Murdoch University Electronic Journal of Law

A Consumer's Analysis Of The Electronic Currency System And The Legal Ramifications For A Transaction Gone Awry

Authors: Mark Ishman
John Marshall Law School
Quincy Maquet
John Marshall Law School

Issue: Volume 6, Number 3 (September 1999)

Contents

Introduction

1. Imagine, instead of walking into a book store to browse and purchase the latest novel, one may simply log onto the World Wide Web (Web), browse through thousands of abstracts and purchase the novel - all in the convenience of your own home. Imagine no more. Today's technology enables yesterday's dreams. Due to the new development of electronic currency, an online purchase is just a few clicks away.

2. This Comment argues that the utilization of digital signatures in electronic currency provides a secure means of conducting transactions in electronic commerce. Additionally, this comment analyzes and argues that both federal and state laws provide more than adequate remedies for an injured party in an electronic currency transaction. Part II of this Comment explains the purpose, the significance and the traditional role of the notary. Part II also provides the basics of the digital signature process as it relates to each participant. The players in the digital signature process consist of the sender, the recipient and the certification authority. Furthermore, Part II explains the development, application and major participants in electronic currency. Part III analyzes and argues why the use of electronic currency is the securest means of conducting transactions in electronic commerce. Part III also argues that since electronic currency transactions use digital signatures, parties to such transactions will enter into legally binding contracts. Finally, Part III argues that both federal and state laws provide more than adequate remedies to damaged parties in an electronic currency transaction. Party IV of this Comment concludes that electronic currency transactions will not only facilitate electronic commerce, but also transform the way we will conduct our daily lives.

Background

Notaries

3. For over 350 years, notaries have been present on the North American continent.[1] Presently, all fifty states and the District of Columbia have statutes governing the actions of notaries.[2] Contained in these statutes are several requirements that most states include in their application procedures. First, most states require that the applicant be at least eighteen years of age.[3] Second, most states require that the applicant obtain a bond.[4] However, most states do not have a minimum residency requirement in their respective notary statutes.[5] Additionally, only a few states mandate testing of notary applicants before receiving their commissions or licenses.[6] According to many scholars, an increase in testing by states would considerably improve the notary's performance.[7]

4. The official duties of today's notary are ministerial or clerical in nature.[8] Even though a notary is described as a "public officer,"[9] notary responsibilities do not encompass an element of judicial discretion.[10] A notary public's authorization extends to "notarial acts" which include: (1) taking an acknowledgment; (2) witnessing or attesting a signature; and (3) administering an oath or affirmation, e.g., given to witnesses, and to public officials when sworn into office.[11] However, the primary duty of today's notary pertains to authenticating a written instrument by attaching his official certificate.[12]

5. When attaching his official certificate, all states require notaries to positively identify the party seeking the notarization.[13] Specifically, the notary "must determine, either from personal knowledge or from satisfactory evidence, that the person appearing before the notary and making the acknowledgment is the person whose true signature is on the instrument."[14] Due to this requirement, courts have found

that the individual seeking a notarization must appear personally before the notary.[15]

6. However, many notaries have accepted the non-appearance of an individual, when the individual telephones and acknowledges the signature and terms of the agreement.[16] Yet, the fact remains that with just a voice and no physical body present to observe, the notary cannot be sure of the speaker's identity. Even if the voice on the other end of the line is familiar to the notary, it is possible that, unknown to the notary, someone is threatening the individual. Therefore, courts have been reluctant to waive the physical presence requirement for a telephone acknowledgment.[17]

7. As technology increases, the requirements of a notary must change with it because the physical presence requirement is not possible for transactions over the Internet. Therefore, many states are implementing digital signature laws that govern notaries in cyberspace. Specifically, these statutes have identified certification authorities (CA), or cybernotaries, which serve the function of a notary, but in cyberspace. A certification authority is a trusted third person or entity that determines the identity of a subscriber and certifies that the public key used to create a digital signature that belongs to that person.[18]

Certification Authority

8. Certification authorities are an essential part of the digital communications process. The reason for this is that the cryptographic system needs an impartial third party, i.e., a CA, to establish the authenticity of electronic transactions.[19] Like notaries, statutes will need to be enacted to create, authorize and regulate certification authorities.[20] Additionally, states will license and commission CAs in a similar manner that presently governs notaries.[21] Thus, CAs will be considered public officers, subject to the obligation to uphold the public trust that is bestowed upon them.[22] Unlike notaries, whom must be human beings, CAs can be entities, such as accounting firms, banks and real estate enterprises.[23]

9. CAs will be employed to confirm credentials in electronic commerce.[24] Naturally, parties to a contract should desire to verify the other's signature.[25] The CAs role is to verify the authenticity of the message sent to the recipient, therefore binding the parties to the transaction.[26] If this process is successful, the CA certifies the digital signature and "allows the deal to proceed under an umbrella of trust."[27] In essence, CAs will guarantee transactions.[28] Therefore, the CAs function is critical to the success of the electronic transactions throughout the United States.

10. The certification process generally works in the following way. First, the subscriber must generate both a public and private key.[29] A private key encrypts the text of the document into a digital signature and is kept in sole possession of the signer of the electronic document.[30] The public key, which can be freely distributed, allows the recipient to decrypt the sender's electronic document.[31] Next, the subscriber proceeds to contact the CA and produces proof of identity, such as a driver's license, passport or any other proof required by the CA.[32] Lastly, the subscriber demonstrates, without disclosing the private key, that he holds the private key that corresponds to the public key.[33]

11. Once the CA verifies that the identified person and a public key are associated, the CA then issues a certificate.[34] A certificate is "a computer-based record that attests to the connection of a public key to an identified person or entity."[35] If the subscriber discovers that the certificate is accurate, he may publish the certificate or direct the CA to do so in a repository.[36] By doing this, the certificate will be available to third parties wishing to communicate with the subscriber.[37]

12. The certification process is accomplished by the use of digital signatures. Therefore, to fully understand the certification process, we must first comprehend how digital signatures operate.

Digital Signatures

13. Digital signature technology has been in existence for nearly twenty years and is universally recognized as the most efficient and secure system for electronic commerce (E-commerce).[38] A "digital signature" is a term of art used within the technical community since the landmark publication regarding public key cryptography and its implementation in its most popular form, the RSA algorithm, by Whitfield Diffie and Martin Hellman in 1976.[39]

14. A digital signature is not a digitized version of a person's handwritten signature, but a transformation of an electronic document's text that is attached to the document itself.[40] The ABA Guidelines has defined a 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.[41]

15. To digitally sign a document, the sender creates a unique message digest (hash value) of the document by running a computer program.[42] Next, the program encrypts this message digest using the sender's private key.[43] This encrypted message digest is the digital signature.[44] Finally, the sender attaches the digital signature to the electronic communication and sends it to the intended recipient.[45]

16. A digitally signed communication looks like this:

    July 30, 1999
    Dear order department:
    We commit to the purchase of 10,000 gadgets at your price of $500 per hundred. Ship to:
    Gadget Products Co.
    1010 Purchase Street
    Chicago, Illinois 65504
    Sincerely,
    Purchasing Department,
    Gadget Products Co.
    --------*BEGIN SIGNATURE*-------
    OWHTwx1Sduuspo+dfdt=22ysbhadhcezamdDGGD5DDiASusffasdfasdUSSasdfdfFDD4dtofsdffusIipPse
    ajw3rlBdR/AnbfoL/ Eed5+adfdsf34343553j3ndsS4DDGcIlsqud3Dffsddrsncnzg34aSDMN2334/
    sdfe34se3ls97n/Tt33d3dNmysge34uyDuqt8msvereWe --------*END SIGNATURE*----------

    A digital signature, as described above, is done using a process of public-key cryptography.

17. **Cryptography**
    Using cryptography,[46] a person creates a digital signature.[47] There are two methods of cryptography: symmetric[48] and asymmetric[49] cryptography.[50]

18. Using asymmetric cryptography,[51] a digital signature is attached to an electronic transmission by the use of an electronic public and private key.[52] First, private keys are created by and should be known only to the document's signer.[53] Using this "secret" key, the signer places a "signature" onto a document.[54] The signature itself is actually a "hash"[55] (a string of letters, numbers, and/or symbols), representing the document coupled with the unique computer-generated code created by the document's signer.[56] To produce the signature, the document's signer types "in a pass[-]phrase (much

like a PIN number for a bank teller machine), and then the private key generates a long string of numbers and letters which represents the 'signature.'"[57] Since the computer-generated signature is unique to each document, the private key will generate a different sequence of digits, and thus, a new "signature" for each document.[58]

19. To ensure that the public record is verified as accurate, a third party, i.e., a CA, may be called upon to confirm that the public key indeed pairs to the private key and is associated with an identified person or company.[59] Using its own private key, the CA signs the public key to verify its accuracy and makes this certificate available to the key holder or to potential message recipients.[60] On the other end of the electronic transmission is the document's recipient, who holds the "public key."[61] Using the public key, the recipient can decrypt the sender's document and signature using a computer program.[62] The program matches the private and public keys to ensure that the document and the signature have not been modified prior to or during transmission.[63] Collectively, this process is known as "public key cryptography."[64]

> "Put simply, if a private key other than one identified with the subscriber. . . is used to encrypt the document, or if the document is changed in any way between execution and verification, the hashes will differ from each other and the signature will fail verification."[65]

Laws Governing the Use of Digital Signatures

20. In July 1997, Germany[66] and Italy enacted digital signature legislation, while the English, Swedish and Dutch governments were addressing the creation of their own digital signature legislation.[67] Likewise, many U.S. states have recently enacted digital signature statutes that permit the use of digital signatures.[68]

21. **American Bar Association Digital Signature Guidelines**
In order to assist legislatures in drafting digital signature legislation, the American Bar Association (ABA) created the ABA Digital Signature Guidelines (Guidelines).[69] These Guidelines are general statements of principle concerning the development of public key infrastructures,[70] with the intent to develop more exact rules within the federal and state legal systems.[71] Ultimately, the Guideline's substantive rules establish the legal duties of CAs, parties using CAs and any person using digital signature certificates.[72] Additionally, the Guidelines have also formed the basis for digital signature legislation in a number of U.S. states, namely Utah.

22. **The Utah Digital Signature Act**
With the assistance of the ABA Information Security Committee, Utah, aiming to promote E-commerce, developed its own digital signature legislation.[73] The Utah approach has four basic parts: (1) CAs must have trustworthy systems; (2) CAs have limited liability when they meet the legislative standards; (3) digital signatures produced by such CAs are legally presumed valid; and (4) giving the executive branch flexibility in regulation.[74]

23. The Utah Act also delineates three primary players in the certification process: (1) the subscriber; (2) the recipient; and (3) the CA.[75] The Utah Act details the CAs responsibilities[76] and limits who can qualify as a CA.[77] Additionally, a licensed CA must post a bond or letter of credit.[78] The Act also sets forth record keeping procedures, requires a regular audit of CAs,[79] and sets out procedures for a CA to follow when they cease to act as a CA or when they issue, revoke or suspend a certificate.[80] Moreover, the Utah Act specifies the information that must be included in the certificate.[81] Finally, licensing under the Utah Act is voluntary.

24. Following Utah's lead, all states have either enacted or proposed digital signature legislation to promote

E-commerce.[82] These statutes will not only allow for secure transactions, but also for new technology to prosper in E-commerce.

Electronic Currency

25. As Jerry L. Jordan, the president and CEO of the Federal Reserve Bank of Cleveland, explains, "[m]oney in the 21st century will surely prove to be as different from the money of the current century as our money is from that of the previous century. Just as fiat money replaced specie-backed paper currencies, electronically initiated debits and credits will become the dominant payment modes, creating the potential for private money to compete with government-issued currencies."[83]

26. With each passing day, new developments in electronic currency are emerging. As a result, novel buzzwords such as smartcards, online banking and electronic currency are being used to discuss money. However, what are these new forms of money? Who will use them? And how do they work?

What Is Electronic Currency?

27. Today, cash is known in various forms as a means of exchange and of storing value.[84] Mussels, gold and silver as well as standardized products such as cigarettes are only a few examples.[85] Although the coins and banknotes that are now abundant in their basic form have existed for thousands of years, the first bank note of the Swiss Federal State, surprisingly did not appear until 1907.[86] In 1918, the Federal Reserve Banks first began to move currency, i.e., manipulated book-entries to clear payment balances among themselves, via a telegraph.[87]

28. However, the widespread use of electronic currency did not begin until the automated clearinghouse was set up by the US Federal Reserve in 1972 to provide the US Treasury and commercial banks with an electronic alternative to check processing.[88] Similar systems also emerged in Europe around the same time. Thus, electronic currency has been widely used throughout the world on an institutional level for more than two decades.[89]

29. Today, nearly all of the deposit currencies in the world's banking systems are handled electronically through a series of interbank computer networks.[90] The Clearing House Interbank Payments System (CHIPS), owned and operated by the New York Clearing House, is one of the largest financial computer networks.[91] It is used for large-value funds transfers.[92] In 19[94] CHIPS and Fedwire combined to handle 117.5 million transactions for a total value of US$506.6 trillion.[93]

30. Although banks have been able to move currency electronically for decades, only recently has the average consumer had the capability to use electronic transfers in any meaningful way.94 The increasing power and decreasing cost of computers, coupled with advancements in communication technology have made global interaction available at vastly reduced costs. Together, these factors make the digital transfer of funds a reality for millions of individuals around the world.[95] As a result, we are now witnessing the development of a digital economy.[96]

31. Now, less than a hundred years after the first bank note was issued, technological progress has undoubtedly created a new direction in the means of payment.[97] The Internet and E-commerce have become an increasingly commercial area, where daily payments are rendered for goods, information and services.[98] As a result, electronic payments are becoming the central part to online business between customer and seller.[99] Traditional applications of rendering payment include credit cards,[100] private label credit/debit cards[101] and charge cards.[102]

32. However, these traditional forms of rendering payment online have posed problems to both the

consumer and the seller. Not all merchants are equipped to accept credit card transactions. Some merchants even prefer not to accept credit card transactions because credit card companies charge merchants a two to six percent service fee for each transaction.[103] Since smaller sales are a significant part of business transacted online, many online merchants do not accept credit card transactions due to their small profit gains.[104]

33. Additionally, consumers have become concerned with "hackers" intercepting and obtaining their credit card number stored on the Internet,[105] as well as the possibility of becoming a victim of fraud on the Internet since the customer and the merchant never physically meet.[106] Furthermore, as the data collection industry continues to grow, credit card companies are invading consumer's privacy by collecting their spending habits and reselling the data to third parties. Consumers are gradually realizing that providing their numbers to online merchants is no more hazardous than reciting it to a clerk over a telephone line.[107]

34. As a result of recent proliferation of computers, modems and telecommunications links, modern methods of rendering payment, i.e., electronic currency (a/k/a digital cash, virtual cash, electronic (e-) cash, digicash, electronic (e-) money, digital money, Internet currency, cybercash or cyberbucks), are receiving a great deal of attention from both consumers and merchants.[108]

35. Electronic currency is essentially a system that allows a person to pay for goods or services by transmitting a number from one computer to another.[109] These transactions are carried out electronically, transferring funds from one party to another, by either a debit or credit.[110] These funds are instantly cleared and secured by using strong encryption, thus eliminating the payment risk to the consumer.[111] It is only a matter of time before electronic currency will replace the present monetary systems. Thus, electronic currency is the digital representation of money, or more accurately, the digital representation of currency.[112]

Types Of Electronic Payment Systems

36. As E-commerce is rapidly increasing, so are the systems available to the consumer. Anything that makes it possible for a consumer to spend money online can be construed as an electronic payment system.[113] As of this Comment, there are many different companies offering various ways of transferring money across the Internet.[114] As a result, the Basle Committee (BC)[115] was formed to examine these new electronic payment systems.

The Basle Committee

37. The Basle Committee consists of banking supervisory authorities from twelve different countries. The BC examined stored-value payment products, and as a result, identified two models of electronic coin payment systems: (1) the single-issuer model; and (2) the multiple-issuer model.

38. In the single-issuer model, the issuer creates and distributes electronic coins to banks.[116] The bank then issues the electronic coins to their customers by loading them onto stored value cards or computer hard drives.[117] When the customers use the coins to purchase goods and services, the merchant then deposits them with their banks.[118] These banks then claim the monetary value from the issuer or system operator.[119] Using this model, consumers can also transfer electronic coins between themselves using electronic wallets.[120]

39. The role of the system operator differs in the multiple-issuer model. In this system, consumers are able to receive electronic coins from a number of different issuers. A merchant is the party in the electronic transaction that receives coins as payment, deposits them with other issuers and then contacts the

system operator.[121] The system operator then consolidates these claims and transmits this information to the issuers.[122]

Mondex

40. The Mondex[123] smart card is an electronic wallet that holds five different currencies[124] and is used to transmit electronic cash over the Internet. Using this system, a consumer can browse any online service that accepts Mondex.[125] In order to purchase, a consumer inserts his Mondex card into the card reader attached to his personal computer.[126] Once the consumer confirms that another valid Mondex device is present on the other end of the transaction, the customer's card transfers value to the vendor's card.[127]

41. For security purposes, Mondex relies on a unique "digital signature" generated by a chip on the consumer's card, which is recognizable by the Mondex card on the other end of the transaction.[128] This "digital signature" guarantees that no one can tamper with the Mondex signals, as well as the authenticity of the Mondex cards involved.[129] This process also identifies the intended recipient of the cash, in order to prevent a third party from intercepting the funds without detection.[130]

42. The Mondex card has a security code that prevents the misusage of electronic cash stored on the computer chip. In addition to a regular transaction, a consumer can also make a payment by inserting his Mondex card into the merchant's Mondex terminal or into another individual's electronic purse.[131] Thus, users can transfer electronic cash among themselves without using an intermediary, i.e., without the issuer or other financial institution being involved in the transaction.[132]

43. Each individual Mondex card contains a "rolling" audit trail that includes sixteen-digit card reference numbers, retailer names, dates of transaction and amount.[133] This audit trail provides users with secure transactions and allows third parties to resolve disputed or "failed" transactions.[134] Currently, the consumer's card stores the details of its last ten transactions. However, the retailer terminal is able to hold details of the last three hundred transactions - equivalent to a day's business for most cash registers.[135] A typical transaction report from the Mondex system provides the amount of the transaction, as well as a history that identifies whether the transaction was person to person or person to merchant.[136] Yet, the report will not identify the person or merchant involved in the transaction.[137]

Mark Twain

44. The electronic currency system at Mark Twain involves two separate bank accounts.[138] A customer first must open a World Currency Access (WCA) account. The WCA is a money market deposit account that bears interest and is available to customers independent of the electronic currency program.[139] To convert WCA value to electronic currency, a customer must transfer funds by telephone, facsimile, mail or e-mail, from the WCA to an individual "electronic currency mint" non-interest-bearing account.[140] Once a user has completed this step, electronic currency value is downloaded from the electronic currency mint to the user's computer via the Internet.[141] At this point, Mark Twain transfers funds from the customer's individual mint account into a pooled account at Mark Twain. This provides merchants and other payees who receive electronic currency the means to redeem these funds and convert them into traditional forms of value.[142]

45. Once a customer downloads electronic currency "coins" onto his computer, these coins can then be spent with merchants or other participants in the electronic currency program. Additionally, unspent coins can be returned to the mint account (and from there to the WCA if desirable).[143] When a consumer spends electronic currency, except for transfers between consumers under a "wild card

option,"[144] the mint automatically receives the electronic currency. This allows the bank to verify that the user has not previously spent the electronic "coins." If the coins are valid, the mint automatically deposits the value into the payee's mint account, where the payee can either leave the electronic currency or download it to a computer.[145] Today, these systems generate billions of dollars in revenues each year.

Analysis

46. North America alone is expected to exceed $36 billion in online revenues by the end of 1999, which more than doubled the $14.9 billion in 1998.[146] Many believe that E-commerce can be facilitated by the appropriate legal framework that includes the use of digital signatures.[147] Unarguably, E-commerce is altering the operation of business and thus transforming the global economy.[148] Moreover, both merchants and consumers are using digital signatures in order to process E-commerce transactions.[149]

47. Parties to these transactions need a reliable and trustworthy means for transmitting electronic value across the Internet. Thus, many argue that the use of digital signatures will provide the means for entering into a legally binding contract.[150] However, like any transaction, potential problems exist, including illegal activity.

48. This Comment analyzes and argues why the use of digital signatures in E-commerce is an effective tool for electronic currency transactions. Next, this Comment argues that the use of digital signatures in electronic currency transactions will ensure that the transactions are legally enforceable. Finally, this Comment provides remedies to damaged parties in an electronic currency transaction.

Purchasing Electronic Currency

49. Using electronic currency is like using a virtual ATM.[151] A user simply connects to the Internet and verifies ownership of the account.[152] The user may then withdraw the desired amount of the electronic currency.[153] At this point, the bank issues a very large, unique random number in an electronic coin format (the "serial number" of the coin) to the user, which the bank signs with their private key.[154] Instead of putting paper cash in your wallet,[155] the user's software stores these electronic coins[156] on the hard drive of the computer.[157]

50. Once receiving the coins, the computer stores these notes until the user desires to make a purchase.[158] When the user finds the desired product online, the computer collects the notes needed to pay for the item.[159] These notes are then sent to the seller, who sends them to the digital bank.[160]

51. Upon receiving the coins, the bank verifies the coin's serial number against its list of spent coins.[161] If the user has not spent the coin previously, the bank credits the account of the vendor and the vendor ships the product to the user.[162] In many ways, this system is similar to using food stamps or coupons.[163] However, these methods are slow, and electronic currency will change that considerably.[164]

Electronic Currency's Unique Feature -- Blinded Coins

52. Since the issuer's digital signature authenticates the serial number on each electronic coin,[165] the coin's redemption links its original holder to the transaction.[166] However, consumers can avoid this by using blinded coins.[167] Using the "blinding" technique,[168] the bank can validate the coins

without knowing the payer's identity. Therefore, this prevents the bank from recognizing the coins as having come from the payer's account.[169]

53. Using public key cryptography,[170] the electronic currency system provides each bank, customer (payer) and merchant (payee) with their own public and private keys.[171]

54. To create a blinded coin, a bank customer must first make a request for electronic currency. The bank will then withdraw this pre-set denomination from the customer's account in the form of digital coins.[172] The customer's software then generates a 100-digit random serial number for each coin.[173] Since the length of the randomly generated serial number is large, it guarantees with high probability that the serial numbers of any two coins will not be the same.[174] The coins are then "blinded" by multiplying them by a random factor.[175] The customer then signs the blinded coins with his private key, encrypts the coins with the public key of the bank and then sends them to the bank.[176]

55. When the bank receives the coins, the bank removes the signature, signs the coins with its own private key and registers its worth -- thereby "stamping" a value on the certificate.[177] The bank then encrypts the coins with the customer's public key and sends them to the customer.[178] The customer then decrypts the coins with his private key and "unblinds" them by dividing out the random factor.[179] By using the blinding/unblinding process, the customer prevents the bank from associating subsequently spent coins with withdrawals from his bank account.[180] Therefore, the bank is unable to know when or where you shopped, or what you bought.[181]

Advantages and Disadvantages of the Electronic Currency Payment System

56. The various payment methods which already exist or are in the trial phase, targets the retail or wholesale markets, small-scale nickel and dime transactions and fund transfers (home banking or large-scale transactions). However, these payment methods have both advantages and disadvantages.

Advantages of Electronic Currency Payment Systems

57. **Confidentiality/Privacy**
Current electronic currency systems vary in their effects on privacy from total anonymity, in which personally identifiable records are not created (blinded coins), to audited systems that collect and store every aspect of each transaction.[182] One of the most attractive features of electronic currency is that, unlike real cash, it is anonymous.[183] That is, when a electronic currency amount is sent from a customer to a merchant, there is no way to obtain information about the customer.[184] This is one significant difference between electronic currency and credit card systems.[185] Unlike credit card companies that collect a customer's spending habits and sell this data to third parties, the bank will have no record of the customer involved in the electronic currency transaction. Thus, by using electronic currency, the bank is unable to obtain personal information about the consumer. Therefore, this adequately protects the privacy rights of the customer.

58. Additionally, banks must adhere to federal laws regarding financial privacy, including the Electronic Funds Transfer Act (EFTA)[186] and the Electronic Communications Privacy Act of 1986 (ECPA).[187] However, it is unclear whether these acts directly apply to electronic currency.[188] In turn, consumers will have to wait for future legislation, as well as judicial precedent to determine whether these laws apply to electronic currency transactions.

59. **Security**
As previously mentioned, the security of electronic currency is provided by the use of encryption.

Some experts are weary about the security of online transactions. However, the use of RSA cryptography makes it almost impossible to break the code of a digital signature.[189] Many commentators point out that the manufacturers of cryptographic technology will eliminate all risks of code breaking by developing longer keys.[190] Additionally, the enacted digital signature statutes require a certification authority to use a trustworthy system. Therefore, even though there is speculation about the security of the Internet, electronic currency consumers are probably more secure in their transactions than the more traditional ways of doing business.

Disadvantages of Electronic Currency Payment Systems

60. **Fraud**
A major disadvantage to electronic currency is fraud. If a consumer somehow misplaces his private key and a perpetrator uses it to withdraw funds, the bank would never know and the consumer would be liable. Credit cards on the other hand, limit the consumer's liability for unauthorized activity to US$50.[191] Additionally, if the security code is broken and the message is intercepted, the hacker will be able to perpetrate fraud on the recipient of the message.[192]

61. However, if either of these scenarios occur, the consumer is protected by the Computer Fraud and Abuse Act.[193] Additionally, due to the advanced technology discussed above, the likelihood that these scenarios would occur is far less than the unauthorized use of a credit card. Thus, although fraud is a potential drawback of electronic currency, this risk is no greater than the traditional forms of payment.

62. **Peer-to-peer double spending**
Double spending of digital coins is another potential disadvantage of electronic currency. However, this is only a potential drawback if the consumer chooses a peer-to-peer transaction. In all other transactions in the electronic currency system, the bank is able to check the serial number of each coin in a transaction against its database of spent coins, and if the coin has been spent, the transaction will be denied.

63. Therefore, the consumer has a choice of whether to include an intermediary (bank) in the transaction. If the consumer chooses not to include an intermediary, and then the coins are intercepted or sent to the wrong recipient, the consumer has no recourse. However, if the consumer included the intermediary, the bank checks the coins for double spending thereby protecting the consumer. Thus, the potential for the double spending of coins is only a drawback if the consumer chooses to bear the risk of the transaction.

64. After evaluating the risks and benefits of electronic currency, this system has a great opportunity to transform today's economic world. The electronic currency systems presently in operation provide greater privacy and security than most present forms of payment. Additionally, the risks involved with these transactions are risks that the consumer chooses to bear. The remedies for potential fraud and double spending have already been accounted for in the systems presently in operation. Therefore, combined with speed of transaction and the availability to the consumer, the privacy and security aspects of electronic currency far outweigh the potential risks.

Enforceable Contract

65. When a consumer purchases an item using electronic currency, this purchase forms a legally binding contract.[194] One of the problems regarding these contracts may be the statute of frauds. However, as early as 1869, a New Hampshire court held that a telegraphed contract was a sufficient writing under the statute of frauds.[195] Additionally, telexes, Western Union Mailgrams, and even tape recordings

have been held to be acceptable under the statute of frauds.[196]

66. The signature[197] on these contracts may also pose problems under the statute of frauds. However, the courts have found many different symbols to be signatures under the statute of frauds. These include names on telegrams,[198] typewritten names,[199] names on telexes,[200] names on Western Union Mailgrams,[201] letterhead names[202] and even faxed signatures (under non-statute of frauds cases).[203] Thus, any symbol or code contained in an electronic transmission should also meet the statute of frauds requirement.[204] Therefore, using the process of digital signatures, a consumer will be able to create a legally binding document and signature. In turn, the consumer will have various remedies available to him if the other party breaches the contract.

Illegal Activity With Electronic Currency

67. The days of smuggling a million dollars in a suitcase may soon be over because electronic currency will allow criminals the same opportunity but with less visibility. The Mondex card will allow a criminal to store millions of dollars in his wallet, while others will be transferring money from the comfort of their own home to an offshore banking account in a matter of seconds. There is no doubt that criminals will prefer electronic cash for the obvious reasons: it is anonymous, portable and easy to hide.

68. Since electronic currency lacks records that identifies who spends, transfer or takes money, money laundering and tax evasion are two potential problems that will be associated with this latest form of currency. First, laundering money via the Internet can easily be accomplished because electronic currency transactions can be undetectable and untraceable. Illegal markets will utilize this technology in order to facilitate their criminal activities. Examples of illegal markets include gambling, bribery or payoffs, contract crimes, fencing or purchasing of illegal goods, illegal online escorts and illegal games. Second, electronic currency also becomes a legal concern when used for tax avoidance. Under this problematic area, criminals may violate laws by conducting offshore funds transfers in an illegal market and practice income hiding to avoid paying income taxes. Again, this is all possible because the spending of electronic currency is hard to detect.

Wire Fraud

69. Although the Internet is a logical or virtual concept, it is manifested in the form of communications lines connecting computers. Thus, fraudulent Internet schemes that involve electronic currency fall under the Federal Wire Fraud Act.[205] For the government to convict a defendant of wire fraud, the government must show: (1) a scheme to defraud by means of false pretenses; (2) defendant's knowing and willful participation in the scheme with intent to defraud; and (3) use of interstate wire communications in furtherance of the scheme.[206] Even if the fraudulent scheme is not successful, an individual may be subject to criminal liability.[207] Even where the defendant did not cause the communication to be transmitted or transmit the communication himself, liability may be attached if the use of interstate wires in the transaction is reasonably foreseeable.[208] Moreover, each separate use of a wire communication constitutes a separate offense, even if the defendant engaged in only a single scheme to defraud.[209] However, prosecuting wire fraud committed on the Internet can be difficult because the communication must cross state lines.[210]

70. Additionally, if the scheme perpetrated through the Internet contemplates the use of U.S. Mails (e.g., victims mailing money to defendant), then the defendant faces additional liability under the Federal Mail Fraud Statute.[211] Penalties for violations of these two acts include up to five years imprisonment and fines of $1000, unless the scheme involves a financial institution, in which case the penalties increase to a maximum of $1,000,000 and 30 years imprisonment.

71. Thus, a person will violate the Wire Fraud Act if they commit or attempt to commit a scheme of fraud using electronic currency. For example, in United States v. Butler & Thornton, a Virginia federal district court held that the defendants violated the Wire Fraud Act when they used interstate communications to misrepresent the quality of their loans by falsifying credit applications.[212]

72. However, experienced criminals are not the only ones who commit mail fraud. For example, a 15 year-old Utah boy was recently arrested for defrauding Internet users out of as much as $10,000.[213] The boy set up a mailbox using a false identity and then advertised computer parts over the Internet.[214] Customers were asked to pay by c.o.d. or certified check. When the customer opened the box that supposedly contained the computer parts, it would be empty.[215] Consequently, the customers were unable to stop payment on the cashier's check and the money would be gone.[216]

73. Conventional fraudulent schemes have also found new life on the Internet. Federal law enforcement officers estimate that over $10 billion worth of data is stolen in the United States each year. Moreover, computer crimes rose forty-three percent from 1997 to 1998.[217] For example, credit card fraud schemes are possible by convincing victims to e-mail their credit card numbers for a free weekend, or some other bogus prize.

74. For example, Louis Rex Curtis advertised the "Computer Matching Institute" on the Internet. Respondents to the advertisements would receive by mail, an application to "psychologically" match them with the perfect partner. After mailing in the application and a fee, the applicants would never hear from Curtis again.

75. In terms of dollars, Jim Lay of North Carolina may have committed the largest fraudulent act. The scam reportedly cost six telephone companies $28 million. Using the computer name, "Knight Shadow," Lay, an MCI Telecommunications, Inc. employee, sold between 50,000 and 100,00 stolen telephone calling-card numbers world-wide. However, Lay is now in Federal prison.

76. The Federal Trade Commission expects consumer fraud to increase on the Internet. Already the FTC investigated and halted several fraudulent schemes over the Internet, including a pyramid scheme that cheated investors out of $6 million. An example of a possible electronic currency fraudulent scheme would be a situation where the purchaser transfers electronic currency to a trader, but never receives the bargained good or service. If the wire communication crossed state lines, the damaged purchaser would be able to bring a cause of action under the wire fraud act.

77. Moreover, if a defendant's activities are found to violate the Federal Wire Fraud Act, such activities may also violate the Racketeer Influenced and Corrupt Organization Act (RICO). The Wire Fraud Act contains the essential elements of RICO, with the additional requirement that the government must prove: (1) that the alleged defendants participated directly or indirectly in an enterprise (two or more people); and (2) through a pattern that constitutes racketeering activity whereby the plaintiff's business or property was injured by such conduct.[218]

78. Therefore, an individual who interferes with an electronic currency transaction may not only be subject to one of the above mentioned Acts but all three.

Computer Fraud and Abuse Act

79. Despite the strong security for an electronic currency transaction, there is always the possibility that a criminal may intercept the transaction. If this slim possibility does occur, a remedy may be found in federal law. The Computer Fraud and Abuse Act (CFA) prohibits any person from intentionally accessing a computer or electronic communication without authorization and obtaining financial, medical, or other proprietary information.[219] The CFA also prohibits any person from using a

computer or electronic communication to commit: (1) fraud; (2) to "trespass" on a protected computer; (3) to transmit programs, information, calls, or commands that intentionally cause damage to a protected computer; and (4) to traffic in unauthorized passwords.[220] "Protected computers" are defined as computers being used in interstate commerce or communications.[221] Therefore, a protected computer is one used for private or commercial business purposes which transverse interstate lines for communication or commerce. Punishment for the foregoing acts include both monetary fines and prison terms up to twenty years. Moreover, the CFA provides civil claims for compensatory economic damages and injunctive or other equitable relief.

80. To understand how the CFA will impact electronic currency transaction, lets first look at some recent cases that have interpreted the CFA. First, in Organization JD Ltda. v. United States Department of Justice, the Second Circuit found that the CFA precisely identified plaintiffs who could bring a cause of action under the CFA to include "originator[s], addressee[s], or intended recipient[s]," and any other "party" to an electronic communication that was damaged due to an intentional and unauthorized access by a party.[222]

81. Second, courts have interpreted "interstate communication" under the CFA to include illegal Internet activity if such activity crossed state lines. For example, a message from Cincinnati to Cleveland may leave the State of Ohio and be routed through Maryland. If so, the communication is interstate communication. However, if the communication does not across state lines, then the statute is not satisfied. In America Online, Inc. v. LCGM, Inc., a Virginia federal district court held that LCGM's use of the Internet to send unauthorized and unsolicited bulk e-mail advertisements (i.e., "spamming") to AOL's customers in numerous states violated the CFA.[223] The court reasoned that the practice of spamming (which also violated LCGM's user agreement with AOL) was considered an interstate communication and thus fell within the scope of the CFA.[224]

82. The Courts have also interpreted "information" under the CFA to include proprietary information. In American Online, Inc. v. LCGM, Inc., LCGM obtained e-mail address of AOL members by intentionally breaking into AOL's network.[225] The court held that the e-mail addresses were protected "information" under the CFA because they were proprietary in nature.[226]

83. Although there are no CFA cases that involve electronic currency, the rational in these cases can be analogized to electronic currency. Like the e-mails in LCGM, the Internet enables electronic currency to exist. If the unauthorized conduct on the Internet interfered with an electronic currency transaction that crossed state lines, such conduct would clearly fall within the meaning of "interstate communication" under the CFA. Moreover, since electronic currency is clearly proprietary in nature, i.e., the manifestation of money, a damaged plaintiff must show that the defendant intended to defraud and wrongfully obtain proprietary information via the Internet. Therefore, any person or party who impairs an electronic currency transaction by "intentionally access[ing] a protected computer without authorization, and as a result of such conduct, causes damages"[227] would violate the CFA.

National Stolen Property Act

84. It would also seem likely that the National Stolen Property Act (NSPA) could be applied to the unlawful transmission of information across state lines via the Internet. The NSPA provides criminal penalties for the interstate transport of any stolen goods, including non-governmental property.[228] The NSPA requires that "goods, wares, merchandise, securities or money" be the illicitly obtained items, which are transferred across state lines.[229] In Dowling v. United States, the United States Supreme Court held that the NSPA applied to physical goods themselves that have been stolen, converted, or taken by fraud.[230] Also, in United States v. Riggs, a Federal district court upheld the indictment of Robert J. Riggs and Craig Neidorff under the Wire Fraud Act and the NSPA for their

theft of a Bell South Text file containing 911 codes.[231] The court reasoned that the defendants had transferred "confidential, proprietary business information."[232]

85. However, in United States v. Brown et al., the Tenth Circuit rejected the governments argument and refused to allow the United States to indict the defendants under the NSPA for retaining a hard disk containing misappropriated source code.[233] The court reasoned that source code contained on a hard disk did not constitute "goods" under the NSPA.[234]

86. Although the Brown court reasoned that the source code did not constitute "goods" under the NSPA, electronic currency is distinguishable from source code. Electronic currency is a manifestation of money, which can easily be converted into physical money. Moreover, electronic currency arguably could constitute "money" under the NSPA because it is a manifestations of money and therefore proprietary information. With electronic currency, a damaged plaintiff could argue that the defendant(s) stole, transferred, converted or took electronic coins by fraud. Since an electronic coin's value is equal to its physical coin value, interstate transmission of illegal money is prohibited under the NSPA. If a hacker or party to an electronic currency transaction illegally obtains electronic currency and transports it across state lines, such illegal conduct would clearly fall within the scope of the NSPA.

Common Law Claims

87. A damaged party may not only have a cause of action under federal statutes, but may also have a cause of action under common law claims. For example, a party who has been damaged from an electronic currency transaction may seek a cause of action under the theories of breach of contract, tortious interference with contract, trespass, nuisance, conversion, negligence, fraud and misrepresentation as well as numerous state computer crime statutes.

88. For example, in America Online, Inc. v. IMS, the court found in favor of AOL on its claims of false designation of origin, dilution and trespass to chattels when the defendant spammed AOL customers.[235] Also, in Hotmail Corporation v. Van$ Money Pie Inc., the court denied the defendant's motion for summary judgment and found that the plaintiff's fraud and misrepresentation claims were likely to succeed.[236] The court reasoned that the defendant falsely obtained several of the plaintiff's accounts knowing that they would not abide by the user agreements and that the defendants falsified their spam to make it appear that plaintiff had authorized their messages.[237]

89. As you can see, both federal and state law adequately protects a consumer that uses an electronic currency system. Even if an electronic currency transaction goes awry, the damaged consumer will have adequate remedies under both federal and state law.

Conclusion

90. Presently, electronic currency is at the early stages of implementation. As we progress into the twenty-first century, a consumer's wallet will hold less paper cash, coins and magnetic strip cards. Instead, smart cards, e.g., Mondex, will contain electronic currency and other financial information that will automatically execute a transaction. In the physical world, consumers will gain immediate access to public transportation, concerts and movie theaters using smart cards. Additionally, a cyberspace mall will allow all entrepreneurs and retailers the ability to instantly reach the global market. This will allow numerous storefronts to be just a click away from a potential sale. Yet, the major issues will continue to be trust and security in ensuring consumers that the chance of a fraudulent transaction or misuse of personal information is slim or non-existent. However, once the electronic currency industry is able to ensure consumers that these transactions are secure and trustworthy, it will change the way we conduct our daily lives.

Notes

[1] See Notaries Public in American History, NOTARY BULL., Apr. 1997, at 3.

[2] On the state level, all fifty states have some form of unified set of laws regulating notaries. See ALA. CODE §§ 36-20-1 to -11 (1998); ALASKA STAT. §§ 44.50.010-.190 (Michie 1999); ARIZ. REV. STAT. ANN. §§ 41-311 to -326 (West 1999); ARK. CODE ANN. §§ 21-14-101 to -111 (Michie 1999); CAL. GOV'T CODE §§ 8200-8230 (West 1999); COLO. REV. STAT. §§ 12-55-101 TO -123 and 12-55-201 to -211 (1999); CONN. GEN. STAT. ANN. §§ 3-91 to -99a and 7-33a (West 1999); DEL. CODE ANN. tit. 29, §§ 4301-4328 (1998); D.C. CODE ANN. §§ 1-801 to -817 (1999); FLA. STAT. ANN. §§ 117.01 to .10 (West 1999); GA. CODE ANN. §§ 45-17-1 to -34 (Harrison 1999); HAW. REV. STAT. §§ 456-1 to -18 (1998); IDAHO CODE §§ 51-101 to -123 (1998); ILL. ANN. STAT. ch. 10

[2] ¶¶ 201-101 to 203-106 (Smith-Hurd 1999); IND. CODE ANN. §§ 33-16-1-1 to 16-2-9 (West 1999); IOWA CODE ANN. § 586.1 (West 1999); KAN. STAT. ANN. §§ 53-101 to -401 (1998); KY. REV. STAT. ANN. §§ 423.010 -.990 (Banks-Baldwin 1999); LA. REV. STAT. ANN. §§ 35:1 -:17 (West 1999); ME. REV. STAT. ANN. tit. 4, §§ 951-958 (West 1999); MD. CODE ANN. art. 68, §§ 1-13 (1998); MASS. GEN. LAWS ANN. ch. 222, §§ 1-11 (West 1999); MICH. COMP. LAWS ANN. §§ 55-101 to -107 (West 1999); MINN. STAT. ANN. §§ 359-01 to -1

[2] (West 1999); MISS. CODE ANN. §§ 25-33-1 to -23 (1998); MO. ANN. STAT. §§ 486-200 to -405 (West 1999); MONT. CODE ANN. §§ 1-5-401 to -420 (1998); NEB. REV. STAT. §§ 64-101 to -215 (1998); NEV. REV. STAT. ANN. §§ 240.010 -.160 (Michie 1999); N.H. REV. STAT. ANN. §§ 455:1 to :14 (1998); N.J. STAT. ANN. §§ 52:7-10 to -21 (West 1999); N.M. STAT. ANN. §§ 14-12-1 to -20 (Michie 1999); N.Y. EXEC. LAW §§ 6-130 to -139 (McKinney 1999); N.C. GEN. STAT. §§ 10A-1 to -16 (1998); N.D. CENT. CODE §§ 44-06-01 to -14 (1998); OHIO REV. CODE ANN. §§ 147.01 -.14 (Anderson 1999); OKLA. STAT. ANN. tit. 49, §§ 1-10 (West 1999); OR. REV. STAT. §§ 194-005 to -990 (1998); 57 PA. CONS. STAT. ANN. §§ 1 to -169 (West 1999); R.I. GEN. LAWS §§ 42-30-1 to -14 (1998); S.C. CODE ANN. §§ 26-1-10 to 26-3-90 (Law.Co-op 1999); S.D. CODIFIED LAWS ANN. §§ 18-1-1 to -14 (Michie 1999); TENN. CODE ANN. §§ 8-16-101 to 309 (1998); TEX. GOV'T CODE ANN. §§ 406.001 -.024 (West 1999); UTAH CODE ANN. §§ 46-1-1 to -17 (1998); VT. STAT. ANN. tit. 24, §§ 441-446 (1998); VA. CODE ANN. §§ 47.1-1 to -33 (Michie 1999); WASH. REV. CODE ANN. §§ 42.44.010 -.903 (West 1999); W.VA. CODE §§ 29-4-1 to -16 (1998); WIS. STAT. ANN § 137.01 (West 1999); WYO. STAT. §§ 32-1-101 to -113 (Michie 1999).

[3] Only two states require that notary applicants be older than eighteen years of age. See ALASKA STAT. §§ 44.50.010-.190 (Michie 1999) (requiring applicant to be 19 years of age); NEB.REV.STAT. §§ 64-101 to -215 (1998) (requiring applicant to be 19 years of age);

[4] See WESLY GILMER, JR., ANDERSON'S MANUAL FOR NOTARIES PUBLIC § 2.5 (5th ed. 1976). Thirty-one states require a notary bond that varies from $20,000 to $500 to "assure the faithful performance of duties, and to compensate any person who may suffer a loss because of the notary's misconduct." Id. See ALA. CODE §§ 36-20-1 to -11 (1998) ($10,000); ALASKA STAT. §§ 44.50.010-.190 (Michie 1999) ($1,000); ARIZ. REV. STAT. ANN. §§ 41-311 to -326 (West 1999) ($5,000); ARK. CODE ANN. §§ 21-14-101 to -111 (Michie 1999) ($4,000); CAL. GOV'T CODE §§ 8200-8230 (West 1999) ($15,000); D.C. CODE ANN. §§ 1-801 to -817 (1999) ($2,000); FLA. STAT. ANN. §§ 117.01 to .10 (West 1999) ($7,500); HAW. REV. STAT. §§ 456-1 to -18 (1998) ($1,000); IDAHO CODE §§ 51-101 to -123 (1998) ($10,000); ILL. ANN. STAT. ch. 102 ¶¶ 201-101 to 203-106 (Smith-Hurd 1999) ($5,000); IND. CODE ANN. §§ 33-16-1-1 to 16-2-9 (West 1999) ($5,000); KAN. STAT. ANN. §§ 53-101 to -401 (1998) ($7,500); KY. REV.

STAT. ANN. §§ 423.010 -.990 (Banks-Balwin 1999) (Varies per county); LA. REV. STAT. ANN. §§ 35:1 -:17 (West 1999) ($5,000-attorneys exempt); MICH. COMP. LAWS ANN. §§ 55-101 to -107 (West 1999) ($10,000); MISS. CODE ANN. §§ 25-33-1 to -23 (1998) ($5,000); MO. ANN. STAT. §§ 486-200 to -405 (West 1999) ($10,000); MONT. CODE ANN. §§ 1-5-401 to -420 (1998) ($5,000); NEB. REV. STAT. §§ 64-101 to -215 (1998) ($10,000); NEV. REV. STAT. ANN. §§ 240.010 -.160 (Michie 1999) ($10,000); N.M. STAT. ANN. §§ 14-12-1 to -20 (Michie 1999) ($500); N.D. CENT. CODE §§ 44-06-01 to -1

[4] (1998) ($7,500); OKLA. STAT. ANN. tit. 49, §§ 1-10 (West 1999) ($1,000); 57 PA. CONS. STAT. ANN. §§ 1 to -169 (West 1999) ($3,000); S.D. CODIFIED LAWS ANN. §§ 18-1-1 to -1

[4] (Michie 1999) ($5,000); TENN. CODE ANN. §§ 8-16-101 to 309 (1998) ($10,000); TEX. GOV'T CODE ANN. §§ 406.001 -.02

[4] (West 1999) ($10,000); UTAH CODE ANN. §§ 46-1-1 to -17 (1998) ($5,000); WASH. REV. CODE ANN. §§ 42.44.010 -.903 (West 1999) ($10,000); WIS. STAT. ANN § 137.01 (West 1999) ($500); WYO. STAT. §§ 32-1-101 to -113 (Michie 1999) ($500). In the three states where the bond is $500, the statutes were enacted between 1849 and 1876 and were never amended to reflect the modern cost of living. See Michael L. Closen, Why Notaries Get Little Respect, NAT'L L.J. Oct. 9, at A23 (1995). Additionally, some states have not changed their notary bond requirements in over one hundred and twenty years. See Michael L. Closen & R. Jason Richards, Notaries Public-Lost in Cyberspace, or Key Business Professionals of the Future?, 15 J. MARSHALL J. COMPUTER & INFO. L. 703, 749-750 (1997).

[5] Only fourteen states have some type of minimum residence requirement incorporated into their respective notary statutes. See ALA. CODE §§ 36-20-1 to -11 (1998) (requiring 1 day); ALASKA STAT. §§ 44.50.010-.190 (Michie 1999) (requiring 30 days); ARIZ. REV. STAT. ANN. §§ 41-311 to -326 (West 1999) (Varies); COLO. REV. STAT. §§ 12-55-101 TO -123 and 12-55-201 to -211 (1999) (requiring 29 days); ILL. ANN. STAT. ch. 102 ¶¶ 201-101 to 203-106 (Smith-Hurd 1999) (requiring 30 days); MO. ANN. STAT. §§ 486-200 to -40

[5] (West 1999) (requiring 30 days); MONT. CODE ANN. §§ 1-5-401 to -420 (1998) (requiring 1 year); NEV. REV. STAT. ANN. §§ 240.010 -.160 (Michie 1999) (requiring 30 days); N.D. CENT. CODE §§ 44-06-01 to -14 (1998) (requiring 30 days); OHIO REV. CODE ANN. §§ 147.01 -.14 (Anderson 1999) (requiring 30 days); 57 PA. CONS. STAT. ANN. §§ 1 to -169 (West 1999) (requiring 1 year); R.I. GEN. LAWS §§ 42-30-1 to -14 (1998) (requiring 1 month); UTAH CODE ANN. §§ 46-1-1 to -17 (1998) (requiring 30 days); W.VA. CODE §§ 29-4-1 to -16 (1998) (requiring 30 days).

[6] Only thirteen states administer an exam before certifying a notary. See ALASKA STAT. §§ 44.50.010-.190 (Michie 1999); CAL. GOV'T CODE §§ 8200-8230 (West 1999); CONN. GEN. STAT. ANN. §§ 3-91 to -99a and 7-33a (West 1999); D.C. CODE ANN. §§ 1-801 to -817 (1999); HAW. REV. STAT. §§ 456-1 to -18 (1998); LA. REV. STAT. ANN. §§ 35:1 -:17 (West 1999); ME. REV. STAT. ANN. tit. 4, §§ 951-958 (West 1999); N.Y. EXEC. LAW §§ 6-130 to -139 (McKinney 1999); N.C. GEN. STAT. §§ 10A-1 to -1

[6] (1998); OHIO REV. CODE ANN. §§ 147.01 -.14 (Anderson 1999); OR. REV. STAT. §§ 194-005 to -990 (1998); UTAH CODE ANN. §§ 46-1-1 to -17 (1998); WYO. STAT. §§ 32-1-101 to -113 (Michie 1999). Additionally, only the state of North Carolina requires notaries to undergo classroom training at community colleges. See N.C. GEN. STAT § 10A-4(b)(1998).

[7] See generally, Closen, supra note 4, at A23 (stating that states can improve notary performance through training and testing); Vincent Gnoffo, Comment, Notary Law and Practice for the 21st Century: Suggested Modifications for the Model Notary Act, 30 J. MARSHALL L. REV. 1063, 1064-65 (1997) (contending that continuous education and testing would solve many notarial problems); Closen & Richards, supra note 4

(suggesting that states should raise standards and requirements to improve the service of notaries).

[8] The United States Supreme Court has stated that "a notary's duties... are essentially clerical and ministerial." Bernal v. Fainter, 467 U.S. 216, 216-217 (1984).

[9] See 58 Am. Jur. 2d Notaries Public, § 1 (1989) (explaining that "[a] notary pubic is defined as a public, civil or ministerial officer..."); Ashcraft v. Chapman, 38 Conn. 230 (1871) (asserting that a notary is a public officer); Britton v. Niccolls, 104 U.S. 757, 765 (1881) (declaring that a notary is a public officer); May v. Jones, 14 S.E. 552, 553 (Ga. 1891) (stating "the notary...is a public officer, sworn to discharge his duties properly"); State v. Clark, 31 P. 545, 546 (Nev. 1892) (noting that "it has been frequently held that a notary is a public officer"); Stork v. Am. Surety Co., 33 So. 742, 743 (La. 1903) (stating that a notary is a public officer); State v. Hodges, 107 Ark. 272 (1913) (stating that a notary is a public officer); Pitsch v. Continental & Comm. Nat'l Bank, 137 N.E. 198, 200 (Ill. 1922) (identifying a notary as a public officer); Comm. Union Ins. Co. v. Burt Thomas-Atiken Constr. Co., 230 A.2d 498, 499 (N.J. 1967) (declaring that "a notary public is a public officer"); Werner v. Werner, 526 P.2d 370, 376 (Wash. 1974) (identifying "the notary, as a public officer, ..."); But see Transamerica Ins. Co. v. Valley Nat'l Bank, 462 P.2d 814, 817 (Ariz. Ct. App. 1969) (stating that "at best, a notary holds a position that is quasi-public in nature because a notary may hold other offices, does not receive compensation from the state and is allowed to charge the public a fee for his services, and he is not elected nor appointed by state").

[10] 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 (1992). A notary public is a public official with the unusual powers for a non-judicial officer. Id.

[11] See Closen & Richards, supra note 4, at 723.

[12] Gerald Haberkorn & Julie Z. Wulf, The Legal Standard of Care for Notaries and Their Employers, 31 J. MARSHALL L. REV. 735, 737 (1998).

[13] Id. at 737-738.

[14] See 5 ILCS 312/6-102 (1998). In Illinois, satisfactory evidence that a person is the person whose true signature is on a document if that person: (1) is personally known to the notary; (2) is identified upon the oath or affirmation of a credible witness personally known to the notary; or (3) is identified on the basis of identification documents. 5 ILCS 312/6-102.

[15] The person seeking notarization must appear personally and provide evidence that he/she is who he/she claims to be. See In re Scott, 464 P.2d 318 (Or. 1970) (declaring that a notary may be reprimanded for notarizing without appearance); Ardis v. State, 380 So.2d 301 (Ala. Crim. App. 1979) (stating that a notary must be provided evidence of the identity of the person whose signature they are notarizing); Bernd v. Fong Eu, 161 Cal. Rptr. 58 (Ct. App.1979) (noting that a notary is negligent when he fails to ascertain the identity of person for acknowledgment); City Consumer Serv., Inc. v. Metcalf, 775 P.2d 1065 (Ariz. 1989) (en banc) (acknowledging that a notary is negligent when he failed to ask for identification).

[16] See Charles N. Faerber, Being There: The Importance of Physical Presence to the Notary, 31 J. MARSHALL L. REV. 749 (1998) (discussing telephone acknowledgments of signature and terms of agreement not acceptable).

[17] Courts have refused to accept telephone acknowledgements. For example, in voiding a deed of trust bearing a signature acknowledged over the phone, a Texas court declared: A notary can no more perform by telephone those notarial acts which require a personal appearance than a dentist can pull a tooth by telephone. If a telephone conversation is a personal appearance, we may suppose that a letter or telegram to a

notary would also be as good or maybe even better. Charlton v. Richard Gill Co., 285 S.W.2d 801, 803 (Tex. App. 1955).

[18] See Thomas J. Smedinghoff, Digital Signatures: The Key to Secure Commerce, OIL GLASS-CLE 201, 222 (1998).

[19] See Closen & Richards, supra note 4, at 739.

[20] See UTAH CODE ANN. §§ 46-3-101 to -502 (1998).

[21] See UTAH CODE ANN. §§ 46-3-101 to -502.

[22] See Closen & Richards, supra note 4, at 739.

[23] Id. In theory, any one can be a certification authority. This includes governmental entities, as well as private persons or entities acting as certification authorities for commercial purposes. See Smedinghoff, supra note 18, at 224. Already, a number of private commercial certification authorities are in operation. Id. These include Verisign, Inc. which issues certificates and offers services to both corporations and individuals who digitally sign documents for any purpose. Id. at 225.

[24] See CLE Liaison Committee, Notaries Public, 43 R.I.B.J. 13 (1994).

[25] See Chuck Appleby, Encryption Making Security a Reality, 508 INFO. WK. 38 (1995).

[26] See Closen & Richards, supra note 4, at 740.

[27] See Appleby, supra note 25, at 38. Ken Gilpatric, a Justice Department lawyer working on the National Performance Review Team, has stated that a digital notary is necessary "to make electronic commerce easy and trustworthy." Glen-Peter Ahlers, Sr., The Impact of Technology on the Notary Process, 31 J. MARSHALL L. REV. 911, 912 (1998).

[28] See Elizabeth Wasserman, Signing on with Digital Signatures-New Laws May Allow Computer Validation, PHOENIX GAZ., Aug. 29, 1995, at A1.

[29] See Smedinghoff, supra note 18, at 222

[30] See R.R. Jueneman & R.J. Robertson, Biometrics and Digital Signatures in Electronic Commerce, 38 JURIMETRICS J. 427, 438 (1998).

[31] See Jane Kaufman Winn, Open Systems, Free Markets, and Regulation of Internet Commerce, 72 TUL. L. REV 1177, 1200-1201 (1998).

[32] See Smedinghoff, supra note 18, at 222.

[33] Id.

[34] Id.

[35] Id. Certification authorities issue a variety of different certificates including: (1) identifying certificates that connect a name to a public key and could be stored on devices such as smart cards to facilitate financial transaction as well as a variety of public functions such as driver license registration, voter registration, and eligibility for various benefits; (2) authorizing certificates that attest to such data as the subscriber's residence, age, membership in a particular organization, or the holding of a license such as that of attorney or physician. See Philip S. Corwin, Administration Entangles Digital Signatures with Encryption Policy, 16 No. 8

BANKING POL'Y REP. 1, 13 (1997). A financial organization might issue: (1) an authorizing certificate linking a public key to a particular account; (2) transactional certificates that attest to some fact about a transaction, such as its witnessing by a cybernotary; and (3) digital time stamps that are unforgeable digital proof that a document was in existence at a particular time. Id.

[36] See Smedinghoff, supra note 18, at 223. A repository is an electronic database of certificates, similar to digital yellow pages. The repository is generally available online and may be maintained by a CA or anyone else providing repository services. Id.

[37] Id.

[38] See Richard L. Field, Digital Signatures: Verifying Internet Business Transactions, 471 PLI/PAT 721, 732 (1997); see also Brian W. Smith & Timothy E. Keehan, Digital Signatures: The State of the Art and the Law, 114 BANKING L.J. 506 (1997). The digital signature, an electronic encoded message containing a unique alphanumerical notation, is a necessary component of electronic commerce. See Sanu K. Thomas, The Protection and Promotion of E-commerce: Should There be a Global Regulatory Scheme for Digital Signatures?, 22 FORDHAM INT'L L.J. 1002, 1012 (1999). It guarantees the level of validity, authenticity, and security needed for electronic transactions. Id.

[39] See Jueneman & Robertson, supra note 30, at 437. The most commonly used method of public key encryption is called "RSA." See Lonnie Eldridge, Internet Commerce and the Meltdown of Certification Authorities: Is the Washington State Solution a Good Model?, 45 UCLA L. REV. 1805, 1812 (1998). RSA has been incorporated into such technological applications as, Internet browsers, secure phones, and drop-in computer cards. Id. Although RSA public key encryption is useful, it is slow compared to single key encryption schemes like DES. Id. at 1816.

[40] See Thomas, supra note 38, at 1012.

[41] AMERICAN BAR ASSOCIATION, DIGITAL SIGNATURE GUIDELINES: LEGAL INFRASTRUCTURE FOR CERTIFICATION AUTHORITIES AND SECURE ELECTRONIC COMMERCE 6 (1996) [hereinafter ABA GUIDELINES]. According to the ABA Signature Guidelines, digital signatures "should indicate who singed a document, message, or record, and should be difficult for another person to produce without authorization." Id. California's statute defines "digital signature" in a technologically neutral manner, saying it "means an electronic identifier, created by a computer, intended by the party using it to have the same force and effect as the use of a manual signature." CAL. GOV'T CODE § 16.5 (West 1999). Additionally, Utah law defines "digital signature" as "a transformation of a message using an asymmetric cryptosystem." UTAH CODE ANN. § 46-3-103 (1998).

[42] See Smedinghoff, supra note 18, at 220.

[43] Id.

[44] Id.

[45] Id.

[46] When a person uses encryption, documents traveling through an electronic medium are scrambled and unscrambled using mathematical formulas, or algorithms. See Michael D. Wims, Law and the Electronic Highway, Are Computer Signatures Legal?, 10 CRIM. JUST. 31, 3 (1995).

[47] See Smith & Keehan, supra note 38, at 507.

[48] Symmetric cryptography uses a single, secret key to either encrypt/transform or decrypt/restore a

message to its original form. See Thomas, supra note 38, at 1009. The U.S. military used symmetric cryptography during the cold war for communication purposes. Id. In 1875, IBM and the U.S. government developed the Data Encryption Standard (DES), the most widely used symmetric cryptosystem. See Eldridge, supra note 39, at 1810. Some experts estimate that an eavesdropper who intercepts a message encoded in DES can crack the encryption in about 3.5 hours with a one-million dollar computer. Id.

[49] Asymmetric cryptography uses two different, but related keys to encrypt/decrypt messages. See Thomas, supra note 38, at 1010. Asymmetric cryptosystem is widely used to create and verify digital signatures. See Smith & Keehan, supra note 38, at 506.

[50] See Winn, supra note 31, at 1199.

[51] Statutes in both Utah and Washington require the use of "asymmetric cryptosystem." See UTAH CODE ANN. § 46-3-103 (1998); WASH. REV. CODE ANN. § 19.34 et. seq. (West 1999)

[52] See Closen & Richards, supra note 4, at 735. A private key and a public key are produced at the same time, and are mathematically linked to each other, along with your secret password. See Gary W. Fresen, What Lawyers Should Know About Digital Signatures, 85 ILL. B.J. 170, 172 (1997).

[53] See Closen & Richards, supra note 4, at 735.

[54] Id.

[55] The sender may run this message through a hash function, which performs a series of mathematical operations on the message. See Daniel J. Greenwood & Ray A. Campbell, Electronic Commerce Legislation: From Written on Paper and Signed in Ink to Electronic Records and Online Authentication, 53 BUS. LAW. 307, 314 (1997). The hash function operates by performing a calculation of all of the binary numbers of each letter or symbol in the document. See Fresen, supra note 52, at 171-172. By using a hash function, an individual can create a number that is called a message digest, which prevents a third party changing the message. See Greenwood & Campbell, supra note 55, at 314. In order to create an encrypted message, the sender then encodes this message digest with the recipient's public key. See Eldridge, supra note 39, at 1811. This operation forms the digital signature for the sender's message. Next, the sender sends the message to the recipient. See Greenwood & Campbell, supra note 55, at 314. Since the typical "message digest" or "hash results" that are compared are 160 bits in length, it would "require an attacker to generate and search through approximately 280 pairs of messages in order to have an approximately even chance of finding even a single pair of messages that would produce the same message digest but yet not be precisely identical, down to the bit level." Jueneman & Robertson, supra note 30, at 439-440. That is 1.2x1024, or approximately a trillion trillion messages that would have to be examined-a patent impossibility. Id.

[56] See Closen & Richards, supra note 4, at 735.

[57] Wims, supra note 46, at 31.

[58] Id.

[59] See Field, supra note 38, at 733.

[60] Id.

[61] The public key can be freely distributed and used by anyone. See Winn, supra note 31, at 1200-1201.

[62] See Wims, supra note 46, at 31. Once the message and signature arrive, the recipient then uses the software to create two new hash results: one derived from the message and one derived from the digital

signature. See Smith & Keehan, supra note 38, at 508. The recipient's software then compares these hash results, as well as the corresponding public key with the digital signature. Id. If the software confirms that the hash results are identical, then the recipient is able to verify that the message has been created by the sender's private key. Id.

[63] The relationship between the public and private keys is so complicated that it is "computationally infeasible" to deduce the private key solely from knowledge of the public key or to create a signed message which can be verified by application of the public key without the knowledge of the private key. See Jueneman & Robertson, supra note 30, at 438.

[64] See Closen & Richards, supra note 4, at 736.

[65] John B. Kennedy & Shoshana R. Davids, Bartleby the Cryptographer, Legal Profession Prepares for Digital Signatures, 215 N.Y.L.J. 54 (1996). The use of digital signatures depends on hash function security. MD-5 is incorporated into different types of software, and is the most commonly used hash function. See Eldridge, supra note 39, at 1816. Although there are no well-known ways to break MD-5, many experts have doubts about its security. Id. at 1816-1817. While hash functions may weaken the overall security of online commerce, the slow speed of RSA dictates that they it presently must be used. Id. at 1817.

[66] On July 22, 1997, Germany enacted the Gesetz zur Digitalen Signatur, or the Act on Digital Signatures. See Thomas, supra note 38, at 1038. The German Act offers individuals a framework for the use of digital signatures over the Internet. See Kimberly B. Kiefer, Developments Abroad May Influence U.S. Policy on Electronic Banking, 17 No. 4 BANKING POL'Y REP. 1, 11 (1998). As delineated in the German Act, a digital signature seals and labels digitized data intended for electronic transmission. See Thomas, supra note 38, at 1039. A CA gives the user a private digital signature. Id. Additionally, the German Act allows for voluntary participation because it does not require users to use a digital signature from a licensed CA. Id. Also, the German Act calls for licensing scheme for CAs, which is set up by the central government. Id. The government gives this power to the German Telekom authority, which can grant a license to persons with the necessary expert knowledge and who is reliable. Id. The CA must also implement a detailed and approved security plan setting forth three things: (1) all security measures; (2) the technology utilized; and (3) an organizational flowchart. See Kiefer, supra note 66, at 11. However, no treaty exists between Germany and the United States regarding the acknowledgement of U.S. digital signatures. See Thomas, supra note 38, at 1040-1041.

[67] See Kiefer, supra note 66, at 8.

[68] See ARIZ. REV. STAT. ANN. § 41-121(13) (West 1999) (authorizing the Secretary of State to approve and use digital signatures for documents filed by all state agencies); CAL. GOV'T CODE § 16.5 (West 1999) (allowing use of digital signatures when communicating with public entity); 1997 GA. CODE ANN. 40-3-21(b) (Harrison 1999) (allowing commissioner to authorize the use of digital signatures in car transactions); WASH. REV. CODE ANN. § 19.34 et. seq. (West 1999) (delineating the Washington Electronic Authentication Act which authorizes the use of digital signatures). See also Robert G. Ballen & Thomas A. Fox, Electronic Banking Products and Services: The New Legal Issues, 115 BANKING L.J. 334 (1998) (stating that Arizona, California, Georgia, and Washington have recently enacted digital signature statutes that permit use of digital signatures). See generally, Kiefer, supra note 66, at 1 (stating that 40 states legislatures are working on electronic authentication statutes).

[69] See Winn, supra note 31, at 1240.

[70] See ABA GUIDELINES, supra note 41, at 20. Under the Guidelines, a CA must disclose digital signature certificates and provide available information regarding the revocation of certificates. Id. at § 3.12. Before issuing a digital signature certificate, a CA must discover the online identity of the recipient. Id. at § 3.7.

Additionally, the CA must maintain a trustworthy system and guarantee that its employees and contractors support the system's maintenance. Id. at §§ 1.35, 3.4 . The Guidelines also shields the CA from liability for losses incurred by a subscriber, if a CA has complied with the rules. Id. at § 1.31.

[71] See ABA GUIDELINES, supra note 41, at 20 (stating the Guidelines are intended as "a common framework of unifying principles that may serve as a common basis for more precise rules in various legal systems").

[72] Id. at 18.

[73] See C. Bradford Biddle, Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace, 34 SAN DIEGO L. REV. 1225, 1232-1233 (1997). It created a legal infrastructure in which users are able to employ repositories, CAs and public-key encryption technology to create and sign electronic documents that are legally binding. Id. Additionally, the Utah Act intended digital signatures to use hash functions. See UTAH CODE ANN. § 46-3-103 (1998).

[74] See UTAH CODE ANN. §§ 46-3-101 to -504 (1998).

[75] See Closen & Richards, supra note 4, at 742. Under the Utah Act, certification authorities must be "a human being or any organization capable of signing a document, either legally or as a matter of fact." UTAH CODE ANN. § 46-3-103 (1998).

[76] See UTAH CODE ANN. § 46-3-301 (1998).

[77] See UTAH CODE ANN. § 46-3-201.

[78] See UTAH CODE ANN. § 46-3-201.

[79] See UTAH CODE ANN. § 46-3-202.

[80] See UTAH CODE ANN. § 46-3-302. A licensed CA can only issue a certificate in Utah "if it : (1) confirms the identity of the requesting person; (2) investigates the identification given by the subscriber with due diligence; and (3) performs a sample encryption with the public secret key pair of the subscriber." UTAH CODE ANN. § 46-3-302.

[81] See UTAH CODE ANN. § 46-3-103 (1998).

[82] See generally, Electronic Commerce, MCBRIDE, BAKER & COLE (visited August 2, 1999) <http://www.mbc.com/ecommerce> (listing both federal and state enacted and proposed digital signature legislation).

[83] See Geoffrey Turk, Money and Currency in the 21st Century, GOLDMONEY.COM (visited Aug. 1, 1999) <http://www.goldmoney.com/futuremoney.html>.

[84] See Dr. Ursula Widmer, The Virtual World of Cyberspace Digital Cash, EFT and the Tax Free Economy of the World, 4 CLA COMPUTER LAW COMPANION 411, 411 (1996).

[85] Id.

[86] Id.

[87] See Turk, supra note 83, at <http://www.goldmoney.com/futuremoney.html>.

[88] Id.

[89] Id.

[90] Id.

[91] Id.

[92] Id.

[93] Id.

[94] Id.

[95] Id.

[96] Id.

[97] See Widmer, supra note 84, at 411.

[98] See Eui-Suk Chung and Daniel Dardailler, White Paper: Joint Electronic Payment Initiative (JEPI), (April 9, 1997) <http://www.w3.org/Ecommerce/white-paper>, at Introduction; see also Study: Online Shopping Revenues To Surge, POINTCAST (visited July 19, 1999) <http://127.0.0.1:15841/v1?catid=18614275&md5=825ca457e5cccacb135761b8e31f12fc>; (explaining that online retailing in North America would top $36 billion by the end of the year); Maryann Jones Thompson, E-commerce to Ring Up $36 Billion in '99, THE STANDARD (visited July 20, 1999)<http://www.thestandard.net/articles/display/0,1449,5576,00.html?home.tf; (explaining that the US and Canada will collect $36.6 billion in online sales during 1999); Online Sales Doubling to $37 Billion, PC WORLD (visited July 20, 1999) <http://www.pcworld.com/pcwtoday/article/0,1510,11851,00.html; (explaining that online sales more than doubled from 1998 to 1999); Online Retailing to Reach $36 Billion in 1999, CyberAtlas at Internet.com (visited July 20, 1999) <http://cyberatlas.internet.com/markets/retailing/article/0,1323,6061_164011,00.html; (explaining that online order in 1998 were up 200 percent and the number of online shoppers was up 300 percent); Marc Graser, Surveys find TV viewers busy Net shopping, POINTCAST (visited July 21, 1999) <http://127.0.0.1:15841/v1?catid=5901315&md5=c2ccfdf310f51af22479b503d0b0df5; (explaining that people who used to watch TV are now busy purchasing goods, information and services on the Internet).

[99] See Hans-Peter Erl, The Emergence of Electronic Commerce and Electronic Forms of Money, (visited July 28, 1999) <http://www.aib.wiso.tu-muenchen.de/lehre/dipl/hperl/c6.htm> at 6.4 Payments methods for electronic commerce.

[100] For example, VISA or MasterCard.

[101] For example, Sears Card or J.C. Penney Card.

[102] For example, American Express Card.

[103] See Edwin L. Rubin & Robert Cooter, THE PAYMENT SYSTEM 752 (2d ed. 1994).

[104] See Internet and Smart Cards Top ABA Conference List, CARD NEWS, Sept. 18, 1995, available in WESTLAW, CARDN database, 1995 WL 8159249 (reporting results from a study conducted by Global Concepts, Inc. derived from an online survey of those who access the World Wide Web).

[105] See David S. Bennahum, The Trouble With Electronic currency, 15.4 MARKETING COMPUTERS, April 1995, at 25, also available at <http://www.memex.org/troublewithecash.html> (visited July 28, 1999) (explaining how hacker Kevin Mitnick was arrested and sentenced for stealing 20,000 credit card numbers

stored on the Interenet).

[106] Id.

[107] See 21st: Reality Check, page 2 of 2, Salon (visited July 23,1999)<http://www.salon1999.com/21st/feature/1997/10/cov_30emoney2.html>.

[108] See generally, Turk, supra note 83, at <http://www.goldmoney.com/futuremoney.html>.

[109] See Digital Cash, INTERNET.COM <http://webopedia.internet.com/TERM/d/digital_cash.html> (visited July 23, 1999).

[110] See Question 138: What is Electronic Money?, RSA LABORATORIES (visited Aug. 1, 1999) <http://www.iie.edu.uy/~mazzara/pgp/q138.html>.

[111] See Turk, supra note 83, <http://www.goldmoney.com/futuremoney.html>.

[112] Id. Although used interchangeably, "money" and "currency" are not synonymous: "money" is simply a means of communicating value; and "currency" is the physical manifestation of money. Id.

[113] See Widmer, supra note 84, at 414.

[114] Id.

[115] The Basle Committee is a committee of banking supervisory authorities which was established in 1975 by the central bank Governors of the Group of Ten countries. See Report by the Committee on Payment and Settlement Systems and the Group of Computer Experts of the Central Banks of the Group of Ten Countries, Security of Electronic Money, at 1 [hereinafter Basle Committee Report]. It consists of senior representatives of bank supervisory authorities and central banks from Belgium, Canada, France, Germany, Italy, Japan, Luxembourg, Netherlands, Sweden, Switzerland, United Kingdom, and the United States. Id. It usually meets at the Bank for International Settlements in Basle, where its permanent Secretariat is located. Id. The Committee on Payment and Settlement Systems established the Task Force on Security of Electronic Money which : Primarily examined consumer-oriented stored-value payment products, a few of which have already been launched in large-scale pilot programmes in various countries; others are expected to be widely introduced in 1996 or 1997. Through interviews with suppliers, the Task Force identified general models of electronic money products and specific characteristics that are relevant to security. The Task Force found that the logical design chosen for the stored electronic "value", as well as the conditions under which such money balances can be transferred to other users, provide the basic framework for examining security measures in the various stored-value products ....The task Force found that various security measures have been developed to protect the integrity, authenticity, and confidentiality of critical data and processes of electronic money products, and that cryptography is the ...critical safeguard for card-based systems and, indeed, the primary safeguard for software-based systems. Id.

[116] See Catherine Lee Wilson, Banking on the Net: Extending Bank Regulation to Electronic Money and Beyond, 30 CREIGHTON L. REV. 671, 702 (1997) (stating that federal banking regulators in the U.S. have indicated that issuers of electronic value do not fall under definition of banks, and are exempt from federal banking regulations).

[117] See Christopher D. Hoffman, Note, Encrypted Digital Cash Transfers: Why Traditional Money Laundering Controls May Fail Without Uniform Cryptography Regulations, 21 FORDHAM INT'L L.J. 799, 818 (1998).

[118] Id. at 818-819.

[119] See Basle Committee Report, supra note 115, at 35.

[120] See Hoffman, supra note 117, at 819.

[121] Id.

[122] Id.

[123] The Mondex system is a product of a joint venture between NatWest and Midland Bank. See Sarah N. Welling & Andy G. Rickman, Cyberlaundering: The Risks, The Responses, 50 FLA. L. REV. 295, 327 n.70 (1998). MasterCard International, Inc. recently has acquired Mondex. Id. Mondex will become a subsidiary of MasterCard and will have access to MasterCard's vast resources and distribution networks, but will keep its board of directors and London headquarters. Id.

[124] See Digital Cash, an overview (visited August 2, 1999) <http://mrmac-jr.scs.unr.edu>. The term electronic purse, commonly used to refer to stored value cards(SVCs), is defined as: An IC card containing an application that stores a record of funds available to be spent or otherwise used by the holder; the record of funds is updated as transactions are made. Additional funds may be added to the stored balance through a withdrawal from a bank account or by other means. Hoffman, supra note 117, at 860 n.2. These stored value cards, also known as "prepaid cards," "smart cards," "chip cards," among other designations, may involve a magnetic stripe, an embedded integrated circuit (microchip) or both. See Ellen d'Alelio, Doing Business in the New World of Electronic Commerce: An Introduction to the Emerging Electronic Payment Products and Systems, 491 PLI/PAT 61, 65-66 (1997). A user may download and store monetary "value" on the cards for later use. Id. Cards may be reloadable or designed for disposal after the customer has spend all of the value originally loaded on the card. Id. They may operate online or off-line. Id. Their operation may require an intermediary, or they may function on a peer-to-peer basis, as does the Mondex smart card. Id.

[125] Id. at 71.

[126] Id.

[127] Id.

[128] Id.

[129] Id.

[130] Id.

[131] See Welling & Rickman, supra note 123, at 306.

[132] Id. Direct value transfers between users, without any financial institution or other intermediary, are referred to as peer-to-peer transfers. Id.

[133] See J. Orlin Grabbe, Internet Payment Schemes: Part 3, ZOLATIMES (visited August 1, 1999) <http://www.zolatimes.com>. The Mondex system does not result in centralized record keeping of transactions, although transactions may be traceable in certain circumstances. See Privacy International, Privacy International's Mondex Complaint Is Upheld: Electronic Cash is Anything but Anonymous, PRIVACY.ORG (visited June 29, 1999) <http://www.privacy.org/pi/activities/mondex/mondex_release.html>. In the United Kingdom in 1995, a formal complaint was filed against Mondex International for allegedly exaggerating the degree to which its product provides anonymity. Id.

[134] See Grabbe, supra note 133, at <http://www.zolatimes.com>.

[135] Id.

[136] See Welling & Rickman, supra note 123, at 306-307.

[137] Id. at 307.

[138] See John D. Muller, Selected Developments in the Law of Cyberspace Payments, 54 BUS. LAW. 403, 441 n.207 (1998). Mark twain has been acquired by Mercantile Bank corporation, and is the only bank licensee of electronic currency in the United States. Id. However, Mark Twain is closing its electronic currency operations. Id.

[139] Id. at 431.

[140] Id. at 431-432.

[141] Id. at 432.

[142] Id.

[143] Id. The electronic currency coins are valid for spending only for a 90-day period. After that period, an individual can redeem them for new coins or for value in the mint, but only by the customer who originally withdrew them. Id. at 441 n.213.

[144] Id. at 432. In the Wild Card Option, the mint does not receive the electronic currency coins to test them for double-spending. Id. If the Wild Card Option electronic currency message is intercepted or sent to an unintended payee, the unintended recipient can deposit the coins in his mint account, and the payer has no recourse. Id. at 441 n.214.

[145] Id. at 431.

[146] See Thompson, supra note 98, at <http://www.thestandard.net/articles/display/0,1449,5576,00.html?home.tf>.

[147] See Randy V. Sabbett, International Harmonization in Electronic Commerce & Electronic Data Interchange: A Proposed First Step Toward Signing on the Digital Dotted Line, 46 AM. U.L. REV. 511, 526-527 (1996) (stating that the legal infrastructure in existence today embraces technology that began over 500 years ago).

[148] See Greenwood & Campbell, supra note 55, at 308.

[149] See Smith & Keehan, supra note 38, at 506 (stating that some large and small financial institutions that have introduced home banking services to their customers is one application of digital signatures).

[150] See Corwin, supra note 35, at 1.

[151] See generally Digital Cash, supra note 124, at <http://mrmac-jr.scs.unr.edu>. Electronic currency works on the concept of public-key cryptography, which is based on the patented RSA system. Id.

[152] Id.

[153] Id. There are two distinct types of digital cash: identified digital cash and anonymous digital cash. Once a customer withdraws anonymous digital cash from his account, it can be spent or given away without leaving a transaction trail. See Jim Miller, Digital Cash Mini-FAQ (visited July 25, 1999) <http://ganges.cs.tcd.html>.

[154] See A. Michael Froomkin, Flood Control on the Information Ocean: Living with Anonymity, Digital Cash, and Distributed Databases, 15 J.L. & COM. 395, 458 (1996). Each coin requires a long, probabilistically unique, random number, but the bank is able to reuse the same private-public key pair to sign every coin of a given denomination. Id. Of course, the actual system involves no physical coins, the messages sent include strings of digits, each string corresponding to a different digital coin. Id. Each coin has a denomination, or value, to withdraw and which to use to make a particular payment. Id. Additionally, the electronic currency software contacts the bank in the rare event that changes need to be made before the next withdrawal, to let it restructure its portfolio of coin denominations. See Lee S. Adams, Materials Related to Digital Cash and Electronic currency Companies, 966 PLI/CORP. 251, 264 (1996).

[155] See Hoffman, supra note 117, at 860 n.5. Digital and paper cash are similar in the sense that neither the paper on which paper money is printed nor the string of bits that represents digital cash has intrinsic value. Id. The value of this money is conferred on a piece of paper or a particular string of bits if, and only if, an institution is willing to accept responsibility for them. Id.

[156] Id. A digital coin is "a unit of value identified by an encrypted serial number and stored on a computer's hard drive or a stored value card." Id. at 818. After a consumer transmits the coin to a merchant, the merchant redeems it for hard currency from the issuer. Id. Once the issuer receives the coin, the issuer can verify the coin's validity by checking its serial number. Id.

[157] Digital Cash, supra note 124, at <http://mrmac-jr.scs.unr.edu>. Digital cash can be stored in any one of a number of places: in the financial institution's computer, in a customer's computer, or on smart cards carried by the customer and the merchant. See Froomkin, supra note 154, at 456.

[158] Digital Cash, supra note 124, at <http://mrmac-jr.scs.unr.edu>.

[159] Id.

[160] Id.

[161] Id.

[162] See Froomkin, supra note 154, at 458. Online digital cash systems require merchants to contact the bank's computer with every sale in order to prevent double spending. Id. A database of all the spent pieces of digital cash is stored in the bank's computer, and can easily indicate to the merchant if a given piece of digital cash is still spendable. See Miller, supra note 153, at <http://ganges.cs.tcd.html>. The bank uses the serial number of each coin to point to where it should be stored in the spent coin database it maintains. See Adams, supra note 154, at 265. If the bank computer indicates that the digital cash has already been spent, the merchant refuses the sale. Id. This system is similar to the verification process of credit cards at the point of sale. See Miller, supra note 153, at <http://ganges.cs.tcd.html>.

[163] Digital Cash, supra note 124, at <http://mrmac-jr.scs.unr.edu>.

[164] Id.

[165] Id. To avoid erosion of privacy, systems such as anonymous electronic cash transactions are not only needed, but also considered essential. Id. This is gained with the use of "signatures." Id. Electronic currency uses digital signatures, which are well suited for public networks, because they do not require totally secure channels of distribution. Id.

[166] See Hoffman, supra note 117, at 828-829.

[167] See Froomkin, supra note 154, at 462. On October 23, 1995, Mark Twain Bank of St. Louis, Missouri

became the world's first financial institution to issue blinded digital coins backed by value. Id.

[168] See Brian Connolly, Digital Commerce Gaining Currency, INTELLECTUAL CAPITOL (visited July 20, 1999) <http://www.intellectualcapitol.com>. David Chaum, the founder of DigiCash, created a blind signature system. Id. Using this system, the electronic money in your "wallet" is double-encrypted-once to imprint it with an authorization tag so that its validity as tender can be verified by the merchant's computer, and a second time to protect the customer's identity from prying eyes. Id.

[169] See Adams, supra note 154, at 265. Using "blinded coins," a person can acquire digital cash from a bank, without allowing the bank to create a record of the coin's serial number. Id. Despite the non-recordation of the serial number, the number's uniqueness helps ensure that a customer cannot spend it twice. See Froomkin, supra note 154, at 460.

[170] Cryptography plays a central role in digital payment systems, as well as ensuring the anonymity of electronic coins. See Basle Committee Report, supra note 115, at 14. Referred to as the cornerstone of digital money, cryptography ensures the confidentiality of electronic payment messages. See Daniel C. Lynch & Leslie Lundquist, Digital Money, The New Era of Internet Commerce 1, 69 (1997). Furthermore, cryptography allows issuers to certify the authenticity of digital money by using digital signatures, and thus preventing the forgery of digital money. Id. Digital signatures also provide for the verification of the signatory's identity and the integrity of the transmission. See Hoffman, supra note 117, at 829-830.

[171] See Grabbe, supra note 133, at <http://www.zolatimes.com>. Digital cash systems implement key encryption technologies, in order to use a digital signature to authenticate a transaction. Id. The debate over encryption focuses on which encryption standard digital cash systems should use, as well as the merits of public/private key encryption. Id. Determining the encryption standards systems should use directly relates to the success of digital cash. Id. As a recent Office of Technology Assessment study warns, "the benefits of electronic commerce might be squandered unless Congress brings privacy laws up to date and helps resolve the debate over key escrow encryption." Catherine M. Downey, Comment, The High Price of a Cashless Society: Exchanging Privacy Rights for Digital Cash?, 14 J. MARSHALL J. COMPUTER & INFO. L. 303, 323 n. 28 (1996).

[172] See Grabbe, supra note 133, at <http://www.zolatimes.com>. "A 'coin,' or piece of electronic currency, consists of two parts: w and H(w)^(1/e), where w is a random number, H() is a one-way hash function such as SHS-1 or RSA's MD5, and e is an public exponent (public key) which could be taken to represent the denomination of the coin. That is, different coin denominations will use different exponents.(Note that in the RSA system, 1/e is the bank's private key.)" Id.

[173] Id.

[174] Id.

[175] Id. The issuance of blind signatures by a bank is a very complex process. The customer's software chooses a serial number w for each of the electronic currency coins. Next, the program calculates the value H(w). Finally, the customer's software chooses a blinding random factor r, which is raised to the power e and multiplied by value H(w), yielding r^e*H(w). The bank signs the coin by raising this number to the 1/e power, modulo its public modulus n, yielding r*H(w)^(1/e) mod n. The bank sends the coin back to the customer. The customer's software divides the number by r, which only the customer knows. This gives H(w)^(1/e) mod n, which together with w comprises the unit of digital cash: (w, H(w)^(1/e)). Id.

[176] Id.

[177] See Digital Cash, supra note 124, at <http://mrmac-jr.scs.unr.edu>.

[178] See Grabbe, supra note 133, at <http://www.zolatimes.com>. Unlike the basic case, however, a bank issuing a blinded coin by affixing its digital signature to the "blinded number," is unaware of the true serial number of the coin. See Froomkin, supra note 154, at 460. All that the bank knows is that a customer has purchased a coin of a given denomination, and that he has submitted the "blinded" number. See David Chaum, Achieving Electronic Privacy, SCI. AM., Aug. 1992, at 96. However, without an anonymous bank account, the bank knows the customer's identity, and knows how many coins of each denomination he is buying. Thus, the customer's privacy depends in part on there being a sufficiently large volume of coins in circulation, so that his use of the coins does not stand out. See Froomkin, supra note 154, at 461.

[179] See Grabbe, supra note 133, at <http://www.zolatimes.com>.

[180] Id. "The blinding operation is a special kind of encryption that can only be removed by the party who placed it there. It commutes with the public key digital signature process, and can thus be removed without disturbing the signature." Froomkin, supra note 154, at 507 n.250.

[181] See Digital Cash, supra note 124, <http://mrmac-jr.scs.unr.edu>.

[182] See Muller, supra note 138, at 420.

[183] See Digital Cash, supra note 109, at <http://webopedia.internet.com/TERM/d/digital_cash.html>.

[184] Id.

[185] Id.

[186] See 15 U.S.C. §§ 1693-1693r (1994). See Muller, supra note 138, at 421. The EFTA requires that financial institutions disclose to a consumer the circumstances under which it will disclose information about the consumer to a third party. Id. However, it is unclear whether the consumer holding electronic currency issued by an institution qualifies as an account under the Act. Id.

[187] See 18 U.S.C. §§ 2510-2518 (1986). The ECPA prohibits an entity from disclosing contents of an electronic communication while in its transmission, or in storage. See 18 U.S.C. §§ 2510-2518. Again, however, it is unclear whether this information would fall within the scope of the Act.

[188] See T.J. Smedinghoff, Online Payment Options, ONLINE LAW, The SPA's Legal Guide to Doing Business on the Internet 116 (1996). Explaining that: [a]t present there are no government regulations that apply directly to digital cash. However, there is much discussion over whether. . . . the Federal Electronic Fund Transfer Act and its also concern that Regulation E will be applied to consumer stored-value cards containing digital cash. Because these cards are used primarily for low-value transactions, it may not be practical or cost efficient to comply with all of its consumer protection requirements. Id.

[189] See generally, section II (B)(1)(a); But see Associated Press, Researchers Say That They Cracked Internet's Global Security System, CHICAGO TRIBUNE, Aug. 28, 1999, at A9 (reporting that Amsterdam researchers "have broken an International security code used to protect millions of daily Internet transactions").

[190] See National Research Council, Computer Science and telecommunications Board, Cryptography's Role in Securing the Information Society 380 n.17 (Kenneth W. Dam and Herbert S. Lin, eds., 1996) (declaring that a cryptographic key which would necessitate a number of operations greater than practical limits of physics could eliminate the problem of advancement in computer technology); Id. at 379-380 (noting that "[w]ith a sufficiently long key, even an eavesdropper with very extensive computer resources would have to take a very long time (longer then the age of the universe) to test all possible combinations").

[191] See Reality Check: Page 2 of 2, SALON (visited July 31, 1999) <http://www.salon1999.com /21st/feature/ 1997/10/cov_30emoney2.html.>

[192] See generally, supra Section II(b)(1)(a). RSA cryptography is such that if the message is intercepted or altered in anyway, the hash result will differ and the receiving party will know that the message has been altered after it left the sender. Therefore, this scenario is very unlikely using public-key cryptography.

[193] See 18 U.S.C.A. § 1030(a)(2)(C)(West Supp. 1994). See generally, infra, section III(D)(2). This Act allows the sender or the recipient to file suit against the unintended recipient, and will be discussed in greater detail later in this Comment.

[194] See Smedinghoff, supra note 188, at 207. Explaining that: [c]ontract law provides requirements that must be met for a contract to be enforceable. The law requires that an agreement be both (1) documented in "writing" and (2) "signed" by the person who is sought to be held bound in order for that agreement to be enforceable. Contract law provides that contracts for the sale of goods for the price of $500 or more, and contracts that will not be fully performed within a year, are not enforceable unless there is both a writing sufficient to indicate that a contract has been made between the parties, and that it is signed by the party against whom enforcement is sought. Id.

[195] See Howley v. Whipple, 48 N.H. 487 (1869). The New Hampshire court stated: [i[t makes no difference whether that operator writes the offer or the acceptance . . . .with a steel pen an inch long attached to an ordinary penholder, or whether his pen be a copper wire a thousand miles long. In either case the thought is communicated to the paper by use of the finger resting upon the pen; not does it make any difference that in one case common record ink is used, while in the other case a more subtle fluid, known as electricity, performs the same office. Id.

[196] See Joseph Denunzio Fruit Co. v. Crane, 70 F. Supp. 117 (S.D. Cal. 1948) (stating that a telex is a writing); McMillan Ltd v. Weimer Drilling & Eng. Co., 512 So.2d 14 (Ala. 1986) (noting that a mailgram is a writing); Ellis Canning Co. v. Bernstein, 348 F. Supp. 1212 (D. Colo. 1972) (holding that a tape recording is a writing); but see Roos v. Aloi, 127 Misc. 2d 864, 487 N.Y.S.2d. 637 (Sup. Ct. 1985) (declaring that a tape recording is not a writing).

[197] See generally, U.C.C. § 1-201 (39). A signature is "any symbol executed or adopted by a party with present intention to authenticate a writing." U.C.C. § 1-201 (39).

[198] See Selma Sav. Bank v. Webster County Bank, 206 S.W. 870 (Ky. 1918); Hillstrom v. Gosnay, 188 Mont. 388, 614 P.2d 466 (1989).

[199] See Watson v. Tom Growney Equip. Inc., 721 P.2d 1302 (N.M. 1986) (holding that a name typed on a purchase order was found to be sufficient signature after signor had filled out other details on the form); In re Save On Carpet of Arizona, Inc., 545 F.2d 1239 (9th Cir. 1976) (stating that a typewritten signature on a UCC financing statement satisfies the signature requirement under the statute of frauds).

[200] See Franklin County Coop. v. MFC Servs., 441 So.2d 1376 (Miss. 1983); Hideca Petroleum Corp. v. Tampimac Oil Int'l Ltd., 740 S.W.2d 838 (Tex. Ct. App. 1987); but see Miller v. Wells Fargo Bank Int'l Corp., 406 F. Supp. 452 (S.D.N.Y. 1975) (questioning whether test key on telex is a signature).

[201] See Hesenthaler v. Farzin, 388 Pa. Super. 37 (1989) (focusing on intent to authenticate); McMillan Ltd v. Warrior Drilling & Eng Co., 512 So. 2d 14 (Ala. 1986).

[202] See Kohlmeyer & Co. v. Bowen, 126 Ga. App. 700, 192 S.E.2d 400 (1972) (holding that a securities brokerage firm's name printed on top of confirmation statement was intended as authentication, and thus met the signature requirement under the statute of frauds).

[203] See Beatty v. First Exploration Fund 1987 & Co. Ltd. Partnership, 25 B.C.L.R.2d 377 (1988) (holding that faxed signatures on proxy documents were sufficient to meet signature requirements under limited partnership agreement); Madden v. Hegadon, 565 A.2d 725 (N.J. Super. 1989) (declaring that a fax signature was effective for filing nomination petition).

[204] Electronic Signature Legislation enacted in some states declare that an electronic signature includes any mark on a message. States using this requirement are Colorado, Florida, Illinois, Indiana, Mississippi, New Hampshire, North Carolina, Rhode Island, Texas, and Virginia. However, some states put limitations on the kinds of digital signatures that will be deemed acceptable. These states have five requirements that are derived from the California legislation enacted in 1995: (1) unique to the person using it; (2) capable of verification; (3) under sole control of the person using it; (4) linked to the data in such a manner that if the data is changed the signature is invalidated; and (5) conforms to Secretary of State regulations. See CAL. GOV'T CODE § 16.5 (West 1999). California, Georgia, and Kansas have all adopted this approach.

[205] See 18 U.S.C.A. § 1343, "Fraud by wire, radio, or television."

[206] See 18 U.S.C.A. § 1343. The wired fraud statute was enacted in 1952 and reads as follows: Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice, shall be fined not more than $1,000 or imprisoned not more than five years, or both. If the violation affects a financial institution, such person shall be fined not more than $1,000,000 or imprisioned not more than 30 years, or both. 18 U.S.C.A. § 1343.

[207] See 18 U.S.C.A. §§ 1343, 1346; see also United States v. Ames Sintering Co., 927 F.2d 232 (6th Cir. 1990).

[208] See, e.g., United States v. Butler, et al., 704 F. Supp. 1338 (E.D. Va. 1989); United States v. Muni, 668 F.2d 87 (2d Cir. 1981); United States v. Calvert, 523 F.2d 895 (8th Cir. 1975), cert. denied, 424 U.S. 911, S.Ct. 1106; see also United States v. Locklear, 829 F.2d 1314, 1318-19 (4th Cir. 1987) (involving mail fraud statute).

[209] See, e.g., United States v. Butler, et al., 704 F. Supp. 1338 (E.D. Va. 1989); United States v. Benmuhar, 658 F.2d 14 (1st Cir. 1981), cert. denied, 457 U.S. 1117, 102 S.Ct. 2927; United States v. Calvert, 523 F.2d 895 (8th Cir. 1975), cert. denied 424 U.S. 911, 96 S.Ct 1106; Sibley v. United States, 344 F.2d 103 (5th Cir.), cert. denied, 382 U.S. 945, 86 S.Ct. 405 (1965).

[210] See United States v. Riggs, 739 F. Supp. 414 (N.D. Ill. 1990); McCoy v. Goldberg, 748 F. Supp. 146 (S.D.N.Y. 1990).

[211] See 18 U.S.C.A. § 1343, "Mail Fraud."

[212] See United States v. Butler & Thornton, 704 F. Supp. 1338 (E.D. Va. 1989).

[213] See Gary H. Anthes, Juvenile charged with Internet crimes; boy allegedly scams users with phony ads for computer parts, COMPUTER WORLD, May 8, at 12 (1995).

[214] Id.

[215] Id.

[216] Id.

[217] See SEC Charges 82 Individuals and Companies in 26 Actions Involving More Than $12 Million in Second Nationwide Microcap Fraud Sweep, SEC (visited Aug. 3, 1999) <http://www.sec.gov/news/press/99-90.txt>; Prepared Statement of the Federal Trade Commission on "Internet Fraud" before the Subcommittee on Investigations of the Governmental Affairs Committee, FEDERAL TRADE COMMISSION (visited July 23, 1999) <http://www.ftc.gov/os/1998/9802/ internet.test.htm> (explaining as of February 10, 1998, the FTC has brought 25 law enforcement actions against defendants whose alleged illegal practices used or involved the Internet).

[218] See 18 U.S.C.A. 1962(a). The RICO claim requires eight essential elements: (1) a defendant, (2) through commission of two or more enumerated predicate acts, (3) which constitute a 'pattern,' (4) of racketeering activity, (5) directly or indirectly participates in conduct of, (6) enterprise, (7) activities of which affect interstate commerce, and (8) plaintiff was injured in its business or property by reason of such conduct. 18 U.S.C.A. § 1962 (a).

[219] See Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030(a)(2)(C) (West Supp. 1994). The CFA prohibits any person from: (1) intentionally access[ing] a computer facility without authorization through which an electronic communication service is provided; or (2) intentionally exceed[ing] an authorization to access that facility, and thereby obtain[ing], alter[ing] or prevent[ing] to authorized access to wire or electronic communication while it is in electronic storage in such system shall be punished .... Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030(a)(2)(C).

[220] See Computer Fraud and Abuse Act, 18 U.S.C.A. § 1030(a)(2)(C).

[221] See 18 U.S.C.A. § 1030(e)(2).

[222] See Org. JD Ltda. v. United States Dep't of Justice, 124 F.3d 354, 359-60 (2nd Cir. 1997), citing 18 U.S.C. § 2511(3)(a) (prohibiting disclosure of the contents of an electronic communication to "any person or entity other than an addressee or intended recipient of such communication"); 18 U.S.C. § 2702(b)(1) (allowing disclosure of information to "addressee or intended recipient of such communication or an agent of such addressee or intended recipient"); 18 U.S.C. § 2702(b)(3) (allowing disclosure of information from electronic communication with the consent of "originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service"); 18 U.S.C. § 2511(2)(c) (providing that "[i]t shall not be lawful ... for a person acting under color of law to intercept a wire, oral, or electronic communication, where such person is a party to the communication or one of the parties to the communication has given prior consent to such interpretation.").

[223] See American Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 449-52 (E.D. Va. 1998); see also American Online, Inc. v. IMS et al., 24 F. Supp. 2d 548, 550-51 (E.D. Va. 1998).

[224] See American Online Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 449-52 (E.D. Va. 1998).

[225] Id.

[226] Id.

[227] See 18 U.S.C. § 1030(a)(5)(C).

[228] See 18 U.S.C. § 2314 (1988 & Supp. IV 1992).

[229] See 18 U.S.C. § 2314.

[230] See Dowling v. United States, 473 U.S. 207, 212 (1985).

[231] See United States v. Riggs et al., 739 F. Supp. 414, 417 (N.D. Ill. 1990).

[232] Id.

[233] See United States v. Brown et al, 925 F.2d 1301, 1302 (10th Cir. 1991).

[234] Id.

[235] See American Online, Inc. v. IMS, 24 F. Supp. 548, 550-51 (E.D. Va. 1998).

[236] See Hotmail Corp. v. Van$ Money Pie Inc.,1998 WL 388389 *6-8 (N.D. Cal.).

[237] Id.
