidly Evolving Technology .......... 1253
I. INTRODUCTION

Commercialization of the Internet has precipitated a lively, wide-ranging debate over how Internet business transactions should be regulated. In recent months, for example, almost every state, the federal government, and the United Nations have considered or taken action on the issue of what constitutes the online equivalent of a signature. This apparently esoteric controversy goes to the heart of how parties will create binding contracts online and is the first of what will certainly be a flood of legal issues arising out of the migration of conventional business transactions to the Internet. The popularity of the Internet has already triggered vigorous debate over the protection of free speech and privacy rights in this new environment, as well as

over such issues as how Internet access should be priced and how domain names should be allocated. Whether commercial transactions conducted over the Internet should be subject to special regulation is now moving to the forefront of these debates. As businesses scramble to exploit the global reach of the Internet and technology vendors compete to build an infrastructure for those transactions, lawmakers are being lobbied to consider a wide array of legislation designed to regulate this nascent market.

This Article addresses the controversy surrounding how to establish both the identity of a party and his or her intent to be legally bound in an Internet business transaction. Authentication procedures comprised of technical, business, and legal elements can solve this problem. In a conventional business environment, establishing intent to be bound is usually unproblematic as a matter of law, because the law regarding signatures, forgeries, and apparent authority is well established. Exactly how these existing doctrines should be translated into the Internet context, however, is far from clear. The Internet is an open, public network. The same openness that attracts businesses into the Internet also gives rise to the thorny computer security problems that have triggered the debate over authentication procedures. Parties can feel confident that they have formed binding contracts while communicating over open networks only if they use reliable authentication procedures. These authentication procedures are, however, only one element to be taken into account in the design of a trustworthy computer system. Their reliability is determined by the overall security of the system, in its design as well as in its administration. What constitutes a reasonable authentication procedure or a trustworthy computer system in government and business environments is unclear, given how rapidly information technologies are changing and developing. How the concepts of a reasonable authentication procedure or trustworthy computer system will be applied to individual consumers entering into contracts online is even less clear.

Part of the current debate over authentication procedures for Internet business transactions is being driven by the marketing of cryptographic technology products. These computer security products resolve some of the problems of establishing identity and intent to be bound in a contract formed over an open network with an authentication procedure generally known as "digital signatures."

2. See INFORMATION SECURITY COMMITTEE, SECTION OF SCIENCE & TECHNOLOGY AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE: LEGAL INFRASTRUCTURE FOR
Proponents of these cryptography products are advocating "technology specific" legislation that endorses what they believe is the best solution available to the problem of authentication over insecure networks. Proponents of "technology neutral" legislation believe that any residual disparities between the legal status of conventional and electronic commerce should be eliminated by new legislation, but that none of the many competing business models for electronic commerce security solutions should yet be given a legislative endorsement.

In order for parties to enter into binding contracts in an open network environment such as the Internet, they must have a reliable way to recognize manifestations of intent to be legally bound. In addition, they must have confidence that the manifestations of intent that they rely upon are genuine and have not been altered in transit over the network. While simple passwords or personal identification numbers are often used to connect a person with activities online, cryptographic solutions bind persons with online actions in a much more sophisticated way. In addition, cryptographic solutions assist in determining whether the message has been tampered with in transit. Without reliable information about the context from which the signed electronic message originates, however, an electronic signature created with cryptography is no more evidence of a party's intent to be bound than a facsimile ink signature made with a signature machine can evidence intent to be bound without any information about how the machine has been used. The recipient of an electronic message can feel confident that a binding contract has been formed not just from the security applied to the message itself, but with the knowledge that it originated from a system that has implemented an appropriate overall level of security procedures.

Business conducted over the Internet is expanding rapidly, but it is not yet encumbered with an intrusive, unresponsive regulatory structure. In the absence of a compelling showing that competitive market forces are failing to achieve a fair and efficient result, legal issues raised by the migration of business activity to the Internet should not become a pretext for heavy-handed government intervention. At this time it is still unclear which technical and business standards, including standards for authentication procedures, will gain widespread acceptance. It is equally unclear what costs and benefits will accrue to businesses moving into the Internet, including the costs of breaches in computer security caused by fraud or
negligence associated with operating in an open network environment. In the absence of any concrete information about what constitutes reasonable business practices and reasonable computer security standards in this new environment, it is unclear what will constitute a fair and efficient loss allocation system.

In crafting a legal framework to govern the novel issues raised by Internet business transactions, costs associated with fraud and negligence should be allocated in a manner likely to reduce the individual incidences of loss and to promote investments that will reduce the overall magnitude of losses incurred in the system. The risk of loss due to fraud should be put on the party most capable of preventing the fraud, to the extent that it has a deterrent effect. However, the cost of unavoidable fraud losses should be distributed among providers or users through an insurance scheme. Similarly, any party capable of designing improvements to the system that will reduce the overall incidence of loss in a cost effective manner should be given incentives to do so.

The parties to Internet business transactions include consumers and merchants, as well as technology vendors, who are competing to build the infrastructure for this emerging marketplace. Large amounts of time and effort have been invested in identifying and addressing legal issues from the perspective of developers of the technology infrastructure, while far less time and effort have been invested in identifying and addressing the legal issues that the merchants and consumers will face in this new environment. As a result, some states have enacted legislation that promotes specific technologies by sheltering the promoters of these technologies from certain liabilities. However, the developers of the technological infrastructure of Internet commerce should not be exempted from certain categories of legal risks, if leaving open the possibility of common law liability provides those promoters with reasonable incentives to design better systems.

No legislative guidance has yet been proposed on what constitutes reasonable security standards for merchants and consumers entering the Internet marketplace. Existing or proposed legislation that promotes the use of cryptographic authentication procedures in business transactions in effect promotes the adoption of a complex and risky technology by relatively unsophisticated parties before adequate safeguards have been established. It is very unlikely that individual end users will be able to implement the same security practices used in the military or sophisticated corporate environments (such as bank wire transfer departments), where computer security programs using cryptography were first developed. However, it is also unclear what
individual end users can reasonably be expected to do. The presumption of validity that attaches to traditional signatures as reliable evidence of intent to be bound is based on a well-established connection consistently observed over centuries. Although some "technology specific" legislation creates a presumption of validity for a digital signature, there is not yet any basis in experience for extending that same presumption of validity to an electronic authentication procedure.

Legislating a partial risk allocation scheme before there are any well-established Internet business practices seems doomed to create an intrusive, unresponsive regulatory framework where none now exists. Until there is more knowledge about how new technologies will actually be used by the merchants and consumers they are designed to benefit, new legislation to enable Internet commerce should be technology-neutral. Meanwhile, existing legislation and common law precedents should be reevaluated in light of new technological business practices. Legislation tailored to promote the fair and efficient operation of the Internet marketplace can be written only in light of that knowledge and experience. In any event, before legislative safe harbors are created exempting the most technologically sophisticated participants in the Internet marketplace from liability, attention should be focused on how these technologies will affect end users and what risk of loss is appropriate for end users to assume.

This Article will first describe the context in which digital signature applications are being developed. The Internet is a novel business environment, because it is a global, open network of computers. Open networks may provide greater access at lower infrastructure costs than closed networks, but they bring along the expense of greater security risks. At present, various groups are advancing different models of how Internet electronic commerce can be accomplished from technical and business perspectives; many of the competing models include digital signature technology administered in different forms. The second part of this Article examines how existing law treats signatures as evidence of intent to be legally bound and allocates the risk of loss due to forgeries or unauthorized signatures. This includes the law of signatures under contract law and negotiable instruments law, as well as the existing laws governing the use of authentication procedures in electronic funds transfers. This Article next reviews the ABA digital signature guidelines as a conceptual framework for "technology specific" legislation and the recent electronic commerce law passed in Rhode Island as a model of technology-neutral legislation. It compares those
models to the existing law of signatures and authentication procedures. Finally, this Article reviews the policy issues raised by "technology specific" legislation, the rules for allocating fraud losses in commercial transactions, and the problem of market failure due to imperfect calculation of risk by consumers in complex transactions.

II. IMPACT OF THE INTERNET ON COMMERCIAL TRANSACTIONS

A. Open Networks and Distributed Computing

Electronic commerce is as old as the telegraph, and businesses have relied on computers for decades. The emergence of the Internet as a global information infrastructure, however, has pushed the issues raised by the use of electronic communications and networked computers to the forefront of developments in commercial law. Businesses in all sectors of the U.S. economy are struggling to understand what impact these new technologies will have on their current operations, to find ways to cope with the rapid pace of change and development in information technologies, and to discover what new opportunities all these changes are producing.

The "information revolution" now unfolding is the result of the convergence of many social and technological forces that has brought major changes in business in its wake. Vice President Albert Gore recently observed that the United States is on the verge of a revolution that is just as profound as the change in the economy that came with the industrial revolution. Soon electronic networks will allow people to transcend the barriers of time and distance and take advantage of global markets and business opportunities not even imaginable today, opening up a new world of economic possibility and progress.

The new opportunities developing from the merging of computing and telecommunications technology has resulted in legal issues that are only beginning to emerge.

While the widespread use of computers in business began forty years ago, the sharp drop in the price of computing power in recent years has accelerated the process of substituting information processing by people with automated information processing. Current desktop computers can provide each employee with more computing

power than was available to entire enterprises in the early days of mainframe computing. The expansion and deregulation of telecommunications has promoted the more rapid exchange of information over networks of computers. Developments in digital technology now permit the conversion of a wide array of traditional media into digital media that can be transmitted over computer networks. The advent of relational database programs and "enterprise management software" has permitted the integration of disparate operating divisions of a business into a single information system.

Information systems based on earlier mainframe computing technology were distinct operations that were spatially segregated from other business operations by the demands of the computer systems themselves. Mainframe computers required temperature controlled, dust-free environments; they were maintained by specially designated and trained staff. Programmers were required to bridge the gap between the complexity and inflexibility of computing processes and the diversity of the end users' needs. Data entry and data processing were distinct tasks with recognizable boundaries defined by staffing and equipment configurations.⁵

The development of personal computers began to change that business/computer interface. Individuals with no knowledge of computer programming could use computers to accomplish a wide variety of tasks. Certain phenomenally popular software programs such as the Visicalc and Lotus 1-2-3 spread sheet programs, or the WordPerfect word processing program, revolutionized the way many routine business tasks were accomplished and made personal computers a necessity in many business environments. In response to these changes, the number of employees charged with maintaining information systems equipment and accessing or inputting data increased.⁶ Information technology personnel no longer needed to be isolated by the demands of the computer system. Instead, they could work in a variety of environments throughout the organization. Professional programmers or information systems managers retained responsibility for maintaining mainframe systems, but those systems were increasingly connected to networks of personal computers. Access to computer resources with mainframe computers was

---


provided through the use of dumb terminals. With the advent of personal computers, the "client/server" model of organizing computer resources came into vogue, allowing multiple local computer "clients" to share files or allocate functions through a "host" or "server" computer.

The use of networked computers in a business environment is not simply a consequence of the widespread use of personal computers. Financial industries were early pioneers in the use of networked computers for funds transfer systems.\(^7\) Also, electronic contracting conducted over electronic data interchange systems generally relied on "value-added networks" that provided secure connections between trading partners.\(^8\) The technical standards that permitted the interoperability of these networks were public standards, such as those developed by the American National Standards Institute (ANSI) or the International Standards Organization (ISO), standards set by trade associations or industry consortia, or private, proprietary standards.

The change from segregated mainframe systems to distributed networks of personal computers resulted in both costs and benefits. The cost associated with distributing access to information systems is not limited to the expense of purchasing and maintaining the hardware and software involved, although that may be very substantial. In order for employees to make use of equipment, obviously they must be adequately trained in its use. Furthermore, in order to safeguard financial and physical assets, computers must be integrated into the existing administrative and control systems. The benefits include the increased flexibility in distributing information within organizations and the ability to collect and process information about products and markets more rapidly. In addition, the rapidly falling price of information processing power has permitted many businesses to collect and manage information as an asset of the organization that was previously undervalued and underexploited. One of the great benefits of linking enterprise information systems with an open network such as the Internet has been the ability to provide marketing and customer service online without the expense of engineering around proprietary or incompatible computer system standards.\(^9\)

\(^7\) See DONALD I. BAKER & ROLAND E. BRANDEL, THE LAW OF ELECTRONIC FUND TRANSFER SYSTEMS § 1.03 (1996).

\(^8\) See BENJAMIN WRIGHT, THE LAW OF ELECTRONIC COMMERCE § 1.1.4 (2d ed. 1996).

\(^9\) See Steve Lohr, Business to Business on the Internet, N.Y. TIMES, April 28, 1997, at Cl.
The Internet is an international network of computers based on open, public technical standards. The Internet began in 1969 as an outgrowth of a military program called "ARPANET." This program "was designed to enable computers operated by the military, defense contractors, and universities conducting defense-related research to communicate with one another by redundant channels[,] even if some portions of the network were damaged in a war." When traffic on ARPANET reached levels that were too high for the network to handle, the National Science Foundation (NSF) stepped in to create a compatible network that would service that portion of the traffic used by different research institutions around the country to facilitate nondefense research. This network became known as NSFNET. Although there is no longer a central organization governing the Internet, there are organizations that formulate the technical standards that permit the Internet to operate and to continue to develop.

The Internet has grown considerably since its birth:

The number of 'host' computers—those that store information and relay communications—increased from about 300 in 1981 to approximately 9,400,000 by ... 1996. Roughly 60% of these hosts are located in the United States. About 40 million people used the Internet [in 1996], a number that is expected to mushroom to 200 million by 1999.

Individuals can obtain access to the Internet from many different sources. Most colleges and universities provide access for their students and faculty; many corporations provide their employees with access through an office network; many communities and local libraries provide free access, and an increasing number of storefront "computer coffee shops" provide access for a small hourly fee. Several major national "online services" such as America Online, CompuServe, the Microsoft Network, and Prodigy offer access to their own extensive proprietary networks as well as a link to the much larger resources of the Internet. In 1996, these commercial online services had almost twelve million individual subscribers [in 1996].

The architecture of the Internet reflects its Cold War origins. The Department of Defense wanted a network that could withstand partial

---
12. Id.
14. See id.
outages (whether from bomb attacks or a backhoe cutting network cables) and still function. The technical solution to this problem was a decentralized network of computers that could communicate with every other computer on the network as a peer. This required a minimum of information to be transmitted and received effectively, assigning the responsibility for completing the communication to the communicating computers, rather than a centralized control system. This system is known as a “packet switching” paradigm for communication. The messages are broken into packets and each packet is routed to the destination without any previously established communication path before the message packets are reassembled and checked for integrity by the receiving computer.

From a technical perspective, the Internet is a network of networks based on TCP/IP protocols, a community of people who use and develop those protocols, and a collection of resources that can be reached from those networks. TCP/IP refers to the networking protocols that establish the Internet: the Transmission Control Protocol and Internet Protocol. While the Internet is a computer network based on these protocols, it also has gateways to other networks and services that are based on other protocols. Each computer connected to the Internet has software that manages the connection to the network. This software can translate data to and from a format that can be transmitted over the Internet and a format that can be used locally.

Under the sponsorship of the National Science Foundation, the Internet was used as a federally funded wide area network for the academic and research communities. As a result of government support, the NSF was able to implement an “acceptable use” policy that prohibited the use of the network backbone services for other than research and education purposes. Commercial development of TCP/IP networking standards began in the early 1990s with private initiatives such as the Computer Internet Exchange Association and CO+RE (commercial and research). Because of interest shown by

---

17. See id.
18. See id.
19. See id.
20. See id.
21. See Moore, supra note 13, at 10-22.
22. See Leiner, supra note 10, at 102.
private enterprises and the uncertainty of future government funding, the NSF began preparing for the future privatization of the Internet which culminated in the 1995 turnover of the backbone to commercial providers, such as MCI, Sprint, and Advanced Network Systems. When there was no longer an acceptable use policy in effect for Internet communications, the commercial exploitation of the Internet began on a large scale. Local and regional networks that had previously developed using the TCP/IP standard were fully integrated into the Internet.

The Internet is composed of many different systems, some that merely support the exchange of e-mail messages between different computer systems and some that support the storage and retrieval of information in a wide variety of formats. The "World Wide Web" consists of information that is formatted with "hyper-text markup language," which permits information to be organized with "hypertext" links or jumps between two related concepts or files. The organization of files by optional jumplinks between related ideas, rather than an enforced hierarchy determined by the author, permits the person accessing the information to delve into matters in as much or as little depth as the reader desires. Files are transferred from the servers where they reside to client machines using the "hypertext transfer protocol." The World Wide Web (the "Web") became a mass media phenomenon with the development of "web browser" programs that permit personal computers to access a wide variety of files from web sites. Web browsers permitted users to view graphics, hear sound files, or watch digital video clips, as well as to read text.

The initial popularity of the web was driven by the development of its graphical user interface, which simplified access to the mountains of data already present on the Internet. The Web continues to develop to allow ever greater interactivity between the user accessing the Web with a browser on a personal computer and the information available on the web server hosting the web site files. For example, web sites may now be constructed that permit visitors to search databases or to have other computing functions performed on

24. See id.
25. The "Very High Performance Backbone Network Service," currently under development by the National Science Foundation to create an upgraded Internet with fiber optic lines, now has an "acceptable use policy" that limits its use to academic and research purposes. See Deborah Shapley, Now Playing in Limited Release: Internet, the Next Generation, N.Y. TIMES, Jan. 27, 1997, at D1.
the web server. These enhanced functions are widely used in Internet electronic commerce applications.

The National Research Council has noted that the Internet is now "open" in at least the following four senses.\(^{27}\) It is open to users because it does not force users into closed groups or deny access to any sectors of society but instead permits universal connectivity, like the telephone system.\(^{28}\) It is open to service providers because it provides an open and accessible environment for competing commercial and intellectual interests.\(^{29}\) For example, competitive access for information providers is permitted. It is open to network providers because any network provider can meet the necessary requirements to attach and become a part of the aggregate of interconnected networks.\(^{30}\) It is open to change because it continually permits the introduction of new applications and services. It is not limited to only one application, as in television. It also permits the introduction of new technologies as they became available.\(^{31}\)

B.Trustworthy Systems and Communication Security

The openness of the Internet is a major factor explaining its revolutionary impact. This same openness, however, exposes the computer systems connected to it to greater security threats than those experienced by closed networks or systems that are not networked. Although the graphical user interface provided by web browsers makes the Internet easy for users to access, the browser software and the corresponding server software are very complex. As a result, Internet participants, both on the client and server side, may face greater security risks than they realize.\(^{32}\)

For example, in July 1997, a test of one computer system linked to the Internet by a security expert inadvertently revealed thousands of unprotected passwords on other computer systems linked to the Internet around the world.\(^{33}\) In July 1997, over 2,000 consumers who

---

27. See National Research Council, Realizing the Information Future: The Internet and Beyond 44 (1994).

28. See id.

29. See id.

30. See id.

31. See id.


33. See id. This followed revelations of flaws in Microsoft's Internet Explorer security that would permit users to access Internet sites booby-trapped to destroy data on the users' computers and flaws in Microsoft's Windows NT operating system that permitted unauthorized access to system users' passwords. See Bill Richards, Microsoft's Windows NT Has a Flaw in Security, Computer Experts Claim, WALL ST. J., Apr. 1, 1997, at B1.
used the popular NBA.com web site (maintained by Starwave Corporation for ESPN Sports Zone) to order NBA merchandise received anonymous e-mail reporting back to them the information they had transmitted to a supposedly secure web site, including their credit card information. The interlopers claimed to be publicizing the lack of security at the popular site to make consumers aware of the risks of Internet commerce.\(^{34}\)

While more limited uses of the Internet, such as displaying graphics and text in the format of a printed document, might seem less at risk from security threats, the Department of Justice learned that this was not the case in 1996, when its web site was vandalized by hackers protesting the perceived censorship of the Internet by the Communications Decency Act.\(^{35}\)

Whether a computer system is secure is something that can never be demonstrated in any absolute sense. Computer security is a relative concept that can be established by identifying potential threats to the system and designing safeguards to protect the system from those threats.\(^{36}\) Computer systems that have been designed to provide the best security available in light of the system's intended functions are therefore referred to as "trustworthy" computer systems.\(^{37}\) A "trustworthy" computer system must provide confidentiality for information that is subject to access restrictions, maintain information integrity by preventing its corruption or destruction, and guarantee system availability so that users have access to information whenever it is needed.\(^{38}\) Computer security policies must address all these issues and be integrated with security policies that safeguard other assets in order to be effective.\(^{39}\)

Threats to the security of computer systems are not limited to computers connected to the Internet. Threats may come from a variety of sources: disgruntled employees, self-help remedies by technology

---

34. Starwave reported that the breach of security had been accomplished through the actions of an insider, not as a result of the penetration of their system from the outside. Although, this was probably little or no comfort to the individuals involved. See Mark Smith, Security Breakdown, PITTSBURGH POST-GAZETTE, July 13, 1997, at C3.


36. See NATIONAL RESEARCH COUNCIL, COMPUTERS AT RISK, supra note 6, at 13.

37. A "trustworthy system" is defined as "[c]omputer hardware, software, and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonably reliable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security principles." INFORMATION SECURITY COMMITTEE, supra note 2, at 69.

38. See RITA C. SUMMERS, THREATS AND SAFEGUARDS 3 (1997).

39. See id. at 103.
providers, attacks from outsiders, or even natural disasters such as disruption in electric power supplies or floods.\textsuperscript{40} Preparations for an attack can be made by social engineering (tricking the people who know how to access the system into voluntarily releasing the information), dumpster diving (collecting computer manuals or printouts from trash bins), or war dialing (computer-controlled dialing of all numbers in a range). Malicious codes can be planted in a system through the use of "trap doors," "Trojan horses," or masquerading and spoofing (assuming the identity of an authorized user or recognized system).\textsuperscript{41} The objectives of attacks include eavesdropping, destruction of valuable data, denial of service (by overloading the system with improper traffic), theft of service, or disarming system safeguards.\textsuperscript{42}

The magnitude of security problems experienced by closed network computer systems gives some indication of the problems that businesses will face in opening their information systems to greater connectivity through the Internet. According to the results of a 1996 survey of 1,300 information technology managers, 54\% of the survey respondents said that their company suffered a loss related to information security and disaster recovery in the past two years; when losses due to computer viruses are included, the proportion rises to 78\%.\textsuperscript{43} In 1997, the General Accounting Office highlighted information security in federal civil agencies as one of five areas in the government that were at "high risk" of fraud, waste, or abuse.\textsuperscript{44} The GAO found that malicious attacks on government computers put billions of dollars worth of assets at risk of loss and vast amounts of sensitive data at risk of unauthorized disclosure.\textsuperscript{45} Even systems designed for secure use by the military and financial institutions are not immune from attack. Hackers hit Pentagon systems an estimated 250,000 times in 1995; about 64 percent of the attacks were successful.\textsuperscript{46} In 1994, a Russian computer programmer removed $10 million from Citibank customer accounts by initiating unauthorized funds transfers from a laptop computer in St. Petersburg.\textsuperscript{47}

\textsuperscript{40} See id. at 71-91.  
\textsuperscript{41} See id. at 86-102.  
\textsuperscript{42} See id. at 83.  
\textsuperscript{43} See Bob Violino, The Security Facade, INFORMATION WEEK, Oct. 21, 1996.  
\textsuperscript{44} See Stephen Barr, Identifying Risky Programs, WASH. POST, Feb. 13, 1997, at 23.  
\textsuperscript{45} See id.  
\textsuperscript{46} See id.  
\textsuperscript{47} Later, all but $400,000 was recovered. See David Gow & Richard Norton-Taylor, Surfing Superhighwaymen Banks Have Good Reason to Fear Thieves Who Hack Into Their Secret Files, THE GUARDIAN (London), Dec. 7, 1996, at 1.
In an information economy, computer security plays role equivalent to accounting and audit standards in a traditional paper-based economy. Information system security principles will need to be integrated into the existing framework of risk management policies used in business. Unlike security systems that safeguard physical and financial assets based on public standards, such as Generally Accepted Accounting Principles, there are not yet any general principles for computer system security that businesses can turn to in developing their security policies. In 1991, the National Research Council advocated the promulgation of a comprehensive set of Generally Accepted System Security Principles. However, no organization has taken the lead in developing such standards in the intervening years. It is unclear which federal agency or private standard-setting organization has both the resources to undertake such a project and the credibility necessary to win support for its proposals. In the private sector it is unclear whether there is any trade association or industry consortium that would have enough credibility with both system designers and end users to propose such standards. In 1996, the Organization for Economic Cooperation and Development issued its Guidelines for the Security of Information Systems, but these guidelines are very general, aspirational statements that provide little concrete guidance to computer system administrators. Furthermore, because the technology of information systems is in a rapid state of development and change, it may not yet be possible to develop a set of public standards similar to those used in accounting and finance.

Although there is no authoritative statement of generally accepted system security principles, many principles are in fact widely recognized as important in the design of secure systems. One principle used in the design of trustworthy security systems is that the security of an entire computer system is only as great as the security of the weakest link in the network of resources and users. Another principle is that it does not make sense to spend more to protect something than it would cost to replace it if it were lost. Thus, the uses of computer systems and the value of the resources they store

48. See National Research Council, Computers at Risk, supra note 6, at 27.
50. See Summers, supra note 38, at 40-45.
51. See id. at 152 (discussing the principle of "complete mediation," in which every access to every object must be controlled).
52. See Holbrook & Reynolds, supra note 5, at 10.
must be analyzed in light of the overall operations and objectives of the organization using the system.

The design of a trustworthy computer system should provide for the following: authentication, access control, integrity, audit, and availability.\(^{53}\) Authentication permits verification of a user's identity and is at the heart of the debate over digital signature legislation. A secure system should provide access control to insure that only legitimate users can access resources within the system. The "least privilege" principle provides that no user should be allowed greater access to system resources than is necessary to accomplish his or her assigned functions.\(^{54}\) Within networks, access control enforces policies about which computers can be accessed and what data can be transferred over the network. Through access control, information integrity is guaranteed at the time the data enters the system, as well as while it resides on the system or is in transit within the system.\(^{55}\) It is also important that information systems are amenable to audit in order to detect misuse that circumvents access controls.\(^{56}\) Finally, availability is paramount because of the cost associated with possible destruction of resources or disruption of services.

These principles have been more fully articulated in standards for individual application designs, as opposed to industry-wide standards. The U.S. Department of Defense developed computer security standards called the Trusted Computer System Evaluation Criteria (TCSEC or the "Orange Book"), which defined different classes of security corresponding to different levels of need.\(^{57}\) The TCSEC guidelines were developed with military objectives in mind, which are unlikely to be identical to the objectives of a business conducting electronic commerce. One reason is that the cost of implementing systems conforming to military standards might be prohibitive in other contexts.

One example of an industry-wide security standard was developed by the National Association of Clearing Houses (NACHA). NACHA has developed data security standards for its members, the regional automated clearing houses (ACHs).\(^{58}\) The ACH network

---

53. See Summers, supra note 38, at 11.
54. See id. at 9.
55. See id. at 11.
56. See id. at 12.
creates a nationwide electronic payment system for businesses and consumers that provide services like direct deposits and preauthorized payments.\textsuperscript{59} The data security standards that govern electronic funds transfers over the ACH system have been developed by the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12.\textsuperscript{60} The ASC X12 sets standards for electronic data interchange, like electronic funds transfers. NACHA participates in ANSI ASC X12 and recommends that its members adopt ANSI standards for data security.\textsuperscript{61}

With regard to Internet standards, the "Guidelines for the Secure Operation of the Internet" (Guidelines) were published in 1991 as one of the "Request for Comments" (RFC) document series that includes descriptions of Internet protocols and other information relevant to the Internet community.\textsuperscript{62} The first guideline provides that users are individually responsible for understanding and respecting the security policies of the systems they are using.\textsuperscript{63} Furthermore, users are

\textsuperscript{59} See BAKER & BRANDEL, supra note 7, § 3.02.

\textsuperscript{60} The American National Standards Institute (ANSI) was established in 1918 and manages and coordinates private-sector standard-setting activities to support U.S. national economic interests. Groups submit proposed standards to ANSI for approval. See CARL F. CARGILL, OPEN SYSTEMS STANDARDIZATION: A BUSINESS APPROACH 244-45 (1997). ANSI approves standards if it determines that the standard-setting process was open, that it included the participation of everyone with a material interest in it, and that the proposed standard represents the consensus among the participants. See id. Private groups seek ANSI approval because ANSI approved standards receive more support in the marketplace than those that are not submitted to ANSI for approval. See id.


\textsuperscript{62} All Internet standards are published as RFCs; however, not all RFCs contain Internet standards. FYI RFCs, for example, contain general background information on the operation of the Internet. See Holbrook & Reynolds, supra note 5. The handbook is a request for comments, not an Internet standard. The Internet standard setting remains an open, consensus-building process that reflects its origins in academia. The Internet Society (ISOC) is an independent, international professional society that is concerned with the growth and evolution of the Internet. See MICHAEL FROOMKIN, THE GOVERNANCE OF THE INTERNET (forthcoming 1998) (on file with author). The board of ISOC approves appointments to the Internet Architecture Board (IAB), which has a veto power over proposed Internet Standards. Standards may be proposed by anyone. Once a standard is proposed, the Internet Engineering Steering Group (IESG) of the Internet Engineering Task Force (IETF) establishes a working group to review the proposal, if the IETF and the IESG conclude that such an action is merited by the proposal. See id. The IETF has no general membership and consists primarily of volunteers. See id. The working group reviews the standard until a rough consensus is achieved. Then, the standard is passed to the IESG for public review and publication as a draft standard. See id. When a draft standard has been tested and found sound, it can become an Internet Standard and is published as an RFC. See id.

individually accountable for their own behavior. The second guideline provides that users have a responsibility to employ available security mechanisms and procedures for protecting their own data and for assisting in the protection of the systems they use. When these guidelines were written, the idea was that individuals would be capable of entering into binding contracts online, and the risk of being held liable for the acts of another impersonating the user online had not yet arisen as a security issue.

The Guidelines provide that computer and network service providers are responsible for maintaining the security of the systems they operate and are responsible for notifying users of their security policies and any changes to these policies. Vendors and system developers are responsible for providing systems that are sound and that embody adequate security controls. Users, service providers, and hardware and software vendors are responsible for cooperating to provide security, while those developing Internet protocols are charged with including security considerations as part of the design and development process.

In addition to the general provisions of the Guidelines, there are more specific Internet security standards set out in RFCs to provide guidance for developers of Internet applications and site administrators. For example, RFC 2078 Generic Security Service Application Program Interface sets out programming standards for a generic communications protocol governing authentication, integrity, or confidentiality security services. RFC 1244 provides a Site Security Handbook.

One dimension of a trustworthy or secure system is network or communication security. Electronic contracting over the Internet requires that parties wishing to enter into binding contracts have a means of ascertaining whether a message is actually coming from the party apparently sending it and whether the message has been altered in transit. This legal concern can be addressed by computer security

64. See id.
65. See id. § 2.
66. See id. § 3.
67. See id. § 4.
68. See id. § 5.
70. See, e.g., Holbrook & Reynolds, supra note 5 (Site Security Handbook).
policies governing authentication procedures and guaranteeing message integrity. Authentication can be based on something that the user knows (such as a PIN or password), something that the user has (such as an ATM card or other token device), or something that the user is or does (such as a fingerprint or manual signature). Authentication procedures based on knowledge are very common and are inexpensive to implement, but they are subject to well-known weaknesses. Passwords chosen by users can often be guessed simply by checking encrypted password files against encrypted dictionary entries. Furthermore, they are often left where interlopers can find them.

Token devices, such as memory cards (including ATM cards) or smart cards (which include an embedded processor chip), cannot be “guessed” but are more expensive to implement than password authentication systems. Token devices also require some interface with the computer system, such as a card-reading device, which can make the authentication procedure expensive to implement. Token devices can also be used in combination with PINs or passwords, thus increasing the system security.

Biometric authentication is based on physical or behavioral characteristics and is often more expensive, more intrusive, and less precise than other authentication procedures. Biometric authentication procedures require that some characteristic of a user be sampled and entered into the system, which is used to build a reference profile. When the user invokes the authentication procedure, the characteristic is measured again and compared with the reference profile. The procedure must be set to tolerate variances between the current sample and the reference profile. Consequently, setting the tolerance lower will improve the accuracy of the authentication procedure, but at a cost of infuriating legitimate users who are incorrectly rejected.

72. See Summers, supra note 38, at 340.
73. See id. at 341.
74. In 1994, a freelance journalist was able to join British Telecom as a temporary employee and access confidential files containing telephone numbers for Buckingham Palace, the Prime Minister’s office at Downing Street, and top-secret national security agency M15 installations. He managed to accomplish this by copying a password his supervisor had taped to the side of a computer monitor. See Tim Kelsey, The BT Hacker Scandal Revealed: How Hacker Penetrated the Heart of British Intelligence, THE INDEPENDENT (London), Nov. 24, 1994, at 1.
75. See Summers, supra note 38, at 348.
76. See id. at 349.
77. See id.
78. See id.
C. Digital Signatures, Certificate Authorities, and Public Key Infrastructure

The term "digital signature" is a term of art used to denote an electronic signature that has been produced through public key cryptography. In order to understand how digital signatures can operate as authentication procedures, it is necessary first to examine the basic functions of public key cryptography and how digital signatures are created.

Cryptography is the process of taking some information (called the plaintext) and passing it through an encryption process to produce an encrypted copy of the information (called the ciphertext) that can be decrypted and restored to the original plaintext through the application of the cipher key.

Modern cryptography is based on encryption algorithms that apply mathematical keys to plain text to produce ciphertext. The strength of a cryptographic key is measured by how hard it would be for an outsider to guess the key from the ciphertext. The longer the mathematical key used, in general, the more secure the encryption system will be from attack by outsiders. The size of a cryptographic key is measured in bits, such as 56 bits or 128 bits. The more samples of ciphertext that are available, the more information the cryptanalyst has to work with in trying to break a key. Thus, an important principle of cryptographic key management is that keys should be retired at regular intervals and replaced with new keys.

79. The Digital Signature Guidelines define "digital signature" as a transformation of a message using an asymmetric cryptosystem and a hash function such that a person having the initial message and the signer's public key can accurately determine (1) whether the transformation was created using the private key that corresponds to the signer's public key, and (2) whether the initial message has been altered since the transformation was made.

INFORMATION SECURITY COMMITTEE, supra note 2, at 42-43. While members of the Information Security Committee (ISC) have attempted to establish this meaning as definitive, the terms "electronic signature," "digital signature," and "digitized signature" are often used interchangeably. See, e.g., 1997 Texas H.B. 984 (defining "digital signature" as an electronic identifier intended by the person using it to have the same force and effect as a manual signature).

80. Captain Midnight decoder rings provide a simple example of encryption. The ring would contain a substitution cipher, in which each letter of the alphabet is substituted for another letter or a number. If the substitution cipher is simply the alphabet in reverse order, the plain text Captain Midnight becomes the ciphertext "Xzkgzrm Nrwmrtsg."


82. See id.


84. See GARFINKEL & SPAFFORD, supra note 35, at 187-208.

85. See id.
There are two main types of cryptography: conventional (also known as secret key or symmetric) and public key (also known as asymmetric or dual key). With conventional cryptography, the same key is used to both encrypt and decrypt a message. The great weakness of conventional cryptography is that the shared key must be kept private. If the sender and recipient of the message are not in direct personal contact, finding a system to distribute the keys securely will present considerable logistical problems. These problems are compounded by the need to retire the keys at regular intervals.

The U.S. military provides an excellent example of the complex logistics necessary to use conventional cryptography successfully. During the Cold War, secret keys were distributed by the U.S. government using couriers that were handcuffed to locked briefcases containing the keys. The couriers had neither the keys to the handcuffs nor the keys to the briefcases. If the courier did not arrive and turn over the contents of the briefcase intact, then the keys it contained would not be put into use.

Such a system is hardly feasible in large-volume commercial contexts. If a single key is needed for each pair of individuals or organizations wishing to communicate securely, then within any large community an extraordinarily large number of keys must be generated and distributed to permit any one individual to communicate with any other individual at will. Development of a strong central administration system that would be necessary for private commercial applications is not likely to be feasible.

Public key or asymmetric cryptography substantially solves the problem of key distribution. Public key cryptography is based on a mathematical breakthrough that permits the use of two different but related keys to be used to encrypt and decrypt messages. One key

86. See id.
87. See GARFINKEL, supra note 83, at 40.
88. See id. at 42.
89. As a practical matter, this may be difficult to achieve even in the context of military security. In 1985, Ronald Pelton, a National Security Administration agent, was discovered to have been revealing U.S. secret cryptographic keys to the Soviets. See id. at 45. This problem could be solved if there were a central key distribution center trusted by all the members of the community; the caveat is that compromise of the key distribution center renders the system vulnerable to attack. See id. Such a system has been in use in the U.S. military and intelligence communities for years, but it requires a strong central administration in order to be effective. See id.
(known as the public key) can be freely distributed and used by anyone. The other key, known as the private key, must be kept secure. Although the two keys have a mathematical relationship to each other, it is extremely difficult to use one key to guess the other. A public key can be used to send a message to the holder of the private key. The sender is assured that no one other than the holder of the private key will be able to read the contents of the message. Furthermore, the private key can be used to encrypt a message that the public key can be used to decrypt. This use of the keys permits a holder of the public key to be certain that a message came from no source other than a holder of the private key corresponding to the public key used to decrypt the message.

One disadvantage of public key cryptography compared with symmetric key cryptography is that the process of encryption is more computationally intensive because of the complex mathematical algorithms necessary to produce the asymmetric keys. As a result, public key cryptography is not well suited for encrypting large messages. However, in cases where the contents of a message do not require a high degree of confidentiality but an authentication is needed, public key cryptography can be used to produce a "digital signature" that assures the recipient of the authenticity of the message and the integrity of the contents, without the guaranteed confidentiality of the text of the message.

While public key cryptography solves the problem of key distribution because the public key can be published widely and distributed freely without compromising the security of the private

92. See id.
93. See id.
94. In order to create a digital signature with public key cryptography, a message digest or message hash must first be produced that represents the text of the message to be signed. This is accomplished by running the entire contents of the message through a hash function that produces a unique value that represents the entire message. The value, know as a message digest or integrity check value, is unique to the message so that any change whatsoever in the message text will produce a different value. The hash function should work only one way, for a given message digest, so it is not possible to guess the text from which it was generated.

A digital signature is produced by running the text to be signed through a hash function and then using the private key of the signer to encrypt the message digest. The encrypted digest is sent with the message to a recipient, who is already in possession of the signer's public key. The recipient runs the message through the same hash function to produce a message digest independently and then decrypts the message digest from the sender and compares the two. If the two message digests are identical, the recipient of the message can feel confident both that the message originated from the owner of the private key and that it has not been altered in transit.
key, significant key management problems remain. The most obvious is that the private key must remain confidential to prevent its unauthorized use. Equally onerous is the problem of determining whether a public key is really associated with the person who claims to be its owner. Until a reliable, inexpensive key distribution system that facilitates identification of the private key holder is created, public key cryptography will probably not be very useful in electronic commerce applications.

The problem of reliable public key distribution could be solved by creating a "public key infrastructure." One model of a public key infrastructure is the "web of trust" idea, a popular public key encryption program. In building a web of trust, each person may either certify the validity of a key or rely on another trusted party to certify the validity of a key. As more people join the web of trust, the keys of people within the web will be certified by more and more other members of the web, building the trustworthiness of the association between any given public key and the real person who claims to be using it. This model works for loosely interacting communities, such as individuals seeking to protect the confidentiality of their e-mail communications. However, the system is not well suited to the needs of electronic commerce, because determining whether to accept an electronic signature encrypted with a PGP public key requires knowledge of at least one of the certifying parties.

95. For example, anyone with the appropriate software loaded on his or her personal computer could generate a public key, post it on the Internet, and announce that it is Bill Gates' public key. Before someone wishing to communicate with Bill Gates in confidence will be willing to use that public key to encrypt a message to be sent to his e-mail address, the sender would want some assurance that the public key labeled as Bill Gates' key was indeed his and not that of an impostor. One solution is to meet with Bill Gates in person and exchange public keys on floppy disks, but the expense of this type of security procedure destroys most of the advantages of public key (rather than symmetric key) cryptography.

96. PGP is a freeware program written by Phil Zimmerman that incorporates patented technology licensed from RSA Data Security, Inc. Zimmerman wrote the program because he believed that the privacy rights of citizens were at risk without access to public key cryptography. See GARFINKEL, supra note 83, at 235-36. In its early days, PGP was surrounded by controversy regarding possible patent infringements and violations of prohibitions on exports of cryptography, but these issues have now been resolved. See id. PGP can be downloaded without charge for noncommercial use by U.S. or Canadian citizens from the Massachusetts Institute of Technology web server at <http://web.mit.edu/network/pgp.html> (visited Jan. 20, 1998). In addition, Counsel Connect, Inc. is offering its members PGP encryption with e-mail services. See PGP 5: Secured Messages at a Click of a Mouse, 6 LAW OFFICE TECH. REV. 93 (Oct. 29, 1997).

97. See GARFINKEL, supra note 83, at 235-36.

Otherwise, there is no way to be sure that all of the certifying parties are not really all the same person trying to perpetrate a fraud.

A more common public key infrastructure involves the use of a certification authority. A certification authority is a trusted third party who is in the business of associating a public key with a particular individual. The certification authority associates an individual with a public key by issuing a certificate that at a minimum contains a copy of the public key in question and the identity of the person associated with it. It may also include information about how long the certificate will be valid or special characteristics identifying the context in which the public key will be used. The certification authority then signs the certificate with its own digital signature. In the ABA Digital Signature guidelines, the party requesting the issuance of the certificate is known as the “subscriber.” The person using the certificate to confirm the association between a public key and an individual is a “relying party.” Any relying party in possession of the certification authority’s public key and the subscriber’s certificate can now verify that a message has come from the subscriber of the certificate.

This merely begs the question of how relying parties know that they can trust the certification authority. Another certification authority could be set up to certify the first certification authority, and so on, but ultimately there will be a certification authority that is not certified by any other, known as the root certification authority. What kind of root certification authority will inspire the confidence necessary to make digital signatures a viable authentication procedure for electronic commerce applications remains to be seen. Utah, in response to this perceived problem, enacted digital signature legislation authorizing the state to act as the root certification authority and providing for the licensing of certification authorities by the state.

Building a public key infrastructure requires more than just a credible certification authority issuing certificates. To enhance the value of a certificate, a certification authority will need to provide a

---

100. See id. at 58.
101. See INFORMATION SECURITY COMMITTEE, supra note 2, at 63-64.
102. See id. at 60.
103. See Froomkin, Essential Role, supra note 99, at 56.
104. See UTAH CODE ANN. §§ 46-3-201 to 46-3-504 (1997) (Utah’s Digital Signature Law).
mechanism for subscribers to notify the certification authority that the security of the private key has been compromised and the certificate must be canceled. A subscriber should also be able to request the cancellation of a certificate if the subscriber has a policy of retiring key pairs on a regular basis in conformity with sound security practices. In addition, the certification authority will need a mechanism to revoke a certificate if it learns after issue that it was procured by fraud on the part of the subscriber. The certification authority will need to provide a means for prospective relying parties to check whether a certificate is still valid or has been revoked for these or any other reasons. The simplest method for providing this information to prospective relying parties is to create a "certificate revocation list." For a relying party to establish that its reliance was in fact reasonable, it will have to first check the certificate revocation list. If the certificate revocation list is maintained online, the software that verifies digital signatures with reference to certificates can be programmed to check the certificate revocation list at the same time as the comparison of the keys is made and to display an error message if the certificate shows up as revoked.

The certification authority will want to limit its possible exposure to relying parties. One step towards achieving this goal is limiting the operational period of the certificate to a finite period of time. The certification authority may further limit the reasonable reliance of the relying party by specifying limits to the application of the digital signature in transactions. The most obvious reliance limit might be set on the value of the transactions for which the relying party can reasonably rely on the certificate. The policies governing the acceptable use of certificates can be specified in the certificate, and the software used by the various parties could be programmed to accept or reject certificates based on their compliance with certain policies. 105

Certification authorities may establish different policies and procedures for associating individual persons with online identities. Certification practice statements that are disclosed to subscribers and potential relying parties provide certification authorities with a mechanism to explain the procedures that the certification authority will use in reviewing certification applications and issuing certificates. The certification authority may establish different classes of

105. The ITU X.509 Version 3 standard permits further qualifications to the use of the certificate to be limited by the application of certain policies through the use of the Certificate Policies extension field. See FORD & BAUM, supra note 98, at 283.
certificates with different prices and different degrees of scrutiny applied in reviewing the application.\footnote{106}

Even when digital signatures are used within a system that includes a fully operational public key infrastructure, it is unclear whether in practice such a system will meet the needs of parties to online commercial transactions. An authentication procedure that securely binds the operation of an encryption program located on a specific machine with an online identity would not be as useful to a prospective trading partner as an authentication procedure that binds a human being that can be held legally accountable for his or her actions to an online identity. The binding of a human being to the software program that manages the digital signature technology is a problem that has not yet been widely addressed, because most commercial applications of digital signature technology were still in development by early 1998.

PGP, a digital signature program that has been widely available in one form or another since the late 1980s, uses a "pass phrase" as an authentication procedure to grant access to the digital signature program. A pass phrase may be longer than a password, such as the standard eight character passwords used in UNIX operating systems, and therefore may be harder to guess; however, any PIN, password, or pass phrase remains susceptible to brute force attacks in which a computer is programmed to try all possible combinations until it has been guessed. If the password is stored in encrypted forms, the brute force attack will take longer but is still possible if the attacker has access to the encryption algorithm used to encrypt the password. If a password is written out and found by the interloper, or is disclosed to the interloper over the telephone in what the user thinks is a conversation with a system administrator, a brute force attack is not necessary.

The Counsel Connect online service for attorneys began making PGP 5.0 available to its subscribers without additional charge in 1997. This version of PGP used only an eight character password to safeguard the private key. This digital signature program has a user-friendly interface designed to make encryption easier for users to add to their e-mail messages sent from the Counsel Connect server, yet the interface of this program provides limited guidance on maintaining the

\footnote{106. \textit{See} INFORMATION SECURITY COMMITTEE, \textit{supra} note 2, at 37-38. In issuing Class 3 IDs, VeriSign ensures the applicant's identity and viability with inquiries to databases maintained by Dun & Bradstreet, InterNIC, and other commercial establishments. \textit{See} Verisign Information Page (visited Jan. 20, 1998) <http://www.verisign.com/about/id_services.html>.}
security of private keys to new users unfamiliar with the problems of computer security. The key generation module of the program contains virtually no information whatsoever on computer security issues; the help module of the program provides some help if the user knows enough to seek its guidance on how to protect private keys.\textsuperscript{107}

If, within a computer, the private key that generates the digital signature is stored in the same location as the digital signature application, then an interloper who has access to that location of the password also has the ability to execute unauthorized digital signatures. There are several methods by which an interloper might gain access to a digital signature application without the legitimate user’s knowledge.\textsuperscript{108} Perhaps the most obvious is when a service technician is given access to the computer. There also is the possibility

\textsuperscript{107} The version of the help program available for download on July 17, 1997, provides the following guidance under the heading “Generate a Private and Public Key Pair” and the subheading “Protecting Your Keys”:

Once you have generated a key pair, it is wise to create a spare set and put them in a safe place in case something happens to the originals. In fact, when you close the PGP keys window after creating a new key pair, you are prompted to save a backup copy.

Your private keys and your public keys are stored in separate keyring files, which you can copy just like any other files to another location on your hard drive or to a floppy disk. By default, the private keyring (secring.pgp) and the public keyring (pubring.pgp) are stored along with the other program files in the PGP file directory, but you can save your backups in any location you like.

When you specify that you want to save a backup copy of your keys, the “Select Backup Destination” dialog box appears asking you to specify the location of the private keyring file that is to be backed up.

Besides making backup copies of your keys, you should be especially careful about where you store your private key. Even though your private key is protected by a pass phrase that only you should know, it is possible that someone could discover your pass phrase and then use your private key to decipher your e-mail or forge your digital signature. For instance, somebody could look over your shoulder and watch the keystrokes you enter or intercept them on the network or even over the airwaves.

To prevent anyone who might happen to get hold of your pass phrase from being able to use your private key, you should only store it on your own computer. If your computer is attached to a network, you should also make sure that your files are not automatically included in a system-wide backup where others might gain access to your private key. Given the ease with which computers are accessible over today’s networks, if you are working with extremely sensitive information, you may want to keep your private key on a floppy disk which you can insert like an old fashioned key whenever you want to read or sign your private mail.

PGP Help (visited July 17, 1997) <http://www.nai.com/download/default.asp>. Another security precaution may include assigning a different name to private keyring files and then storing that password somewhere other than in the default PGP file directory where it will not be so easy to locate. The PGP KEYS Preferences dialog box can then be used to specify a name and location for private and public key ring files.

\textsuperscript{108} Telephone interview with Cern Kaner, Ph.D., J.D. (July 22, 1997).
of a "rogue applet" entering the user's computer through a network connection. Such a rogue applet might be programmed to copy certain files and upload them to a remote location without the local user's knowledge. In addition, software support companies are developing technology that either captures large amounts of information off the local user's computer and transmits it back to the software support company's system or that permits the software support company's system to take over the local user's machine entirely. Uploading information about the local machine's configuration will permit the support provider to diagnose and solve problems more easily, which is a perfectly legitimate business objective given the virtually infinite variety of different applications and peripherals that might be part of the local user's system. However, the programs that upload this information are not currently designed to inform the local user what information is being uploaded; or to prevent the transfer of information that the user might wish to protect. Similarly, applications that grant root access on the local computer to the remote service organization do not have any mechanism for the local user to review or stop the actions of the remote service organization. Many of these security risks can be controlled by storing the private key off the system; however, it is unclear whether this prudential standard will be adopted by the developers of digital signature applications.

Given the weaknesses inherent in any form of authentication procedure, attention has been focused on developing systems that use a combination of authentication procedures together to reduce the probability of unauthorized use. For example, a biometric authentication procedure such as a fingerprint scan might be required to access the application that generates the user's digital signature. Likewise, a smartcard bearing a secret key can be used to encrypt a password that is transmitted to a computer system through a card

109. This would be a miniature program written in either Microsoft's ActiveX technology or the Java programming language.
110. This risk was demonstrated by a programmer in 1996 who wrote an ActiveX control that would simply shut down the local machine. See GARFINKEL, supra note 83, at 77. This was designed to demonstrate without inflicting any harm what an ActiveX control is capable of doing on a client computer. The programmer became embroiled in a dispute with Microsoft and VeriSign over whether the ActiveX control was malicious, which resulted in his "Authenticode" certificate being revoked. See id.; see also Richard Hornbeck, EDI FORUM 1997
112. See id.
The smart card then forms a sort of "firewall" to protect against interlopers whose only point of access is within the computer system trying to invoke the digital signature application. While such combination authentication procedures may be more expensive to implement than digital signature authentication procedures based on software applications alone, the higher initial investment may be more than offset by an overall reduction in fraud losses.\footnote{114. These tradeoffs involved in establishing policies to minimize losses are discussed more fully in Part IV, infra.}

\section*{D. How Will Internet Authentication Procedures Be Used?}

Authentication procedures will be used in a wide variety of contexts in Internet electronic commerce. For web sites that simply disseminate information, no authentication procedures may be required at all unless restrictions are to be placed on who may access the information. In order to control access, password protections may be placed on certain sites. However, in order to engage in Internet commerce where parties enter binding contracts over the Internet, passwords are an inadequate means of verifying identity.

The Internet can be used as a medium of communication between parties who wish to enter into contracts. The parties themselves will determine whether they are willing to rely only on information that is provided through contacts over the Internet, or whether the Internet will be used merely to supplement the current means of communication in business transactions, such as telephone, mail, and fax. Security arrangements will be least problematic where the parties have a preexisting business relationship and are merely adding the Internet as a new channel for communications. For these parties, authentication procedures can be devised that build on existing policies and procedures in much the same way that electronic data interchange (EDI) trading partner agreements provide for authentication procedures.\footnote{115. See ABA Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange—A Report, 45 BUS. LAW. 1645, 1650 (1990) [hereinafter ABA, Commercial Use].} For parties wishing to solicit new business over the Internet and enter into binding contracts with parties known to them only through online contacts, security concerns are dramatically greater and much harder to resolve.

\footnote{113. See SUMMERS, supra note 38, at 349.}
EDI has been in use since the 1970s for business-to-business communication. Businesses that exchange information using paper forms can design communication systems that permit the computers in each business to exchange electronic messages in a format that can be interpreted within each system. Data is communicated using standardized formats that permit the messages to be sent in highly condensed forms. The use of EDI in purchasing transactions experienced exponential growth beginning in the 1980s as businesses implemented "just-in-time" inventory systems. EDI messages may be communicated directly between the trading partners, or over "value-added networks" (VANs) organized by service providers. Despite the widespread use of EDI in some sectors of the economy, such as manufacturing, many businesses have not adopted EDI because of the effort and expense required to integrate EDI communications systems with existing computer operations. One of the appeals of Internet electronic commerce is that the total cost of adopting electronic contracting practices may be lower than the cost of adopting EDI systems. Many businesses are in the process of integrating Internet access into their existing computer systems, for example to build corporate "Intranets" that distribute information within the organization and exclude public access or to build web sites to advertise their services. The purchase price of Internet electronic commerce systems that integrate hardware and software is falling rapidly, while the cost of integrating those services into existing information systems and maintaining them is falling as familiarity with the Internet becomes more widespread within business information systems departments.

It is possible to lay out a spectrum of different types of contractual transactions that might be entered into over the Internet, arranged from those raising the least difficult security problems to

116. See ABA Electronic Messaging Services Task Force, Model Electronic Data Interchange Trading Partner Agreement and Commentary, 45 BUS. LAW. 1717, 1718 (1990) [hereinafter ABA, Model Agreement].
118. See id.
120. See Steve Lohr, Business to Business on the Internet; Companies Go on Line to Trim Costs and Find Ways to Make Money, Too, N.Y. TIMES, Apr. 28, 1997, at D1.
those raising the most difficult. The least difficult security problems are raised in what are loosely labeled “closed” systems, the most difficult in “open” systems. The contrast between open and closed systems is not very helpful, however, as the factors differentiating the approaches to Internet electronic commerce involve too many variables to permit simple categorization into two groups. While there is not yet a generally recognized taxonomy of Internet transaction types, the following list of categories may be helpful for this discussion. This list is merely intended to be suggestive of possible business models for contracting over the Internet for goods and services; it is not exhaustive, nor does it propose categories for sorting out the different types of financial transactions over the Internet.

1. Closed—Bilateral

In a closed—bilateral transaction, one party (such as a governmental unit or a business with substantial bargaining power vis-à-vis its customers) agrees to accept electronic messages with legal significance from parties who have agreed to follow the security procedures announced by the governmental unit. Between private parties, a closed—bilateral system might be established through the negotiation of contracts (similar to EDI trading partner agreements) that define the rights and obligations of the parties with regard to standards governing all aspects of electronic communications between them. The benefit to the party that sets the standard is reduced transaction costs; however, if many such units set up radically different security schemes, then the cost to the customers of accommodating many, inconsistent security schemes may be very substantial.

The Cisco Systems, Inc. extranet site is an example of a closed—bilateral system. After parties execute an “electronic commerce enrollment agreement” in which the parties agree which individuals are authorized by the purchaser to submit purchase orders to Cisco, the party may engage in commerce with Cisco. Other terms and conditions, including the security procedures to be used, are disclosed in the contract.

123. See ABA, Model Agreement, supra note 116, at 1718.
124. The Cisco web site is located at <http://www.cisco.com> (visited Jan. 20, 1998). The site provides a wealth of general information about electronic commerce using Cisco products and services; however, the “Electronic Commerce Enrollment Agreement” and other pages related to on-line ordering of Cisco products are accessible only to parties who have a preexisting relationship with Cisco. See id.
2. Closed-Bound Community

In a closed-bound community, a preexisting group such as a trade association or industry group decides to move intragroup communications online and designates a central organization to act as administrator of the system. The group agrees upon a security procedure that meets the needs of the members and that, once in place, can be used for communications between any member of the group without further preparation or clearance. The benefit to the members that set the standard is that it may reduce transactions costs for intragroup communications. However, if members belong to several groups simultaneously because of varied business operations, then the member organizations may incur substantial costs in accommodating many inconsistent schemes established by each group.

3. Closed-Subscription

In this type of system, a standard is established by a body designated for the purpose, such as an industry consortium, that will define a group that will implement the security procedures in the standard before commencing communications online. The Secure Electronic Transaction (SET) protocol developed by Visa and MasterCard, currently being marketed around the world as a secure Internet application for any type of bank or credit card, is an example of a closed-subscription model. In 1997, the Secure Electronic Transaction standard was still under development and was only in use in pilot projects, but it is likely that the final Secure Electronic Transaction standard will have some or all of the following characteristics. The consumer will be able to use digital signature technology to verify the merchant's identity and the merchant will be able to use digital signature technology to verify the cardholder's identity. Cardholders will be able to send purchase information encrypted in a form readable only by the merchant operating the web site, and to send credit card information encrypted in a form only readable by the merchant's financial institution. The digital signature process executed by the consumer will be used only with credit card transactions, so any risk of unauthorized use of the digital signature


will be subject to the limitations on cardholder liability for unauthorized use of credit cards.\textsuperscript{127} Any party wishing to join the system may do so as a card issuer or bank for a merchant, as a merchant, or as a card holder, provided that the party independently meets the standards to join the credit card system.\textsuperscript{128} Merchants will also need to insure that their Internet sites conform to the published Secure Electronic Transaction standard.\textsuperscript{129} Currently, independent software developers are creating electronic commerce applications that incorporate the Secure Electronic Transaction standard.\textsuperscript{130}

4. Open—Server Security

When parties with no prior contact off of the Internet decide to enter into contracts for the purchase of goods or services, they may choose to do so based merely on the exchange of unencrypted e-mail messages. It seems unlikely that many businesses will be willing to assume the risks entailed in this type of communication, although some may be willing to do so after using an "out of band" or "back channel" communication with the prospective purchaser or vendor, such as a telephone call or fax. Internet electronic commerce conducted today using the Secure Socket Layer (SSL) protocol developed by Netscape is an example of the open-server security model.\textsuperscript{131} This is because it uses digital signature technology to provide server side security but does not provide a mechanism to identify the potential customer.

The Dell Computer web site is an example of a successful application of the open-server security Internet electronic commerce model.\textsuperscript{132} Dell customers use SSL technology to secure the transmission of credit card information to Dell in the following manner. Most recent versions of Netscape or Microsoft's web browser

\begin{footnotesize}
\begin{enumerate}
\item See Larry Loeb, The Stage Is SET, INTERNET WORLD, Aug. 1996, at 55.
\item See id.
\item See id.
\item See id.
\item The Secure Socket Layer was the subject of a March 1996 Netscape Internet Developer Conference. The graphical presentations of that conference are available through the Netscape web site and provide information on Netscape's conception of the SSL protocol. See Netscape Internet Developer Conference Proceedings, Commerce and Security (visited Feb. 26, 1998) <http://search.netscape.com/misc/developer/conference/proceedings/cs1/index.html>.
\item Dell's web site is located at <http://www.dell.com> (visited Jan. 20, 1998). The secure pages of the web site are discernible in Netscape or Microsoft when the broken key or open lock in the lower left- or right-hand corner of the computer monitor image changes to an unbroken key or closed lock. These pages can be accessed by following the instructions for purchasing a computer.
\end{enumerate}
\end{footnotesize}
programs come with certain digital certificates installed for certification authorities such as VeriSign, Inc.133 These preinstalled certification authority digital certificates can be used to verify the public key associated with the merchant’s web server. When a potential customer accesses a secure web site, the local client downloads a copy of the server’s digital certificate. Once the server’s public key certificate has been checked against the certificate of the certification authority that issued the certificate, the server’s public key is used to encrypt a symmetric key that is sent to the server and used to encrypt all subsequent communications between the visitor’s site and the server during that session. A symmetric key is used for encryption rather than the server’s public key, because symmetric encryption is less computationally intensive and therefore quicker for the average personal computer to perform without degrading the web server’s response time to such a degree that a potential customer would be unwilling to complete the transaction.134 The secure socket layer protocol does not address what type of data is transmitted between the client and server, although it is widely used to transmit credit card information.135 Adding the requirement that purchases be made using credit cards provides merchants using secure socket layer security with a way to qualify prospective customers independent of Internet security.

Commercial Internet sites are not the only ones taking advantage of this technology. For example, the Commonwealth of Massachusetts Registry of Motor Vehicles permits motor vehicle registration renewals and traffic citations to be paid at its Internet site by credit card using Secure Socket Layer.136 Also, the University of Texas at Austin accepts applications for admissions online and allows

133. VeriSign is a spinoff of RSA Data Encryption, Inc., the holder of the RSA patent for public key encryption (the patent was granted to Ron Rivest, Adi Shamir, and Leonard Adelman, former MIT professors). See GARFINKEL, supra note 83, at 135. VeriSign was the largest commercial certification authority doing business in the United States, with various information on their services available on their central web site. See VeriSign Web Site (visited Jan. 20, 1998) <http://www.verisign.com>. Certificates can be viewed in a web browser under a menu entry for “security preferences” under the “options” menu tab (Netscape Navigator 3.0) or “security information” under the “communicator” menu tab (Netscape Communicator 4.0).

134. See WRIGHT & WINN, supra note 121, § 3.6.5.

135. See id.

graduates to register with alumni relations online through secure web sites.\textsuperscript{137}

5. Open—Client Security

This category includes applications that require the client, or local user, as well as the web server, to have its own digital signature, and might also be known as the global stranger-to-stranger model of Internet electronic commerce. In discussions of public key infrastructure that refer to something like the open-client security model, it is generally assumed that the role of the certification authority will be limited to binding the real world identity of a signer with an online identity.\textsuperscript{138} The degree of scrutiny applied to perform this binding function would be spelled out in the certification authority's certification practice statement. This type of transaction will occur when one party will be able to locate a prospective trading partner from only information gleaned online and proceed to enter into a binding contract online with no "out of band" or "back channel" communication, all within a system secured by a global public key infrastructure. This does not yet exist in practice, and even among those who believe that this model will ultimately dominate online commercial activity there is no consensus regarding how long it will take to achieve in practice.\textsuperscript{139}

Many participants and observers of Internet electronic commerce developments believe that, if technical and legal standards governing certification authorities and the rights and responsibilities of subscribers and relying parties can be agreed upon by the relevant businesses and government agencies, global stranger-to-stranger Internet electronic commerce will become a reality in the foreseeable future.\textsuperscript{140} Proponents of this open-client security model believe that, through the use of technical and legal standards, a system can be built that permits parties to verify signatures through certification authorities with whom they have not dealt on any prior occasion.\textsuperscript{141} Certification authorities and relying parties will be able to establish quickly and

\begin{verbatim}
137. See Secure Membership Sign-Up (last modified May 23, 1997) <http://www.utexas.edu/alumni/Forms/secure_Annual.html>.
138. One example of an Internet discussion group concerned with public key infrastructure issues is the "digsig" listserv owned by Professor Amy Boss of Temple University School of Law, begun in July 1997. The archives are available at <http://listserv.temple.edu/archives/digsig.html>.
139. See Public Key Infrastructure Symposium, JURIMETRICS (forthcoming 1998).
140. See generally FORD & BAUM, supra note 98 (discussing the perceived future of Internet commerce).
141. See id. at 309-10.
\end{verbatim}
easily the reliability of certificates issued by remote certification authorities. This model presents the largest technical and theoretical challenges to designing a secure electronic commerce system, because it requires uniformly agreed-to policies and procedures that ensure the interoperability of systems designed by different vendors and the continued expansion of the system to include an indefinitely large number of participants.

Other observers are more dubious. One information technology specialist within the financial services industry compared the development of public key cryptography and the idea of a public key infrastructure to the development of the internal combustion engine and macadam as a road building material. While the tools may now be at hand to begin building a global infrastructure for stranger-to-stranger commerce, the gap between recognition of the significance of public key cryptography and actually completing the construction of that global marketplace is immeasurable. All parties involved agree that the information technology infrastructure necessary to support global Internet commerce between strangers will be considerable, and at present there is no way to know whether the optimistic or the pessimistic assessments of the time and investment required to achieve it are more accurate.

In early discussions of the design of open Internet electronic commerce models, there was discussion of the idea of a "universal certification authority" that would bind the identity of a person to an online identity for all purposes. The appeal of this idea is that individuals would not be burdened with remembering dozens of different passwords or carrying around dozens of different tokens to establish their online identity. This idea was soon recognized as being too simplistic for several reasons. First, persons in the United States do not possess identity cards for purposes unrelated to online transactions, so the idea of establishing the online equivalent of national identity cards would be expected to meet with stiff opposition from civil liberties activists. It is also unclear whether individuals would actually feel overly burdened by using different authentication procedures for different types of online transactions, given that most

142. See id. at 290.
143. E-mail from Dwight Arthur, Managing Director: Systems, National Securities Clearing Corporation (July 1, 1997) (on file with author).
144. See id.
145. See FORD & BAU, supra note 98, at 309-10.
146. See WRIGHT, supra note 8, § 1.2.5.
147. See id.
people use a variety of different authentication procedures today. Second, the certification authority would have the responsibility of establishing the identity of a natural person for all legal and business purposes. Companies likely to provide certification authority services are technology companies, not private investigators or even credit reporting services. Given the lack of a system of national identity cards, it is unclear what would constitute due diligence by a certification authority in establishing the identity of a person. As a result of these uncertainties, businesses interested in entering the certification authority market withdrew from the idea of a universal certificate.

6. Closed—Robust Local Administration

One way to reduce the administrative complexity of the open-client security model would be to delegate certain functions from the central certification authority to local registration authorities. The central certification authority functions might be limited to maintaining the certificate revocation list and issuing certificates in response to requests from local registration authorities. The functions of the local registration authority may be defined by the participants in the closed system—they may provide only the narrow range of services included in the standard model of the central certification authority, or they may provide a more "robust" service. The real-world connection between the local registration authorities and the local business environment in which potential subscribers operate may make it possible for the local registration authority to offer more robust screening services at a price that participants in the system are willing to pay. Important business services that a local registration authority may be able to provide beyond identification include credit checking and more rigorous background checks to support the association of a person with an online identity.

148. See id.
149. See id.
150. The U.S. Postal Service was an early contender for the role of universal CA, but has apparently lost interest in the project. In 1996, Cylink Corporation was part of a widely publicized project with the United States Postal Service to establish a USPS certificate authority. In 1998, there was no information on either the Cylink web site (<http://www.cylink.com>) or the USPS web site (<http://www.usps.gov>) reporting on the status of the project, which is apparently dead. In 1997, industry observers expressed skepticism regarding the likely success of the Post Office's electronic commerce initiative. See Christy Hugdins-Bonafield, Postmark Misses the Mark, NETWORK COMPUTING, Apr. 1, 1997, at 60.
The OASIS (Open Access Same-Time Information System) Internet site is an example of a closed—local administration model. In 1996, the Federal Energy Regulatory Commission mandated that electric power utilities participate in a nationwide trading system for electric power to be established on the Internet. In 1997, OASIS came online. Eight out of twelve of the regional power pools appointed Tradewave, a technology vendor, to act as certification authority with regional power pools or individual companies acting as local registration authorities.

III. WHAT IS THE ELECTRONIC EQUIVALENT OF A SIGNATURE FOR INTERNET COMMERCE?

Whenever one party claims rights under a signed agreement, it is always possible that the party seeking to avoid liability will deny the validity of the signature. This issue arises in many contexts, and the legal doctrines addressing this problem vary depending on the specific context within which the agreement arose. The elements required to establish a binding obligation and the allocation of losses due to forgery or other fraud vary depending on the business and social context in which the agreement arises. The law must address not only the problem of malfeasance by forgers or other impostors, but also the problem of parties wrongfully repudiating their own undertakings.

A. Common Law of Signatures

1. What Is a Signature?

A signature is any mark or symbol affixed to a writing to manifest the signer’s intent to adopt it as his or her own and to be bound by it. It need not be the full name of the signer placed at the end of the text—it may appear at any place on the document, and it may be any mark, the signer’s initials, or simply an

---

155. “Subscription” is the act of signing in writing at the bottom or end of a writing. See Lawson v. Dawson’s Estate, 53 S.W. 64, 65 (Tex. Civ. App. 1900).
identification number. It need not be handwritten—it may be typewritten, made with a rubber stamp, printed, lithographed or engraved, or made with a signature facsimile machine. There is no requirement that a signature be witnessed to be effective. Unless a contract is required by statute to be in writing, it need not be signed to be valid. If there is no signature, then the party seeking to establish that a contract exists will need to show that the parties by some other means manifested their intent to be bound by its terms. The party to be bound by the signature need not personally execute the signature. The person intending to be bound may delegate the act of signing to another person. Even if there is no formal agreement between the parties, principles of agency law may determine whether the person signing on behalf of another acted pursuant to a valid grant of authority, whether express or implied. Express authority “is [manifested fully and specifically] to the agent,” while implied authority is a natural consequence of the express authority granted by the principal to the agent and must be consistent with that express grant. For example, the express designation of an individual to act as a manager of an enterprise includes the implied authority to carry out all normal operative functions of the enterprise. If the authority to sign for another has been granted, the principal’s signature executed by the agent is binding.

164. See infra text accompanying notes 179-182 for a discussion of the use of facsimile signature machines for private contracts. Many states have adopted the Uniform Facsimile Signatures of Public Officials Act to resolve any issues associated with the official use of facsimile signatures in connection with the issuance of public securities or payment instruments. See UNIFORM FACSIMILE SIGNATURES OF PUBLIC OFFICIALS ACT § 2 (1997).
172. See id. at 42.
173. See id. at 43.
on the principal just as though the principal herself signed. 174 If the agent exceeds the scope of his authority, the signature may nevertheless be binding if the act is within the apparent or ostensible authority of the agent. 175 If a third party in good faith believes the agent to be acting within the scope of his or her authority because of the behavior of the principal, then the principal will be estopped from later disputing the agent's authority. 176 A signature made by an agent without any authority may nevertheless be effective as the signature of the principal if the principal later accepts the benefits that accrue as a result of the signature. 177 Ratification is the subsequent affirmance of an act originally done by the agent without authority. 178

2. When Can a Signature Machine Produce a Valid and Binding Signature?

A signature may be executed through the use of a facsimile signature device. 179 Even though an unauthorized signature produced with a signature machine may be identical in appearance to a genuine signature, it is without effect unless it can be shown that the signature was made by someone with apparent authority or that the purported signer has ratified it. 180 Given the difficulty of establishing who was operating the machine that produced a facsimile signature, it is common for parties receiving them to require an agreement from the owner of the machine that the owner will not deny the validity of any signatures made with the machine. 181 This is because, in the absence of such an agreement, the party relying on the validity of the signature may have to establish the circumstances under which the facsimile signature device was in fact used. 182

174. See id. at 57.
175. See id.
176. See id. at 58.
177. See id. at 65-66.
178. See id. at 72-73.
182. See infra text accompanying notes 237-274 for a discussion of commercially reasonable security procedures under UCC Article 4A and a discussion of the same problem as it arises in the electronic funds transfer context.
3. What Is the Significance of Notarizing a Signature?

Signatures made in the presence of a notary public may be attested to by the notary. In witnessing or attesting a signature, the notarial officer must determine, either from personal knowledge or from satisfactory evidence, that the signature is that of the person appearing before the officer. The typical procedure for having a notary attest to the validity of a signature is to have the person whose signature is to be notarized appear before the notary with sufficient evidence that the person is who he or she claims to be. The person signs the document in the presence of the notary, and then the notary formally witnesses the signature by affixing the notarial seal or stamp and by signing and dating the document. While the notary does not insure the identity of the subscriber, the notary may nevertheless be liable if he or she acts negligently or recklessly in the conduct of his or her office.

The Federal Rules of Evidence provide that documents accompanied by a certificate of acknowledgment executed by a notary public do not require extrinsic evidence of authenticity as a condition precedent to admissibility. This is advantageous because it obviates the need for testimony from witnesses or submission of other extrinsic proof to demonstrate the authenticity of a proffered piece of evidence. The rule does not address the persuasiveness of the evidence, nor its relevance, nor does it create any presumption as to the accuracy of the proffered document. The justification for this form of authentication is that the person whose name is on the

---

183. A notary public is a public official authorized to perform many functions in addition to witnessing signatures, including taking an acknowledgment, administering an oath or affirmation, taking a verification upon an oath or affirmation, certifying or attesting a copy, and noting a protest of a negotiable instrument. See Uniform Law on Notarial Acts § 1 (1997) (defining a "notarial act."). The law governing notaries is largely state law. Most states regulate notaries by statute; many states have adopted the Uniform Law on Notarial Acts approved by the National Conference of Commissioners on Uniform State Laws in 1983. See Michael L. Closen & G. Grant Dixon, III, Notaries Public from the Time of the Roman Empire to the United States Today and Tomorrow, 68 N.D. L. Rev. 873, 876-77 (1992).

185. See id.
186. See Closen & Dixon, supra note 183, at 883-84.
187. See id. at 888-89.
188. See Fed. R. Evid. 902(8).
190. See id. § 902.02[3].
document must have come before the notary and proved his or her identity.¹⁹¹

4. What Is a Signature in Electronic Commerce?

While the popular understanding of signature might limit the concept to handwritten or even cursive autographs affixed to paper at the conclusion of the authenticated text that the signer is authenticating, it is clear that the legal definition of signature is much more flexible. In theory, courts should have no problem adapting the legal definition of any mark or symbol made with the intention of authenticating a text to the online environment where the text may consist of a computer record and the signature may consist of a typed name at the bottom of an electronic mail message. In practice, most courts faced with the question have in fact responded by looking to the intent of the purported signer and the evidence provided by the parties regarding the context in which the alleged signature was made.¹⁹² As long ago as 1869, a New Hampshire court upheld the validity of a contract formed by the exchange of telegrams under a statute of frauds requiring a signed writing.¹⁹³ As recently as 1996, however, a Georgia court held that a fax did not constitute a written notice because it was only “chirps and beeps.”¹⁹⁴ Thus, while most courts have looked beyond the technology in use to consider the evidence of the parties’ intentions and the circumstances of the transaction, including the reliability of the computer procedures involved, it is not certain that all courts will act accordingly.

In order to eliminate any risk that a court might deem that the exchange of electronic messages fails to meet the writing and signature requirements of a statute of frauds, EDI trading parties often enter into written trading partner agreements.¹⁹⁵ These agreements can provide that, for the purposes of the parties, the exchange of certain electronic messages will give rise to a valid and binding contract for the sale of goods.¹⁹⁶ The trading partner agreement meets any legal requirement that a contract be signed and establishes the framework within which the parties attach legal significance to different forms of

¹⁹¹. See id. § 902.10(1).
¹⁹². See WRIGHT & WINN, supra note 121, at 16-17.
¹⁹⁵. See ABA, Model Agreement, supra note 116, at 1657-58.
¹⁹⁶. See id.
electronic communications. Written trading partner agreements can also include express provisions that allocate the risk of losses arising through unauthorized access to the network or failure to maintain the level of communication or system security agreed upon by the parties.

B. Negotiable Instruments Law

Negotiable instruments are a special category of contracts that originated within the merchant community of western Europe in the early modern era. Negotiable instruments law developed in the succeeding centuries as a body of formal doctrines in England as merchants brought their disputes to the royal courts for resolution. As a result of this venerable provenance, many of the principal tenants of negotiable instruments law differ markedly from those of general contract law. In particular, certain doctrines of negotiable instruments law emphasize the importance of form to a much greater degree than is characteristic of modern contract law. As a result, holders of negotiable instruments seeking to recover from the instrument’s maker enjoy the benefit of certain liability rules and evidentiary presumptions that make it easier for the holder to recover than would be the case in an action on a general contractual obligation. As a result of these liability rules and evidentiary presumptions, the possibility increases that someone who is not in fact the maker of a negotiable instrument will nevertheless be held liable to pay the amount of the instrument.

The formalism of negotiable instruments law and the apparent harshness of the results that it produces for the purported signer in certain cases contrasts with the common law emphasis on the intent of the signer as the decisive element distinguishing a signature from a mere autograph or a forgery. Negotiable instruments law had its

197. See id.
199. See id. at 12.
200. Contemporaneous with the development of negotiable instruments law in the law of merchants were the common law forms of action for covenant under seal and debt. These forms of action were characterized by a high degree of formalism. See J.H. BAKER, AN INTRODUCTION TO ENGLISH LEGAL HISTORY 326 (3d ed. 1990). Covenant under seal and debt were eventually supplanted by the more flexible form of action for trespass on the case in assumpsit, which became the foundation of modern contract law in the 19th century with the abolition of the forms of action. See id.
201. One noteworthy liability rule that applies in negotiable instruments law but not in general contract law is the rule that a holder in due course can enforce an instrument without regard to many competing claims of ownership or defenses to the payment obligation. See U.C.C. § 3-305(b) (1996). The relevance of holder in due course doctrines to electronic commerce are beyond the scope of this Article.
origins in the medieval law of merchants, and in the need of parties in commerce to effect payment for goods in the absence of modern banking and payment systems.\textsuperscript{202} In order to make the merchant’s written obligations more acceptable, the terms of the obligations and the procedures for their assignment or negotiation became very stylized and formalistic.\textsuperscript{203} While the rigidity of these rules can operate as a trap for unwary parties,\textsuperscript{204} to the extent that negotiable instrument doctrines are a reflection of commercial custom and negotiable instruments primarily circulate among merchants who are familiar with those customs, the formalism and rigidity of negotiable instruments law helps to create an efficient, decentralized payment mechanism.\textsuperscript{205}

1. What Is a Signature?

Under the Uniform Commercial Code, the use of the term “signed [is defined to] include[] any symbol executed or adopted by a party with present intention to authenticate a writing.”\textsuperscript{206} Official Comment 39 adds that “authentication” is included in the definition to make clear that a complete signature is not necessary.\textsuperscript{207} Rather, authentication may be printed, stamped, or written; it may be merely initials or a thumbprint, or even in appropriate cases found on the letterhead of a writing.\textsuperscript{208} The comment emphasizes that the determinative element is the present intent of the signer to authenticate the writing that creates a signature, so common sense and commercial experience must be used to decide hard cases.

\textsuperscript{205} While it might have this effect in theory, many authors have questioned the continued relevance of the concept of negotiability in modern commercial law. See Grant Gilmore, Formalism and the Law of Negotiable Instruments, 13 CREIGHTON L. Rev. 441, 461 (1979); Mann, supra note 203, at 956; James Steven Rogers, The Irrelevance of Negotiable Instrument Concepts in the Law of the Check-Based Payment System, 65 TEX. L. Rev. 929, 920-31 (1987); Albert J. Rosenthal, Negotiability—Who Needs It?, 71 COLUM. L. Rev. 375, 379 (1971); see also Charles W. Mooney, Jr., Beyond Negotiability: A New Model or Transfer and Pledge of Interests in Securities Controlled by Intermediaries, 12 CARDOZO L. Rev. 305, 398-402 (1990) (suggesting that the traditional model of transfer rights and negotiability poorly fits modern commercial practices).
\textsuperscript{206} U.C.C. § 1-201(39) (1996).
\textsuperscript{207} See id. § 1-201, Official Comment 39.
\textsuperscript{208} See id.
Within UCC Article 3, more specific provisions govern the validity of signatures on negotiable instruments. The basic rule is that no one is liable on an instrument unless that person signed the instrument or the instrument was signed by that person's agent or representative. However, this rule is subject to certain exceptions discussed below. In addition, Article 3 expressly provides that a signature may be made either manually or by means of a machine, by the use of any name including a trade name or assumed name, or by any word, mark, or symbol adopted by a person with the present intent to authenticate a writing. With regard to signatures by authorized representatives that are binding on the represented persons, the default rule in Article 3 is that common law rules of agency law apply. Article 3 also includes special provisions governing the effect of signatures by representatives, such as officers of corporations that sign checks issued by corporations, and other common problems involving authorized representatives that arise in modern commercial transactions. In addition, a signature that was unauthorized when made may nevertheless be ratified after the fact.

2. When Can a Party Be Held Liable for a Signature He or She Did Not Produce?

The general rule of negotiable instruments law is that a party cannot be liable on an instrument that he or she did not sign. A forged signature, because it is ineffective as the signature of the purported signer, operates instead as the signature of the forger. However, Article 3 provides for several circumstances under which the purported signer will be precluded from avoiding liability for a forged signature. With regard to the signature of a maker or drawer of an instrument, this includes situations where the purported signer has substantially contributed to the making of a forged signature.

209. See id. § 3-401(a).
210. See infra notes 215-223 and accompanying text.
211. See U.C.C. § 3-401(b).
212. See id. § 3-402(a), Official Comment 1.
213. See id. § 3-402(b), §3-402(c), Official Comment 2, Official Comment 3.
214. See id. § 3-403(a), Official Comment 3.
215. See id. § 3-401(a).
216. See id. § 3-403(a), Official Comment 2.
217. In addition, a purported signer may be precluded from avoiding liability for a forged signature based on the common law doctrine of estoppel, which supplements the UCC. See id. § 1-103. Also, a bank customer who fails to examine his or her bank statement may be precluded from demanding that the bank recredit the account after the bank has paid on a check with a forged signature. See id. § 4-406.
through his or her failure to exercise ordinary care. The Official Comments provide examples of the type of negligence that can be the basis of preclusion under UCC § 3-406(a), such as failure of an employer to safeguard a rubber signature stamp that is then used by an employee fraudulently to sign checks.

The party whose negligence contributed to the forger is liable only to certain persons for the amount of the instrument. These include those who in good faith pay the instrument (in the case of a check, this would include the bank on which the check was drawn) or those who in good faith take the instrument for value (in the case of a check, this would include a third party such as a merchant who paid the forger for the check). In the event that the party paying or taking the instrument for value was also negligent, the 1989 revisions of Article 3 created a comparative negligence standard for allocating the loss due to the forgery between the purported signer and the party that paid or gave value for the instrument. The revisions substituted the comparative negligence standard for the contributory negligence standard embodied in the prior version of Article 3. The former rule provided that any person who by his or her negligence substantially contributes to the making of an unauthorized signature is precluded from asserting that lack of authority against a holder in due course or someone who in good faith and in accordance with reasonable commercial standards pays or gives value for the instrument.

3. When Is a Signature Presumed To Be Authentic?

Some of the primary advantages of evidencing obligations in the form of negotiable instruments rather than simply as agreements subject to the general law of contracts are the significant procedural advantages that plaintiffs enjoy while seeking to recover in litigation.
based on negotiable instruments. These procedural advantages may permit the plaintiff to reduce the obligation to a judgment and to proceed to execution on the judgment much more quickly than would be possible in litigation on contracts generally. These procedural advantages may flow from the provisions of the UCC, from state law outside the UCC, or from the rules of evidence.

UCC Article 3 provides that, unless specifically denied in the pleadings, each signature on an instrument is admitted. This simplifies the plaintiff's task in proving his or her case and requires the defendant to put the plaintiff on notice at the outset of the litigation that the validity of a signature will be at issue. When the validity of a signature is put in issue, the party claiming under the signature has the burden of establishing it, but she enjoys the benefit of a presumption that the signature is genuine or authorized. A mere denial of the signature's genuineness is normally insufficient to overcome this presumption; the party seeking to avoid liability must introduce some evidence to support a finding that the signature is a forgery. If enough evidence is introduced by the defendant to overcome the presumption, however, the plaintiff must prove that it is more probable than not that the signature is genuine or authorized.

Some states provide similar procedural advantages for holders of instruments outside of UCC Article 3. For example, the New York Civil Practice and Remedies Code has a procedure designed to permit actions based on an instrument for the payment of money only to be started with a motion for summary judgment. This procedure is used primarily in cases dealing with commercial paper, whether or not it complies with all of the technical requirements of negotiable instruments law.

225. See infra notes 228-232 and accompanying text.
226. See infra notes 233-234 and accompanying text.
227. See infra notes 235-236 and accompanying text.
228. See U.C.C. § 3-308(a).
229. See id. § 3-308, Official Comment 1.
230. See id. § 3-308(a). However, where the purported signer is dead or has become incompetent before the time of the litigation, there is no presumption of authenticity. See id.
232. See Lawrence, supra note 224, at 216.
The Federal Rules of Evidence provide that commercial paper, signatures on commercial paper, and documents relating to commercial paper are self-authenticating to the extent provided by commercial law. This rule is designed to recognize the nationwide implementation of the UCC and to allow its evidentiary presumptions to govern in appropriate cases.

C. UCC Article 4A and Commercially Reasonable Security Procedures

Although payment by checks constitutes the largest number of transactions in the United States today, the largest volume of payments based on amount is transferred through electronic funds transfer systems. Several funds transfer systems exist in the United States: the Federal Reserve Banks maintain a wire transfer system known as the Fedwire; a group of commercial banks in New York maintains a wire transfer system known as CHIPS (the Clearinghouse Interbank Payments System); the National Automated Clearinghouse Association (NACHA) represents a national network of automated clearinghouses for funds transfers; retail customers of banks make electronic funds transfers using automated teller machines and home banking services. The daily volume of transfers over the two wholesale funds transfer systems—Fedwire and CHIPS—usually exceeds $1 trillion.

Prior to 1989 there was no comprehensive set of statutory or regulatory rules governing the wholesale wire transfer system. Applicable law was derived from the regulations and operating rules of the Board of Governors of the Federal Reserve System, the operating rule of private systems such as CHIPS, and common law principles developed by analogy from the law of other payment systems. With regard to many issues, however, this body of law was sparse and underdeveloped. Beginning in the mid-1970s, the National Conference of Commissioners on Uniform State Laws

235. See Fed. R. Evid. 902(a).
236. See Weinstein & Berger, supra note 189, § 902.11[1].
238. See id.
239. See id.
240. See Wright & Winn, supra note 121, §1.03(2).
241. Consumer electronic funds transfers are discussed infra notes 295-318 and accompanying text.
243. See id.
244. See Baker & Brandel, supra note 7, ¶ 13.02.
INTERNET COMMERCE REGULATION

(NCCUSL) and the American Law Institute (ALI) began the process of proposing statutory rules to bridge this gap, first with an unsuccessful proposal for a New Payment Code that would have integrated and homogenized the law governing all types of payment systems.245 Following the abandonment of the New Payment Code in 1984, a drafting committee was set up with the narrower charge of producing a law governing only wholesale wire transfers.246 This drafting committee produced UCC Article 4A, which was officially promulgated by NCCUSL in 1990247 and which by 1997 had been adopted in all fifty states.

The drafters of Article 4A were charged with developing a statutory framework for a set of institutional arrangements that were already well established before the arrival of the drafting committee on the scene. Participants in the wholesale wire transfer system were largely confined to major corporations and commercial banks, and they were not only quite sophisticated in their understanding of the wire transfer system but were also well represented at the drafting committee meetings.248 The drafters of Article 4A were able to forge a consensus from the often sharply divergent notions of appropriate liability regimes advocated by banks providing the wire transfer services and their corporate customers who used those services.249

In drafting a comprehensive statute to govern a commercial practice that had been from its inception wholly within the realm of electronic commerce, the drafters of Article 4A were forced to find novel solutions for many of the problems of electronic commerce. One of the most noteworthy innovations of Article 4A was the concept of a "security procedure" as a means to authenticate payment orders from bank customers to banks in lieu of a traditional signature.250 One of the loss allocation issues that the drafters confronted was the

246. See id.
247. See id. at 780 n.132.
248. See id. at 763.
249. The issue of consequential damages for a bank's failure to execute a wire transfer is one example. Although legal academics had long been persuaded of the need for formal law to govern the wire transfer system, actual participants in the system were persuaded by the Evra case. See Evra Corp. v. Swiss Bank Corp. 673 F.2d 951 (7th Cir. 1982). In Evra, Judge Posner raised the specter of consequential damages for failure by a bank properly to execute a wire transfer, which was not an acceptable risk for the banks operating the system. See id. at 958-59. Also, the UCC provides that a bank cannot be liable for consequential damages to the extent provided by an express written agreement. See U.C.C. § 4A-305(a) (1996).
250. See U.C.C. § 4A-201.
problem of unauthorized payment orders, or the subsequent fraudulent repudiation of a valid payment order.\(^2\) This problem is addressed in Article 4A with the concept of a "commercially reasonable security procedure."\(^2\)

1. **What Is a Commercially Reasonable Security Procedure?**

A security procedure is defined in Article 4A as a procedure "established by agreement of a customer and its receiving house for the purpose of (i) either verifying that a payment order or other communication ... that of the customer, or (ii) detecting error in the transmission or the content of a payment order or communication."\(^3\) Article 4A does not set any formal rules regarding what may qualify as a security procedure, other than to note that merely comparing a signature on a payment order with an authorized specimen signature is not by itself a security procedure.\(^4\) A security procedure may require the use of algorithms or other codes, identifying words or numbers, encryption, callback procedures, or similar security devices.\(^5\)

Just because a security procedure conforms to UCC § 4A-201 does not mean that it is a "commercially reasonable" security procedure. What constitutes a commercially reasonable security procedure is determined in light of the wishes of the bank's customer that are expressed to the bank, the circumstances of the customer known to the bank (including the size, type, and frequency of payment orders normally issued by the customer to the bank), alternative security procedures offered by the bank to the customer, and security procedures in general use by customers and receiving banks similarly situated.\(^6\) The burden of making available commercially reasonable security procedures is imposed on banks because they generally determine what security procedures can be used and are in the best position to evaluate the efficacy of procedures necessary for bank customers to combat fraud.\(^7\) Once a commercially reasonable security procedure has been agreed upon by the bank and the customer, the burden is on the customer to supervise its employees to assure compliance with the security procedure and to safeguard

\(^{251}\) See id. art. 4A, Prefatory Note.
\(^{252}\) See id. § 4A-202, Official Comment 3.
\(^{253}\) See id. § 4A-201.
\(^{254}\) See id.
\(^{255}\) See id.
\(^{256}\) See id. § 4A-202(c).
\(^{257}\) See id. § 4A-203, Official Comment 3.
confidential security information and access to transmitting facilities so that the security procedure cannot be breached.258

2. When Can a Party Be Held Liable for a Payment Order It Did Not Originate?

One of the contentious issues addressed in the drafting of Article 4A was the question of liability for unauthorized payment orders.259 In some cases, it might be possible to trace the source of the unauthorized order to an interloper who had penetrated the security system of either the bank or its customer, or to a rogue employee of either the bank or its customer. In hard cases, however, the malfeasant would evade detection, leaving the bank and its customer to allocate the loss without any information as to whose security system had been breached. In this case, the banks felt that the default rule should allocate the loss to their customers who, as the less technologically sophisticated party, the banks deemed more likely to be the probable cause of the loss.260 The cash managers of the banks’ customers, however, took issue with this assessment.261 The representatives of the banks’ customers at the drafting committee refused to accept a simple loss allocation rule that would make the customer take the loss for unexplained unauthorized payments out of their accounts.262 The representatives of the banks and their customers attending the drafting committee meetings eventually worked out a compromise acceptable to all involved.263

The default rule in Article 4A for determining whether a payment order received by a bank is in fact a duly authorized order of its customer is the same as the default rule in Article 3: the party claiming that the order is an authorized order must establish that it was sent by someone with authority to represent the customer under the law of agency.264 In the wire transfer context, however, this simple rule imposes a difficult evidentiary burden on the bank receiving and acting upon the customer’s orders if those orders are sent and received electronically. The bank will receive at a computer workstation within the bank an electronic message that purports to be from the bank’s customer. Without taking steps to confirm the terms of the order using

258. See id.
259. See Rubin, supra note 245, at 764.
260. See id.
261. See id.
262. See id.
263. See id.
an "out of band" or "back channel" communication with the bank’s customer, the bank may have a very hard time establishing the true origin of the order; however, personal contact between the bank and its customer for each wire transfer order may not be feasible.265

In order to avoid this difficult evidentiary problem, the bank must make a commercially reasonable security procedure available to the customer, the bank and the customer must agree to a procedure that they will use, and the bank must follow that procedure.266 The commercial reasonableness of the security procedure agreed upon by the bank and its customer may be established with reference to the customer’s circumstances,267 or the bank’s customer may decide to reject the bank’s advice with regard to what an appropriate security procedure would be and expressly agree in writing that the customer will be bound by any payment order issued in its name and accepted by the bank in compliance with the security procedure chosen by the customer.268 The drafters of Article 4A thus used the contrast between the default rule of agency law and the statutory safe harbor of a commercially reasonable security procedure to give the bank, as the technologically more sophisticated party, an incentive to bring participants in the wire transfer system up to an appropriate level of security in their systems for administering wire transfer orders.

The customer has one small opportunity to shift liability for an unauthorized payment order back to the bank in the event that the customer can demonstrate that the order was not caused, directly or indirectly, by a person entrusted by the customer with any responsibilities for executing wire transfer orders, or by a person who obtained access to the wire transfer system through the customer’s facilities.269 The customer must prove that the unauthorized order did not originate through the actions of anyone acting on its behalf or through its systems. Therefore, the most likely allocation of liability for unauthorized payment orders remains squarely on the bank’s customer once a commercially reasonable security procedure has been put in place.

Difficult is not the same as impossible, as one example illustrates. In 1994, a Russian computer programmer removed $10 million from Citibank customer accounts by initiating unauthorized funds transfers

265. See id. § 4A-203, Official Comment 2.
266. See id. § 4A-202(b).
267. See id. § 4A-202(c).
268. See id. § 4A-202(c).
269. See id. § 4A-203(a)(2).
from a laptop computer in St. Petersburg. Later, all but $400,000 was recovered and no bank customers were held liable for any of the losses.

There are similarities between the law governing the use of facsimile signature devices, which precludes the defense of forgery based on negligence under negotiable instruments law, and the Article 4A rules concerning liability for unauthorized payment orders. For both facsimile signature devices and electronic messages containing wire transfer orders, in the absence of a formal written assumption of the risk of unauthorized orders by the bank's customer, the bank is put in the difficult position of establishing the factual basis for a claim that the payment instruction was in fact authorized by the bank's customer. For wire transfer payment mechanisms, once a security procedure has been agreed upon for check-based payment systems, the bank's customer must accept responsibility for payment instructions sent by employees who breach the customer's internal security systems. For negotiable instruments, however, unlike wire transfers, the bank's customer is presumed by law to be capable of discerning what constitutes ordinary care in the supervision of its employees with responsibility for handling its checking accounts. In the realm of electronic commerce, the customer is not presumed to know what constitutes reasonable care until the bank, as the more technologically sophisticated party, has evaluated its circumstances and made a recommendation regarding appropriate security procedures.

D. Consumer Electronic Funds Transfers Under Regulations Z and E

Credit cards originated in the United States in the 1920s. Proprietary credit cards were issued by retail merchants to their customers to simplify the administration of sales on credit. Travel and entertainment cards developed in the 1950s to solve the problem of the unacceptability of out-of-town checks. A third-party administrator such as Diners Club or American Express handled the process of crediting the merchant and collecting payment from the

270. See Gow & Norton-Taylor, supra note 47, at 1.
272. See id. § 3-404(b).
273. See id.
274. See id. § 4A-202(b)(c); id. § 4A-203, Official Comment 3.
276. See id.
277. See id.
purchaser of goods and services, payment for which was due in full upon receipt of each statement.\textsuperscript{278} Bank of America offered the first bank credit card in 1958, but it was not until the 1960s that the idea of using a charge card as a mechanism for administering an open line of bank credit to consumers became popular.\textsuperscript{279} In 1967, a consortium of banks formed an interbank card known as Mastercharge (later MasterCard) to compete with Bank of America to provide a “universal” credit card to consumers that would be acceptable anywhere in the country.\textsuperscript{280} In 1970, Bank of America reorganized its credit card operations as a separate company, Visa.\textsuperscript{281} Visa and MasterCard now operate as “for-profit nonstock corporations” for the benefit of their members who vote in governance matters on the basis of the volume of payments they process through the system.\textsuperscript{282} Membership in Visa and MasterCard is limited to financial institutions or those organizations who qualify for federal deposit insurance.\textsuperscript{283}

The credit card payment system is organized by contracts between the cardholder and the card issuer, between the merchant and the bank that purchases the customer charges from the merchant ("merchant bank"), and between the interchange (a centralized computer clearinghouse) provided by Visa or MasterCard in which card issuers and merchant banks must participate.\textsuperscript{284} In the 1960s, these relationships were governed only by the contracts drawn up by the card issuers and the merchant banks, except for generic regulations applying to credit transactions such as usury laws.\textsuperscript{285}

In response to the development of practices that were deemed irresponsible and unfair by regulators, in 1970 the federal government amended the Consumer Credit Protection Act\textsuperscript{286} to deal with aspects of the credit card system. Regulation Z issued by the Board of Governors of the Federal Reserve System\textsuperscript{287} implements the provisions of that statute. Among the abuses of the credit card industry that the Consumer Credit Protection Act and Regulation Z

\begin{itemize}
\item \textsuperscript{278} See id. at 713.
\item \textsuperscript{279} See id. at 713-14.
\item \textsuperscript{280} See id. at 714.
\item \textsuperscript{281} See id.
\item \textsuperscript{282} See id.
\item \textsuperscript{283} See id. at 715. This discussion focuses on Visa and Mastercard because they are the two largest credit card issuers in the U.S. market; other major issuers include American Express, Discover Card, and Diners Club. See id. at 714.
\item \textsuperscript{284} See id. at 715.
\item \textsuperscript{285} See id.
\item \textsuperscript{287} See 12 C.F.R. § 226 (1997).
\end{itemize}
were designed to stop were the mailing of unsolicited cards through the mail and the allocation of risk for unauthorized use to the consumer.  

In the late 1960s and early 1970s, the first automated teller machine (ATM) systems were installed by retail bank networks.  

Various state and federal legislative initiatives addressing the need for consumer protections in the area of electronic funds transfers (EFT) culminated in 1978 in the Electronic Funds Transfer Act, which applies to automated clearinghouse (ACH) debit and credit transfers, as well as to ATM transactions, point-of-sale (POS) transactions, and home banking services. Regulation E issued by the Board of Governors of the Federal Reserve System implements the provisions of that statute. Regulation E has consumer protection provisions similar to those of Regulation Z dealing with unsolicited issuance of EFT access devices and the allocation of risk between the bank and customer for unauthorized use of the access device.  

Although currently there are regulatory regimes under federal law governing credit cards on the one hand and ATM or debit cards on the other, both sets of regulations are substantially similar with regard to consumer liability for unauthorized payments. The historical differences that led to one set of regulations that apply when a financial institution permits a consumer to make a payment with a credit advance and another set of regulations that apply when a consumer pays with a debit to the consumer’s outstanding credit balance at the financial institution are rapidly diminishing in significance.

1. How Is a Consumer Payment or Electronic Funds Transfer Authorized?  

Before a credit card can be used to effect payment for goods or services, the card itself must be requested by the consumer. The

---

289. See BAKER & BRANDEL, supra note 7, ¶ 1.03.  
291. See id. § 1693(a)(6).  
293. See id. § 205.1(b).  
294. In response to growing consumer concern over disparities in the treatment of branded debit cards and credit cards, Visa and MasterCard both voluntarily undertook to apply the Regulation Z liability rules (which are more generous to consumers) to debit cards in lieu of the Regulation E rules (which are less favorable to consumers). See Bruce Mohl, Visa Eases Theft Rules; Liability Protection Boosted for Customers, THE BOSTON GLOBE, Aug. 14, 1997, at Cl.  
card issuer should also provide a means to identify the cardholder on the account or the authorized user of the card.\textsuperscript{296} This is generally accomplished through the use of a signature tape on the back of the card, permitting the merchant to compare the specimen signature on the tape with the signature on the charge slip, although it may also be accomplished through the use of a photograph or fingerprint on the card.\textsuperscript{297} It may also be accomplished through the use of a PIN number if, for example, the charge card is to be used with an ATM machine.\textsuperscript{298} In addition, the issuer should provide the cardholder with the information that the cardholder would need to report the loss or theft of the credit card.\textsuperscript{299}

The Federal Reserve Board staff has provided guidance to card issuers regarding certain common situations in which certain common commercial practices will be deemed not to have met the card issuer’s obligation to provide a means by which the cardholder may be identified.\textsuperscript{300} The Official Commentary provides that a magnetic strip (or similar device not readable without physical aids) alone that is not used in connection with a secret code or the like is not an adequate means of identifying the cardholder.\textsuperscript{301}

Consumer Electronic Fund Transfers (EFTs) may take a wide variety of forms, including POS transfers, ATM transfers, direct deposits or withdrawals of funds from a consumer account, and transfers initiated by telephone.\textsuperscript{302} An EFT is authorized through the use of an “access device,” which may include a card, a code, or other means of access to a consumer’s account, or any combination that is used by a consumer for the purpose of effecting an EFT.\textsuperscript{303} Thus, an ATM card together with the associated PIN may constitute an “access device.”\textsuperscript{304} As with credit cards, a consumer cannot be liable for EFTs effected with an access device that the consumer has not requested or

\begin{itemize}
\item \textsuperscript{296} See id. § 226.12(b)(2)(iii). If a means of identification is not provided, the issuer may not hold the cardholder liable for any unauthorized charges.
\item \textsuperscript{298} See id. § 226.12(a)(1)-8.
\item \textsuperscript{299} See id. § 226.12(b)(2)(ii)(1)-8. If this information is not provided, the issuer may not hold the cardholder liable for any unauthorized charges.
\item \textsuperscript{300} See id. § 226.12(b)(2)(iii)-1.
\item \textsuperscript{301} See id. § 226.12(b)(2)(ii)(1)-8. This commentary provides that there is insufficient means of identifying the user of a card if a corporate card is signed only by a corporate representative who will not be the person using the card. See id.
\item \textsuperscript{302} See Federal Reserve Board, Official Staff Interpretations, 12 C.F.R. pt. 205, § 205(g) (1997).
\item \textsuperscript{303} See id. § 205.2(a)(1).
\item \textsuperscript{304} See id. § 205.2-1.
\end{itemize}
INTERNET COMMERCE REGULATION

received in exchange for a previously accepted access device.\textsuperscript{305} Also, the financial institution should provide the consumer with information regarding the consumer’s possible liability for unauthorized EFTs under certain circumstances and the information the consumer would need to report that an unauthorized EFT has been, or may be, made.\textsuperscript{306}

2. When Can a Party Be Held Liable for a Payment or Funds Transfer He or She Did Not Authorize?

The limitations on the liability of consumer credit card holders for unauthorized payments are among the most radical, and successful, consumer protection initiatives of the 1970s. Regulation Z provides that a cardholder may be held liable for not more than $50 or the actual amount of unauthorized charges, whichever is less, and even that small amount cannot be charged to the card holder unless the card issuer has met the following requirements: the card was accepted by the consumer, the card issuer provided the consumer with adequate notice of his or her potential liability, the issuer provided the consumer with an adequate means of notifying the issuer in the event the card is lost or stolen, the issuer provided a means of identifying the authorized user of the card, and the unauthorized use must have occurred prior to notification by the cardholder to the issuer of the loss or theft of the card.\textsuperscript{307} This loss allocation rule places almost all of the risk of unauthorized use squarely on the merchants accepting credit card charges as a form of payment, merchant banks processing charge slips, and card issuers.

As a result of this loss allocation rule, huge amounts have been invested in system security features to reduce the incidence of credit card fraud losses. Fraud loss prevention techniques include the addition of cardholder photographs or holograms on credit cards to make the manufacture of bogus cards using credit card information more expensive and data mining techniques that permit the card issuer to spot usage patterns that correlate with theft or fraudulent credit card use before the cardholder may even be aware of the problem.\textsuperscript{308} While this loss allocation rule may seem to remove the economic incentives

\textsuperscript{305} See id. § 205.2(a)(2). This is subject to certain exceptions contained in § 205.5(b), which regulates the issuing of ATM cards, such that ATM cards cannot function until the consumer takes affirmative steps to validate them.

\textsuperscript{306} See id. § 205.6(3). If this information is not provided, the financial institution may not hold the consumer liable for any unauthorized charges.

\textsuperscript{307} See id. § 226.12(b)(2).

\textsuperscript{308} See Homer Brickey, Credit Firms, Crooks at War: Fraud Losses Reach $1 Billion A Year, ARIZ. REPUBLIC, Jul. 15, 1995, at E1.
that would encourage consumers from taking reasonable precautions, this is apparently not the case.\(^{309}\)

The limitation on consumer liability for unauthorized use has been very significant in building the market for telephone sales by credit card. The Official Commentary to Regulation Z makes it clear that the practice of accepting credit card information over the telephone is done entirely at the merchant’s risk in the event a cardholder later claims a payment is unauthorized.\(^{310}\) Because the issuer has not provided the merchant with a means to identify the user under these circumstances, the issuer has not fulfilled one of the conditions for imposing liability on the cardholder.\(^{311}\) The Official Commentary points out that merchandise may be ordered by telephone by someone other than the cardholder using credit card information that may have been improperly obtained in any number of ways; in the event that the consumer contests a telephone charge as unauthorized, the card issuer will be required to charge back the payment to the merchant’s bank.\(^{312}\)

The favorable treatment of consumers in dealing with losses caused by unauthorized use of credit cards is reinforced by other rights bestowed on consumers by Regulation Z. Subject to certain limitations, consumers retain the right to assert claims or defenses arising in their transactions with merchants against the credit card issuer and refuse payment for the amount in dispute.\(^{313}\) In addition, Regulation Z defines an error resolution procedure that requires the card issuer to wait for payment pending its investigation into the consumer’s allegation of billing errors.\(^{314}\)

With regard to unauthorized EFTs, the provisions of Regulation E are similar to those of Regulation Z, although less generous to the consumer. When hearings were conducted on the need for consumer protections in the EFT arena, consumer advocates argued that the same degree of protection should be extended to EFTs, but representatives of the financial services industry argued that the


\(^{311}\) See id.

\(^{312}\) See id. §§ 226.12(c)(2)-1, 226.13-2.

\(^{313}\) See id. § 226.12(c). The cardholder is required to make a good faith attempt to resolve the dispute with the merchant. The credit card issuer is not required to be involved in disputes that involve less than $50 or disputes that arise within the cardholder’s state or within 100 miles of the cardholder’s address. See id. § 226.12(c)(3)(ii).

\(^{314}\) See id. § 226.13.
INTERNET COMMERCE REGULATION

negligence standard in UCC § 3-406 should apply. The result was a more complicated loss-allocation formula that provides nonnegligent consumers with the same protection as provided to credit card holders but that imposes a greater proportion of any losses on the consumer as the consumer’s negligence in reporting the loss or theft of the access device grows. The consumer who promptly reports the loss or theft of the access device is liable for the lesser of $50 or the amount of the unauthorized EFTs, but a consumer who fails to notify the financial institution within two business days of learning of the loss or theft may be liable for up to $500. A consumer who fails to report the loss or theft of the access device within sixty days of the account statement being transmitted to the consumer may be liable for the entire amount of unauthorized charges that occur after the sixty days and before the consumer finally gives notice to the institution.

E. Proposed Revisions to the UCC Definition of Signature and Writing

The National Conference of Commissioners on Uniform State Laws and the American Law Institute have appointed drafting committees to prepare revisions to UCC Articles 1, 2, 2A, and 9 and to prepare a draft of a proposed new Article 2B governing software contracts and information licensing. Among the changes being considered are the substitution of the term “record” for the term “writing” and the term “authenticated” for the term “signed” in order to permit electronic contracts to meet statute of frauds requirements. For example, the March 1998 draft of proposed UCC § 2B-102 provides the following definitions:

“Authenticate” means to sign, or to execute or adopt a symbol or sound, or to encrypt or process a record in whole or in part, with intent by the authenticating party to

(a) identify that party;
(b) adopt or accept a record or term that contains the authentication or to which a record containing the authentication refers; or

316. See 12 C.F.R. § 205.6(b).
317. See id.
318. See id.
(c) attest to the integrity of a record or term.

"Attribution procedure" means a procedure established by law or regulation or established by agreement or adopted by the parties for the purpose of verifying that an electronic authentication, record, message, or performance is that of the respective party or for detecting changes or errors in content. 320.

In the July 1997 draft of Article 2B, the draft official comment provided that "attribution procedures" per se constitute authentication, but this suggestion was removed from subsequent drafts. At the time this Article was written, these changes had not yet been officially adopted by NCCUSL or ALI.

IV. HOW SHOULD AUTHENTICATION PROCEDURES USED IN INTERNET COMMERCE BE REGULATED?

A. Different Approaches to Regulating Open Network Authentication Procedures

Although electronic commerce is arguably as old as the telegraph, the possibility of reducing transaction costs while improving speed and accuracy in commercial transactions through the use of networked computers has only achieved widespread attention in the last decade. In the 1980s, the popularity of EDI contracting triggered a debate on the issues of adapting existing commercial law to take into account new computer messaging and record processing technologies. 321. However, EDI technology was introduced largely through the creation of proprietary systems that were operated by the participants themselves or by value-added networks. 322. As a result, participation in EDI electronic contracting often required a substantial investment in proprietary network technologies. 323. This requirement of an initial investment in proprietary communications technology served as a sort of de facto channeling mechanism, limiting the implementation of electronic commerce procedures to parties with existing commercial relationships, as well as to parties willing to make a substantial investment in the technology required. 324

The emergence of the Internet as a possible medium of communication for electronic commerce has introduced a new and

321. See ABA, Commercial Use, supra note 115, at 1645.
323. See id.
324. See id.
different environment for online contracting. Much of the initial investment in Internet technology is being made by businesses who wish to use web sites for general marketing and Intranet to distribute internal materials; redeploying these same resources for electronic commerce in effect substantially lowers the initial investment required to enter the arena. The ubiquitousness of the Internet means that consumers, as well as businesses, are able to participate in electronic commerce. The use of open standards for Internet network protocols means that the array of potential participants in Internet commerce is virtually unlimited in number and in geographic distribution.

Unlike the electronic contracting practices that prevailed when EDI conducted over proprietary VANs was the state-of-the-art technology, Internet commerce brings problems of computer security to the forefront of the issues facing prospective participants. The contracting parties must now consider not only all of the standard issues involved in any contract, such as the reliability of the representations or the creditworthiness of the other party, but they must also factor in the security of their own access to the Internet from the threat of attacks by interlopers, as well as the security of the other party’s computer system. While the threat of attacks by interlopers was present with EDI electronic contracting, the openness of the Internet obviously increases the magnitude of the threat of attack. The Internet also lays the technical foundation for entering into online contracts with strangers whose real-world identity has not been confirmed with “out of band” or “back channel” communications.

In response to these new challenges posed by open network electronic commerce, state legislatures have responded in a variety of ways; the federal government and UNCITRAL are now debating what, if any, action is appropriate in those arenas.325 One of the first attempts to deal systematically with these issues, however, came from the American Bar Association Section of Science and Technology in 1992 when the Information Security Committee began work on a project that culminated in 1996 with the publication of the ABA Digital Signature Guidelines.326 The Guidelines do not purport to be a


326. See generally INFORMATION SECURITY COMMITTEE, supra note 2. These guidelines developed in tandem with legislation that was enacted in Utah in 1995. See UTAH CODE ANN. §§ 46-3-101–504 (1997). The Utah legislation differs in certain respects from the
model law, but rather try to offer general statements of principle regarding the development of public key infrastructures with the intention of influencing the more precise rules that will develop within various legal systems.\textsuperscript{327}

1. ABA Digital Signature Guidelines

The ABA Digital Signature Guidelines are the path-breaking project of a large number of attorneys and technologists who were familiar with public key cryptography and who believed that the full commercial exploitation of this technology could only take place once some of the legal uncertainty surrounding its implementation had been resolved.\textsuperscript{328} In the late 1980s and early 1990s, when the promise of public key cryptography for commercial applications was becoming more widely recognized, there were no legal precedents upon which to build a business model of a public key infrastructure. This lack of a recognized legal framework was felt to have a chilling effect on the development of commercial applications of public key cryptography, and it was this problem that the drafters of the Digital Signature Guidelines set out to address.\textsuperscript{329}

The Guidelines list the names of seventy-seven individuals who contributed to the project, in addition to the nine members of the editorial committee. These eighty-six individuals came from a variety of backgrounds including government service, academia, information technology and security, notaries from various legal systems, as well as law practice.\textsuperscript{330} Notwithstanding the active participation of this large group of individuals, the Guidelines represent a fairly focused analysis of certain specific issues raised by the creation of a public key infrastructure. One of the explicit objectives of the Guidelines was the promotion of a specific technology: the use of digital signature

\begin{flushright}
\textsuperscript{327} See \textit{INFORMATION SECURITY COMMITTEE}, supra note 2, at 23.
\textsuperscript{328} Alan Asay and Michael Baum were among the most influential leaders of the process. Alan Asay, who served as a reporter for the project, was an attorney with the Information Technology Division of the Utah Administrative Office of the Courts and one of the principal architects of the Utah digital signature law. Michael Baum, who served as chair of the Information Security Committee, was author of one of the first books to address the legal and policy implications of creating a public key infrastructure. \textit{See generally MICHAEL S. BAUM, FEDERAL CERTIFICATION AUTHORITY LIABILITY AND POLICY: LAW AND POLICY OF CERTIFICATE-BASED PUBLIC KEY AND DIGITAL SIGNATURES} (1994).
\textsuperscript{329} \textit{See \textsuperscript{327}}.
\textsuperscript{330} \textit{See id.} at 1-2.
\end{flushright}
technology based on the X.509 standard established by the International Telecommunications Union.\footnote{331}{See id. at 18. The ITU X.500 series of technical standards provides the basis for constructing a multipurpose distributed directory service by interconnecting computer systems belonging to service providers, governments, and private organizations, on a potentially global scale. See FORD & BAUM, supra note 98, at 213.} The drafters of the Guidelines conceptualized their undertaking as giving "legal effect to the general import of the technical standards for authentication of computerized messages."\footnote{332}{Id. at 21.} In the Introduction to the Guidelines, the drafters state: "Modern cryptography can make information safe from eavesdropping, tampering, or forgery, regardless of the security of a communication channel ... [with the support of public key infrastructure] ... cryptographic technology can also authenticate a message by assuredly linking it to an identified person and guarding the message's integrity."\footnote{333}{See Digital Signature Symposium, JURIMETRICS (forthcoming 1998).} One of the implied objectives of the Guidelines was the creation of a legal framework within which commercial developers using the X.509 directory standard and patented encryption technology, such as that licensed by RSA Data Security, Inc., would feel that the risks of potential liability to users of the system could be kept within tolerable limits. The focus on creating a framework within which commercial developers would feel confident in marketing new products and services was not directed at all, or even most, of the models of electronic commerce currently in use. The consensus among the participants was that closed system applications of public key cryptography did not pose the same theoretical or legal challenges in their commercial development as the case of global stranger-to-stranger commerce over an open network.\footnote{334}{See generally INFORMATION SECURITY COMMITTEE, supra note 2.} Therefore, the Guidelines have minimal relevance to the development and marketing of closed systems based on bilateral, bound community, membership, or robust local administration models, or to an open system based on server security in which individual users are not assigned their own keys.\footnote{335}{See id. at 21.} In closed systems, all of the relevant parties are presumed to be either in contractual privity with each other or bound into some other form of community that will provide some of the essential administrative infrastructure and dispute resolution mechanisms required to manage public key cryptography.

The Guidelines deal with the type of infrastructure needed for a system in which trusted third parties in the role of certification
authorities (CAs) provide a service limited to screening the online identity of parties at the moment the decision is made to issue a digital signature certificate. There is no substantive regulation of how the CA makes the decision to issue a certificate beyond requiring that it disclose in its certification practice statement the procedures that it will follow. A CA has certain duties with regard to disclosing digital signature certificates and making information regarding the revocation of certificates available to relying parties; however, the Guidelines do not contemplate any active monitoring by the CA of the continued validity of any of the information provided by a subscriber. The Guidelines provide that a CA that has complied with the Guidelines, including fulfillment of the obligations that it has undertaken in its certification practice statement, is not liable for any losses incurred by a subscriber or by a relying party.

This limit on the potential liability of the CA to subscribers and relying parties, above and beyond any liability that it has expressly undertaken and set forth in its certification practice statement, is a pivotal risk allocation rule in the Guidelines. It stands in marked contrast to the Article 4A wire transfer rules and the consumer credit card and EFT rules, in which the providers of the technology remain on the hook for at least some of the risk of unauthorized or fraudulent use of the technology. The drafters of the Guidelines recognized that, without contractual privity between the CA and the relying party, and in spite of contractual terms that attempt to bind the subscriber to the terms of the CA's certification practice statement, there was a substantial risk that a court might entertain the claims of disgruntled subscribers or relying parties that the CA should be held liable for some or all of the losses that those parties might suffer in transactions in which the CA's certificates were used. The lack of legal precedent regarding the duties of CAs created an undesirable ambiguity from the point of view of potential CAs, particularly because case law drawn from analogous situations was not very favorable to the CA position. For example, in Kline v. First Western Government Securities, Inc., the court refused to grant summary judgment to a law firm that denied its liability to investors based on opinion letters that the law firm issued to an investment firm marketing tax shelters. The opinion letter

336. See id. § 3.7, at 86-87.
337. See id. § 3.2, at 80-81.
338. See id. § 3.11, at 89-95.
339. See id. § 3.14, at 99-100.
340. See supra notes 198-318 and accompanying text.
341. 24 F.3d 480, 490 (3d Cir. 1994).
described the effectiveness of those investments as tax shelters, after the IRS disallowed the investments as tax shelters. The court noted that, notwithstanding the attempt of the law firm to limit its potential liability to investors by stating in the opinion letters that they were for the exclusive use of the investment firm, the law firm knew that the investment firm was distributing copies of the opinion letters to prospective investors to encourage them to invest. Cases such as *Kline* indicate that a CA might reasonably be concerned about its ability to limit its liability to the terms set out in its certification practice statement. If the Guidelines are as influential as their drafters hope in shaping legislation on authentication procedures, then CAs will enjoy statutory limitations on their potential liability to subscribers and relying parties.

Because the starting point for the analysis of security issues in the Guidelines is public key cryptography, the Guidelines place a great deal of emphasis on communication security and much less emphasis on system security beyond the system maintained by the CA. While the Guidelines require that a CA maintain a "trustworthy" system and insure that its employees and contractors support the maintenance of that trustworthy system, there is no requirement that a subscriber maintain a trustworthy system except when generating a key pair. However, a subscriber is obliged to safeguard a private key corresponding to the public key in the certificate; the commentary to the Guidelines suggests that the standard of care involved in safeguarding a private key should be higher than the standard of care imposed by federal law on credit card or ATM card holders. While it might be possible to define what constitutes a trustworthy system for a CA with reference to guidelines developed in military and financial services contexts, it is unclear what an appropriate level of security is for an individual using public key cryptography for household or personal use on an individual personal computer.

Although the Guidelines provide no guidance on the question of how subscribers or relying parties are expected to implement this technology, and thus no basis for predicting its reliability in actual commercial applications, the Guidelines nevertheless recommend the

---

342. See id. at 482-83.
343. See id. at 483-84.
344. See generally INFORMATION SECURITY COMMITTEE, supra note 2 (dealing at length with communication security in particular).
345. See id. §§ 1.35, 3.1, 3.4, 4.1, at 69-101.
346. See id. § 4.3, Comment 4.3.2, at 104.
347. See supra notes 32-47 and accompanying text for a discussion of security risks to personal computers that are not understood by most individual computer users.
enactment of presumptions regarding the validity of electronic messages that have been digitally signed using public key cryptography.\textsuperscript{348} The commentary makes clear that these presumptions are meant to track the presumptions in negotiable instruments law, although at the time the Guidelines were written there were no commercial applications of this technology in use.\textsuperscript{349} However, the presumption of validity of signatures associated with negotiable instruments developed slowly in response to actual experience with commercial practices.\textsuperscript{350} Any presumption of validity that attaches to the use of public key cryptography at present must be based on confidence in the efficacy of the design of the technology itself, not on any evidence of how the technology is actually used in practice in electronic commerce systems.

By focusing a particular vision of the type of public key infrastructure necessary to facilitate a form of global electronic commerce that may develop in the future, the Guidelines may fulfill their stated mission of giving legal effect to the technology. Yet they fail to address in a systematic fashion the fundamental business concerns of the electronic contracting parties today who will play the roles of subscribers and relying parties under the Guidelines. Electronic commerce is still commerce, and parties enter into contracts when all the business risks associated with the transaction have been estimated and assessed. In addition to the risks of mistaken identity or lack of message integrity addressed by public key cryptography, contracting parties need other information regarding possible conflicts of laws. For example, if the parties do not reside in the same jurisdiction, there is the risk of being haled into court in a remote and hostile jurisdiction in the event of a dispute arising out of the transaction. Other unknowns are the legal capacity of the other party to enter into a contract if the other party is a business organization rather than a natural person and, perhaps most fundamentally, the ability of the other party to fulfill its contractual undertaking. The Guidelines are silent on how these basic business concerns will be addressed in electronic commerce based on public key cryptography.\textsuperscript{351}

\textsuperscript{348} See \textsc{Information Security Committee}, supra note 2, § 5.6 at 117-18.

\textsuperscript{349} See id. § 5.6, Comment 5.6.5, at 119.

\textsuperscript{350} The presumption did not exist in the Negotiable Instrument Law, the uniform law that was the predecessor to UCC Article 3. See U.C.C. § 3-307, Comment 1 (1989).

\textsuperscript{351} See generally \textsc{Information Security Committee}, supra note 2 (declining to address these issues).
Instead, the Guidelines discuss at great length the rights and obligations of the parties with respect to what the drafters presumed would be the primary activity of a CA—issuing certificates. The model of organization of the CA’s services in the Guidelines corresponds closely with the organization of some of the services offered by VeriSign, Inc., the first commercial CA to offer its services to the public in the United States. VeriSign offers “Digital IDs” from its web site, which are essentially all-purpose IDs for the Internet. In July 1997, VeriSign had three classes of digital signature certificates for individuals. These include Class 1 Digital IDs that indicate only the uniqueness of a name and e-mail address in VeriSign’s database; in issuing a Class 1 Digital ID, VeriSign verifies the applicant’s e-mail address. VeriSign does not intend these certificates for commercial use where proof of identity would be required; rather, these certificates are intended for use in web-browsing and certain e-mail applications. Class 2 Digital IDs provide a slightly higher level of assurance of the applicant’s identity, as VeriSign checks his or her personal identity information against a commercial credit database and performs other validation procedures. However, there is no requirement that the subscriber appear in person before a trusted third party as part of the identification process. VeriSign intends that these certificates be used in such applications as e-mail applications, online subscription services, and password replacement. A Class 3 Digital ID from VeriSign requires the applicant to personally present appropriate identification documents to a notary public or a VeriSign-approved local registration authority. VeriSign intends these certificates to be used in such applications as e-banking, corporate database access, personal banking, and membership-based online services. In response to the criticism that

355. See id. ¶ 2.2.2.
356. See id.
357. See id. ¶ 2.2.3.
the VeriSign marketing strategy exposes consumers to unreasonable risks for unauthorized use of their digital ID, VeriSign’s Class 1 Digital IDs include $1,000 of insurance against the loss of use or corruption of the ID; the Class 2 Digital ID+ product includes $25,000 of insurance.\textsuperscript{359}

In applying for and accepting a Digital ID, the subscriber agrees to the terms of the Subscriber Agreement,\textsuperscript{360} which incorporates by reference VeriSign’s Certification Practice Statement (CPS).\textsuperscript{361} The VeriSign CPS Version 1.2 is 104 pages long. The “Quick Summary of Important CPS Rights and Obligations” points out that the subscriber has an obligation to keep his or her private key secure from compromise in a trustworthy manner but assures the subscriber that the software system should provide this functionality.\textsuperscript{362} Within the CPS itself, however, the allocation of risk is made more explicit, and without any reassurances as to the likely functionality of the subscriber’s software system:

\begin{quote}
EACH CERTIFICATE APPLICANT (AND, UPON APPROVAL, EACH SUBSCRIBER) ACKNOWLEDGES THAT SUCH PERSON, AND NOT VERISIGN (OR THE APPLICABLE IA [issuing authority]), IS EXCLUSIVELY RESPONSIBLE FOR PROTECTING HIS, HER, OR ITS PRIVATE KEY(S) FROM COMPROMISE, LOSS, DISCLOSURE, MODIFICATION, OR UNAUTHORIZED USE.\textsuperscript{363}
\end{quote}

The public key infrastructure as described in the ABA Digital Signature Guidelines and as currently marketed by VeriSign provides consumers with some insurance coverage to lower their possible liability for unauthorized use. This is in marked contrast with the federal regulatory regimes for credit cards and EFTs that cap consumer

\begin{itemize}
\item \textsuperscript{359} The NetSure protection plan is an enhanced warranty service provided to subscribers (not to relying parties) that protects against certain risks of compromise, impersonation, delay in properly communicating a request for revocation or suspension, unauthorized suspension or revocation, loss of use, or erroneous issuance. See id., NetSure Protection Plan (visited Mar. 3, 1998) <http://www.verisign.com/repository/netsure/>,
\item \textsuperscript{361} See id., VeriSign Repository (visited Mar. 3, 1998) <http://www.verisign.com/repository>.
\item \textsuperscript{363} See id. ¶ 4.1.1.
\end{itemize}
At this time, there is no way to know whether or not the NetSure insurance offered to VeriSign subscribers will adequately offset any potential liability arising out of using the Internet for financial and commercial transactions. The risk that it will not is on the promoter and developer of the technology.  

The allocation of risks between the CA as the vendor of a technology service and the consumer of that service is in marked contrast with the allocation of risks between the bank and its customer set up under UCC Article 4A. The drafters of Article 4A conditioned the ability of the technologically more sophisticated party to shift the risk of unauthorized payment orders onto the less technologically sophisticated party on the implementation of a commercially reasonable security procedure. This allocation of rights and responsibilities corresponds with the creation of closed systems in which the parties are willing and able to negotiate individual agreements and within which new customers are signed up only after considerable "out of band" or "back channel" communications.

The business model implicit in the Guidelines and implemented by VeriSign is based on the assumption that the CA will not invest any effort in learning about the subscriber's circumstances, nor will it make any meaningful disclosure to the subscriber regarding the appropriate level of security procedures that the subscriber should implement. Instead, VeriSign uses a complex, lengthy legal document, incorporated by reference into the subscriber's agreement, to disclaim any responsibility for ascertaining the subscriber's competence to live up to its assigned responsibilities or its comprehension of the potential risks that it is undertaking in subscribing to VeriSign's service. This allocation of risk is a logical consequence of its mass-market, low-price business model. For an annual fee of $9.95 or $19.95, VeriSign has not collected enough in fees to cover the costs of negotiating individually with its subscribers or investigating their circumstances.

The service that VeriSign is offering consumers has a very low initial price and, in combination with the new NetSure insurance program, may offer very good value to the consumer. However, until the risks of Internet electronic commerce are better understood, it is possible that consumers may discover to their dismay that the real

364. See supra note 307 and accompanying text.
costs of a VeriSign Digital ID are much higher than they initially understood. The real costs to merchants and consumers participating in the emerging Internet marketplace should be measured by adding the costs of adequate system security to the costs of communication security provided by public key cryptography and a digital signature certificate. Closed systems for Internet commerce more accurately reflect this real total cost in their pricing structure by explicitly pricing the costs of setting up a public key infrastructure that is adapted to the special requirements of the group using it. In the absence of the kind of safe harbor for CAs that the Guidelines advocate, a mass-market CA such as VeriSign will be under pressure to modify upward its pricing structure, with any increase in prices representing an implicit insurance premium collected to compensate the CA for assuming more of the risks associated with Internet commerce. A similar result could be achieved by mandating a cap on total subscriber liability, not just liability per transaction as VeriSign now offers. For a certificate to have much value for merchants in a system with caps on total subscriber liability, the CA would have to add some sort of online monitoring of the subscriber’s total liability similar to that now provided by credit card issuers. The overhead associated with such a monitoring service would drive up the prices charged subscribers for certificates.

In the Guidelines, as in the VeriSign product line, it is presumed that the person signing is the proper customer of the CAs services, not the contracting party relying on the signature. If this is the case in practice, merchants relying on public key certificates have no overhead beyond maintaining their own digital signatures and software capable of processing information about their customers’ signatures. The merchants as relying parties are presumed not to be the primary customer of the CA’s services. In order to bridge the gap between the technology of public key cryptography and the legal concept of a signature as evidence of intent to be legally bound, the party accepting the digital signature certified by the CA should have to have some evidence of the context within which the digital signature was affixed to the record. Knowledge of the security built into the encryption software is one part of what the contracting partner will wish to know. However, as with the facsimile signature devices or the wire transfer security procedures, mere evidence that the software was used without any information about who was using the software will make it very hard for a contracting party to overcome a claim that the use of the

367. See generally INFORMATION SECURITY COMMITTEE, supra note 2.
software was unauthorized. The mass market certification services offered by VeriSign and contemplated by the Guidelines therefore offer only a partial solution to the merchant wishing to market goods and services over the Internet. The merchant will have the choice of going outside a public key infrastructure by either directly contacting its customers using an “out of band” or “back channel” communication, contracting with another service provider for additional screening services, or including in its pricing a higher risk of default due to unauthorized use of authentication procedures.

2. Minimalist Enabling Legislation

In 1997, Rhode Island enacted digital signature legislation that rejects the approach taken by the Guidelines, adopting instead a “technology neutral” approach that creates a level playing field between traditional commercial practices and electronic commerce without modifying any existing loss allocation rules or creating any new ones.\textsuperscript{368} The Rhode Island legislation was based on a model developed by the legal staff of the Information Technology Division of the Commonwealth of Massachusetts through an open consultative process.\textsuperscript{369}

The Rhode Island legislation defines “[e]lectronic signatures” as “an electronic identifier, created by a computer, and intended by the party using it to have the same force and effect as the use of a manual signature.”\textsuperscript{370} With regard to any rule of law that requires a signature, that rule is now deemed satisfied by an electronic signature.\textsuperscript{371} With regard to whether an electronic signature was executed or adopted with respect to an electronic record by a particular person, the trier of fact may consider any relevant information or circumstances, including whether the signature is unique to the signer, whether unauthorized persons have had the opportunity to create the signature, whether the signature is capable of verification, and whether the reliability of the method used to create, store, and communicate the signature was appropriate for the purposes for which it was created.\textsuperscript{372} However, the statute further provides that its terms shall not apply when its application would involve a construction of a law that is

\begin{footnotesize}
\begin{enumerate}
\item[368.] See Rhode Island Electronic Signatures and Records Act, R.I. GEN. LAWS § 42-127 (1997).
\item[369.] Information on the Massachusetts ITD efforts is available from the ITD web site at \texttt{<http://www.magnet.state.ma.us/itd/legal>} (visited Jan. 21, 1998).
\item[370.] R.I. GEN. LAWS 42-127-3(a).
\item[371.] See id. § 42-127-4(a).
\item[372.] See id. § 42-127-4(c).
\end{enumerate}
\end{footnotesize}
clearly inconsistent with the manifest intent of the lawmaking body or is repugnant to the context of the law, provided that the mere requirement of a "signature" or that a record be "signed" shall not be itself sufficient to establish such an intent.\(^{373}\)

This legislation is neutral with regard to the various models of Internet electronic commerce currently in use—closed models based on bilateral, bound community membership, or robust local administration models, or open models based on server or client security. Each of these models will face the same risks of being tested in litigation, and none will benefit from a statutory blessing for its internal model for allocating risk and responsibility.

Within concrete dispute resolution processes, the equities of actual cases will be weighed and the actual circumstances of the parties involved will be taken into account. The provisions of the statute provide guidance to a finder of fact in identifying circumstances that will clarify the issue of what the parties' actual intent was when using the electronic signature as an authentication procedure.\(^{374}\) No legislative imprimatur is given to a particular implementation of a specific technology, so there is no impediment to the continued development of new commercial authentication products, whether based on cryptography, biometrics, tokens, or some combination of all three.\(^{375}\)

**B. UCC Article 8 and the Danger of Drafting Technology-Specific Commercial Law**

The first article of the UCC expressly to address the impact of information technology on commercial practice was Article 8 governing investment securities.\(^{376}\) Article 8 was systematically revised first in 1978, and then again in 1994, in an effort to accommodate the use of new technology to streamline the process of clearing and settling securities trades.\(^{377}\) The 1978 revision of Article 8 was courageous in its effort to anticipate the manner in which new technologies would be implemented, yet ultimately failed to achieve its goal of ushering in a new era of efficiency in the securities settlement system. The 1994 revision was based on a careful

\(^{373}\) See id. § 42-127-4(e).

\(^{374}\) See id.

\(^{375}\) See id. § 42-127-4(a).

\(^{376}\) See U.C.C. art. 8 (1996).

\(^{377}\) See James Steven Rogers, Policy Perspectives on Revised UCC Article 8, 43 UCLA L. Rev. 1431, 1435 (1996).
examination of actual industry practices and adopted provisions that harmonized with those practices.\textsuperscript{378}

The original 1957 version of Article 8 was based on the assumption that possession and delivery of physical certificates were the basis of the securities holding system.\textsuperscript{379} Stock certificates were sent to the issuer or a transfer agent to be reissued in the name of the new owner. By the late 1960s, this cumbersome, time-consuming process began to threaten the ability of banks and broker-dealers to achieve timely settlement for stock trades. The drafters of the 1978 revisions envisaged a system in which uncertificated securities would be maintained as computer records on the books of issuers or their transfer agents and stock transfers would be effected by electronic book entry.\textsuperscript{380} This vision was a generalization from the first large-scale implementation of electronic securities transfers accomplished for United States government securities. U.S. government securities have existed only as electronic records in federal government computers since the 1970s, and the drafters reasonably inferred that the private sector would adopt this model for converting paper-based transfer systems to electronic systems.\textsuperscript{381}

Many of the arguments being made today in support of technology-specific legislation to promote the development of a public key infrastructure is remarkably similar to the rhetoric used to justify the technology-specific approach of the 1978 Article 8. The drafters of Article 8 argued that, without the certainty that their statute would provide, the natural and inevitable movement of the securities industry toward the most efficient new electronic practices would be needlessly delayed.\textsuperscript{382}

The system envisaged by the drafters of the 1978 Article 8 failed to materialize, however. The banks and broker-dealers, in cooperation with the Depository Trust Company (DTC—a trust company organized for the benefit of its participants) and the National Securities Clearing Corporation (NSCC), devised their own solution to the problem. A system of “indirect” holding developed in which DTC maintained “jumbo” certificates, representing shares in its possession, and transferred securities by adjustments to participant’s accounts at

\begin{itemize}
  \item \textsuperscript{378} See id.
  \item \textsuperscript{379} See U.C.C. art. 8, Prefatory Note (1995).
  \item \textsuperscript{380} See Charles W. Mooney, Jr., Beyond Negotiability: A New Model for Transfer and Pledge of Interests in Securities Controlled by Intermediaries, 12 CARDOZO L. REV. 305, 311 (1990).
  \item \textsuperscript{381} See Martin J. Aronstein, Robert Haydock, Jr. & Donald A. Scott, Article 8 Is Ready, 93 HARV. L. REV. 889, 890-93 (1980).
  \item \textsuperscript{382} See id. at 914.
\end{itemize}
Participant banks and broker-dealers in turn provided similar services to their own customers. The 1978 Article 8 could not accommodate this system, because it was based on the assumption that investors would own securities directly, either in the form of physical certificates or as book entries in the accounts of issuers or transfer agents. Following record trading levels during the stock market crash in October 1987, serious concerns arose over the ambiguous legal status of actual industry practices and how that might adversely affect the ability of regulators or industry to respond to the failure of a major market participant.

Given the failure of the 1978 revisions to anticipate the direction of future developments, together with the fact that both direct and indirect holdings of securities are now in use in the current system, the drafters of the 1994 Article 8 strove to maintain neutrality with regard to how market participants would implement technology. In addition, the drafters sought to establish clear and certain rules that would make the operation of the securities holding system more transparent. This would promote finality of settlements, reducing investors' risk of loss from the failure of another financial intermediary within the system.

Rather than try to capture the complex relationships between investors and financial services intermediaries in the provisions of Article 8, the drafters defined new terms, including "security entitlement" and "entitlement holder." A security entitlement arises when a financial asset is credited to a securities account maintained with a financial intermediary. Article 8 describes what a holder of a securities entitlement can expect from a financial intermediary—that it must maintain sufficient financial assets to satisfy the claims of all its entitlement holders and that the intermediary's financial assets that are held for the entitlement holders are not the property of the intermediary nor are the assets subject to the claims of the intermediary's general creditors. The drafters of

383. See Mooney, supra note 380, at 317-18.
384. See id.
385. See Rogers, supra note 377, at 1445-46.
386. See id.
387. See id. at 1446.
388. See id. at 1442-45.
389. See U.C.C. § 8-102(a)(17) (1996); see also Mooney, supra 380 (for the first suggestion of this concept).
391. See id. § 8-501.
392. See id. §§ 8-503-8-504.
revised Article 8, like the drafters of the ABA Digital Signature Guidelines, worked to create an original conceptual framework for commercial practices that differed markedly from historical models. The drafters of revised Article 8, unlike the drafters of the Guidelines, were defining new legal concepts to describe existing commercial practices. The agenda of the drafters of the Guidelines was set not simply by a desire to anticipate future developments but also to guide those developments toward the use of what the drafters believed was a superior technological solution. The experience of the drafters of the 1978 Article 8 demonstrates how uncertain the outcome can be of attempts to use law to direct the choice of technology in commercial practices.

C. Assigning Liability for Fraud or Error in the Use of Rapidly Evolving Technology

The rapid emergence of Internet commerce and the jockeying of various interest groups for places in this emerging landscape is putting pressure on legislatures to consider devising a regulatory regime even before it is clear which business models will be successful for the Internet and which will not. The Clinton administration’s position on Internet electronic commerce is that, in the absence of information indicating the need for regulation, legislatures should hesitate to intervene in the working of the marketplace. Nevertheless, in light of the existing law of signatures, the experience of revising the UCC to take account of emerging technologies, and current legislative initiatives in the area of electronic commerce, certain conclusions may be drawn regarding appropriate legislation in this area.

1. Presumptions and Reasonable Authentication Procedures

No presumptions of validity should attach to an authentication procedure based exclusively on an assessment of the technology embodied in it. The validity of signatures under general principles of contract law is determined in light of the circumstances surrounding the execution of the signature. While negotiable instruments law departs from this general rule to create the presumption of the validity of a signature, this is based on generations of experience with the use

393. The mere willingness of major multinational corporations to invest millions of dollars in a business model is no guarantee of its likely success, as was recently demonstrated by the flop of interactive TV. See Mike Mills, Time Warner to Drop Interactive TV Project, WASH. POST, May 2, 1997, at G1.

of negotiable instruments in commerce. Furthermore, the harshness of negotiable instruments law is ameliorated with regard to consumers generally by modern regulatory modifications of traditional commercial law doctrines. With regard to electronic commercial practices designed for and primarily targeted at consumers, there are caps on consumer liability for unauthorized use that mitigate the need to disclose fully and accurately to consumers the potential risks that they face from adopting the technology.

Commercial applications of the Internet are being aggressively marketed at consumers with disclosures that seem unlikely to communicate effectively to consumers the potential risks that they face from adopting these technologies. In the absence of any caps on liability for consumers or provisions for dispute resolution procedures on terms that guarantee consumers a meaningful opportunity to contest their liability, there should be no presumption that increases the already substantial burdens that any consumer will face in contesting the validity of an unauthorized use of an authentication procedure. The strategy of the Guidelines in proposing evidentiary presumptions regarding the validity of digital signatures seems to be to promote the acceptance of digital signatures by granting relying parties an effective enforcement mechanism. A more equitable and efficient way to promote the use of digital signatures can be accomplished by the development of digital signature applications that are cheap and easy for consumers and merchants to use. This is because the prudent design of security systems will include digital signatures as a matter of principle once the total cost of adopting this technology is less than the expected loss that might result from a breach of security that this technology can prevent.

If any authentication procedure should be presumed valid, it should be a “reasonable authentication procedure” modeled after the commercially reasonable security procedure of UCC Article 4A or the evidentiary factors that the Rhode Island electronic commerce statute advises the trier of fact to consider. The concept of reasonable authentication procedure should include some reference to the circumstances of the signer that are or that should have been known by the other contracting party. These factors might include: information about how access to the authentication procedure is controlled by the signer; whether the product of the authentication procedure will reveal any attempts to modify it after the completion of the authentication procedure; whether the product of the authentication procedure can be verified with reference to some external and trustworthy standard of comparison; whether the product of the authentication procedure is
unique to the party to be bound by its use; and the reliability of the authentication procedure in light of the intended use of the procedure.

2. Assigning Liability in Order to Reduce the Rate of Loss

Fraud losses are inevitable in any commercial market. While it is not yet clear whether fraud losses in Internet commerce will be greater or less than those in more established markets, it is certain that losses will occur. Public key cryptography is a powerful tool to counteract some of the threats to electronic commerce, but unless its deployment is integrated into an overall strategy of risk management then the security that it offers may be illusory. The power of public key cryptography to safeguard communications may create a "steel doors and paper walls" problem if those who rely on it fail to consider the other factors contributing to system security.395

The intense focus on the length of keys used to encrypt messages is an example of this kind of skewed emphasis in analyzing computer security problems. A great deal of publicity has surrounded the recent successful brute force attacks on 40-bit and 56-bit keys.396 The press coverage of these feats of cryptanalysis often fail to point out the huge commitment of computing resources required to break these keys to decrypt a single message. The risk to a security system from attacks on the system, or on the human administrators of the system, may be much greater because it can achieve greater results for the interloper with much less effort.397

Incentives for the more technologically sophisticated participants to define and encourage the maintenance of an appropriate level of security for the merchants and consumers in the Internet marketplace should be incorporated into any statutory regime that governs the legal

395. This metaphor was suggested by Susan Nycum, Esq., of Baker & McKenzie, Palo Alto, California.
396. Responding to a $10,000 challenge from RSA Data Security, Inc., U.C. Berkeley graduate student Ian Goldberg broke a 40-bit key—the most secure data encryption the U.S. government allows for export—in three and a half hours. Goldberg broke it by linking 250 workstations and programming them to run all possible combinations at a rate of 100 billion per hour. See Sharon Machlis, RSA Stunt Shows Up Encryption Weakness, COMPUTER WORLD, Feb. 3, 1997, at 1. In June 1997, responding to a $10,000 challenge from RSA Data Security, a loosely organized group of cryptography industry experts managed to break a 56-bit key after five months of work. The group distributed code-breaking software over the Internet and used idle computers around the world to perform the calculations. See Lynda Radosevich, Hackers Prove 56-bit DES Is Not Enough, INFOWORLD, June 30, 1997.
397. For example, video pirates sold decoder boxes to unscramble satellite TV broadcasts that did not break the encryption but penetrated the system that deployed the encryption. See GARENFEL & SPAFFORD, supra note 35, at 199. Similarly, some successful attacks on Netscape's SSL protocol have been based on the weakness of the system, not on the encryption. See id.
effect of authentication procedures in Internet commerce. It is clear that many of the merchants and consumers entering or considering participation in the Internet marketplace today are not competent to evaluate the security of the systems they are using and that the information being provided by many technology developers with their products is not likely to build that competence. Technology vendors are so busy racing to stake claims on the frontier of electronic commerce that the experience of the end users is not fully considered. The technology of Internet commerce is changing and developing rapidly. However, with appropriate incentives, technology vendors may be able to develop products that permit less technologically sophisticated parties to maintain trustworthy systems with a minimum of effort.

VeriSign’s response to the criticism that consumers of its Digital IDs face unreasonable risks from losses due to unauthorized use of the subscriber’s private key is an example of this process. VeriSign as CA provides only the limited review functions described in its CPS before issuing a certificate and does not have any involvement in subsequent transactions conducted in reliance on the information in the certificate, beyond making a certification revocation list available for the reference of a relying party. However, a relying party can be expected to take note of information included in the certificate itself or incorporated into it by reference to some document available elsewhere. For example, a certificate will normally have an operational period, and reliance on the certificate after the expiration of that operational period would not be reasonable. The X.509 version 3 standard for digital signature certificates permits relevant information in the certificate to be added by the subscriber. Through the use of these extensions, the subscriber may set a dollar limit above which reliance on the certificate is not reasonable.

Setting a reliance limit in the certificate is only a partial solution, however. This certificate-based limitation on subscriber liability does not solve the problem for a subscriber if the private key and the certificate could be used by an interloper to enter into a large number of transactions in an extremely short period of time, creating an aggregate liability far in excess of the transaction limit. VeriSign’s NetSure insurance scheme is a partial solution to this problem in that it

399. See INFORMATION SECURITY COMMITTEE, supra note 2, § 5.4, at 112-13.
400. See FORD & BAUM, supra note 98, at 384.
401. See id. at 223.
INTERNET COMMERCE REGULATION

provides warranties to the subscriber that it will not be liable for unauthorized use or disclosure of the subscriber's private key during the period in which the Digital ID certificate is valid.\footnote{\textsuperscript{402}}

The problem might be capable of resolution through the use of policy extensions that communicate to a relying party additional limitations on the authorized use of the digital signature.\footnote{\textsuperscript{403}} One such policy extension that a consumer might request would be that no transaction over $10 is a valid obligation of the consumer unless the relying party establishes some "out of band" or "back channel" communication with the consumer, such as a phone call to confirm the agreement.\footnote{\textsuperscript{404}} While use of such a policy extension will raise the transaction cost for each transaction entered into by a consumer using a digital signature, the increased transaction cost will not necessarily reduce the total number of transactions conducted over the Internet. If consumers come to believe that the Internet is not yet secure enough for retail transactions in the absence of an absolute cap on consumer liability such as the liability limit on credit card transactions, then in the absence of consumer protection legislation capping consumer liability the total volume of consumer transactions not conducted using credit cards may remain small.

If consumers of new technologies are provided adequate disclosures regarding reasonable security practices, then consumers can make a meaningful contribution to the overall incidence of losses due to unauthorized use or fraud. However, empirical evidence on the behavior of market participants, whether consumers or supposedly more sophisticated parties, indicates that there are very real cognitive limitations on the ability of market participants to make decisions on a fully informed and rational basis.\footnote{\textsuperscript{405}} In the words of Herbert Simon, the Nobel laureate economist, "The scarce resource is computational capacity—the mind."\footnote{\textsuperscript{406}} Simon noted that market participants will exercise a bounded rationality in decisionmaking because of the inherent limitations on time, effort, and comprehensional capacity. The fact that human actors are not capable of achieving perfect

---

\footnote{\textsuperscript{402}} The warranty to the subscriber does not apply, however, if the subscriber fails to exercise "reasonable care" in safeguarding his or her private key. See VeriSign Web Site, Netsure Protection Plan (visited Jan. 21, 1998) <http://www.verisign.com/repository/netsure/>.

\footnote{\textsuperscript{403}} See FORD & BAUM, supra note 98, at 285.

\footnote{\textsuperscript{404}} Cem Kaner, J.D., Ph.D., suggested this.


rationality in analyzing problems does not suggest that their problemsolving techniques are unpredictable or random. The deviations from formally rational analysis of problems is often quite predictable with reference to concepts such as endowment effects and loss aversion, framing, self-serving bias, unrealistic optimism, and anchoring. 407

If the biases and heuristics used by consumers in analyzing electronic commerce problems can be established empirically, then the manner in which liability is allocated to consumers and the magnitude of the risks of loss allocated to consumers can be designed to take advantage of the contribution to system security that consumers realistically can be expected to make. Beyond that point, however, a rational system of loss allocation for electronic commerce should shift the losses either to the technology developers or to an insurance system. For example, a technology developer might incorporate greater use of biometric or token technologies that do not depend on constant vigilance for their effectiveness in consumer electronic commerce applications. The increased cost of personal computers incorporating biometric technologies, such as authentication procedures using fingerprints or smartcard readers, charged to all users of the system would operate as a form of insurance.

V. CONCLUSION

Commercial law is in the process of adapting to meet the challenges posed by electronic commerce conducted over open networks. Authentication procedures are an essential element in the security policies and procedures that will be essential to the commercial exploitation of the Internet. Although electronic communications are an integral element of Internet commerce, and encryption provides a strong solution to the problems of authentication and communication security, the mere fact that public key encryption has been used is only part of the information needed to establish the intent of the parties to form a binding contract.

The rush to bring to market products using public key encryption has encouraged the developers and promoters to seek legislative safe harbors to permit them to focus on the work of constructing a public key infrastructure of potentially global reach. However, sheltering the developers of these new technologies while allocating the risk of loss due to unauthorized or fraudulent use of the technology to less sophisticated consumers of the technology will undermine the

developers' incentives to continue to improve the overall security of Internet commerce systems. Refraining from legislation, or legislating to provide some protection to less sophisticated consumers, will permit the market to continue to develop without the distorting effects of unresponsive or burdensome regulation.